

The background of the entire page is composed of several large, overlapping, rounded geometric shapes in various shades of orange and red. These shapes create a dynamic, layered effect, with some appearing as if they are floating or overlapping others. The colors range from a deep, dark red to a bright, vibrant orange.

# Axcient

## Unified Management Console User Guide

**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.



# Table of Contents

Preface .....	8
Intended Audience .....	8
Introduction .....	8
Administration .....	8
Logging in to the UMC .....	8
UMC Dashboard .....	10
Backup Status Information .....	12
Disk Utilization Panel .....	18
Devices Panel .....	19
Resources Monitoring Panel .....	20
Version Information Panel .....	21
Device Management .....	22
Add a Device .....	22
Add Multiple Devices on a Network Segment .....	24
Add Devices Using Active Directory .....	27
Modify a Device .....	28
Remove a Device .....	30
Update Credentials for Multiple Devices .....	30
Enable or Disable Backup Jobs for All Devices .....	31
Test Device Access .....	33
Manage VSS Storage Locations for Windows Devices .....	34
Backup Strategy .....	37
Back Up Files .....	39
Set Local Graduated Retention .....	46
Excluded Files (Windows Devices Only) .....	49
Backup System Images .....	50
Modify Backup Job .....	59
Reduce Backup Job Size .....	63
Edit File Include or Exclude List Manually .....	66
Manage VSS Writers .....	69
Prune Backup Job .....	70
Configure the AutoVerify Feature (Data Integrity Check) .....	73
Remove Backup Job .....	76
Schedule Offsite Backup Job .....	77
Copy Backup Job to DAS .....	79
Restore Operations .....	80
Tree View Restore .....	80
Search Restore .....	85

System State Restore .....	89
<b>Bare Metal Restore .....</b>	<b>92</b>
Restore Device (BMR) Overview .....	92
Start BMR .....	93
Restore Device Using BMR Recovery Disk .....	97
Stop BMR .....	107
<b>Virtual Machine Overview .....</b>	<b>110</b>
Test Virtual Machine .....	112
Start Virtual Machine .....	116
Discard Virtual Machine .....	120
Edit Running Failover .....	121
BMR Virtual Machine .....	124
Shutdown and Restart Virtual Machine .....	126
View Virtual Machine and BMR Status .....	129
<b>System Management .....</b>	<b>130</b>
Set Networking Parameters .....	130
Set Bandwidth Usage (Quality of Service) .....	132
Set Time Zone .....	136
Configure SNMP .....	137
Configure Web Proxy .....	141
Configure E-Mail .....	143
Configure PSA Settings .....	144
Configure Graduated Retention Defaults .....	146
Use Configuration Tools .....	152
Check Network Connections .....	155
Check Entitlements .....	160
Set System Access and Availability .....	163
<b>User Management .....</b>	<b>168</b>
Add a User .....	169
Modify a User .....	170
Deactivate a User .....	172
Manage Roles and Permissions Overview .....	173
Add a Role .....	174
Modify a Role .....	175
Delete a Role .....	176
<b>Reports .....</b>	<b>177</b>
View Reports .....	177
Backup History Report .....	178
Backup Job Profile Report .....	181
Schedule Backups Report .....	184

Backup Times Report .....	186
Current Disk Usage Report .....	189
<b>Event Logging .....</b>	<b>192</b>
View Log Messages .....	192
Log Messages Format and Types .....	194
Configure Event Notification .....	203
Save Log Messages .....	207
Purge Log Messages .....	208
<b>Event Messages .....</b>	<b>209</b>
Device Events .....	209
Backup Job Definition Events .....	211
Onsite Backup Events .....	212
Offsite Backup Events .....	221
Restore Events .....	227
Exchange Mailbox Events .....	231
Image Job and Virtual Machine (VM) Events .....	235
Bare Metal Restore (BMR) Events .....	239
System Events .....	240
User Events .....	246
DAS Events .....	248
Export Copy Events .....	252
Entitlement Events .....	254
Device Error Messages .....	257
BMR Error Messages .....	259
<b>Optimizing .....</b>	<b>262</b>
Setup Summary .....	262
Installation Guidelines .....	263
Device Guidelines .....	265
Initial Backup Strategy .....	267
Image Job Considerations .....	268
File Job Considerations .....	270
Additional Job Considerations .....	271
Initial Backup Strategy .....	275
Laptop Backup Strategy .....	277
Appliance Configuration Guidelines .....	278
System Settings .....	279
Third-Party Support .....	284
Remote Hardware Maintenance .....	285
Backup Fails Because of Windows VSS Problem .....	286
Backup Fails Because of Permission Problem .....	290
Backup Fails Because of Windows Redirection .....	291
Backup Fails Because of Mount Problem .....	296

Backup Fails Using Samba .....	297
Backup Fails Due to Symbolic Links (Windows 7) .....	298
Backup Hangs After Lost Connection .....	299
Open Files Not Backed Up .....	300
Files Missing When Creating Backup (XP) .....	301
Cannot Backup Windows Encrypted Files .....	302
Cannot Set "On Demand" Job Retention Period .....	303
Not All "Active" Backup Jobs Running .....	304
Offsite Backups are Slow .....	305
Restoring UNIX Files on Windows Device Fails .....	307
Restore Fails Using Samba on MAC OS X .....	308
Cannot Restore to Target Location .....	309
Cannot Restore Files (Tree View Does Not Expand) .....	310
Cannot Restore Exchange Mailbox (Account Deleted) .....	311
BMR Fails at Final Boot (Windows 2003) .....	312
BMR Fails at Final Boot (Active Directory Server) .....	313
Failover VM Pause Shut Down Server .....	314
Exchange Not Working in VM .....	315
Cannot Access Running VM .....	316
Cannot Log in to Test VM .....	317
Restored Device Cannot Join Domain (Password Problem) .....	319
Cannot Connect to Web Application .....	320
System Performance Slows .....	321
System Time Incorrect .....	322
Cannot Register Appliance .....	323
Offsite Progress Bars Do Not Update .....	326
Appliance Running out of Space .....	327
Cannot Access Device .....	328
Cannot Add Device Overview .....	329
Incorrect Device Credentials .....	330
Firewall Blocking Access (Windows and Vista) .....	331
Local Workgroup Credentials Not Accepted (Vista) .....	332
Local User Not Authenticated (Windows XP) .....	333
File Sharing Not Enabled (XP) .....	335
File Sharing Not Enabled (Vista) .....	337
File Sharing Not Enabled (MAC OS X) .....	338
File Sharing Not Enabled (Samba) .....	341
File Sharing Not Enabled (Windows 7) .....	343
Exchange and SQL Server Database Backup .....	348
Virtual Network Computing (VNC) Usage .....	348
Hyper-V Virtual Machine Guidelines .....	349
VSS Configuration .....	352
Windows Configuration .....	357
Autotask Integration .....	362
ConnectWise Integration .....	368
ConnectWise Appendix .....	370

How to Configure Alerting .....	377
Access BMR Utilities .....	379
Memory Test Utility .....	379
Disk Partitioning Utility .....	380
Unknown Device Identifier Utility .....	382
SNMP View MIB Information .....	384
Configuring MIB Browser .....	392
Required Firewall Ports .....	393

# Preface

## Intended Audience

This guide is intended for administrators who manage and monitor an Axcient appliance.

## Introduction

The Unified Management Console (UMC) is the user interface for a specific Axcient appliance. Device management, protection, and recovery are all possible for devices protected by the appliance.

The Axcient appliance sits inside the corporate firewall. When the backup job schedule is configured, the Axcient appliance automatically replicates and stores data collected from the target devices. For disaster protection, the appliance sends encrypted data to the Axcient Cloud through the Internet.

The Axcient appliance is typically on the same subnet as the devices it protects, but can support devices anywhere on the network.

## Administration

The UMC includes the following areas for administrative:

- **Dashboard** - Displays status information about backup jobs, virtual machines, and bare metal restore operations, as well as system resources and system activities.
- **Devices** - Allows you to manage devices, define and execute backup jobs, restore data, and configure devices for failover and restore protection.
- **Reports** - Displays a set of usage, history, and scheduling reports.
- **Events** - Displays the event log and allows you to configure email alerting for selected events.
- **Users** - Allows you to add and administrative users and specify their roles.
- **System** - Allows you to set system parameters including network, quality of service (bandwidth throttling), data, Cloud backup, SNMP, web proxy, and email.

## Logging in to the UMC

To log in to the UMC of an Axcient appliance:

1. Open an Internet browser and enter the **IP address** or **hostname** of the appliance.
2. Alternatively, on the *Service Details* page of the Axcient Web Application, click the **Login** button.
3. On the *UMC Login* page, enter the **UMC login** credentials. The default credentials for the UMC are:

- **Username:** Admin
- **Password:** Welcome1

**Figure 1** - The UMC Log In Page

**Axcient**  
Unified Management Console

## login

Username:

Password:

4. When you log in for the first time, you will be presented with a pop-up notification, alerting you that the UMC stores cookies on your computer. Please note that these cookies are needed to provide personalized services to you, and do not track your information. Click the **OK** button to continue. You will not be presented with this warning again unless the cookies are cleared.
5. For security reasons, you will also be prompted to change your password when logging in for the first time. Update your password and click the **save** button to continue.

**Figure 2** - The Change Password Page

**Axcient**  
Unified Management Console

dashboard | devices | reports | events | users | system | docs

## change password

You must change your password before you may continue

Current Password:

New Password:

Retype Password:

**Information**  
This website stores cookies on your computer. These cookies are used to improve your website and provide more personalized services to you, both on this website and through other media. We don't track your information when you visit our site.

# UMC Dashboard

The UMC Dashboard is the landing page of the UMC, and displays status information about jobs, backup jobs, recovery processes, system activities, and resources.

## 1 Backup Status Information

Contains status information regarding backup jobs (running and idle), virtual machines and BMRs, restore operations, and system events.

## 2 Disk Utilization

Shows total local storage usage, local storage used by device, the most recent cloud backup job status, and the cloud backup job status when running.

## 3 Devices

List of devices protected by the appliance. Click a device to view details, or click **Add New Device** to add a new device to be protected.

## 4 Resource Monitor

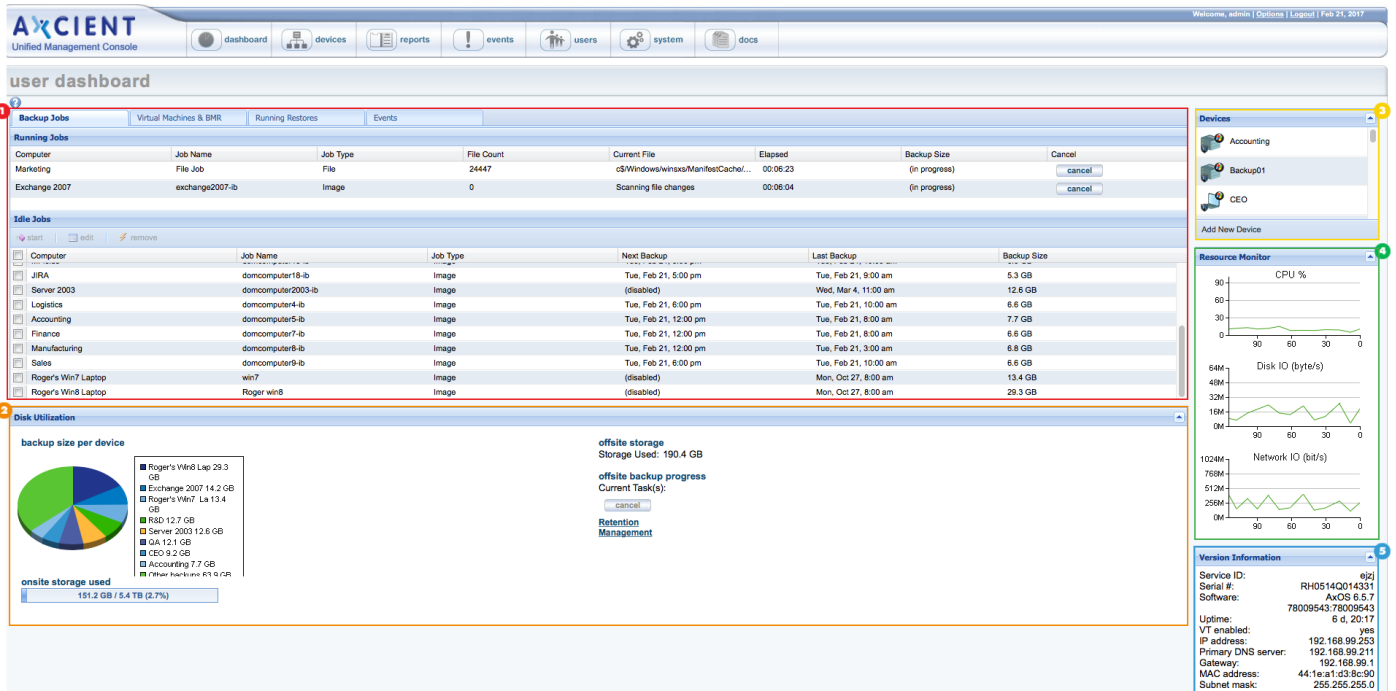
Displays three dynamically updated monitors showing CPU usage, disk I/O, and network I/O for the appliance.

## 5 Version Information

Displays the service ID, serial number, software version, and network information of the appliance.



Figure 3 - The UMC Dashboard



## Backup Status Information

The backup status information section of the UMC Dashboard includes the following:

- Backup Jobs tab
- Virtual Machines & BMR tab
- Running Restores tab
- Events tab

**Figure 4 - The Backup Status Information Panel**

Backup Jobs

Virtual Machines & BMR

Running Restores

Events

Running Jobs

Computer	Job Name	Job Type	File Count	Current File	Elapsed	Backup Size	Cancel

Idle Jobs

start

edit

remove

Computer	Job Name	Job Type	Next Backup	Last Backup	Backup Size
<div><div></div><div>JSmith</div></div>	domcomputer10-ib	Image	Tue, Jun 9, 3:00 pm	Tue, Jun 9, 7:00 am	8.4 GB
<div><div></div><div>Marketing</div></div>	domcomputer11-ib	Image	Tue, Jun 9, 1:00 pm	Tue, Jun 9, 7:00 am	9.9 GB
<div><div></div><div>JDoe</div></div>	domcomputer12-ib	Image	Tue, Jun 9, 3:00 pm	Tue, Jun 9, 7:00 am	8.3 GB
<div><div></div><div>CEO</div></div>	domcomputer2-ib	Image	Tue, Jun 9, 1:00 pm	Tue, Jun 9, 7:00 am	10 GB
<div><div></div><div>R&amp;D</div></div>	domcomputer17-ib	Image	Tue, Jun 9, 4:00 pm	Tue, Jun 9, 10:00 am	10.9 GB
<div><div></div><div>QA</div></div>	domcomputer16-ib	Image	Tue, Jun 9, 4:00 pm	Tue, Jun 9, 10:00 am	15.9 GB
<div><div></div><div>MFields</div></div>	domcomputer13-ib	Image	Tue, Jun 9, 3:00 pm	Tue, Jun 9, 10:00 am	9.9 GB
<div><div></div><div>JIRA</div></div>	domcomputer18-ib	Image	Tue, Jun 9, 5:00 pm	Tue, Jun 9, 9:00 am	9.7 GB
<div><div></div><div>Server 2003</div></div>	domcomputer2003-ib	Image	(disabled)	Wed, Mar 4, 11:00 am	12.6 GB

## Backup Jobs Tab

The *Backup Jobs* tab provides information about all defined backup jobs, including:

- The *Running Jobs* section lists all jobs that are currently running or queued to run.
- The *Idle Jobs* section lists all defined jobs that are not currently running or queued.

The *Running Jobs* and *Idle Jobs* sections each display the following fields:

### Running Jobs Term Definitions

Column	Description
Computer	Displays the name of the device. The name is either the device alias entered when the device was added, the IP address, or the device name.
Job Name	Displays the name of the job, which was specified when the job was created.
Job Type	Displays the type of data to be backed, including: <ul style="list-style-type: none"> <li>• File</li> <li>• Image</li> <li>• Exchange</li> </ul>
File Count	Displays the number of files backed up. This is a dynamic count that increments as the backup progresses.

Column	Description
Current File	Dynamically lists the full path of the file currently being backed up. Displays <i>Initializing</i> during set up, <i>Waiting to Run</i> when waiting in the job queue, and <i>Scanning Files</i> while searching for files.
Elapsed	Displays the elapsed time since the backup job started (in the form of <i>hh:mm:ss</i> ).
Backup size	Displays the size (in KB, MB, GB or TB) of backed up files while the backup job is initializing or waiting in the queue. While the job is running, this field displays an <i>In Progress</i> indicator.
Cancel (button)	<p>Aborts the running backup job. Canceling the backup job will undo any replication made by the backup job. In some instances, the backup job cannot be canceled depending on the current state of the backup. When a backup is canceled, the following messages will display:</p> <ul style="list-style-type: none"> <li>• <i>Your backup job was canceled</i> indicates that the backup job was successfully canceled.</li> <li>• <i>Your backup job was <b>not</b> canceled</i> indicates that the backup job was completed (successfully or unsuccessfully) before the request could be implemented. Check the event log for more information about this job.</li> </ul>

### Idle Jobs Terms and Definitions

Column	Description
Computer	Displays the name of the device. The name is either the device alias entered when the device was added, the IP address, or the device name.
Job Name	Displays the name of the job, which was specified when the job was created.
Job Type	<p>Displays the type of data to be backed up, including:</p> <ul style="list-style-type: none"> <li>• File</li> <li>• Image</li> <li>• Exchange</li> </ul>
Next Backup	Lists the start time for each backup job scheduled within the next 60 minutes (in the form of <i>ddd hh:mm am/pm</i> ).
Last Backup	Lists the finish time of the last back up of this job (in the form of <i>mm/dd/yyyy - hh:mm:ss am/pm</i> ).
Backup Size	Displays the size (in KB, MB, GB or TB) of backed up files while the backup job is initializing or waiting in the queue. While the job is running, this field displays an <i>In Progress</i> indicator.
Start, Edit, and Remove (buttons)	<p>Directly below the Idle Jobs header are the following three buttons:</p> <ul style="list-style-type: none"> <li>• The <i>Start</i> button is used to start one or more backup jobs immediately. This will not change the schedule but simply begins the selected jobs. These jobs will start again at the scheduled time unless the manually started jobs are still running at that time.</li> <li>• The <i>Edit</i> button is used to edit a backup job. This button launches the summary page for that backup job. From this page, you can edit, delete, restore, or initiate VMs or BMRs.</li> <li>• The <i>Remove</i> button deletes one or more backup job.</li> </ul>

## Virtual Machine & BMR Tab

The *Virtual Machine & BMR* tab provides status information for all image backup jobs defined for the Axcient appliance.

**Figure 5 - The Virtual Machine & BMR Tab**

Backup Jobs	Virtual Machines & BMR	Running Restores	Events		
Virtual Machines & BMR					
Protected Computer	Computer Status	Restore Status	Backup Status	Last Backup	Control
JSmith	Online	Test VM Running	Complete	Tue, Jun 9, 7:00 am	<button>control...</button>
Marketing	Online	Idle	Complete	Tue, Jun 9, 7:00 am	<button>control...</button>
JDoe	Online	Test VM Running	Complete	Tue, Jun 9, 7:00 am	<button>control...</button>
CEO	Online	Idle	Complete	Tue, Jun 9, 7:00 am	<button>control...</button>
Backup01	Online	Idle	Complete	Tue, Jun 9, 10:19 am	<button>control...</button>
R&D	Online	Idle	Complete	Tue, Jun 9, 10:00 am	<button>control...</button>
QA	Online	Idle	Complete	Tue, Jun 9, 10:00 am	<button>control...</button>
MFields	Online	Idle	Complete	Tue, Jun 9, 10:00 am	<button>control...</button>
JIRA	Online	Idle	Complete	Tue, Jun 9, 9:00 am	<button>control...</button>
Server 2003	Online	Idle	Complete	Wed, Mar 4, 11:00 am	<button>control...</button>
Logistics	Online	Idle	Complete	Tue, Jun 9, 10:00 am	<button>control...</button>
Accounting	Online	Test VM Running	Complete	Tue, Jun 9, 8:00 am	<button>control...</button>
Finance	Online	Idle	Complete	Tue, Jun 9, 8:00 am	<button>control...</button>

Clicking the **control** button launches a window that displays status information about the image backup job and the most recent Virtual Machine (VM) failover or Bare Metal Restore (BMR) action. It also includes the following drop-down menus:

- The *Failover VM* menu allows you to manage a production failover VM (*start*, *shutdown*, *restart*, *discard*, or *bare metal restore*). A production failover VM uses the same IP address as the original device.
- The *Test VM* menu allows you to manage a VM used for testing purposes (*start*, *shutdown*, *restart*, or *discard*). A test VM failover uses an alternate IP address.
- The *Bare Metal Restore* menu allows you to manage a BMR operation (*start*, *stop*, or *restart*).

Note that some options are not available at certain times. Any tab or menu item that is not an available option will be grayed out and cannot be selected.

The following table outlines each column in the Virtual Machine & BMR tab:

Column	Description
Protected Computer	Displays the name of the device. The name is either the device alias entered when the device was added, the IP address, or the device name.
Computer Status	Displays whether the protected computer is online or offline.
Restore Status	<p>Indicates whether a VM or BMR is active for the protected device.</p> <ul style="list-style-type: none"> <li>• An <i>Idle</i> status indicates no active VM or BMR operation, and that the image job is unlocked.</li> <li>• A <i>VM Starting</i> status indicates that a production or test failover VM is initializing.</li> <li>• A <i>VM Running</i> status indicates that the production or test failover VM is online and running. No backup jobs for this device will run while the VM is running.</li> <li>• <i>VM Discarding</i> - The production or test failover VM is being shut down permanently. All data changes while the VM was running are discarded.</li> </ul>

Column	Description
	<ul style="list-style-type: none"> <li>• <i>VM Stopped [Stopping]</i> - The production or test failover VM is in the process of shutting down. All data is preserved and the VM can be restarted at a later time.</li> <li>• <i>VM Restarting</i> - A previously stopped production or test failover VM is being restarted.</li> <li>• <i>VM Starting BMR</i> - The BMR process is starting using the VM image. The VM is shutdown while the BMR process is active.</li> <li>• <i>BMR Started [Starting]</i> - The image job is in the process of locking and preparing to start. This initiates the BMR process. The image job is suspended, and no backups or failover VMs can run while the BMR is running.</li> <li>• <i>BMR Stopping</i> - The BMR process is stopped, and backups can resume.</li> <li>• <i>BMR Starting VM</i> - The BMR process is stopped, and the shutdown VM restarts. This option applies only if the BMR was initiated through a VM Starting BMR action.</li> </ul>
Backup Status	<p>Indicates whether there is a system image available:</p> <ul style="list-style-type: none"> <li>• If the image backup job has not run for the first time, the status is <i>Not Done</i>.</li> <li>• If at least one version is available, the status is <i>Complete</i>.</li> </ul>
Last Backup	<p>Lists the finish time of the last image backup job. Note that this field is blank if the Backup Status is <i>Not Done</i>.</p> <ul style="list-style-type: none"> <li>• <b>Form</b> - <i>mm/dd/yyyy - hh:mm:ss AM PM</i></li> <li>• <b>Example</b> - <i>03/20/2015 - 11:09:37 AM</i></li> </ul>
Control Button	<p>Opens a window that displays status information about the image job and the most recent VM or BMR activity, including backup information and information about the most recent VM/BMR startup.</p>

## Running Restores Tab

The *Running Restores* tab provides information about all restore operations currently running. Each line represents one active restore operation.

The table below describes each column in the Running Restores section:

### Running Restores Terms and Definitions

Column	Description
Schedule	Displays the name of the job.
Destination Device	Displays the name of the device. The name is either the device alias entered when the device was added, the IP address, or the device name.
Elapsed Time	Displays the elapsed time since the restore operation started (in the form of <i>hh:m:ss</i> ). This display updates dynamically.
File Count	Displays the number of files restored. This is a dynamic count that increments as the restore progresses.
Total File Count	Displays the total number of files to be restored.
Current File	Dynamically lists the full path of the file currently being restored.
Cancel (button)	<p>Click the <b>Cancel</b> button to abort the restore operation immediately.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>Only file or mailbox restores can be canceled. System image and system state restores cannot be canceled.</li> <li>This button stops the restore process, but it does not roll back the transaction. Any files restored prior to canceling will remain on the destination device.</li> </ul>

## Events Tab

The *Events* tab provides information about events that occurred within the last hour (60 minutes).

**Figure 6 - The Events Tab**

Backup Jobs			
Virtual Machines & BMR			
Running Restores			
Events			
Type	Date	Action	User
<a href="#">Events in the last 1 hour</a> <a href="#">See All Events (8 Items)</a>			
USER_LOGIN	06/10/2015 - 01:20:44 PM	User: admin logged in	admin
BACKUP_DATA_CHANGE	06/10/2015 - 01:16:43 PM	Backup size for domcomputer2-ib on machine CEO has changed by 221 bytes	UBS
SERVER_ALIVE_BACKUP_SUCCEEDED	06/10/2015 - 01:16:43 PM	Backup Hourly for domcomputer2-ib on domaincomputer2 completed Successfully ( Included drives - C: )	admin
SERVER_ALIVE_BACKUP_WARNING	06/10/2015 - 01:16:41 PM	Backup Hourly for domcomputer2-ib on domaincomputer2 Warning - StdErr - Permission denied warnings have been encountered. Pl... Error: Unable to query path "Windows/System32/LogFiles/WM/RtBackup/EtwRTEventLog-Application.etl". Skipping.. Cause: Permission denied Error: Unable to query path "Windows/System32/LogFiles/WM/RtBackup/EtwRTEventLog-System.etl". Skipping.. Cause: Permission ... Error: Unable to query path "Windows/System32/LogFiles/WM/RtBackup/EtwRTEventLog-Security.etl". Skipping.. Cause: Permission ...	admin
BACKUP_DATA_CHANGE	06/10/2015 - 01:15:25 PM	Backup size for domcomputer11-ib on machine Marketing has changed by 3 KB	UBS
SERVER_ALIVE_BACKUP_SUCCEEDED	06/10/2015 - 01:15:25 PM	Backup Hourly for domcomputer11-ib on domcomputer11 completed Successfully ( Included drives - C: )	admin
SERVER_ALIVE_BACKUP_STARTED	06/10/2015 - 01:00:47 PM	Backup Standard Started for domcomputer11-ib on domcomputer11	admin
SERVER_ALIVE_BACKUP_STARTED	06/10/2015 - 01:00:47 PM	Backup Standard Started for domcomputer2-ib on domaincomputer2	admin

The table below describes each column in the *Events* tab.

### Events Terms and Definitions

Column	Description
Type	Displays the category of the event (for example, <i>DEVICE_ADDED</i> or <i>USER_LOGIN</i> ).
Date	Displays when an event occurred (in the form of <i>mm/dd/yyyy - hh:mm:ss AM PM</i> ).
Action	Displays the event message (for example, <i>Added Device: IP_address</i> or <i>login</i> ).
User	Displays the name of the user that generated the event (for example, <i>admin</i> ).

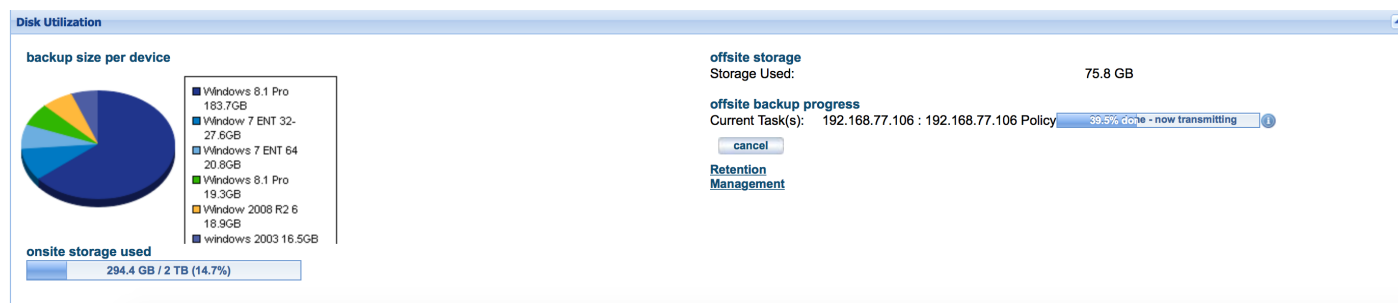
## Disk Utilization Panel

The *Disk Utilization* panel outlines the following information:

### Disk Utilization Panel Terms and Definitions

Column	Description
Onsite storage by device	Displays onsite storage usage by device.
Onsite storage used	Displays the total storage space used on the Axcient appliance. Please note that the appliance uses additional space independent of saved jobs, so the <i>onsite storage used</i> value is greater than zero even before the first backup job is run. In addition, the appliance includes a separate partition where the config-database information is stored that is not included in the total. The reported number refers to the available storage capacity, not the total capacity of the appliance.
Offsite storage	Displays the status of the last cloud backup job and space used for the Axcient appliance in the Axcient Cloud.
Offsite backup progress or Offsite backup progress - verification	<p>Displays dynamic status information when there is a cloud backup job or a cloud verification task in progress. This cloud verification task runs periodically to ensure data integrity, and might run longer than a normal cloud backup job.</p> <p>When a cloud backup is in progress, the following lines report status information:</p> <ul style="list-style-type: none"> <li><i>Current Task(s)</i> displays progress information about the individual backup jobs being processed. Click the <b>Information</b> icon next to the progress bar to view more detailed information about a specific cloud backup job.</li> <li><i>Tasks Finished</i> displays the number of completed jobs in the cloud backup.</li> <li><i>Files Scanned</i> displays the total number of files processed across all jobs being backed up to the cloud.</li> <li><i>Files Changed</i> displays the total number of changed files processed across all jobs being backed up to the cloud.</li> <li><i>Total Time</i> displays the total processing time across all jobs being backed up to the cloud.</li> </ul>
Start (button)	Click the <b>Start</b> button to manually start a cloud backup job.
Cancel (button)	<p>Click the <b>Cancel</b> button to stop an active cloud backup job. Please note that stopping a cloud backup job might not be possible depending at what point in the job progress the <i>Cancel</i> button is clicked. When the action is complete, one of the following messages displays</p> <ul style="list-style-type: none"> <li><i>Your backup job was canceled</i> indicates the backup job was successfully canceled.</li> <li><i>Your backup job was not canceled</i> indicates the backup job completed (either successfully or unsuccessfully) before the cancel request could be implemented.</li> </ul>

**Figure 7 - The Disk Utilization Panel**





## Devices Panel

The *Devices* panel displays a list of devices protected by the appliance. Using the panel, you can:

### Devices Panel Terms and Definitions

Item	Description
Device name	Click a <b>device</b> to open the device summary page. On this page you can manage the device and backup jobs for the device.
Add New Device (button)	Click the <b>Add New Device</b> button to open the <i>Add a Device</i> page.

**Figure 8** - The Devices Panel



## Resources Monitoring Panel

The *Resource Monitoring* panel displays three dynamically updated monitors. In each case, the vertical axis represents space used, and the horizontal axis represents time. The display time period for all monitors is a rolling two-minute interval moving from right-to-left and labeled in seconds (0, 30, 60 and 90).

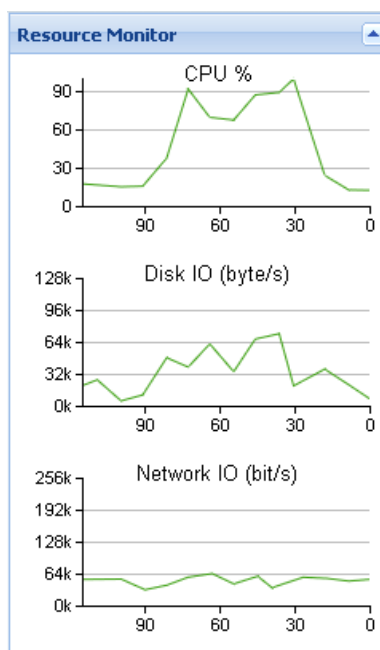
By default, the *Resource Monitoring* panel is collapsed on the dashboard. Click the **down arrow** to display the panel.

Using this panel, you can view the following information:

### Resources Monitoring Panel Terms and Definitions

Item	Description
CPU %	Displays the CPU utilization percentage per second. The vertical axis is the percentage used (0-100%).
Disk I/O	Displays the number of disk operation in bytes per second. The vertical axis is the number of bytes. The scale labels change to K (kilobytes), M (megabytes), and so on as the number of operations increase in magnitude.
Network I/O	Displays the number of bits per second for the network port. The vertical axis is the number of bits. The scale labels change to K (kilobits), M (megabits), and so on as the number of operations increase in magnitude.

**Figure 9** - The Resource Monitoring Panel



## Version Information Panel

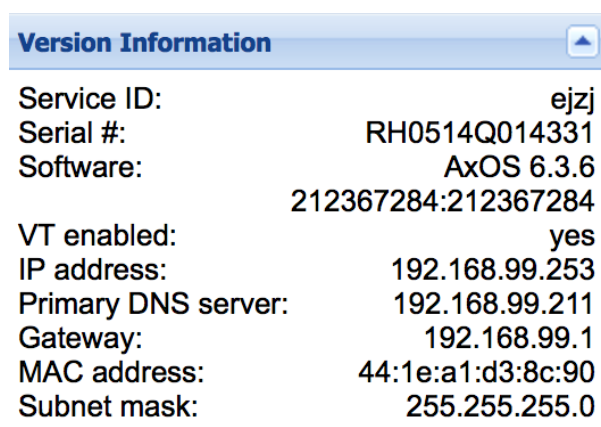
The *Version Information* panel displays version or address information for various system parameters.

The table below outlines the version parameters in the *Version Information* panel.

**Version Information Panel Terms and Definitions**

Column	Description
Service ID	Displays the unique service identification number of the Axcient service.
Serial #	Displays the unique serial number assigned to the Axcient appliance. This number is associated with the physical appliance.
Software	Displays the version of the software running on the Axcient appliance.
VT Enabled	Identifies whether the processor in the Axcient appliance is VT-enabled. You must enable VT to support the VM and BMR features.
IP Address	Displays the IP address of the Axcient appliance.
Primary DNS Server	Displays the IP address of the primary DNS server used by the Axcient appliance.
Gateway	Displays the IP address of the main gateway used by the Axcient appliance.
MAC Address	Displays the Media Access Control (MAC) address for the network interface card (NIC).
Subnet Mask	Displays the subnet mask used by the Axcient appliance.

**Figure 10** - The Version Information Panel



Version Information	
Service ID:	ejzj
Serial #:	RH0514Q014331
Software:	AxOS 6.3.6
	212367284:212367284
VT enabled:	yes
IP address:	192.168.99.253
Primary DNS server:	192.168.99.211
Gateway:	192.168.99.1
MAC address:	44:1e:a1:d3:8c:90
Subnet mask:	255.255.255.0

# Device Management

## Add a Device

The file sharing service must be enabled to read files on a device. See the [Cannot Add Device Section](#) for more information.

For devices running Windows, Axcient provides scripts that help configure these devices to properly support all Axcient features. After adding a device, it is recommended that you run the VSS and Windows configuration scripts. See the [VSS Configuration](#) and [Windows Configuration](#) sections for more information.

To add a device:

1. Click the **Add New Device** button on the *Devices* panel of the Dashboard.
  - a. Alternatively, on the UMC, click the **devices** tab. The *Devices* page displays.
  - b. On the *Devices* page, click the **add new devices** option on the left navigation menu. The *Add Device* page displays.

**Figure 11** - The Devices page

The screenshot shows the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'devices' section with options: add a device, add multiple devices, remove devices, change credentials, enable all jobs, and disable all jobs. The main content area is titled 'add a device' and contains the following form fields:

- Hostname or IP: 192.168.77.151
- Operating system: AUTODETECT
- Device type: DESKTOP
- Administrative username: admin
- Administrative password: (masked with asterisks)
- Device alias: Joe desktop
- Additional user assigned: --- Select a User ---

Buttons for 'cancel' and 'save' are located at the bottom of the form.

2. On the *Add Device* page, enter the appropriate information and then click the **save** button. The table below describes each parameter.

### Add a Device Terms and Definitions

Parameter	Description
Hostname or IP	Enter the <b>hostname</b> or <b>IP address</b> of the device. When entering a hostname, you can enter the name of the device if the device is in the same domain as the appliance.  When using DHCP, enter the hostname rather the IP address because the appliance treats the IP as a static address, and the connection will be lost if the IP address is reassigned later by DHCP.
Operating System	Select the <b>device operating system</b> from the drop-down menu. The default option is <b>AUTODETECT</b> . In most instances, you can select <b>AUTODETECT</b> .

Parameter	Description
Device Type	Select the <b>type of device</b> from the drop-down menu. This setting determines the icon display for the device in the UMC, and helps configure device-specific functionality.
Administrative username and password	For Windows devices, provide credentials of a member from Backup Operator Group or a user account with backup privileges. For Linux devices, provide credentials of a user with read-write permissions to the files and folders you want to back up.
Device alias (optional)	Optionally, enter an <b>alias name</b> for the device. This alias displays in the UMC.
Additional user assigned (optional)	Grant an additional user access to the device. Only the administrative users have access by default, but additional users can be added through this parameter. User permissions dictate what actions they can perform. For more information, please reference the <a href="#">User Management</a> section of this guide. The three predefined users are listed below, but additional users can be created as well: <ul style="list-style-type: none"> <li>• <b>admin</b></li> <li>• <b>backupuser</b></li> <li>• <b>limitedbackupuser</b></li> </ul>

The Axcient appliance verifies it can connect to the device and returns a *device has been added* notification.

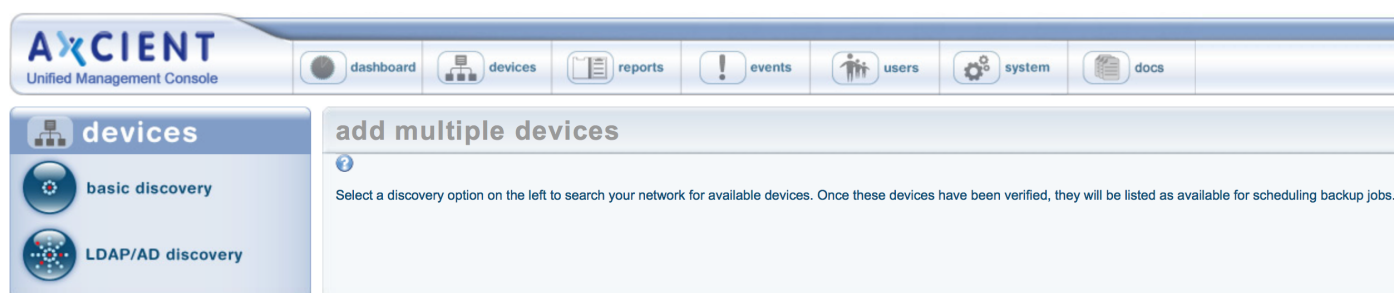
## Add Multiple Devices on a Network Segment

Optionally, you can use the *Basic Discovery* process to detect all devices within the Axcient appliance network segment. When the discovery process is complete, the total number of devices found are displayed. You can then review the list of devices and add or remove devices as needed.

To add multiple devices on a network segment:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, click the **add multiple devices** link on the left navigation menu. The *Add Multiple Devices* page displays.

Figure 12 - The Add Multiple Devices page



3. On the *Add Multiple Devices* page, click the **basic discovery** option on the left navigation menu. The *Basic Discovery* page displays.

Figure 13 - The Basic Discovery page



4. On the *Basic Discovery* page, enter the administrative **username** and **password** and click the **save** button.

Please note that the username and password will be used to authenticate all devices. A device that requires different credentials will not be added through this process, and the following error message will display:

*Could not connect to device: xxxx.*

The Basic Discovery process might take some time depending on the number of devices on the subnet. When the discovery process is complete, each discovered device will display. Review the list of devices and individually add or remove devices as needed.

Figure 14 - Basic Discovery Summary

**AxCIENT**  
Unified Management Console

Welcome, admin | Options | Logout | Mar 9, 2020

dashboard devices reports events users system docs

**devices**

basic discovery  
LDAP/AD discovery

**devices**

**devices that failed to add:**

- Could not connect to device: aurora
- Could not connect to device: axcient-aadesk
- Could not connect to device: axcient-asandru
- Could not connect to device: axcient-icano
- Could not connect to device: demo
- Could not connect to device: ebr-exch-01
- Could not connect to device: ebr-qa1
- Could not connect to device: meeko
- Could not connect to device: niblets
- Could not connect to device: rverkler-pc

**desktops**

ascari	ax77234	axcient-714f04f	axcient-rpham	axcient-xo0pcfd	climax
destroyer	kliw2k3std32	kliw2k8r2std64	pinto	tamora	win-401gqmvqjc3



## Add Devices Using Active Directory

You can optionally integrate with an Active Directory (LDAP) source to retrieve a list of devices within a network.

To add devices from an Active Directory (LDAP) source:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, click the **add multiple devices** option on the left navigation menu. The *Add Multiple Devices* page displays.
3. On the *Add Multiple Devices* page, select the **LDAP/AD discovery** option on the left navigation menu. The *Active Directory Network Discovery* page displays.

**Figure 15** - The Active Directory Network Discovery page

4. Enter the appropriate information and then click the **save** button. The table below outlines each parameter.

### Active Directory Terms and Definitions

Parameter	Description
Active Directory server	Enter the <b>IP address</b> or <b>server name</b> of the Active Directory server. For example, <i>activated.mycompany.com</i> or <i>192.168.66.232</i> .
Windows domain	Enter the <b>Windows domain name</b> .
DNS domain	Enter the <b>DNS domain name</b> .
Administrator login	Enter the <b>administrator username</b> .
Administrator user principal name	Enter the unique <b>administrator user principal name</b> for Active Directory (in the form of <i>user_name@ad_domain_name</i> ).
Password	Enter the administrator <b>password</b> .

## Modify a Device

To modify the configuration of an existing device:

1. On the UMC, click the **devices** button. The *Devices* page displays.
2. On the *Devices* page, select the target device that needs to be modified.

Figure 16 - The Edit Devices page

3. On the *Edit Devices* page, update the fields as needed and then click the **save** button located in the appropriate section. The following table describes each parameter.

### Add a Device Terms and Definitions

Parameter	Description
Hostname or IP	Enter the <b>hostname</b> or <b>IP address</b> of the device. When entering a hostname, you can enter the name of the device if the device is in the same domain as the appliance.  When using DHCP, enter the hostname rather the IP address because the appliance treats the IP as a static address, and the connection will be lost if the IP address is reassigned later by DHCP.
Operating System	Select the <b>device operating system</b> from the drop-down menu. The default option is <b>AUTODETECT</b> . In most instances, you can select <b>AUTODETECT</b> .
Device Type	Select the <b>type of device</b> from the drop-down menu. This setting determines the icon display for the device in the UMC, and helps configure device-specific functionality.
Device alias (optional)	Optionally, enter an <b>alias name</b> for the device. This alias displays in the UMC.
Additional user assigned (optional)	Grant an additional user access to the device. Only the administrative users have access by default, but additional users can be added through this parameter. User permissions dictate what actions they can perform. For more information, please reference the <a href="#">User Management</a> section of this guide. The three predefined users are listed below, but additional users can be created as well: <ul style="list-style-type: none"> <li>• admin</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"><li>• backupuser</li><li>• limitedbackupuser</li></ul>
Administrative username	Enter the <b>administrator username</b> . In some instances, such as Exchange servers, it is necessary to include the domain as part of the username (in the form of <i>domain\name</i> ).
Administrative password	Enter the unique <b>administrator user principal name</b> . Please note that this field must be updated whenever the password changes for the device. Otherwise, the Axcient appliance will not be able to connect to the device.

Please note that entering incorrect information, such as the wrong administrative username or password, could break the device connection and require an additional edit to enter the correct information.

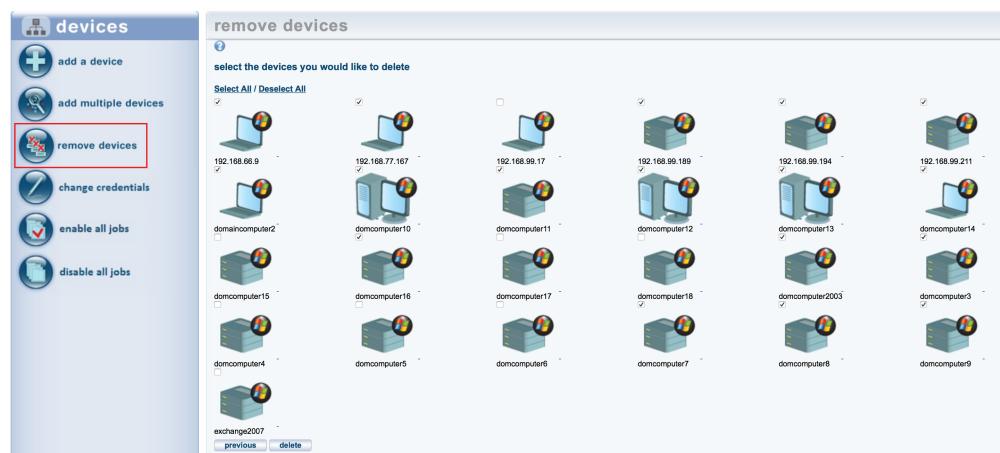
## Remove a Device

You can delete devices as necessary. Please note that all backup jobs must be deleted from a device before it can be removed.

To remove the Axcient appliance connection to a device:

1. On the UMC, click the **devices** button. The *Devices* page displays.
2. On the *Devices* page, click **remove devices** from the left navigation menu. The *Remove Devices* page displays.
3. On the *Remove Devices* page, use the checkboxes to select or deselect the devices to be remove. Please note that by default, all devices are selected for removal.
  - Optionally, click the **Select All** link to select all devices for removal.
  - Optionally, click the **Deselect All** link to deselect all devices. Deselected devices will not be removed.
4. Click the **delete** button when you are finished.

Figure 17 - The Remove Devices page



## Update Credentials for Multiple Devices

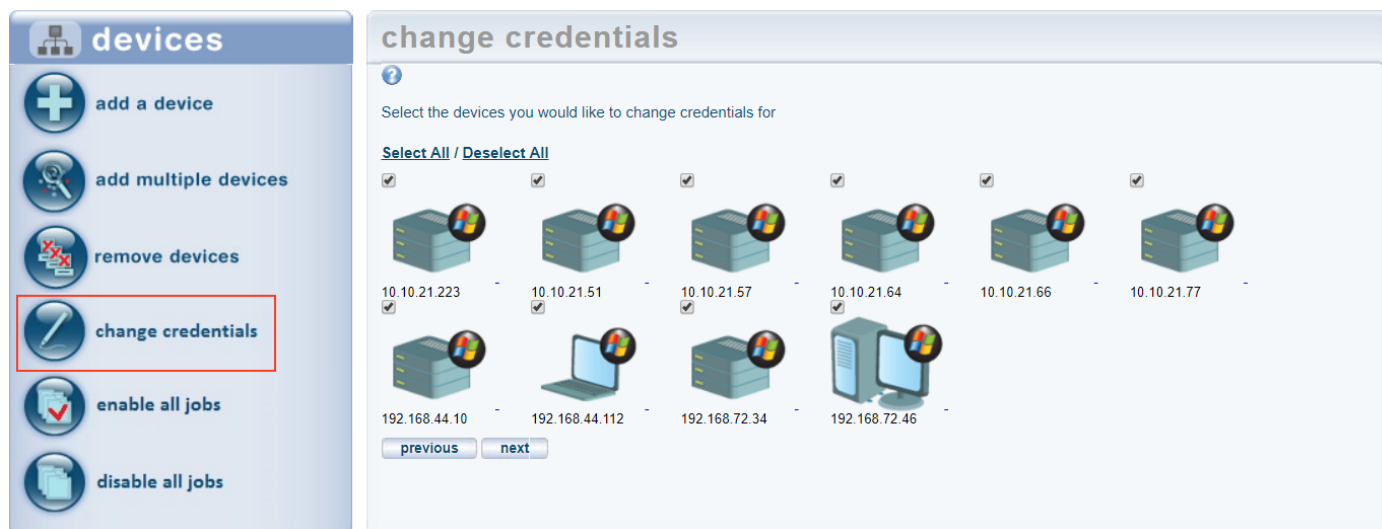
In some instances, you might need to update credentials for multiple devices at one time. For example, certain password change policies require that all passwords be updated periodically.

To change the credentials of multiple devices at one time:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, select the **change credentials** option from the left navigation menu. The *Change Credentials* page displays.
3. On the *Change Credentials* page, use the checkboxes to select the devices that need to be updated, and then click the **next** button.

- On the *Enter Credentials* page, enter new credentials in the *Username* field and *Password* field, and then click the **set** button.

Figure 18 - The Change Credentials page



## Enable or Disable Backup Jobs for All Devices

In some instances, you might need to enable or disable all backup schedules on an appliance. For example, you can disable all backup schedules during a planned maintenance window to prevent backups from starting and failing.

To enable or disable all backup schedules:

- On the UMC, click the **devices** tab. The *Devices* page displays.
- On the *Devices* page, select the **disable all jobs** option from the left navigation menu to *turn off* all backup schedules. Alternatively, select the **enable all jobs** option to *turn on* all backup schedules.
- In the confirmation dialog box, click the **OK** button to confirm.

Figure 19 - Enable All Jobs

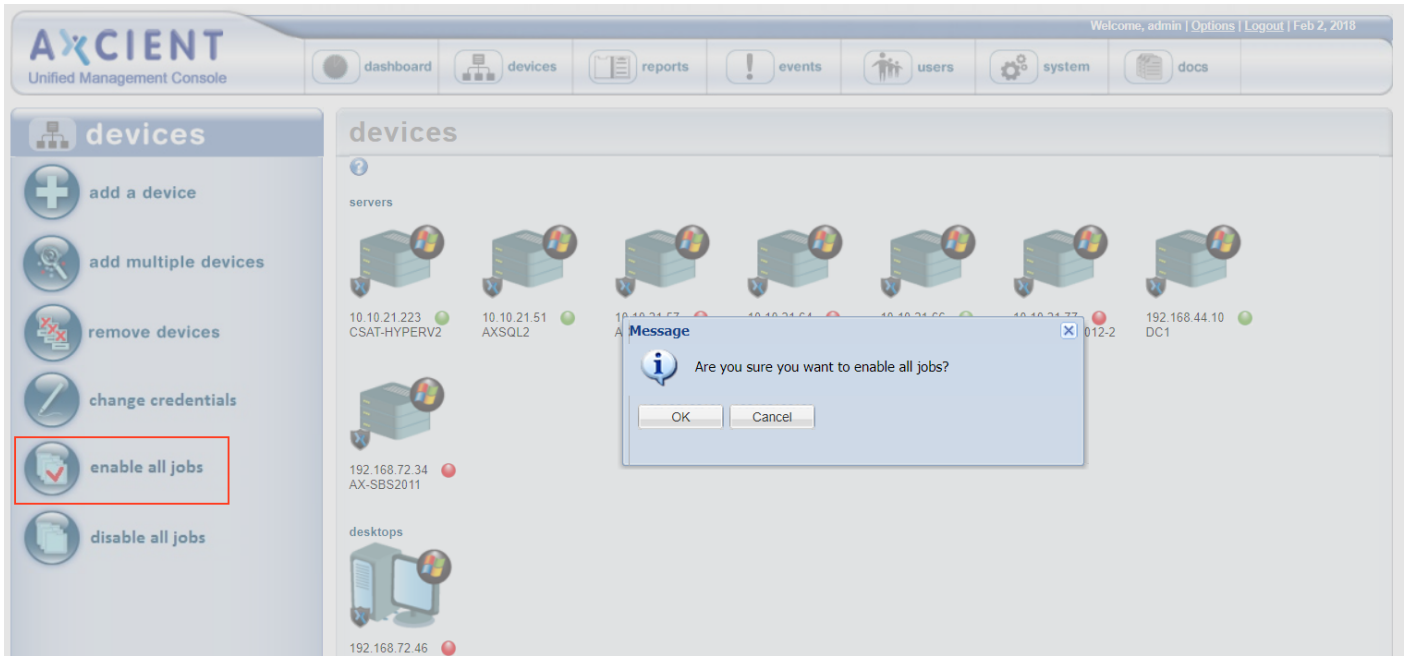
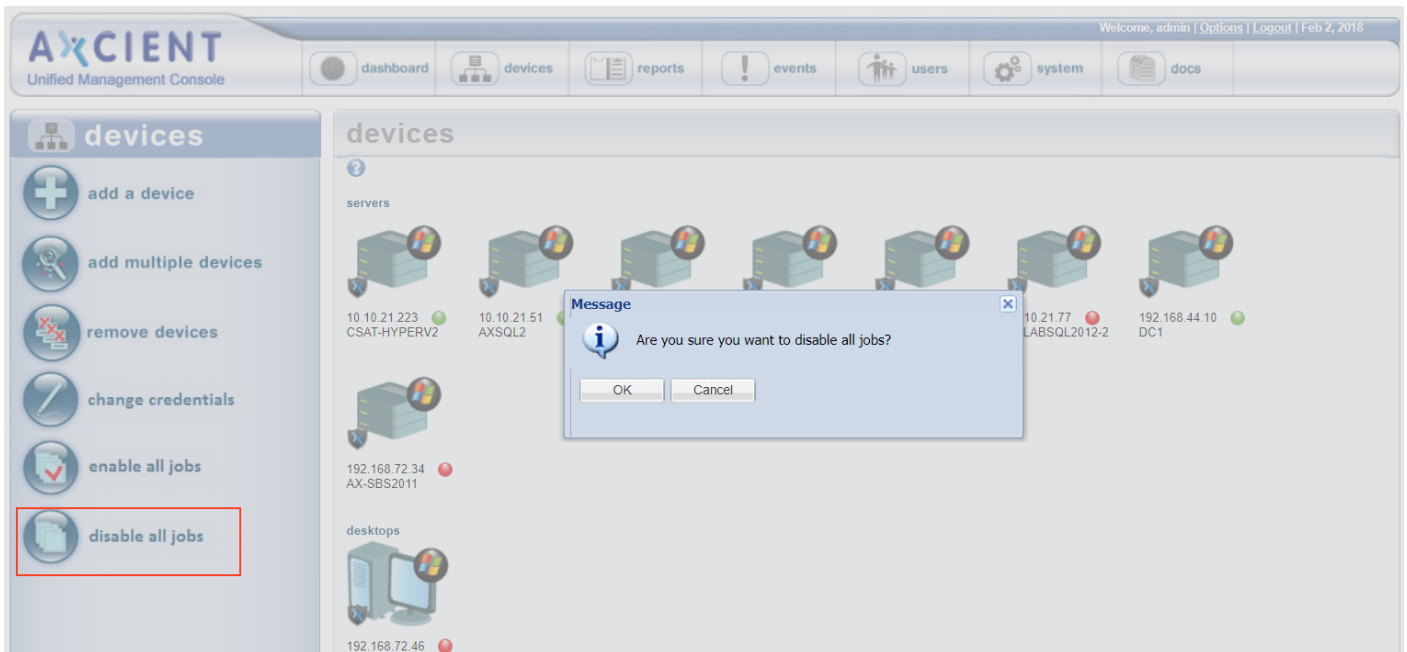


Figure 20 - Disable All Jobs



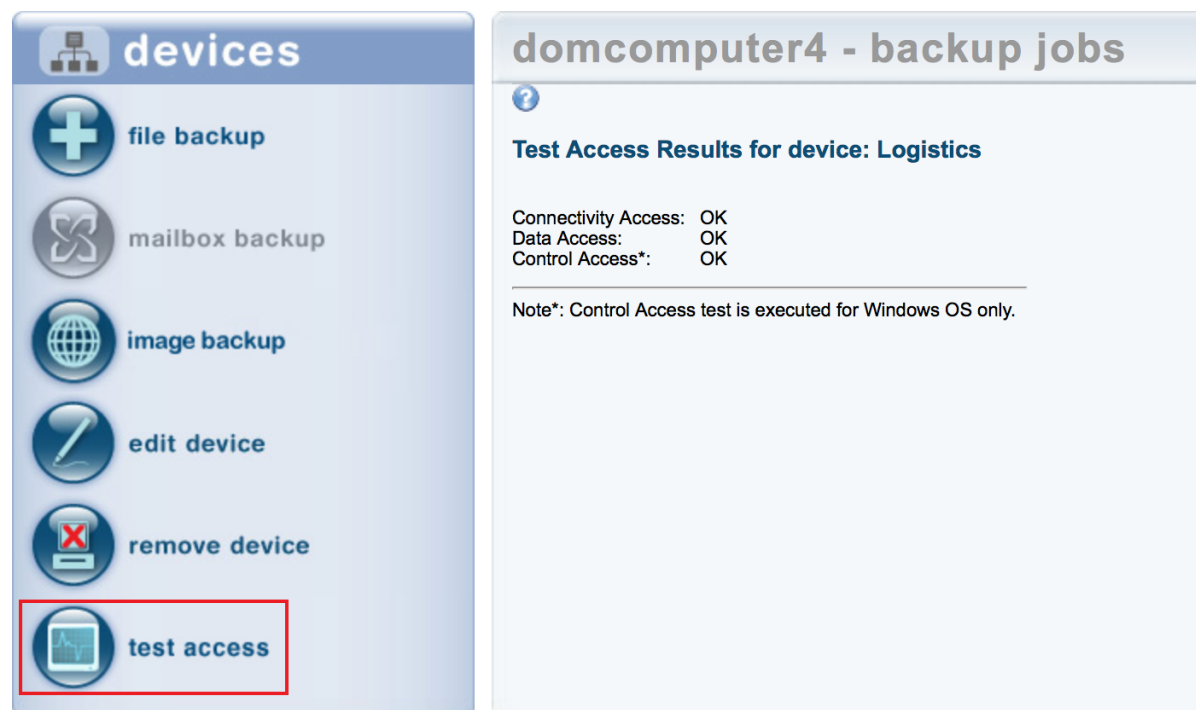
## Test Device Access

After adding a device, you can test that the Axcient appliance has proper access to the device.

To test device access:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, click the **device name** that will be tested.
3. Click the **test access** option from the left navigation menu.

**Figure 21** - The Test Access page



4. On the *Test Access* page, view the three available tests:
  - *Connectivity Access* tests whether the Axcient appliance has network access to the device.
  - *Data Access* tests whether the Axcient appliance can log into the device, recognize the operating system, and exchange information with the device.
  - *Control Access* (Windows devices only) tests whether the Axcient appliance can perform its data protection function, such as executing backup jobs.

Each test has two possible outcomes:

- *OK* indicates that the test passed. No action is necessary.
- *Failure* indicates that the test failed and action is required. The Control Access test provides information about the failure. The table below describes the corrective actions that can be taken if a test fails.

### Test Access Corrective Action List

Test	Corrective Action
Connectivity Access	<p>If this test fails, the Axcient appliance cannot find the device in the network. Check the standard network connections:</p> <ol style="list-style-type: none"> <li>1. Verify the device is powered on and active, the IP address or hostname is correct, and the DNS can resolve the hostname (if used).</li> <li>2. Run the connectivity health script to verify the Axcient appliance is properly connected to the network. See the <a href="#">Check Network Connections</a> section for more information.</li> <li>3. Use other network tools (such as <i>tracert</i>) to debug the problem. See the <a href="#">Check Network Connections</a> section for more information.</li> </ol>
Data Access	<p>If this test fails, the Axcient appliance cannot communicate with the device. Check the following:</p> <ol style="list-style-type: none"> <li>1. The most common problem is authentication. Verify that the login credentials are correct. For example, if the password was changed on the device, the device credentials must be updated on the Axcient appliance. See the <a href="#">Modify a Device</a> section to make any updates.</li> <li>2. Verify the correct operating system was specified for the device. See the <a href="#">Modify a Device</a> section to make any updates.</li> <li>3. Verify that file sharing on the device is enabled. See the <a href="#">Device Problems</a> section for more information.</li> </ol>
Control Access (Windows systems only)	<p>If this test fails, the Axcient appliance cannot perform its data protection functions on the device. Failing this test typically involves a more complex problem.</p> <ol style="list-style-type: none"> <li>1. Download and run the <b>windows configuration</b> script. This script might be able to debug and correct the problem. See the <a href="#">Windows Configuration</a> section for more information.</li> <li>2. If the script does not solve the problem, Call <a href="#">Axcient customer support</a> for help.</li> </ol>

## Manage VSS Storage Locations for Windows Devices

If you are protecting a Windows device, you can use the Manage VSS Storages page to specify a drive where VSS snapshots should be stored.

To specify VSS storage settings:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, click the **device name**.
3. Click the **manage VSS storages** option from the left navigation menu.



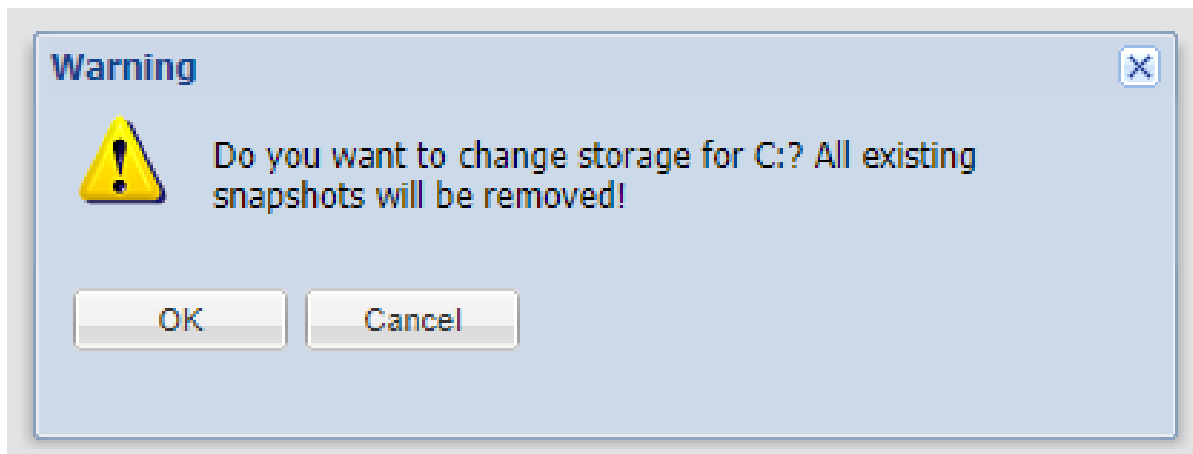
Figure 22 - The Manage VSS Storages page

The screenshot displays the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, and users. The left sidebar, under the 'devices' heading, lists several options: file backup, mailbox backup, image backup, edit device, remove device, test access, and manage VSS storages. The 'manage VSS storages' option is highlighted with a red rectangular box. The main content area is titled '172.18.50.66 - manage VSS storage' and contains a table with two columns: 'PATH' and 'STORAGE VOLUME'.

PATH	STORAGE VOLUME
C:	--- Disabled --- ▼
E:	F: ▼
F:	F: ▼

- On the *Manage VSS Storages* page, drive letters display in the left-hand column, and the VSS storage location options display in the right-hand column. Use the *Storage Volume* drop-down menus to select the preferred location where VSS snapshots will be stored. If no selection is made, then the storage location will be set automatically during a backup.
- If you change the drive to be used for storing VSS snapshots, a dialog box will display, alerting you that the existing snapshots will be deleted.

*Figure 23* - Changing the VSS Storage Location Warning Message



6. Click the **OK** button to delete existing snapshots and change the VSS storage location. Alternatively, click the **Cancel** button to cancel the operation.

# Backup Strategy

Axcient protects devices in two main ways:

- *File Backup* lets you select a set of files and folders (directories) to back up, including any combination of user files, application files, system files, and so on. Please reference the [Backup Files](#) section for more information.
- *Image Backup* (for Windows devices only) lets you back up a device as a single system image. Please reference the [Back Up System Image](#) section for more information. A system image can be used for any of the following:
  - Recover selected files. Please reference the [Tree View Restore](#) section for more information.
  - Restore a system image onto new hardware, commonly called a Bare Metal Restore. Please reference the [Restore Device \(BMR\) Overview](#) section for more information.
  - Create a virtual failover server (servers only). Please reference the [Virtual Machine \(VM\) Failover Overview](#) section for more information.

Because files can be restored from a system image, file backups are not needed for devices protected by an image job. However, the retention period of an image job is typically short (a week by default). To retain some files for a longer period of time, create a file backup job for those files and set the retention period to the desired length. Having both image and file backup jobs is data duplication, so only use a file backup job for files that *must* be retained for longer than the image job.

Please note that a Bare Metal Restore job and a failover VM extend *only to devices protected with in image job*.

Axcient Provides two levels of backup storage:

- During a *Local Backup*, all data is backed up and stored on the Axcient appliance. The backup and restore process is rapid because the appliance is local and all data is contained within the local network.
- During a *Cloud Backup*, the Axcient appliance sends a copy of the backed up data to the Axcient data center over an outbound Internet connection. Cloud storage ensures that data is protected from any source of local data loss such as a natural disaster.

Consider the following when deciding what backup jobs to create:

- Determine the type of data to protect, and whether you need to protect the entire device (image job) or a specific set of data (file job). You should also consider whether you need to create an image job *and* an additional file job for longer data retention.
- For file backup jobs, determine the scope of each job. Creating multiple smaller backup jobs targeted to specific data sets might be more efficient than a single large backup job for all the data on a device.
- Determine the type of protection needed (just local, or both local and Cloud) for each job. Mission-critical data should always be saved in the Cloud, as well as locally.
- Determine when to back up each job. Data that you have identified as dynamic and critical to your business might warrant daily or even hourly backups, whereas a weekly or monthly backup might be adequate for data that rarely changes.

- Schedule when to begin the Cloud backup job. Local backups occur as scheduled according to the job definition. Users can opt-in to Unbundled Offsites, or choose for a single Cloud replication job. See the [Schedule Cloud Backup Job](#) section for more information.

Please reference the [Initial Backup Strategy](#) section for initial set up recommendations.

## Back Up Files

Please note that it is not necessary to create a file backup job for devices protected by an image backup job unless you want a longer retention period for the target files.

Additionally, if *Windows folder redirection* is being used, the default permissions prevent Axcient from backing up the redirected folders. See the [Backup Fails Because of Windows Redirection](#) section for instructions on how to set proper permissions.

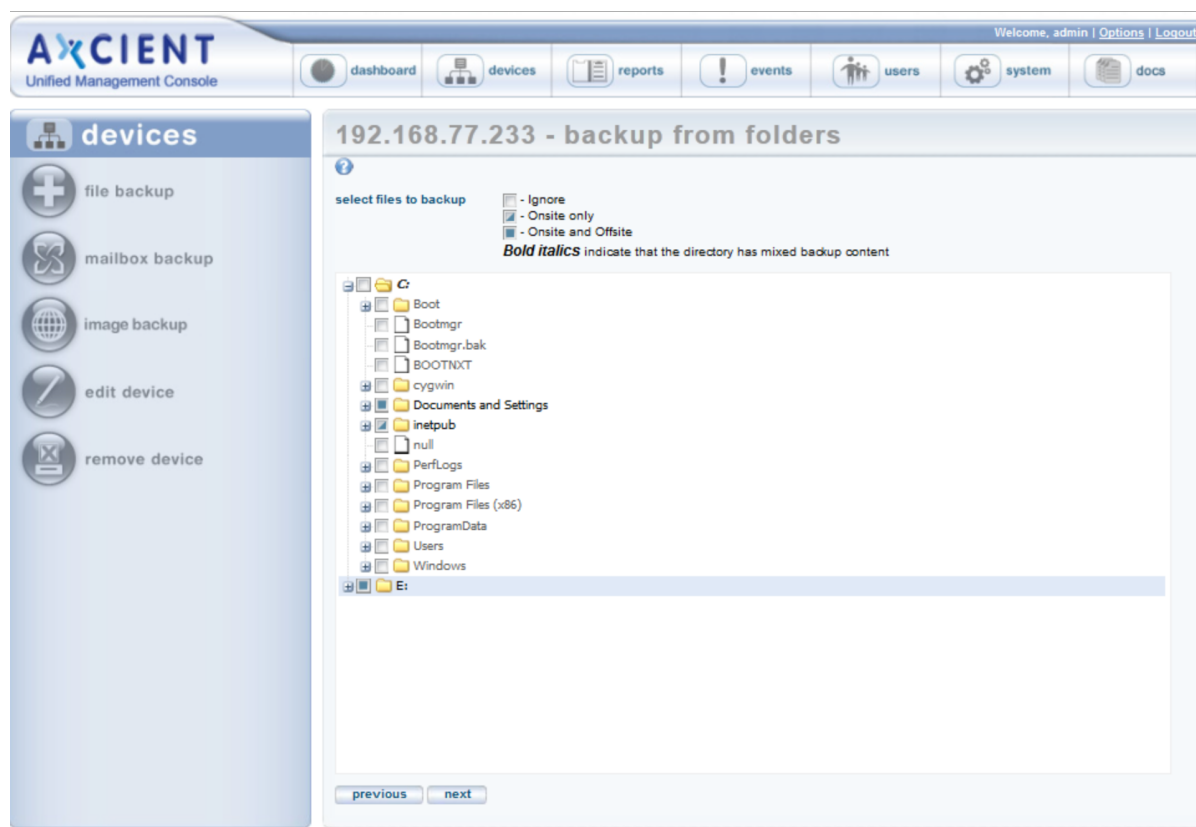
To create a file backup job for a device:

1. Select the target device using one of the following methods:
  - On the *Devices* pane on the *UMC*, click the **target device**.
  - Alternatively, click the **devices** tab at the top of the *UMC*. On the *Devices* page, click the **icon** of the target device.
2. On the *Backup Jobs* page for the device, click the **file backup** option located on the left navigation bar.
3. A list of drives (icons) displays in the center of the page. Click the **target drive** icons. For example, in the figure below, the device includes C and E drives.

### Caution!

We recommend that all backed up data reside on internal drives only. While you can optionally include USB drives in a file backup job, the assigned drive letter is part of the backup definition. If a USB is unplugged and then plugged in again, subsequent backup runs will fail if the USB drive is assigned to a different drive letter. In addition, USB drives are subject to transient changes that could cause a backup job to fail.

Figure 24 - The Backup from Folders Page



4. A file structure displays, allowing you to select target files and folders:
  - a. Expand the file structure on each drive to locate the target files.
  - b. Select the files to be backed up. Clicking a folder (directory) will select all its files and subfolders recursively.
  - c. Determine whether the files should be backed up locally only, or both locally and in the Cloud. A **solid box** (one click) next to a folder or file indicates a local *and* Cloud backup; a **half-solid box** (two clicks) indicates a Cloud-only backup.
  - d. After specifying all of the files to be backed up, click the **next** button.
5. On the *Backup Schedule* page, update the required fields. Please reference the table below for more information about each parameter.
6. Click the **save** button. When the **Enable Graduated Retention** box is checked, a **save & edit graduated retention rules** button appears. Click this button instead if you want custom rules for this job. See the [Set Local Graduated Retention Rules](#) section for more information.

The backup request is saved, and the backup job displays on the *Device Summary* page. If this is an on-demand backup, the job will begin immediately. Other backup types are scheduled accordingly. If the backup job is large, it can

take a substantial amount of time for the initial seed. We recommend that you monitor the progress and outcome to verify the backup job completes successfully.

Figure 25 - The Backup Schedule Page

**10.10.21.223 - backup schedule**

Create a schedule for your backup job. Select a backup schedule type and complete the corresponding details. An explanation of your schedule configuration is given in the summary below.

Schedule name:

Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Relative Offsite Priority:  (Enter any integer to raise this schedule's offsite priority relative to others. Larger value means higher priority.)

Backup schedule type:

Start time:  :  (9:00 AM)

Start a backup every:  hours

Keep starting backups until:  :  (7:00 PM)

On these days:

- ☒ Monday
- ☒ Tuesday
- ☒ Wednesday
- ☒ Thursday
- ☒ Friday
- ☐ Saturday
- ☐ Sunday

Keep backups for:  hours (about 7.0 days)

Use Open File Manager: ☒ (e.g., MS Exchange Server, MS SQLServer)

Preserve any Access Control Lists (ACLs): ☐ (increases time and size of backup slightly)

Enable Graduated Retention: ☐ (Restore points become less granular over time.)

Save System State: ☐ (Allows for the saving of system state)

Turn on Log Flushing (Pre Backup): ☒ (e.g., MS Exchange Server, MS SQLServer. Select Open File Manager to enable this.)

**Summary**

Your backup will run on Monday, Tuesday, Wednesday, Thursday, Friday, on an hourly basis, between the hours of 9:00 AM and 7:00 PM.  
Backups will be retained for 168 hours (about 7.0 days)

[previous](#) [save](#)

Please note that some files are always excluded for devices running a Windows Operating system. See the [Excluded Files \(Windows Devices\)](#) section for more information.

## Common Settings Terms and Definitions

Parameter	Definition
Schedule Name	Sets the backup job name.
Enabled	<p>Enables the backup job. When <i>enabled</i>, the backup job will run according to the specified schedule. When <i>disabled</i>, the job will not run, but all history is preserved and can be restored from.</p> <p>In most instances, a backup job should be enabled at all times. There are two reasons to disable a job:</p> <ol style="list-style-type: none"> <li>1. The device is no longer used, but the backup history needs to be preserved.</li> <li>2. There is a need to suspend running of a job for a period of time for things such as maintenance windows.</li> </ol>
Relative Offsite Priority	<p>Specifies a run priority relative to other Cloud backup jobs. All Cloud backup jobs are put in a queue and run serially starting at a specified time each day (see the <a href="#">Schedule Cloud Backup Job</a> section for more information). Job priority is not considered by default when setting a queue order, so all Cloud jobs start with a blank (zero) value in this field.</p> <ul style="list-style-type: none"> <li>• To set a job to run before the other, enter a positive integer value in this field.</li> <li>• To set a job to run after the others, enter a negative integer value in this field.</li> </ul>

Parameter	Definition
	The Cloud job with the highest value will run first, the next highest second, and so forth. The actual number does not matter, only the ordinal position (magnitude relative to other Cloud jobs) in the queue.
Backup Schedule Type	Sets the backup interval schedule from a drop-down list. Each schedule type has default settings that can be modified. See the following table for each default and optional settings for each type.
Use Open File Manager	<p>Sets whether to back up open files. By default, this parameter is enabled (box checked), which causes the appliance to back up open files. Such files typically are database or similar application files such as MS Exchange Server or MS SQL Server. To disable this feature and bypass (not back up) open files, uncheck the box. Note the following:</p> <ul style="list-style-type: none"> <li>Open File Manager uses Microsoft Volume Shadow Service (VSS). To configure VSS, see the <a href="#">VSS Configuration</a> section.</li> <li>Open File Manager is supported for any Windows device except for VP. It is not supported for Mac OS, Linux, or other operating system devices.</li> <li>The backed up version is a snapshot of the last committed version of the open files. Restoring the open files could result in some inconsistency within the application. After a restore, use the application tools to make sure the application files are in a consistent state.</li> </ul>
Enable Graduated Retention	<p>Sets graduated retention for this backup job. Select the checkbox to enable (disabled by default). You can select either global or local rules:</p> <ul style="list-style-type: none"> <li>To select the global rules, check the box. See the <a href="#">Configure Graduated Retention Defaults</a> section for more information.</li> <li>To specify local rules, select the checkbox and then click the <b>Save &amp; Edit Graduated Retention Rules</b> button. See the <a href="#">Local Graduated Retention Rules</a> section for more information.</li> </ul>
Save System State	<p>Sets whether to save all system state information. Checking this box allows you to restore a device back to a known system state in the event the device crashes or becomes unstable. Note the following:</p> <ul style="list-style-type: none"> <li>This is an option for devices running Windows Server or SBS 2012, 2008 or 2003 only.</li> <li>Backing up system state requires substantial storage space. Actual size varies, but testing suggests the initial SBS/Windows Server 2008 backup is about 6GB with each incremental backup adding about 600MB. When storage space is an issue, frequent schedule (hourly or daily) is not recommend for a system backup job.</li> </ul>
Turn on Log Flushing (Pre-Backup)	Enables pre-backup log flushing (on by default). When Open File Manager is enabled, this causes the VSS writers to do a log flush prior to creating the backup, which usually reduces the amount of Exchange data to back up (and might reduce the data to back up for other VSS-associated applications).

### Backup Schedule Types Terms and Definitions

Backup Schedule Type	Default	Start Time	Start a Backup Every	Backup on Connect (Laptops Only)	Keep Starting Backups Until	On these Days	Keep Backup For
On Demand	Sets a backup job to start immediately. An <i>on demand</i> backup runs just once. You can start it again manually at any time by selecting the <b>Start</b> link or button. There is only one on-demand version, so subsequent requests write	N/A	N/A	N/A	N/A	N/A	N/A



Backup Schedule Type	Default	Start Time	Start a Backup Every	Backup on Connect (Laptops Only)	Keep Starting Backups Until	On these Days	Keep Backup For
	over the existing version. An on-demand backup is retained indefinitely. It is deleted only by removing that backup job.						
Hourly	Sets a backup job to run on an hourly basis starting at 9:00am and continuing through 7:00pm on Monday through Friday (five days). Backup versions are retained for 168 hours (one week).	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. Each backup is run every interval (see the <b>Start a backup every</b> description) after the start time. For example, if the start time is 7:18am and the interval is set to one hour, the first backup starts at 7:18am, the next backup starts at 8:18am, and so on.	Sets the interval duration. By default, the interval is one hour, but you can specify a longer duration from the drop-down menu. For example, if this is set to <b>2</b> and the start time is <b>7:00am</b> , the first backup starts at 7:00am, the second starts at 9:00am, and so on.	Sets automatic (immediate) back up for laptops when they connect if they missed the most recently scheduled backup. By default, offline devices are ignored during a backup run and simply miss being backed up. Setting this parameter causes the Axcient appliance to monitor an offline laptop and begin a backup as soon as the laptop connects.  On a Windows laptop, a pop-up window displays when the backup begins, notifying the user that a backup is in progress and cautioning the user not to disconnect until the backup is complete. (To implement the pop-up window on Linux or Mac laptops, see the “Laptop Backup Strategy” section.)  <b>Note:</b> This field appears only if the Device Type for the device is set to LAPTOP.	Sets the backup run stop time. The specified time is the last hour that day a backup is started. By default, the stop time is 7:00pm, but you can change this to any hour from the drop-down menu. The minutes value is determined by the minutes setting in the Start Time parameter.	Sets which days the job runs. Check (click) the boxes next to the desired days. By default, Monday through Friday are checked.	Sets the retention period (amount of time a backup version is saved). After the specified interval, a version is deleted and cannot be restored. The default is 168 hours (7 days), and the maximum value allowed is 744 hours (31 days).  <b>Note:</b> If graduated retention is enabled, this field is ignored.
Daily	Sets backup jobs to run once a day Monday through Friday (five days) starting at 7:00pm. Backup versions are retained for 30 days (one month).	Sets the start time for daily backups. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time each day selected in the <b>On These Days</b>	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which days to run a daily backup. Check (click) the boxes next to the desired days. By default, Monday through Friday are	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The

Backup Schedule Type	Default	Start Time	Start a Backup Every	Backup on Connect (Laptops Only)	Keep Starting Backups Until	On these Days	Keep Backup For
		parameter.				checked.	default is 30 days (one month), and the maximum value allowed is 1827 days (five years).  <b>Note:</b> If graduated retention is enabled; this field is ignored.
Weekly	Sets a backup job to run once a month starting at 8:00pm on the last day of the month. Backup versions are retained for 12 months (one year).	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected in the <b>Day of Month</b> parameter.	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the day from the drop-down menu. The default day is Friday.	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 12 weeks (three months), and the maximum value allowed is 104 weeks (two years).  <b>Note:</b> If graduated retention is enabled; this field is ignored.
Monthly	Sets a backup job to run once a month starting at 8:00pm on the last day of the month. Backup versions are retained for 12 months (one year).	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected in the Day of Month parameter.	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the day (1-31) from the drop-down menu. The default day is "31", which resolves to the last day of the month for months with fewer than 31 days.	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 12 months (one year), and the maximum value allowed is 36 months

Backup Schedule Type	Default	Start Time	Start a Backup Every	Backup on Connect (Laptops Only)	Keep Starting Backups Until	On these Days	Keep Backup For
							(three years). <b>Note:</b> If graduated retention is enabled, this field is ignored.
Yearly	Sets a backup job to run once a year starting at 8:00pm on December 31st. Backup versions are retained for five years.	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected in the <b>Day of Year</b> parameter.	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the date from the interactive calendar or enter the value directly into the field in the form <i>mm/dd/yyyy</i> . The default day is <i>12/31/current_year</i> .	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 5 years, and the maximum value allowed is 10 years. <b>Note:</b> If graduated retention is enabled, this field is ignored.

## Set Local Graduated Retention

When creating an image or file backup job, you can optionally apply either global or local graduated retention rules to the job. Please note that the Graduated Retention settings configured here will only apply to the specific backup job.

If the local rules are not set, the global rules apply when Graduated Retention is enabled. See the [Configure Graduated Retention Defaults](#) section for more information.

To set local rules for a job:

1. When creating a job, click the **Enable Graduated Retention** checkbox and then click the **Save & Edit Graduated Retention Rules** button. See the [Backup Files](#) or [Backup System Images](#) sections for more information. The *Local Graduated Retention Rules* page displays.
2. In the *Local Graduated Retention Rules* page, the four schedule frequency fields (hourly, daily, weekly and monthly) display the global values by default. Enter new values for one or more of these fields. Only the relevant fields display. For example, on a weekly backup job, only the week and month fields display.
3. When all field values are correct, click the **Save** button to return to the *Job Schedule* page.

Please note that this procedure creates a persistent Graduated Retention record for the job. If graduated retention is subsequently unchecked for this job and then enabled again at a later date, the local values set in this page (not the global values) will still apply.

Figure 26 - Local Graduated Retention Rules page

**Backup Job: Doc and Web Backup**

Retain  most recent hourly restore points.

Then retain  daily restore points.

Then retain  weekly restore points.

Then retain  monthly restore points.

## Graduated Retention Requirements

In order for Graduation Retention to work properly, you will need to have consistent and regular backup jobs running. Additionally, you will need to give the appliance time to build enough recovery points for Graduation Retention to function.

If you miss a recovery point due to a backup job failing for any reason, the appliance will correct itself by applying the next successful backup job to the graduated retention order.

For example, if there are 48 hourly backup jobs scheduled and the 48th backup job fails, the 49th backup job will be used to complete the set of 48 backup jobs, or to complete a daily backup job, as per the configured Graduated Retention Default settings. The same methodology applies for all daily, weekly, and monthly backup jobs.

## Graduated Retention Limits

Graduated Retention does not apply retroactively. This means that Graduated Retention configuration changes will not apply to any previously created backups. This applies to when you initially enable Graduated Retention, and if you update configuration settings.

When reconfiguring the existing Graduated Retention settings, all configuration changes applied to the Graduated Retention policy will only apply to backup data created after the changes were committed. All backup data existing before changes to the Graduated Retention were made will be preserved using the Graduated Retention settings in place at the time.

## Excluded Files (Windows Devices Only)

Some files are always excluded in backup jobs for devices running the Windows operating system. The table below lists the files that are *never included* as part of a backup job. This list of exclusions is applied to all volumes (disks) included in a backup job.

Windows Device Excluded Files

Description	File/Folder Name
Axcient-specific files	<code> axcient</code> <code> Axcient</code>
Pagefile and Hybernate files	<code> hiberfil.sys</code> <code> pagefile.sys</code>
System volume information files	<code> System Volume Information</code> <code> SYSTEM VOLUME INFORMATION</code>
Recycle Bin files	<code> recycled</code> <code> RECYCLED</code> <code> RECYCLER</code> <code> Recycle.Bin</code> <code> RECYCLE.BIN</code> <code> \$RECYCLE.BIN</code> <code> \$Recycle.Bin</code> <code> recycler</code>
Client-side caching files	<code> Windows csc</code> <code> Windows CSC</code> <code> WINDOWS csc</code> <code> WINDOWS CSC</code>
Virtualization caching files	<code> .vdiskcache</code>

### Caution!

You can exclude the `|Windows|temp` folder, which can reduce permission denied problem when trying to back up temporary files. However, some applications store needed files in this folder. If this folder is excluded on a device with such applications, the application might not function properly after a restore operation (VM, BMR, or file restore).

## Backup System Images

You can back up a device as a complete system image. Unlike a file backup that simply backs up selected files or folders, an image backup job copies everything on the device (selected disks) and treats that backup as a single image.

Image backup jobs can be created for any device that runs a supported version of the Windows operating system. See the Axcient Release Notes for a list of the supported versions and the [Appliance Specifications](#) appendix for appliance model limits. Image backup jobs use the **Microsoft Volume Shadow Service (VSS)**. To configure VSS, please reference the [VSS Configuration](#) appendix for more information.

### Caution!

The first time running an image backup job can be processor intensive. Therefore, schedule the initial image job to run when no other backup jobs are running. Additionally, setting the local network connection below the default 1GB/sec is not recommended. The image job will still run, but performance might be unacceptably slow. Please reference the [Set Bandwidth Usage \(Quality of Service\)](#) section for more information.

To create an image backup job for a device:

1. Select the target device using one of the following methods:
  - On the *Devices* pane on the *UMC*, click the **target device**.
  - Alternatively, click the **devices** tab on the UMC. On the *Devices* page, click the **icon** of the target device.
2. On the *Backup Jobs* page for the device, click the **image backup** option on the left navigation bar. The *Image Backup* page displays.
3. On the *Image Backup* page, update the required fields. Please refer to the table below for descriptions of each parameter.
4. By default, all files on a drive are included in the system image with a few exceptions (please reference the [Excluded Files \(Windows Devices\)](#) section for more information). Optionally, to exclude files, click the **Manually Edit Files** link, expand the tree-view, and deselect folders as needed.

Do not exclude any files needed by the operating system or applications. Excluding required files could result in unusable VM or BMR images.

When the file and folder settings are correct, click the **save** button.

5. Click the **save** button when you are finished. The backup request is recorded and saved. If you selected the **Run Initial Backup Now** checkbox, the backup begins immediately. Otherwise backups start as scheduled. The first time an image backup job runs might take a significant amount of time. Subsequent runs are faster because only differences from the previous job are backed up.



If you are using more than one Axcient appliance at a site, do not use multiple appliances to protect a single system. Creating an image backup for the same device on multiple appliances can cause the failover VM and BMR features to fail. This restriction only applies to image backup jobs.

Figure 27 - Image Backup Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system docs

**devices**

- file restore
- failover VM
- test VM
- bare metal restore
- edit
- manage VSS writers
- prune
- data integrity checks
- remove backup job

### image backup

Schedule name: 2012

Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Relative Offsite Priority: (Enter any integer to raise this schedule's offsite priority relative to others. Larger value means higher priority.)

Disk drives: C:

Backup schedule type: Daily

Backup Offsite: ☒

Refresh interval: No Refresh

Start time: 19:00 (7:00 PM)

On these days: ☒ Monday, ☒ Tuesday, ☒ Wednesday, ☒ Thursday, ☒ Friday, ☐ Saturday, ☐ Sunday

Keep backups for: 30 days (about 4.3 weeks)

Enable Graduated Retention: ☐ (Restore points become less granular over time.)

Turn on Log Flushing (Pre Backup): ☒ (e.g., MS Exchange Server, MS SQLServer)

Allow Axcient to override VSS storage size limit for the duration of backup: ☒

Backup scan mode: Block level scan (fast delta)

Reminder\* If Quality of Service (bandwidth throttling) is on, make sure the internal service download and upload rate limits are set to 1 Gbit/sec (default value). A lower setting will cause unacceptable performance degradation for an image backup job.

**Summary**  
Your backup will run on Monday, Tuesday, Wednesday, Thursday, Friday, starting at 7:00 PM.  
Backups will be retained for 30 days (about 4.3 weeks)

**Return To Device**  
The following directories/files will be saved on the Axcient appliance:  
The following directories/files will be saved on the Axcient appliance and Offsite Storage:  
C:  
The following directories/files will be explicitly excluded:  
[Manually Edit File Selections](#)

**search for files inside this backup set**  
Search Term: From: 9/24/2019 To: 10/24/2019 submit

Figure 28 - Image backup Advanced Page

The screenshot displays the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar is titled 'devices' and contains icons for file backup, mailbox backup, image backup, edit device, and remove device. The main content area is titled '192.168.99.201 - create image backup'. It features a 'select files to backup' section with three checkboxes: '- File or Folder excluded from backup', '- File or Folder included in backup (offsite and onsite | onsite-only)', and '- Inclusion or exclusion mandated (excluded | offsite and onsite | onsite-only)'. Below these is a file selection area showing 'C:' and 'E:' drives. At the bottom of the main area are 'cancel' and 'save' buttons.

## Common Settings Terms and Definitions

Parameter	Definition
Schedule Name	Sets the backup job name.
Enabled	<p>Enables the backup job. When <i>enabled</i>, the backup job will run according to the specified schedule. When <i>disabled</i>, the job will not run, but all history is preserved and can be restored from.</p> <p>In most instances, a backup job should be enabled at all times. There are two reasons to disable a job:</p> <ol style="list-style-type: none"> <li>1. The device is no longer used, but the backup history needs to be preserved.</li> <li>2. There is a need to suspend running of a job for a period of time for things such as maintenance windows.</li> </ol>
Relative Offsite Priority	<p>Specifies a run priority relative to other Cloud backup jobs. All Cloud backup jobs are put in a queue and run serially starting at a specified time each day (see the <a href="#">Schedule Cloud Backup Job</a> section for more information). Job priority is not considered by default when setting a queue order, so all Cloud jobs start with a blank (zero) value in this field.</p> <ul style="list-style-type: none"> <li>• To set a job to run before the other, enter a positive integer value in this field.</li> <li>• To set a job to run after the others, enter a negative integer value in this field.</li> </ul> <p>The Cloud job with the highest value will run first, the next highest second, and so forth. The actual number does not matter, only the ordinal position (magnitude relative to other Cloud jobs) in the queue.</p>
Disk drives	<p>Lists the disk drives included in the image backup. The system drive (typically C:) is always included, but other drives can be included (checked) or removed (unchecked) as needed. Do not remove a disk drive unless you are certain it is not needed for the system to function properly. Additionally, the system volume (typically C: drive) <i>cannot exceed 2TB</i>. We recommend that you reassign any drive letters X and Z if present. The BMR recovery tool reserves these drive letters.</p>

Parameter	Definition
	If an image contains these two drive letters, the BMR cannot be performed.
Backup Schedule Type	Sets the backup interval schedule from a drop-down list. Each schedule type has default settings that can be modified. See the following table for each default and optional settings for each type.
Use Open File Manager	<p>Sets whether to back up open files. By default, this parameter is enabled (box checked), which causes the appliance to back up open files. Such files typically are database or similar application files such as MS Exchange Server or MS SQL Server. To disable this feature and bypass (not back up) open files, uncheck the box. Note the following:</p> <ul style="list-style-type: none"> <li>Open File Manager uses Microsoft Volume Shadow Service (VSS). To configure VSS, see the <a href="#">VSS Configuration</a> section.</li> <li>Open File Manager is supported for any Windows device except for VP. It is not supported for Mac OS, Linux, or other operating system devices.</li> <li>The backed up version is a snapshot of the last committed version of the open files. Restoring the open files could result in some inconsistency within the application. After a restore, use the application tools to make sure the application files are in a consistent state.</li> </ul>
Enable Graduated Retention	<p>Sets whether to enable graduated retention for this backup job. Check the box to enable (disabled by default). You can select either global or local rules:</p> <ul style="list-style-type: none"> <li>To select the global rules, check the box. See the <a href="#">Configure Graduated Retention Defaults</a> section for more information.</li> <li>To specify local rules, check the box and then click the <b>Save &amp; Edit Graduated Retention Rules</b> button. See the <a href="#">Local Graduated Retention Rules</a> section for more information.</li> </ul>
Save System State	<p>Sets whether to save all system state information. Checking this box allows you to restore a device back to a known system state in the event the device crashes or becomes unstable. Note the following:</p> <ul style="list-style-type: none"> <li>This is an option for devices running Windows Server or SBS 2012, 2008 or 2003 only.</li> <li>Backing up system state requires substantial storage space. Actual size varies but testing suggests the initial SBS/Windows Server 2008 backup is about 6GB with each incremental backup adding about 600MB. When storage space is an issue, frequent schedule (hourly or daily) is not recommend for a system backup job.</li> </ul>
Turn on Log Flushing (Pre-Backup)	Enables pre-backup log flushing (on by default). When Open File Manager is enabled, this causes the VSS writers to do a log flush prior to creating the backup, which usually reduces the amount of Exchange data to back up (and might reduce the data to back up for other VSS-associated applications).
Allow Axcient to override VSS storage size limit for the duration of the backup	Allows the backup process to temporarily override the VSS storage size limit set on the protected device. If this option is selected, the VSS storage size limit will return to its original value when the backup completes.
Backup scan mode	<p>Allows you to select your preferred backup scan mode, including:</p> <ul style="list-style-type: none"> <li>Full scan (legacy)</li> <li>Optimized scan (IR) - provides a faster backup scan by scanning only changes.</li> <li>Block level scan (fast delta) - an enhanced backup scanner that allows you to achieve faster backups when protecting Exchange and SQL servers.</li> </ul>

## Backup Schedule Types Terms and Definitions

Schedule Type	Default	Start Time	Start Date	Start Every	Backup on Connect (Laptops Only)	Keep Starting Until	On these Days	Keep Backup For
On Demand	Sets a backup job to start immediately. An <i>on demand</i> backup runs just once. You can start it again manually at any time by selecting the <b>Start</b> link or button. There is only one on-demand version, so subsequent requests write over the existing version. An on-demand backup is retained indefinitely. It is deleted only by removing that backup job.	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Hourly	Sets a backup job to run on an hourly basis starting at 9:00am and continuing through 7:00pm on Monday through Friday (five days). Backup	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. Each backup is run every interval (see the <b>Start a backup every</b> description) after the start time. For example, if the start time is 7:18am and the interval is set to one hour, the first backup starts at 7:18am, the next backup starts at 8:18am, and so on.	N/A	Sets the interval duration. By default, the interval is one hour, but you can specify a longer duration	Sets automatic (immediate) back up for laptops when they connect if they missed the most recently scheduled	Sets the backup run stop time. The specified time is the last hour that a backup is started. By default, the stop time is 7:00pm, but you can	Sets which days the job runs. Check (click) the boxes next to the desired days. By default, Monday through Friday are checked.	Sets the retention period (amount of time a backup version is saved). After the specified interval, a version is deleted

Schedule Type	Default	Start Time	Start Date	Start Every	Backup on Connect (Laptops Only)	Keep Starting Until	On these Days	Keep Backup For
	versions are retained for 168 hours (one week).			from the drop-down menu. For example, if this is set to <b>2</b> and the start time is <b>7:00am</b> , the first backup starts at 7:00am, the second starts at 9:00am, and so on.	backup. By default, offline devices are ignored during a backup run and simply miss being backed up. Setting this parameter causes the Axcient appliance to monitor an offline laptop and begin a backup as soon as the laptop connects. On a Windows laptop, a pop-up window displays when the backup begins, notifying the user that a backup is in progress and cautioning the user not to disconnect until the backup is complete. (To implement the pop-up	change this to any hour from the drop-down menu. The minutes value is determined by the minutes setting in the Start Time parameter.		and cannot be restored. The default is 168 hours (7 days), and the maximum value allowed is 744 hours (31 days). <b>Note:</b> If graduated retention is enabled, this field is ignored.

Schedule Type	Default	Start Time	Start Date	Start Every	Backup on Connect (Laptops Only)	Keep Starting Until	On these Days	Keep Backup For
					<p>window on Linux or Mac laptops, see the “Laptop Backup Strategy” section.)</p> <p><b>Note:</b> This field appears only if the Device Type for the device is set to LAPTOP.</p>			
Daily	Sets backup jobs to run once a day Monday through Friday (five days) starting at 7:00pm. Backup versions are retained for 30 days (one month).	Sets the start time for daily backups. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time each day selected in the <b>On These Days</b> parameter.	N/A	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which days to run a daily backup. Check (click) the boxes next to the desired days. By default, Monday through Friday are checked.	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 30 days (one month), and the maximum value allowed is 1827 days (five years). <b>Note:</b> If graduated retention is enabled; this field is ignored.

Schedule Type	Default	Start Time	Start Date	Start Every	Backup on Connect (Laptops Only)	Keep Starting Until	On these Days	Keep Backup For
Weekly	Sets a backup job to run once a week. Backup versions are retained for 12 months (one year).	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected.	N/A	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the day from the drop-down menu. The default day is Friday.	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 12 weeks (three months), and the maximum value allowed is 104 weeks (two years). <b>Note:</b> If graduated retention is enabled; this field is ignored.
Monthly	Sets a backup job to run once a month.	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected in the <b>Day of Month</b> parameter.	Using the <b>Day of Month</b> field, sets the day of the month the backup will start.	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the day (1-31) from the drop-down menu. The default day is "31", which resolves to the last day of the month for months with fewer	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 12 months (one year), and the maximum

Schedule Type	Default	Start Time	Start Date	Start Every	Backup on Connect (Laptops Only)	Keep Starting Until	On these Days	Keep Backup For
							than 31 days.	value allowed is 36 months (three years). <b>Note:</b> If graduated retention is enabled, this field is ignored.
Yearly	Sets a backup job to run once a year. Backup versions are retained for five years.	Sets the backup start time. You can specify both the hour and minute from the drop-down menus. For example, if the start time is 9:15pm, a backup begins at that time on the day selected in the <b>Day of Year</b> parameter.	Using the <b>Day of Year</b> field, sets the day of the year the backup will start.	N/A	See the <b>Hourly</b> explanation.	N/A	Sets which day to run. Select the date from the interactive calendar.	Sets the retention period. After the specified interval, a version is deleted and cannot be restored. The default is 5 years, and the maximum value allowed is 10 years. <b>Note:</b> If graduated retention is enabled, this field is ignored.



## Modify Backup Job

To modify a backup job for a device:

1. Select the target device using one of the following methods:
  - On the *Devices* pane on the *UMC*, click the **target device**.
  - Alternatively, click the **devices** tab at the top of the *UMC*. On the *Devices* page, click the **icon** of the target device.
2. In the *Backup Job* page, click the backup job name to be modified.

Figure 29 - Backup Jobs Page

The screenshot shows the Axcient Unified Management Console (UMC) interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'devices' section with various backup and management options. The main content area is titled '192.168.77.222 - backup jobs' and contains a table of backup jobs.

**image jobs**

Job Name	Backup Type	Refresh Interval	Job Status	Date of Last Backup	Next Backup	Backup Size
<a href="#">Image Backup</a>	Image	0 Minutes			Fri, Mar 11, 8:00 PM	
	<b>Image Status</b>	<b>Failover VM Status</b>				
	Online	Idle				

**file and mailbox jobs**


Job Name	Backup Type	Schedule Frequency	Job Status	Date of Last Backup	Next Backup	Backup Size
<a href="#">FFderServ222Ver001</a>	File	Daily		03/04/2011 - 7:04:59 PM	Mon, Mar 7, 7:00 PM	0.0 bytes

**backup information**  
Current Device Data: 0.0 GB

3. If this is an image job, click the **edit** button on the left navigation menu. The *Edit Image Backup* page displays. Use this page to update fields as needed, and click the **Save** button when you are finished.

Figure 30 - Edit Image Backup Page

**172.18.8.45 - edit image backup**





Schedule name:


Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Relative Offsite Priority:  (Enter any integer to raise this schedule's offsite priority relative to others. Larger value means higher priority.)

Disk drives:

 C: [refresh drive list](#)

☒  E:

☒  F:

Backup schedule type:

Backup Offsite: ☒

Refresh interval:

Start time:  :  (8:00 PM)

On:

Keep backups for:  weeks

Enable Graduated Retention ☐ (Restore points become less granular over time.)

Turn on Log Flushing (Pre Backup): ☒ (e.g., MS Exchange Server, MS SQLServer)

MSSQL DB Password:

Allow Axcient to override VSS storage size limit for the duration of backup: ☒

Backup scan mode:

Reminder\* If Quality of Service (bandwidth throughput) is set to a value other than "Unlimited", service download and upload rate limits are set to 1 Gbit/sec (default value). A lower setting will cause unacceptable performance degradation for an image backup job.

[Advanced Options](#)

Automatic Validation: ☐

**Summary**

Your backup will run weekly, on Friday, starting at 8:00 PM.  
Backups will be retained for 12 weeks

[cancel](#) [save](#)

The following directories/files will be saved on the Axcient appliance:

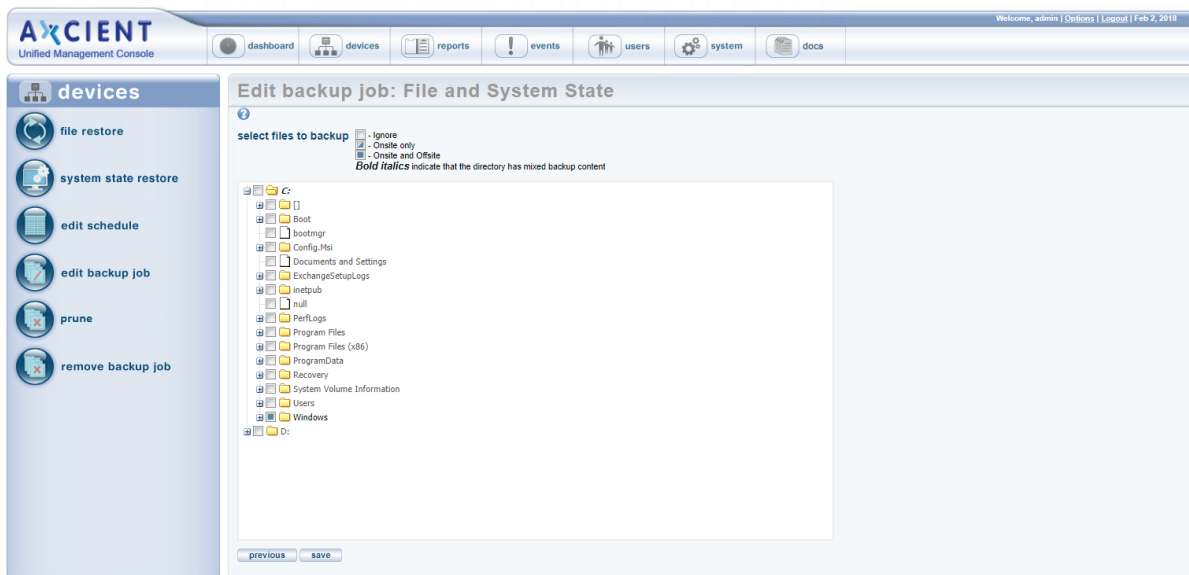
The following directories/files will be saved on the Axcient appliance and Offsite Storage:

F:  
E:  
C:

The following directories/files will be explicitly excluded:

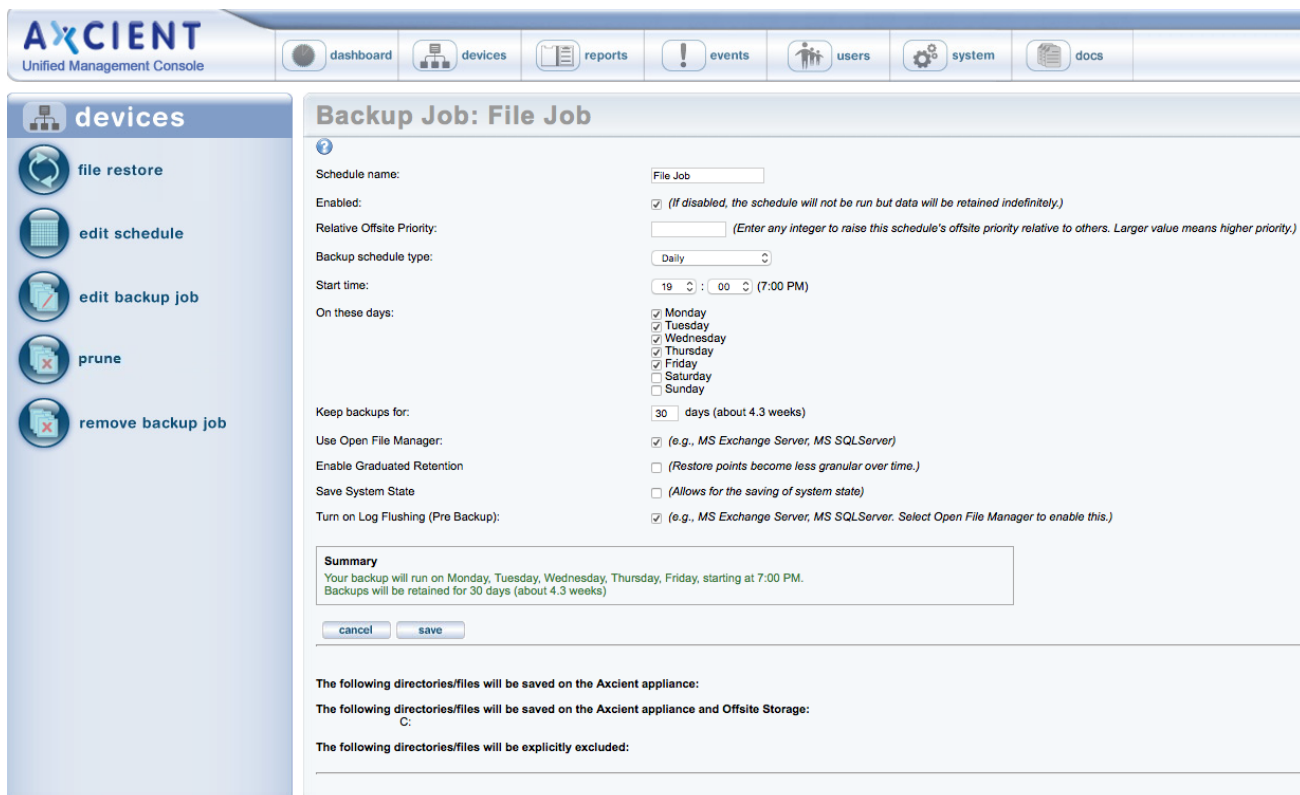
- To modify the name or schedule of the image backup job, click the **edit schedule** button on the left navigation menu and update the fields as needed. Click the **save** button when you are finished.
- Alternatively, if this is a file backup job, click the **edit backup job** option located on the left navigation menu, and use the tree-view to select and deselect files and folders as needed. Click the **save** button when you are finished.

Figure 31 - Edit Backup Job Contents



- To edit the schedule and other settings of a file job, click the **edit schedule** button option on the left navigation menu and update the schedule and other settings as needed. Click the **save** button when you are finished.

Figure 32 - Edit File Job Schedule





## Reduce Backup Job Size

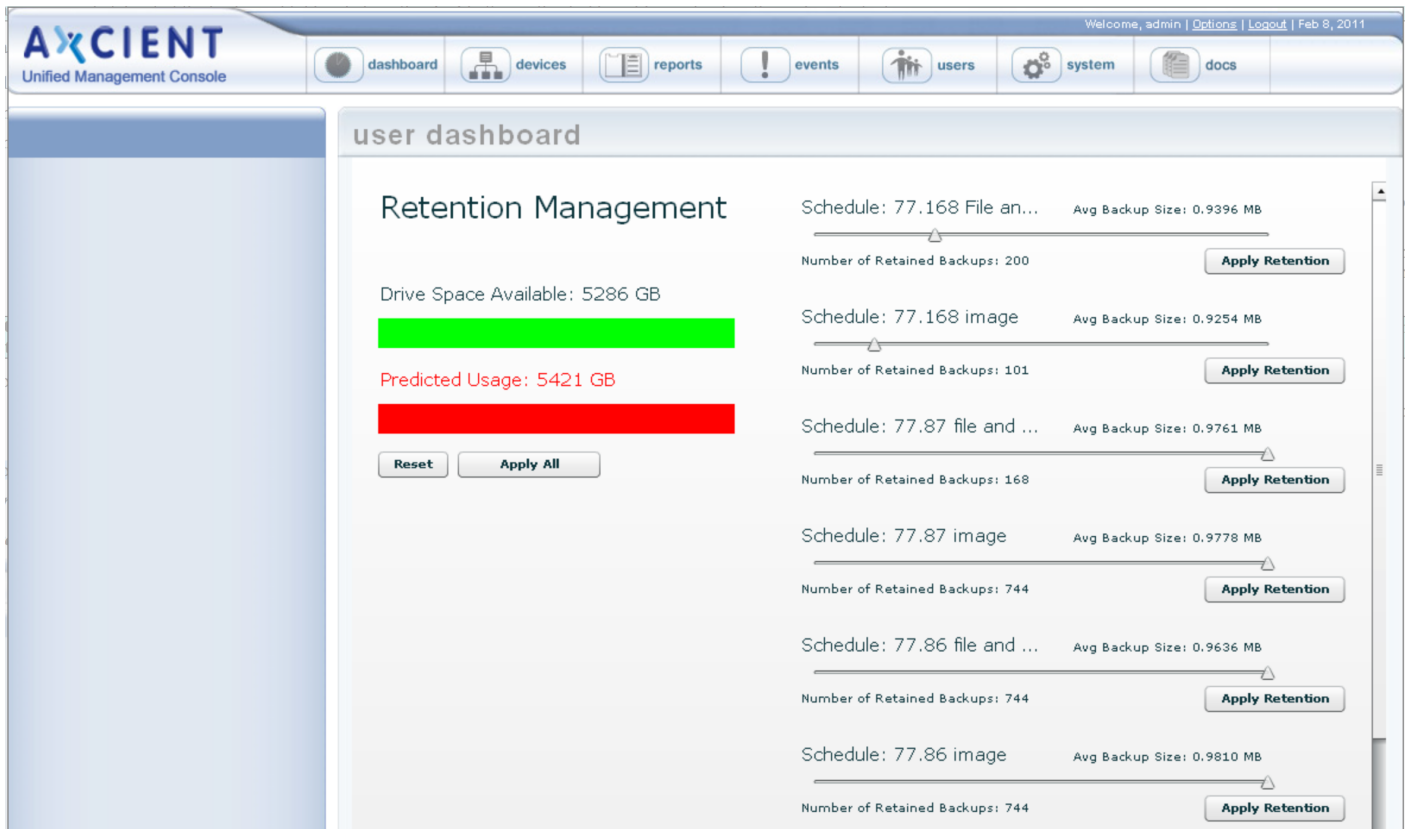
If storage space becomes an issue, you can modify a backup job to reduce its size by removing unneeded data or reducing the retention period. Please note that there is no way to remove unwanted data from a previous version, or to remove a previous version on demand. Instead, you can modify the backup configuration in the following ways:

- **Exclude data from backup job specification** - Modify the backup job and deselect unneeded data. This ensures that data is not backed up in subsequent job runs. For example, you might initially include a */tmp* folder (in a file job) or a disk dedicated to temporary data (in an image job) and then realize the Axcient appliance is filling up to capacity because each backup version includes this unnecessary data. To remove the unneeded data, modify the job as follows (see [Modify Backup Job](#) section for more information):
  - **File job** - Set the unwanted folders to **Ignore**.
  - **Image job** - Deselect the unwanted disk(s).
- **Reduce the retention period** - Reducing the retention period results in fewer saved incremental backup runs, and therefore saves disk space. Please note, however, that reducing the interval also reduces the saved history, which means you can no longer recover certain time periods. You can reduce the retention period in three ways:
  - Reduce the *Keep backups for* value for one or more backup jobs. For example, a daily file backup job is retained for a month (30 days) by default. Reducing this interval to a week (7 days) reduces the number of versions that are stored from 30 to 7. To change the *Keep backups for* value, see the appropriate section for the backup type ([Back Up Files](#) section or [Back Up System Images](#) section).
  - Turn on the *Activate the Auto Prune Detection* feature (off by default), which causes the Axcient appliance to automatically (1) check whether there is enough free disk space before starting a backup job run, (2) delete the oldest backups if space is inadequate (just enough to store the new run), and (3) reset the *keep backups for value* to the new value. For example if this is a daily job with a 30 day retention and the 5 oldest backups were deleted, the *keep backups for* value is reset to **25 days**. Please reference the [Use Configuration Tools](#) section to activate this feature.
  - Profile usage and reduce retention for a set of backup jobs. The UMC provides a quick way to manage retention for up to 10 backup jobs. For more information, please reference the section below.

To manage job retention for up to 10 backup jobs:

1. On the UMC, click the **dashboard** tab. The *Dashboard* page displays.
2. In the Disk Utilization panel (bottom left of the page), click the **Retention Management** link. The *Retention Management* page displays.
3. In the *Retention Management* page, review the following fields:
  - The *Drive Space Available* field displays the amount of free space on the disk. This is a fixed value that does not change until retention changes are applied.
  - The *Predicted Usage* field displays the amount of space needed to store the jobs listed on the right. This is a dynamic value that changes as you try different retention values for the individual jobs (before applying the changes).
  - The *Schedule: job\_name* field displays the average size of a backup for the job (the average size of each incremental backup) and the number of retained backups. It also includes a sliding bar that allows you to preview how the size of the job would change if you reduced the number of retained backups. The sliding bar is dynamic and can be moved at any time. Moving the sliding bar changes the number of retained backups and the corresponding effect on the total value in the *Predicted Usage* field.
4. Optionally, to adjust a single backup job, move the sliding bar for that job to the desired number of retained backups, and then click the **Apply Retention** button. Repeat this step for any job you want to change.
5. Optionally, adjust the group of jobs as a whole, move the sliding bar for each job you want to change to the desired number of retained backups, and then click the **Apply All** button.
6. To reset the page without applying any changes, click the **Reset** button.

Figure 33 - The Retention Management Page



## Edit File Include or Exclude List Manually

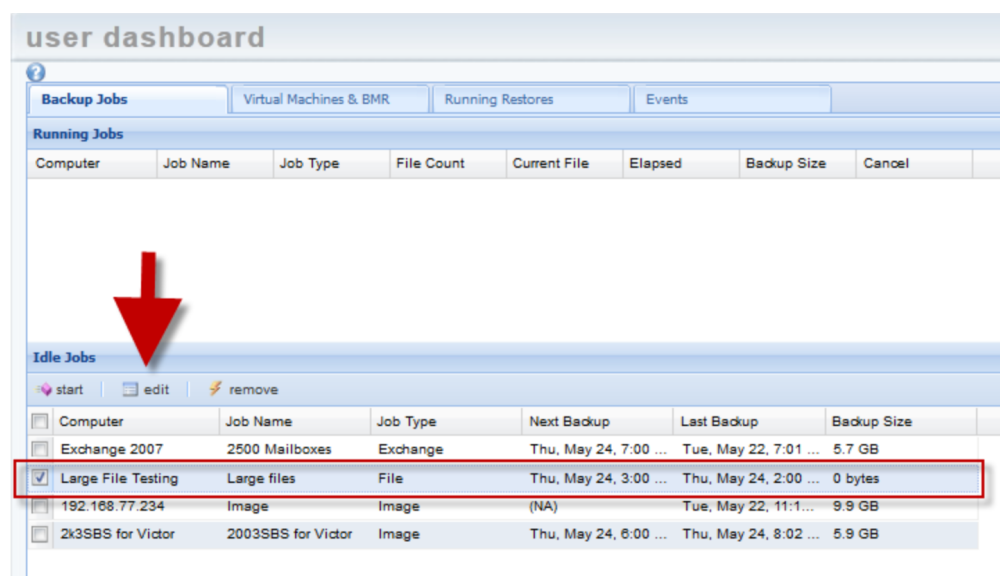
Typically, when you configure a file or image backup job, you select files to include or exclude from a directory tree. However, when you *edit* a file or image backup job, you can manually specify files to include or exclude. This method can be useful in the following situations:

- The folder or file in question does not appear in the tree-view.
- The long path is difficult to traverse in the tree-view.
- You are unable to exclude the file within the tree-view, but would like to proceed regardless of this restriction (not recommended).

To manually edit the file list for an image or file job:

1. On the UMC, click the **dashboard** tab. The *Dashboard* page displays.
2. On the *Dashboard* page, select the target job and click the **edit** button.

**Figure 34** - Dashboard Job Edit Page



3. On the *Backup Job* page, click the **Manually Edit File Selections** button found below the listing of directories and files to be saved and excluded.



Figure 35 - Backup Job Edit Page

**Backup Job: Large files**

Schedule name:

Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Backup schedule type:

Start time:  :  (12:00 AM)

Start a backup every:  hours

Keep starting backups until:  :  (11:00 PM)

On these days:

- ☒ Monday
- ☒ Tuesday
- ☒ Wednesday
- ☒ Thursday
- ☒ Friday
- ☒ Saturday
- ☒ Sunday

Keep backups for:  hours

**Summary**  
Your backup will run every day, on an hourly basis, between the hours of 12:00 AM and 11:00 PM.  
Backups will be retained for 3 hours


[Return To Device](#)

---

The following directories/files will be saved on the Axcient appliance:

The following directories/files will be saved on the Axcient appliance and Offsite Storage:  
E:\2TB\_FOLDER\1TB\_FILE\_DIR  
E:\2TB\_FOLDER\1GB\_FILES\_DIR

The following directories/files will be explicitly excluded:  
E:  
C:

[Manually Edit File Selections](#) 

4. In the *Edit File Set* page, a line displays for each unique path defined in the backup job. You can add, delete, or modify entries as needed. Each entry identifies a set of files (whatever the path specifies) and whether the files should be backed up locally only, both locally and in the Cloud, or excluded from being backed up. The path for each line begins with the volume designation (for example, c\$ or e\$).
  - To add a new entry, click the **add new path** link. Enter the full path of the target folder or file and then use the Inclusion column to determine how this path should be handled during the backup. You can select from **Exclude** (exclude from backup), **Onsite** (save onsite only), or **On/Offsite** (save both onsite and offsite).
  - To modify an existing entry, use the *Inclusion* column to edit the path and/or select a different setting.
  - To delete an existing entry, click the **Remove** link.
5. When all the entries are correct, click the **save** button.

### Caution!

Saving the changes does not mean the changes are valid. Changes are saved without a validation check. If a path is not valid, the files in that path will not be backed up. Please reference the event log after the backup runs for possible error messages related to an invalid path.

Figure 36 - Edit File Set Page

## Large files - edit file set

### add or remove file paths from the file set

This page enables the manual editing of files selected for backup and is appropriate for unusual situations, such as when you might want to select for backup a single file that resides in a folder containing thousands of other files. Most of the time, using the "tree" view to select files is faster and better. You can access the normal, tree view by clicking on "edit backup job" icon.

Path	Inclusion	
<a href="#">Add new path</a>		
c\$	Exclude	<a href="#">Remove</a>
e\$	Exclude	<a href="#">Remove</a>
e\$/2TB_FOLDER/1GB_FILES_DIR	On/Offsite	<a href="#">Remove</a>
e\$/2TB_FOLDER/1TB_FILE_DIR	On/Offsite	<a href="#">Remove</a>

cancel
save

## Manage VSS Writers

In some instances, one or more Microsoft Volume Shadow Service (VSS) writers on a device might cause a backup to fail. In other instances, backup jobs might interfere with other VSS-aware software running on the protected device. When these events happen, you can exclude specific VSS writers from a backup job to enable the job to complete successfully.

### Caution!

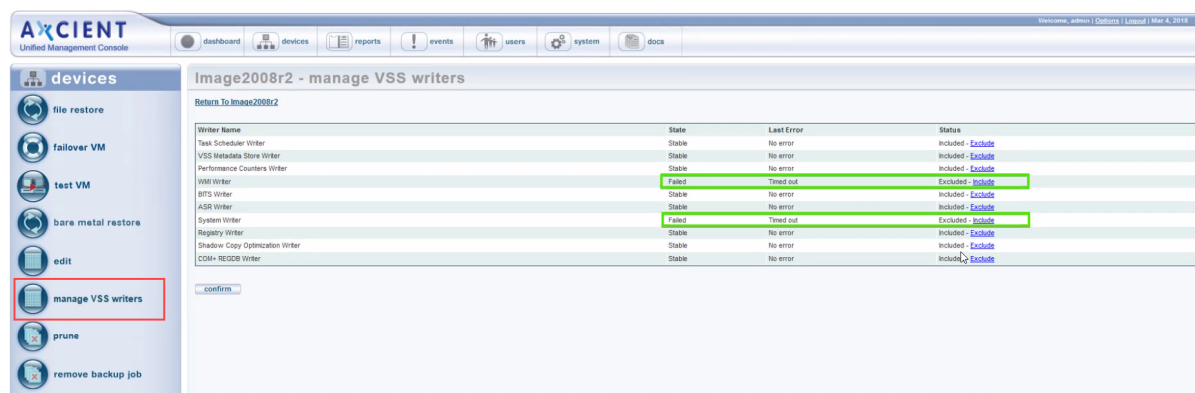
Excluding a VSS writer might result in inconsistent backups. This feature must be utilized with extreme caution.

For more information on troubleshooting VSS writers, please reference the [Backup Fails Because of Windows VSS Problems](#) section of this guide.

To exclude a VSS writer from a backup:

1. Navigate to the device backup job.
2. On the *Image Backup* page, click the **manage VSS writers** option on the left navigation menu. The *Manage VSS Writers* page displays.
3. On the *Manage VSS Writers* page, review the *State* column to find which VSS writers are in a failed state.
4. In the *Status* column, click the **Exclude** link to exclude the VSS writer from the backup job.
5. Click the **confirm** button to save your changes.

Figure 37 - Manage VSS Writers



## Prune Backup Job

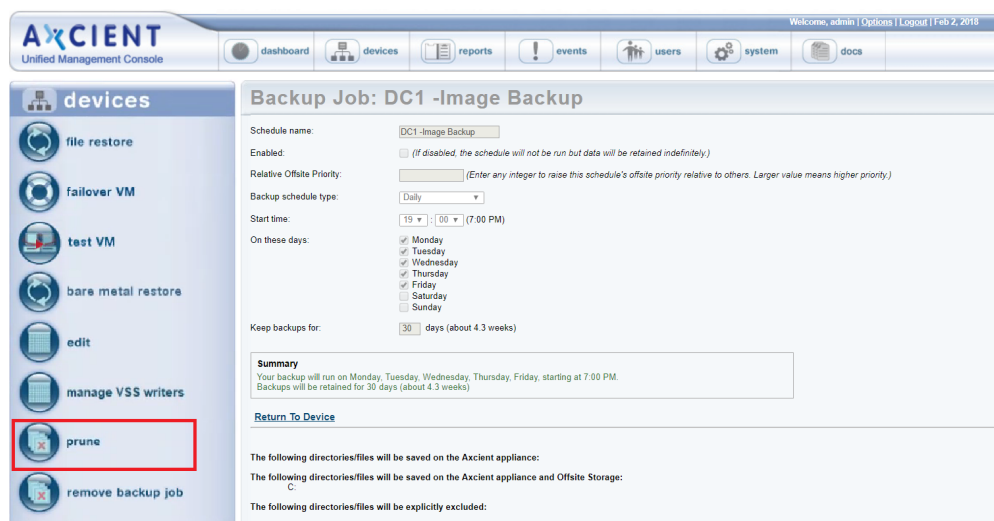
You are able to prune backup data on an appliance to create additional free space.

Please note that this action is *final*. All data that is pruned will be permanently deleted and will not be recoverable.

To prune any backup data:

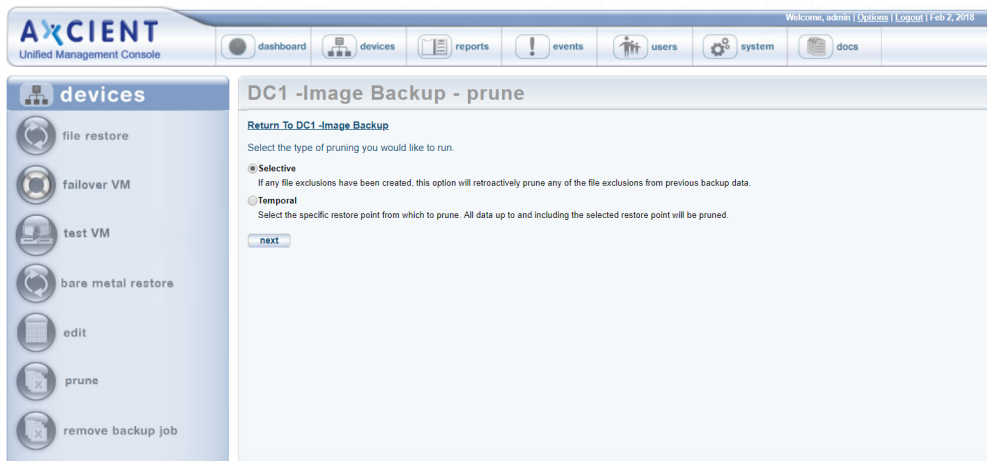
1. On the UMC, navigate to the appropriate device backup job.
2. On the *Image Backup* page, click the **prune** option in the left navigation menu.

Figure 38 - Prune Button



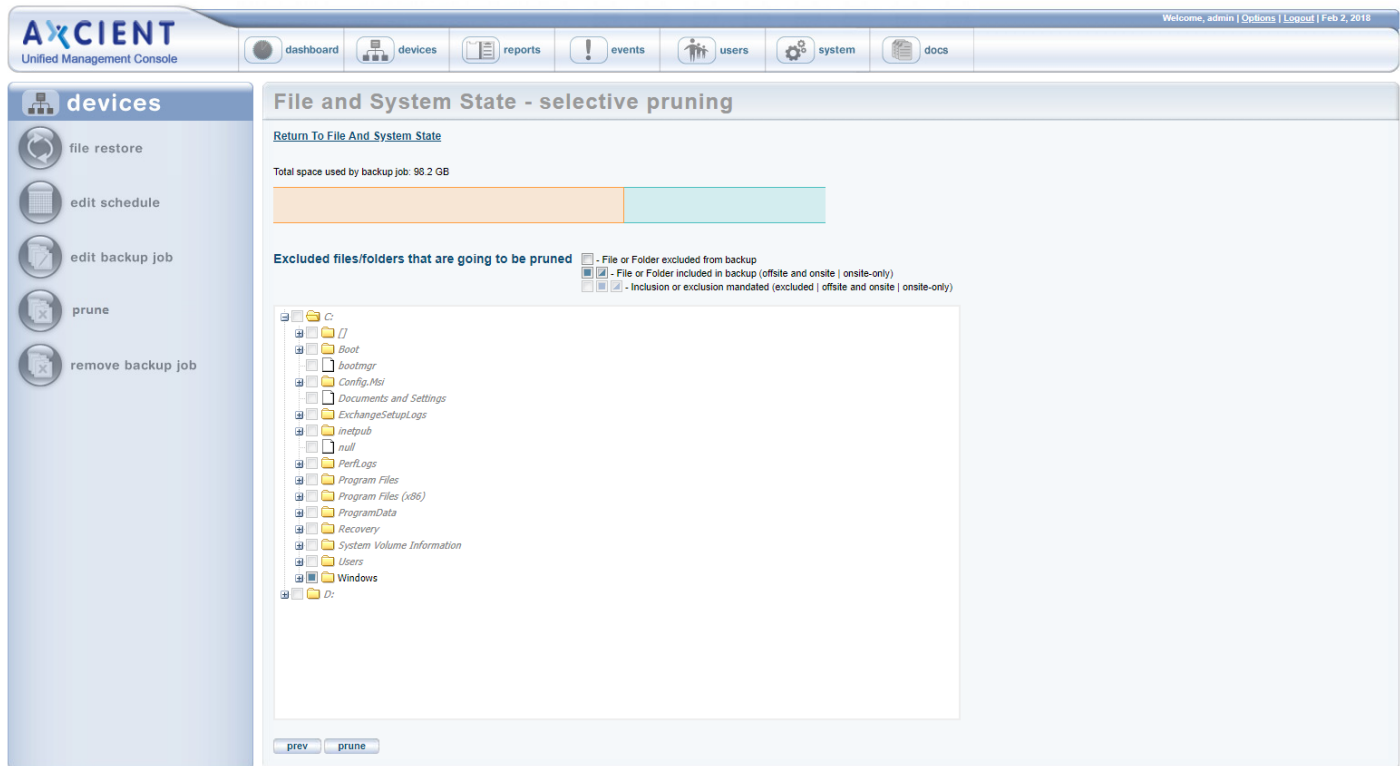
3. Select the pruning type, and then click the **next** button to continue. You can select from the following pruning types:
  - **Selective** - This option will prune selected files and folders from previous backup data.
  - **Temporal** - This option will prune all data from the selected restore point.

Figure 39 - Prune Page



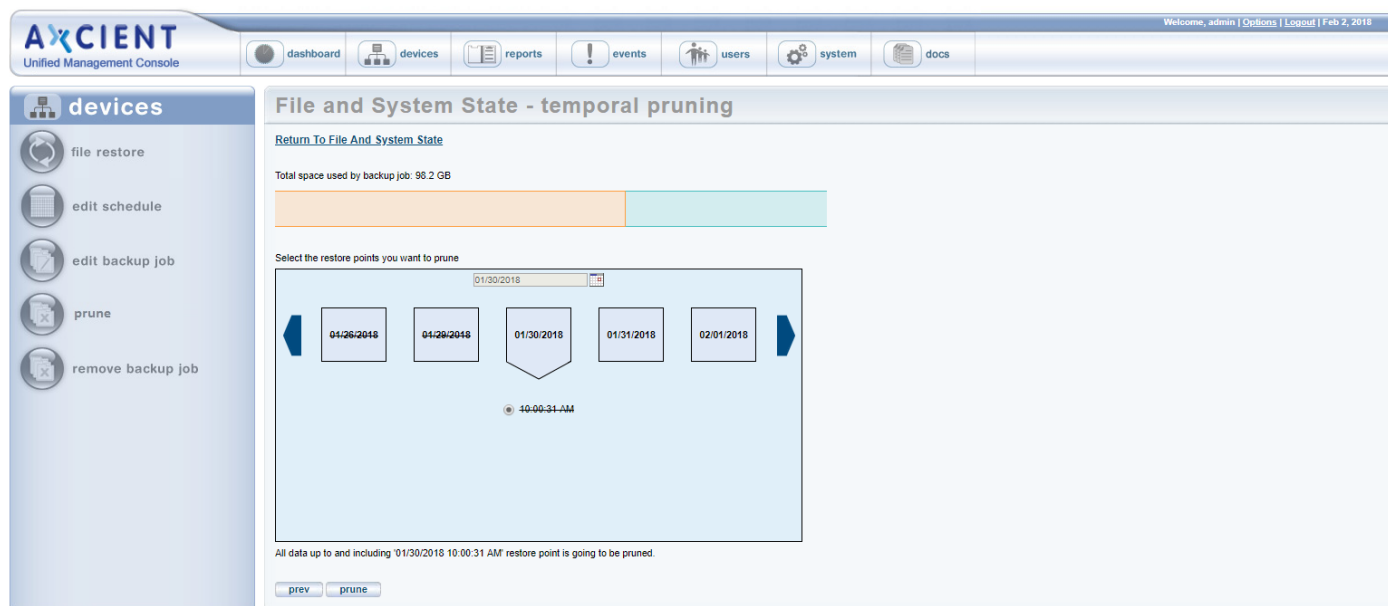
4. If **Selective** was selected, use the *Selective Pruning* page to view the total data on the appliance. Select the appropriate files and folders, and click the **prune** button.

Figure 40 - Selective Pruning Page



5. If **Temporal** was selected, use the *Temporal Pruning* page to view the total data on the appliance. Use the calendar to select the restore points to be pruned, and click the **prune** button.

Figure 41 - Temporal Pruning Page



## Configure the AutoVerify Feature (Data Integrity Check)

You can optionally configure the AutoVerify feature to validate and test the integrity and recoverability of your protected services. This feature performs a series of deep system integrity checks within the running virtual machine to ensure that the protected device backup is both healthy and ready to recover in the event of a disaster.

You can select from one or more of the following types of integrity checks, depending on your business needs:

- **Windows System Files Integrity Checks**

These checks use System File Checker tool (SFC) to detect windows system files corruption.

- **SQL Integrity Checks**

These checks verify the consistency of SQL Databases. If enabled, AutoVerify performs page-level checksum validation to detect the database corruption. These checks are expensive; they might potentially run for days. Axcient does not recommend running these checks more frequently than once per month.

**Note:** Please note that SQL Integrity Checks require database administrator credentials.

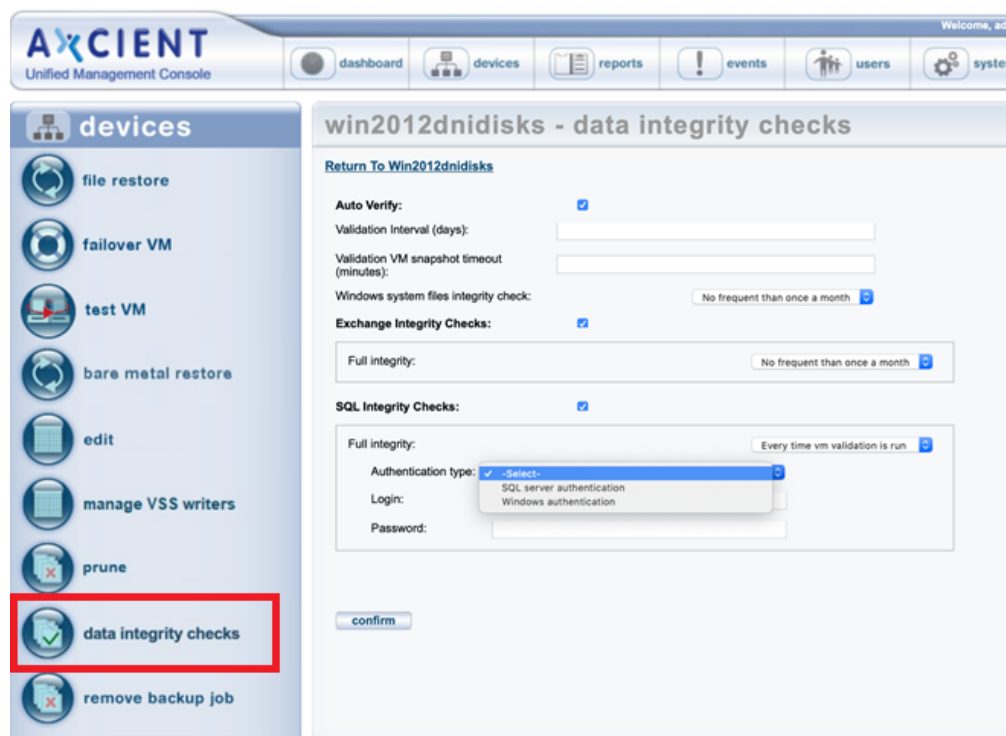
- **Exchange Database Integrity Checks**

These checks verify the consistency of Exchange Databases. If enabled, AutoVerify performs page-level checksum validation to detect the Exchange database corruption. These checks are expensive; they might potentially run for days. Axcient does not recommend running these checks more frequently than once per month.

To configure the AutoVerify feature:

1. Within the UMC, click the **devices** tab.
2. In the *Devices* page, click the **icon** of the target device.
3. In the *Backup Job* page, click the **backup job name** to be modified.
4. In the *Image Backup* page, click the **data integrity checks** option in the left navigation menu.

Figure 42 - Data Integrity Check Button



5. Click the **AutoVerify** checkbox to turn on the AutoVerify feature.
6. In the *Validation Interval* field, enter the frequently of the validation process (in days).
7. In the *Validation VM snapshot timeout* field, enter how long the VM should run before taking the desktop screenshot (in minutes). The screenshot should not be taken until the operating system is booted, and the boot time varies. In most cases, 10 minutes is sufficient, but you should increase this number for devices that take longer to boot.
8. To configure Windows System Files Integrity Checks, click the **Windows system files integrity check** drop-down menu and select the **frequency** of these checks.
9. To configure Exchange Integrity Checks:
  - Click the **Exchange Integrity Checks** checkbox.
  - In the *Full integrity* drop-down menu, select the **frequency** of these checks.



10. To configure SQL Integrity Checks:

- Click the **SQL Integrity Checks** checkbox.
- In the *Full integrity* drop-down menu, select the **frequency** of these checks.
- In the *Authentication type* field, select whether you want to enable **SQL server authentication** or **Windows authentication**.
- In the *Login* field, enter the **username** of the database administrator.
- In the *Password* field, enter the **password** of the database administrator.

11. Click the **Confirm** button to save your settings.

## View Validation Test Results

You can view the results of AutoVerify tests within the *Backup Times* page.

1. Within the UMC, click the **Reports** tab.
2. In the *All Reports* page, click the **backup times** option in the left navigation menu.
3. In the *Backup Times* page, select the **backup schedule** and click the **Get Results** button.

Figure 43 - Validation Test Results

The screenshot displays the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'reports' section with sub-items: backup history, scheduled backups, backup times (highlighted), and current disk usage. The main content area is titled 'backup times' and features a 'Schedule' dropdown menu set to 'es\_2010\_ws\_2008/2 - es2010ws2008/2'. Below this, a 'Rows per page' selector is set to 20. A 'get results' button is present. The table below lists backup details:

Backup Name	Machine	Machine Description	User	Start Time	End Time	Elapsed Time	Dirs & Files	Data	Validation snapshot	Validation log
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	08/13/2019 - 12:12:34 PM	08/13/2019 - 12:25:01 PM	12 mins 27 secs	136993	17.03 GB	View	View
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	08/09/2019 - 8:40:52 AM	08/09/2019 - 8:58:49 AM	17 mins 57 secs	136984	16.83 GB	-	-
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	08/08/2019 - 11:56:54 AM	08/08/2019 - 12:07:04 PM	10 mins 10 secs	136972	16.70 GB	View	View
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	07/29/2019 - 7:28:52 AM	07/29/2019 - 7:37:55 AM	9 mins 3 secs	136963	16.53 GB	View	-
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	07/29/2019 - 4:15:34 AM	07/29/2019 - 4:30:36 AM	15 mins 2 secs	136985	16.40 GB	View	-
es2010ws2008/2	172.18.50.12	es_2010_ws_2008/2	admin	07/29/2019 - 1:05:18 AM	07/29/2019 - 2:55:57 AM	1 hr 50 mins 39 secs	136977	22.57 GB	View	-

Export options: CSV | Excel | XML

## Remove Backup Job

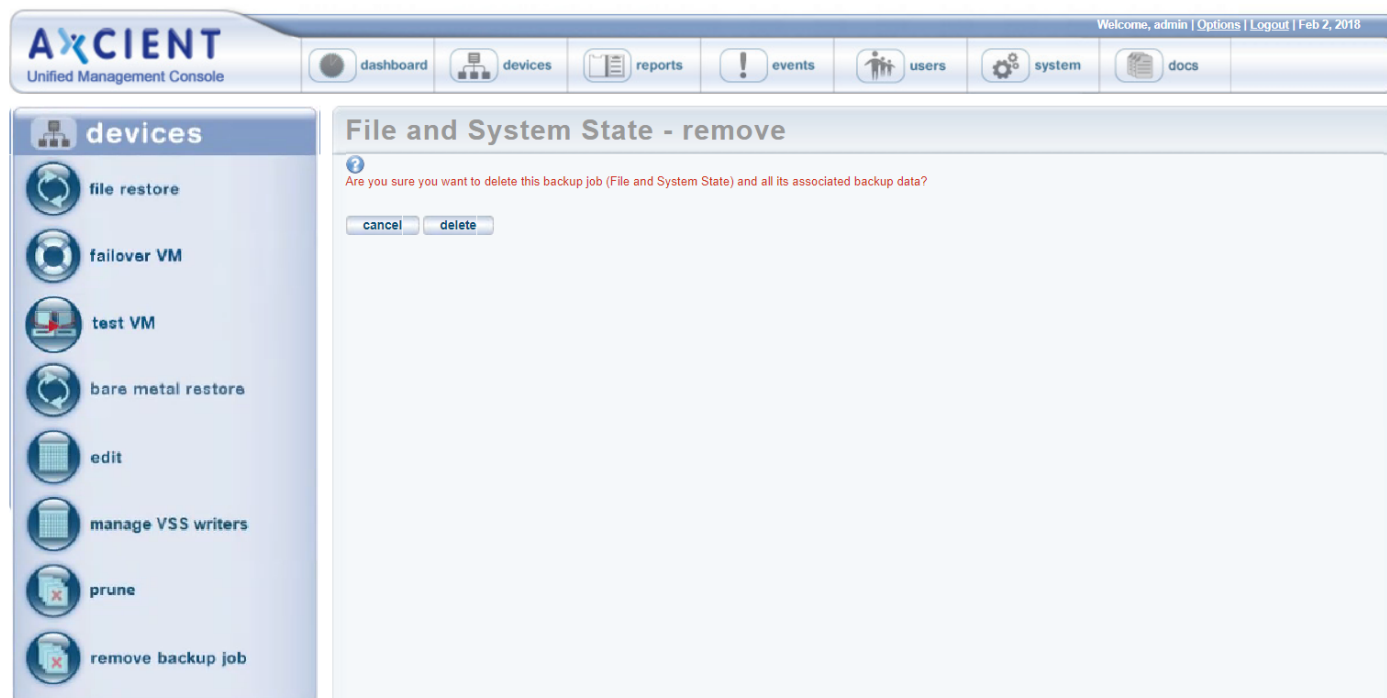
You can remove existing backup jobs.

Removing a backup job deletes all records of that backup, including all saved versions both local and in the Cloud. When a backup is removed, it is *no longer possible to recover any data from that backup job*. If it is an image job, failover VMs and BMR protection are no longer available until you create a new image backup job.

To remove a backup job:

1. On the UMC, click the **devices** tab. The *Devices* page displays.
2. On the *Devices* page, click on the icon of the target device. The *Backup Jobs* page displays.
3. On the *Backup Jobs* page, click on the backup job name to be deleted.
4. On the summary page for the selected backup job, click the **remove backup job** button located on the left navigation menu. The *Remove Backup Job* page displays.
5. On the *Remove Backup Job* page, click the **delete** button. The page refreshes with the backup job deleted from the list and a verification message.

**Figure 44** - The Remove Backup Job Page



## Schedule Offsite Backup Job

When creating a backup job, you specify what data should be saved in the Cloud. When a backup job runs, the Cloud data is placed in a queue in a Cloud staging area on the Axcient appliance, but the data is not immediately transmitted to an Axcient data center.

Cloud backups are not scheduled to run by default. To activate Cloud backups and set the Cloud backup start time:

1. On the UMC, click the **system** tab. The *Systems* page displays.
2. On the *Systems* page, click the **offsite configuration** button on the left navigation menu.
3. On the *Offsite Schedule* page, you can enable Cloud backups and configure the start time.

Users can create a data replication schedule in two different ways: *Manually* or *Unbundled Offsite*.

### Manually Scheduled Cloud Job

You can manually schedule Cloud backup jobs so that transmission to the Axcient data center begins at the preconfigured time, and all pending Cloud backup jobs are transmitted in order (some parallel processing). Transmission continues until all queued jobs have been sent.

Figure 45 - Offsite Schedule Page (Manual)

The screenshot displays the Axcient Unified Management Console interface. The top navigation bar includes tabs for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'system' menu with options: network settings, quality of service, date and time, offsite configuration (selected), SNMP, and web proxy. The main content area is titled 'off-site schedule' and contains settings for off-site Backup. It includes a checkbox for 'Off-site backups enabled' which is currently unchecked, and a time selector for 'Off-site backup will start at' set to 21:00. There are 'cancel' and 'save' buttons at the bottom of the settings area.

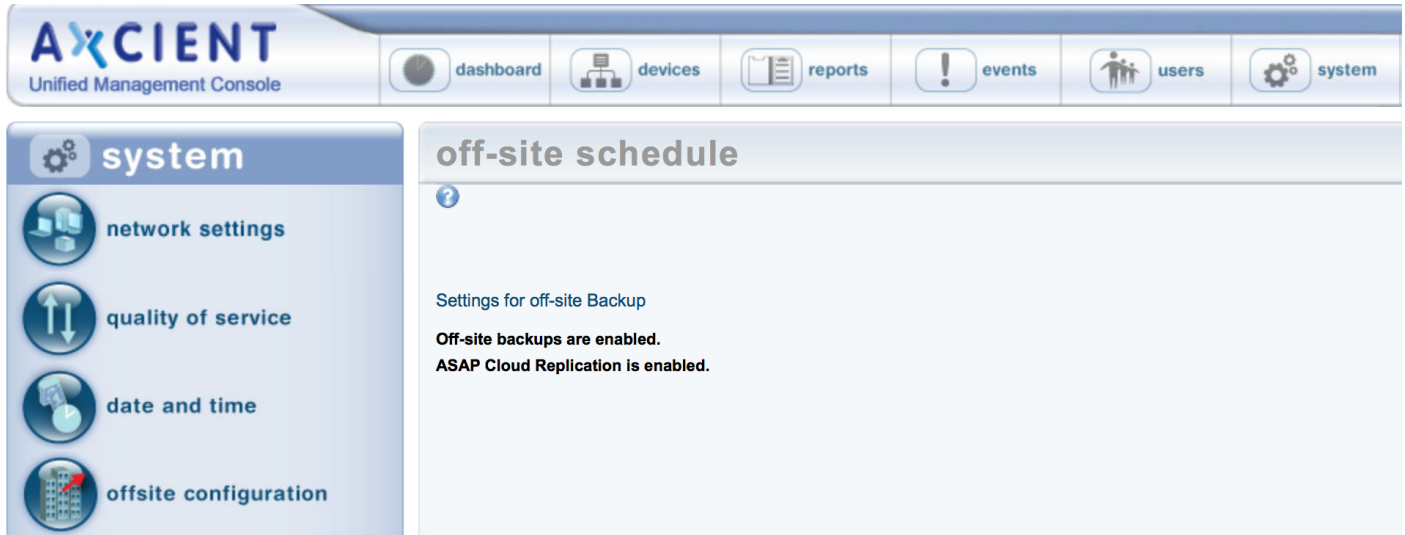
### Unbundled Offsite Cloud Job

On the Axcient Web Application, you can optionally enable the *Unbundled Offsite* feature for Cloud backups. This feature ensures that individual device backups automatically replicate to the Axcient Cloud as soon as the local backup for the device

completes. When this feature is enabled, individual devices are backed up to the Axcient Cloud independently, placing less demand on the network.

To enable or disable the Unbundled Offsites feature, please refer to the [Axcient Web Application User Guide](#).

**Figure 46** - Offsite Schedule Page (Unbundled Offsites)



## Copy Backup Job to DAS

Axcient provides the option of copying the backup jobs to a direct attach storage (DAS) device for the following purposes:

- The initial run of a Cloud backup job could take substantial time because all data must be copied and speed is limited by your Internet connection. If the initial Cloud backup would take more than 14 days to complete, you have the option to use a DAS device for the data transfer. (See the [Initial Backup Strategy](#) section to estimate transmission time.) In this case, a DAS device is connected to the Axcient appliance, the Cloud backup job data is copied to the DAS device, and the DAS device is then shipped to an Axcient data center where the data is transferred into the Axcient storage system.
- The Axcient appliance and the data center provide backup protection both local and in the Cloud. However, you have the option to use a DAS device as a separate backup archive. In this case, an export drive (DAS device) is attached to the Axcient appliance, and selected (or all) backup jobs are copied to the export drive. You can then store the export drive in a safe location. The data can be restored from the export drive to any Axcient appliance at a later date.

In either case, the first step is to contact Axcient technical support and request a DAS device. See the [Axcient DAS Transfer Guide](#) for detailed instructions.

# Restore Operations

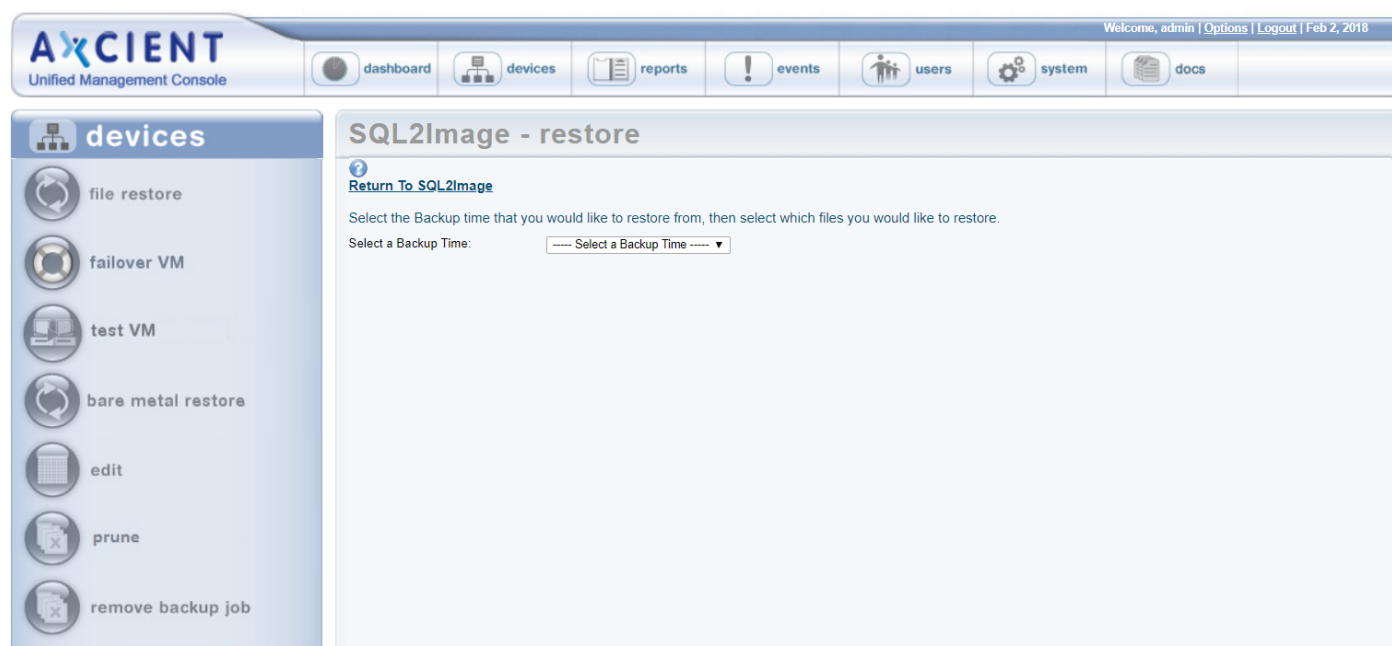
## Tree View Restore

This feature is available for both file and image backup jobs. The example page shots in this section are from an image backup job.

To selectively restore files from the folder tree view:

1. Navigate to a target device by doing one of the following:
  - Click the desired device in the **devices** pane of the UMC dashboard.
  - Click the **devices** tab at the top of the UMC page. On the *devices* page, and then click on the desired device.
2. On the *jobs* page for the device, click on the target backup job name.
3. On the *job details* page, click the **file restore** option from the left navigation menu.
4. On the *Restore* page, select the backup time (version) to restore from the drop-down menu list.

**Figure 47** - Tree View Restore: Select Backup Time

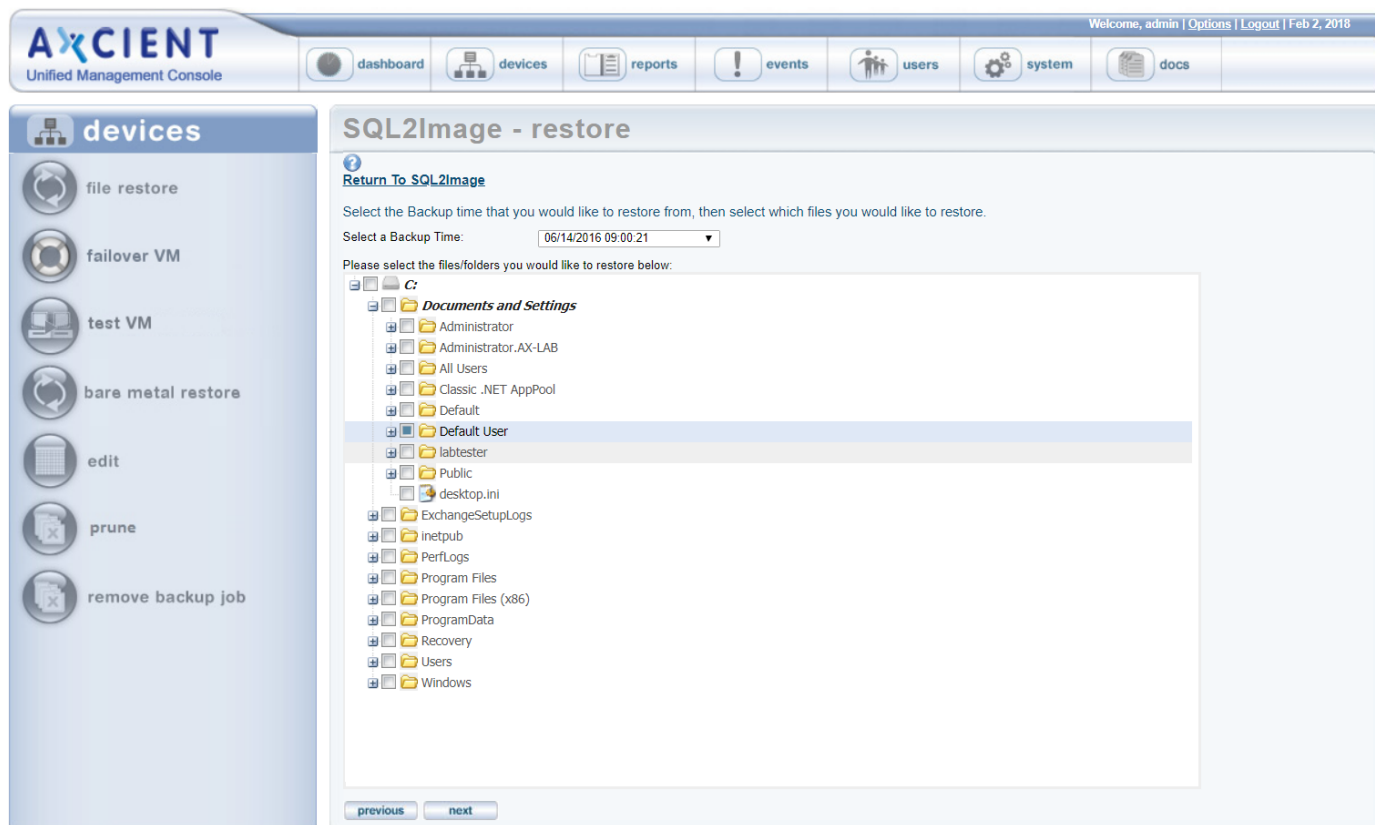


5. Icons for the backed up drives appears. Expand the file structure under the drives as far as necessary to locate the target files.

If the number of files in a folder exceeds a browser-specific thresholds (typically 1K or 2K), a warning box appears. Selecting to continue displays the long list of files. If the number of files exceed higher threshold (typically 16K or 32K) no warning box appears. Instead an empty folder is displayed.

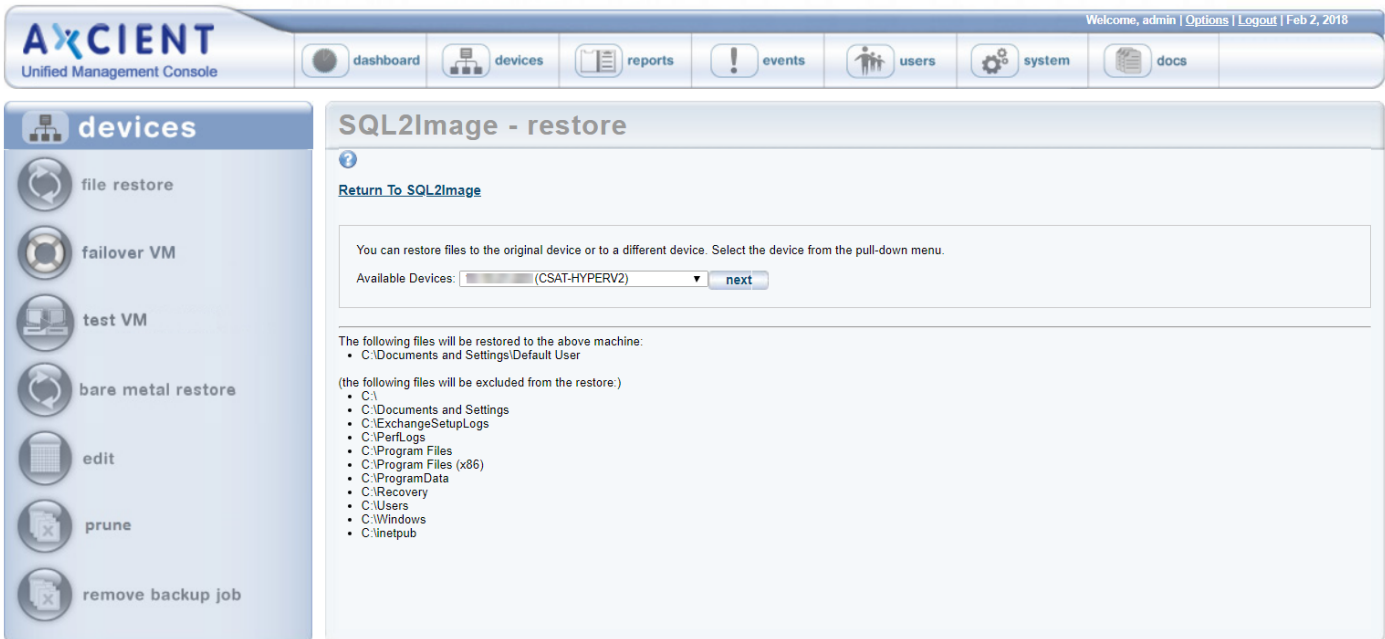
- Click the box next to each folder or file to be restored. A solid square appears indicating that the file has been selected. When the selection is complete, click the **next** button.

Figure 48 - Tree View Restore: Select Files



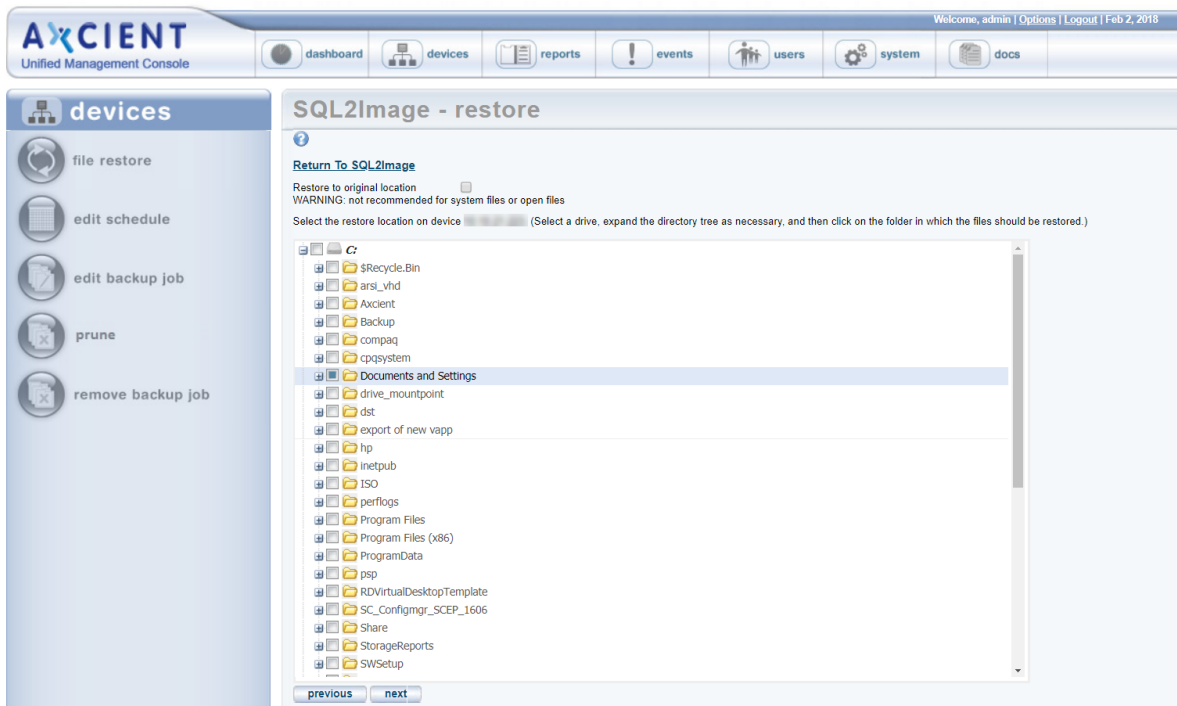
- On the *target device* page, you can restore on any available device, not just the one from which the backup was made. Select a device from the drop-down menu and verify the list of files to be restored. When both are correct, click the **next** button.

Figure 49 - Tree View Restore: Select Restore Device



- On the *restore location* page, click on the target drive icon in the middle of the page which displays the file structure to the right. Expand the file structure as far as necessary to locate the restore location and click the box next to that folder. A solid square appears indicating that the folder has been selected. Click the **next** button.

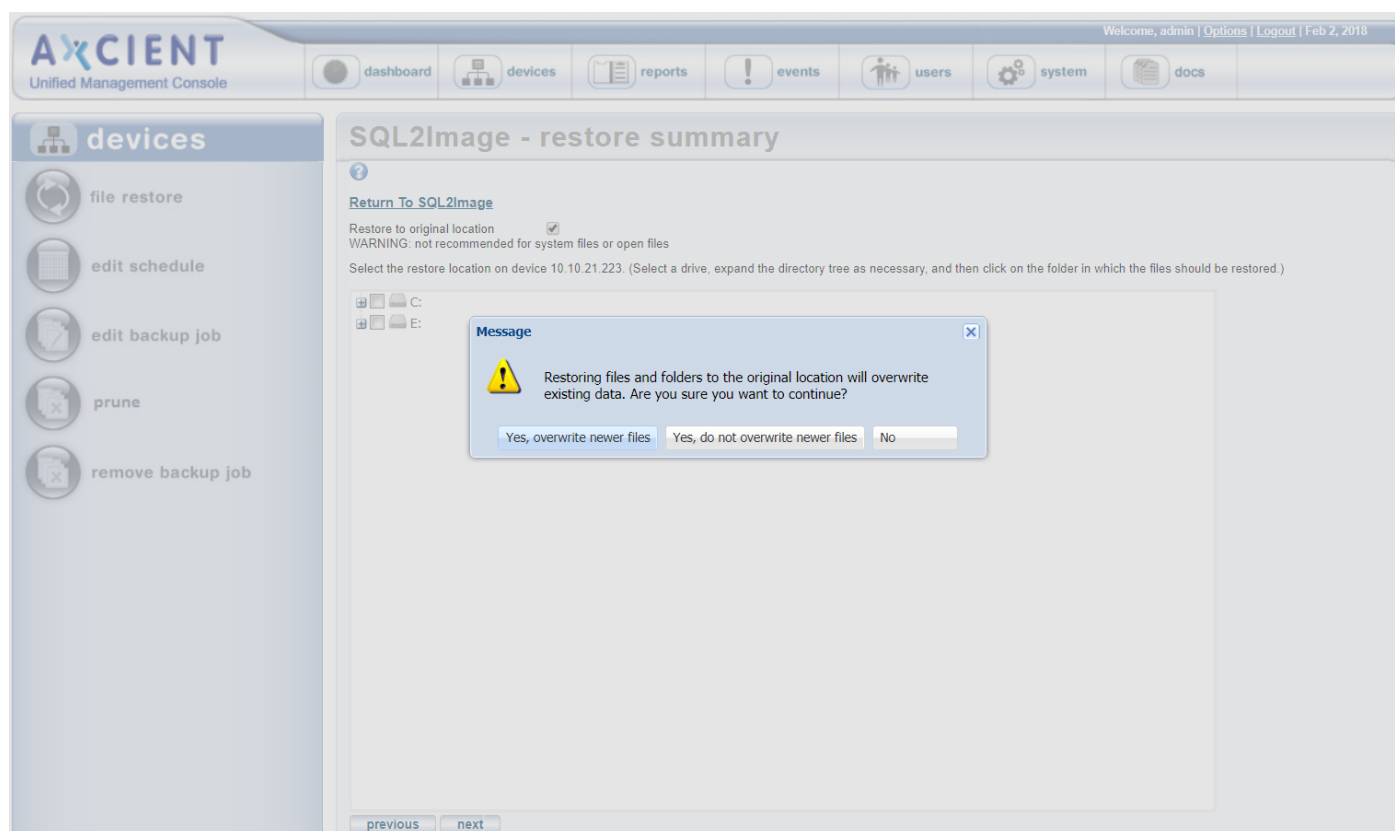
Figure 50 - Tree View Restore: Select Target Location





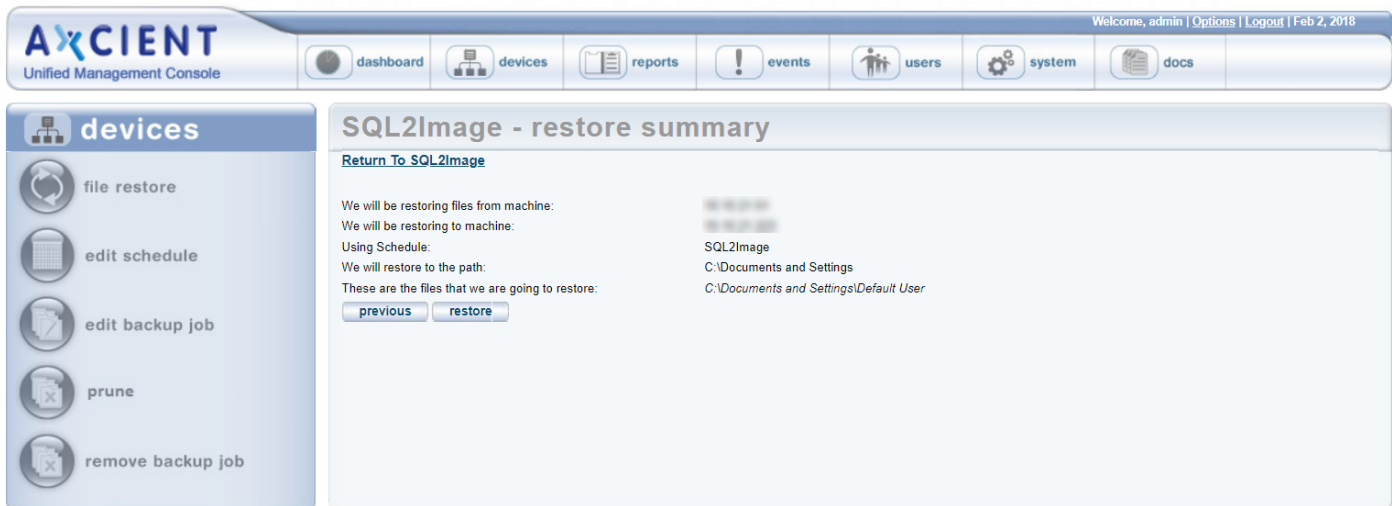
9. Alternatively, in the *Restore Location* page, click the **Restore to original location** check box to overwrite existing data. Please note that restoring files and folders to the original location will overwrite existing data, and is not recommended for system files or open files. Then, in the confirmation dialog box, select from the following options:
- **Yes, overwrite newer files** - This option allows you to proceed with the overwrite process, and will replace newer files with older files from the backup.
  - **Yes, do not overwrite newer files** - This option allows you to proceed with the overwrite process, but will not replace newer files with older files from the backup.
  - **No** - This option cancels the overwrite process.

**Figure 51** - Tree View Restore: Restore to Original Location



10. On the *Restore Summary* page, verify all the information is correct and click the **restore** button.

Figure 52 - Tree View Restore: Summary



11. The restore process begins. A message indicates the restore has been started. The process can be monitored from the *Running Restores* tab in the UMC dashboard. When the restore is complete, a *RESTORED* folder (or *RESTORED#* if conflicting name) appears in the restore location which contains all the restored files. Copy the restored file to the desired location.

When restoring multiple drives, a separate *RESTORED* folder is created for each drive.

## Search Restore

This feature is available from either a file or image backup job. The example page shots in this section are from a file backup job.

To search for and restore files by name:

1. Navigate to a target device by doing one of the following:
  - Click the desired device in the **devices** pane of the UMC dashboard.
  - Click the **devices** tab at the top of the UMC page. On the *devices* page, click on the desired device.
2. On the *jobs* page for the device, click on the target backup job name.
3. On the *job details* page, enter the search parameters as follows:
  - In the **Search Term** box *under search for files inside this backup set*, enter the search text. You can include a path to narrow the search. For example in the figure below, the search for “technote” retrieves any file in the backup job that includes the string “technote” in the name. If instead the search string was “\JoeFiles\Templates\technote”, only such files from the *Templates* directory would be retrieved. When entering a path, do not include the disk designation. For example, enter `\JoeFiles\Templates\technote`, not `C:\JoeFiles\Templates\technote`. Use standard path notation for the operating system (slashes for UNIX-based and backslashes for Windows).
  - In the **From** and **To** fields, select the range of backup jobs to search. All versions of that job created during the specified period will be searched (but no versions outside that date range). The search is based on file modification date (not the backup job time stamp).
4. The Axcient appliance returns a list of all files that include the text in the file name. Click the box so a check mark appears next to each file to restore, and then click the restore button. (In the example the search text is *technote* and the period of backup jobs to search is *1/02/2013-2/01/2013*. Five files are returned, and the bottom two, *technote\_template1.doc* and *tecnote\_template2.doc* in the `C:\JoeFiles\Templates` folder, are selected for restore.)

Figure 53 - Search Restore: Select Files

**AxCIENT**  
Unified Management Console

Welcome, admin | [Options](#) | [Logout](#) | Feb 1, 2013

dashboard devices reports events users system docs

**devices**

- file restore
- edit schedule
- edit backup job
- remove backup job

### Backup Job: Doc-Training Backup

Schedule name:   
 Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)  
 Backup schedule type:   
 Start time:  :  (2:00 PM)  
 Backup on connect: ☐  
 On these days: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday ☐ Sunday  
 Keep backups for:  days (about 4.3 weeks)

**Summary**  
 Your backup will run on Monday, Tuesday, Wednesday, Thursday, Friday, starting at 2:00 PM.  
 Backups will be retained for 30 days (about 4.3 weeks)

[Return To Device](#)

The following directories/files will be saved on the Axcient appliance:

The following directories/files will be saved on the Axcient appliance and Offsite Storage:  
 C:\Users\jmuench\JoeFiles

The following directories/files will be explicitly excluded:

[Manually Edit File Selections](#)

**search for files inside this backup set**

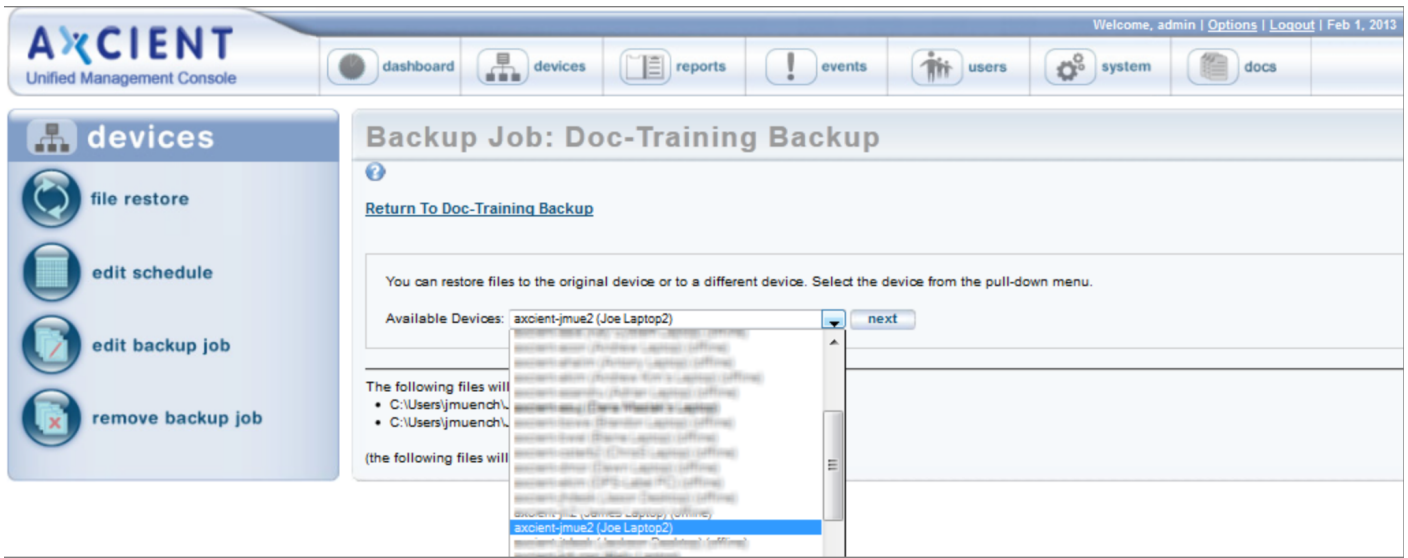
Search Term:  From:  To:

Results found: 6 (maximum 1000)...

Select	Name	In Path	Size	Date Modified
<input type="checkbox"/>	technote_note1.doc	C:\Users\jmuench\JoeFiles\Reference\Other	169 KB	2009-04-09 11:02:34
<input type="checkbox"/>	technote_note2.doc	C:\Users\jmuench\JoeFiles\Reference\Other	167 KB	2009-04-09 11:02:32
<input type="checkbox"/>	technote_note3.doc	C:\Users\jmuench\JoeFiles\Reference\Other	167 KB	2009-04-09 11:02:32
<input checked="" type="checkbox"/>	technote_template1.doc	C:\Users\jmuench\JoeFiles\Templates	169 KB	2009-04-09 11:02:34
<input checked="" type="checkbox"/>	technote_template2.doc	C:\Users\jmuench\JoeFiles\Templates	167 KB	2009-04-09 11:02:32

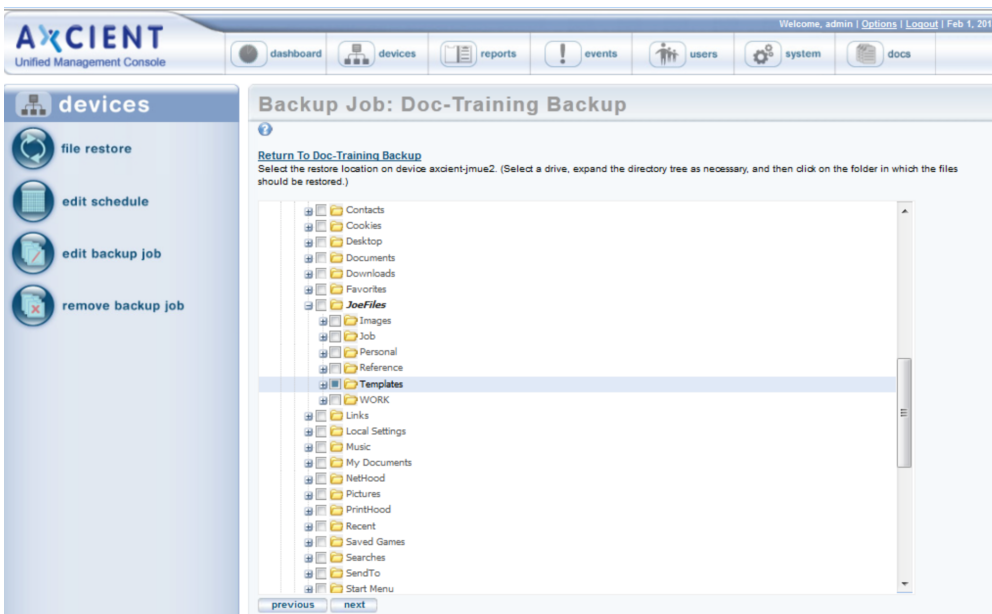
- On the *target device* page, you can restore on any device available. Select a device from the drop-down menu and verify the list of files to be restored. When both are correct, click the **next** button.

Figure 54 - Search Restore: Select Restore Device



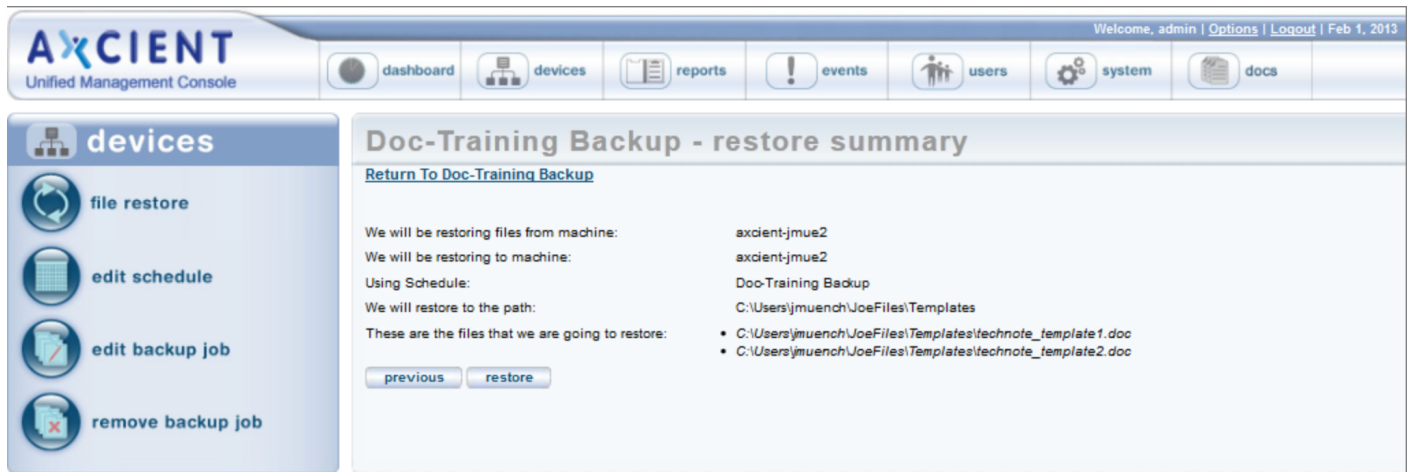
- On the *restore location* page, click on the target drive icon in the middle of the page which displays the file structure to the right. Expand the file structure as far as necessary to locate the restore location and click the box next to that folder. A solid square appears indicating that the folder has been selected. Click the **next** button.

Figure 55 - Search Restore: Select Restore Location



- On the *Restore Summary* page, verify all the information is correct and click the **restore** button.

Figure 56 - Search Restore: Summary



8. The restore process begins. A message indicates the restore has been started. The process can be monitored from the *Running Restores* tab in the UMC dashboard. When the restore is complete, a *RESTORED* folder (or *RESTORED#* if conflicting name) appears in the restore location which contains all the restored files. Copy the restored file to the desired location.

When restoring multiple drives, a separate *RESTORED* folder is created for each drive.

## System State Restore

If the system state is backed up as part of a file backup job (see [Back Up Files](#) section), you can restore that device to a known system state. (You cannot restore system state to a different device.) Restoring the system state allows you to repair a crashed or unstable system, such as from registry corruption.

While a single file backup job can contain both regular file and system state data, restoring system state is a separate step from restoring regular files from that job.

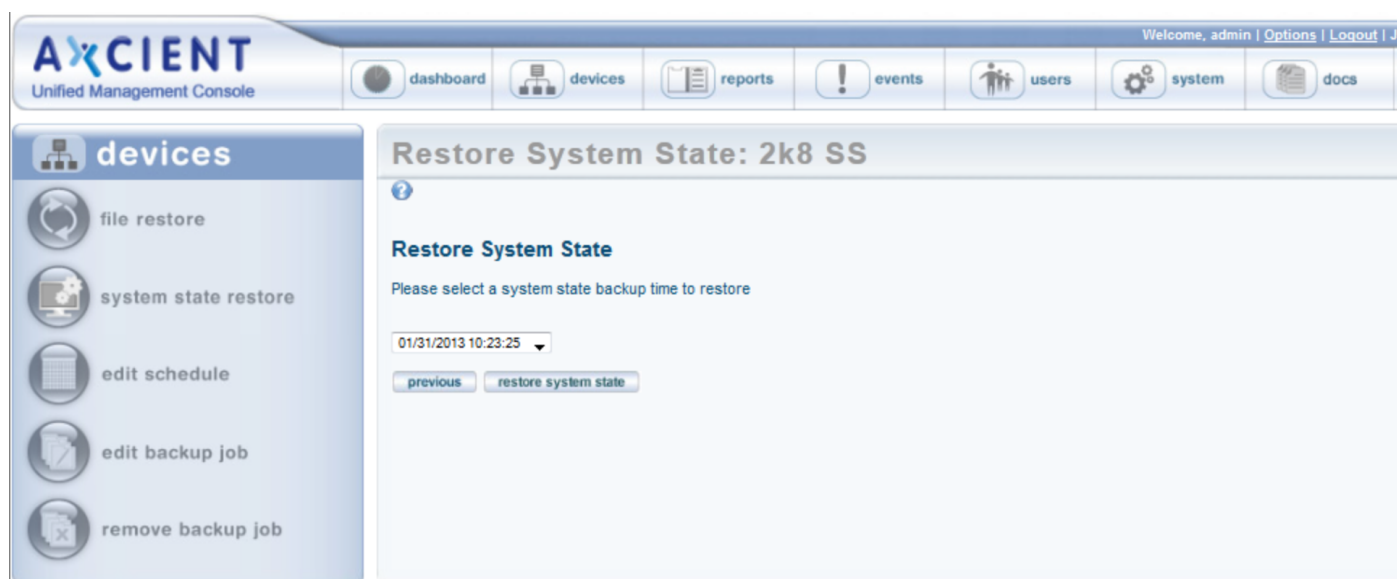
To restore the system state of a device:

1. Navigate to a target device by doing one of the following:
  - Click the desired device in the **devices** pane of the UMC dashboard.
  - Click the **devices** tab at the top of the UMC page. On the *devices* page, click on the desired device.
2. On the *job* page for the device, click on the target backup job name.

On the *job detail* page, select the **system state restore option** on the left of the page. (This option appears only when system state was backed up for the device.)

3. The *Restore System State* page for that job appears. Select the backup time (version) to restore from the pull-down list and then click the **restore system state** button.

Figure 57 - Restore System State Page



4. The process begins and a finish page with instructions appears.

Check the event log for a *system state restore completed* message. After this message appears, reboot the device.

- b. Wait for the system restore to complete. The amount of data to restore is substantial (typically GBs), but it normally takes less than 30 minutes. However, it can take hours in some cases depending on the type of hardware



Figure 58 - Restore System State Finish

The screenshot displays the Axcient Unified Management Console interface. The top navigation bar includes the Axcient logo and the text 'Unified Management Console'. To the right of the logo is a horizontal menu with icons and labels for 'dashboard', 'devices', 'reports', 'events', 'users', 'system', and 'docs'. Further right, a user status bar shows 'Welcome, admin | Options | Logout | Jan'. The left sidebar is titled 'devices' and contains a list of actions: 'file restore', 'system state restore', 'edit schedule', 'edit backup job', and 'remove backup job'. The main content area is titled 'Restore System State Finish: 2k8 SS' and contains a blue information icon followed by the text: 'The system state restore has begun. Do the following:'. Below this, a numbered list provides instructions: '1. Wait for the restore to complete (typically less than 30 minutes but sometimes hours).', '2. Check the event log for a "system state restore completed" message.', and '3. Reboot the device.'

# Bare Metal Restore

## Restore Device (BMR) Overview

The Bare Metal Restore (BMR) feature allows you to restore a complete system image on new hardware. BMR can protect from catastrophic failure of any device by restoring that system on new hardware or re-imaging the existing hardware. See [Virtual Machine and BMR Overview](#) section for more information about the BMR feature. An image backup job must first be run (see [Back Up System Images](#) section).

The BMR process to restore a system image on a new device (or re-image the current device) includes the following steps:

1. Select and prepare a system image on the Axcient appliance (see [Start BMR](#) section).
2. Restore the system image on a new device (see [Restore Device Using BMR Recovery Disk](#) section).
3. Resume the image backup job that was stopped when the BMR started, or restart a shutdown VM (see [Stop BMR](#) section).

BMR status information is available from either the dashboard or devices tabs (see [View Virtual Machine and BMR Status](#) section).

BMR-related actions are state dependent, and some actions cannot be invoked when certain states exist. A grayed out button or option means that operation cannot be selected at that time.

## Start BMR

The image backup job is suspended when a BMR is started. The image backup job will not run again until the BMR is stopped (see [Stop BMR](#) section).

You can run multiple BMRs simultaneously (restoring more than one device at a time). However, each BMR will run slower because the resources are split among the running instances. If you need to BMR multiple devices, weight the benefits of getting a server back up as soon as possible with the convenience of restoring multiple devices simultaneously.

To start a BMR operation, follow the steps for either the dashboard or devices method:

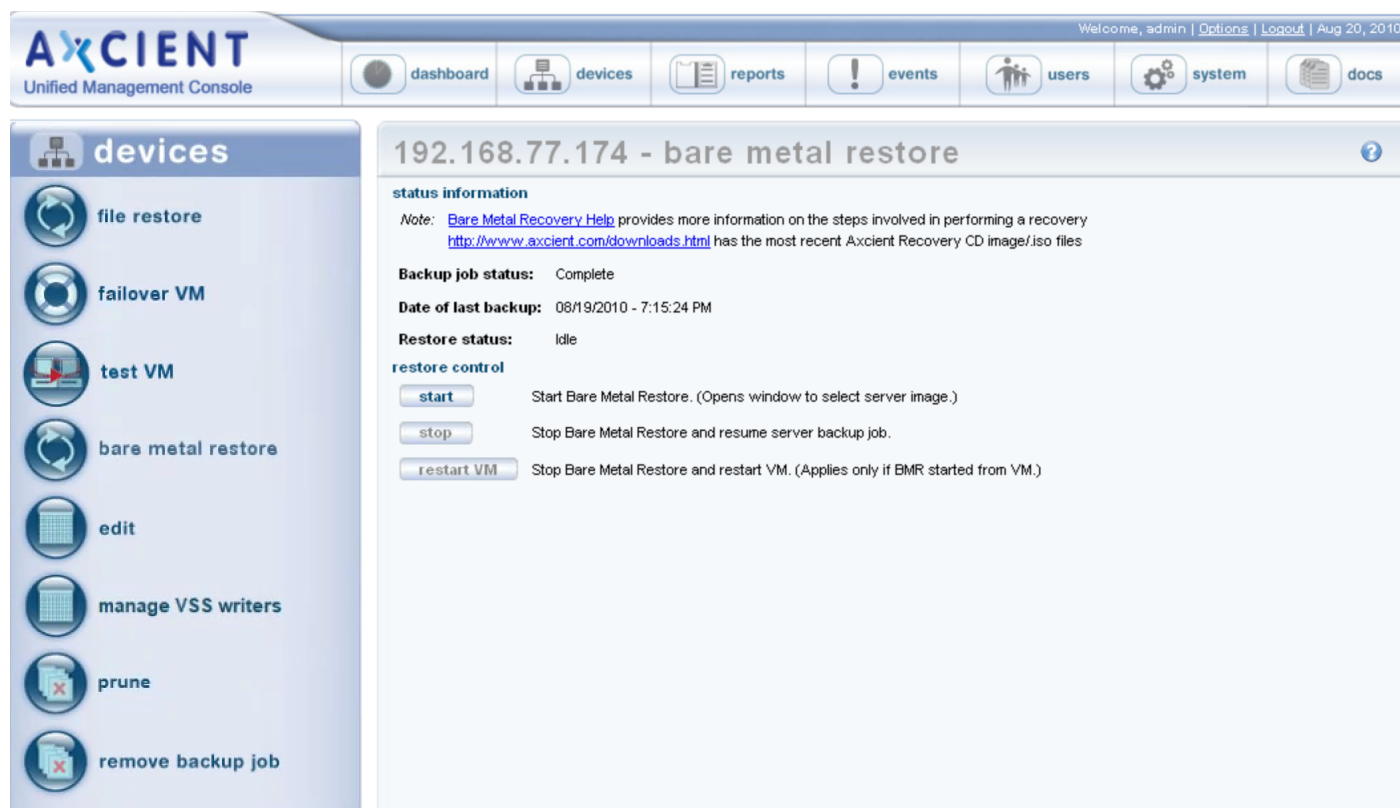
1. *Dashboard method*

- a. Click the dashboard option at the top of the UMC page, and then select the *Virtual Machines & BMR* tab (see [Virtual Machine & BMR Tab](#) section).
- b. Select the line for the target device, and click the **control** button.
- c. A VM/BMR window appears. Select the *Bare Metal Restore* tab, and then select **start** from the drop-down menu.

2. *Devices Method*

- a. Click the **devices** option at the top of the UMC page, the icon of the target device, the image backup job, and the **bare metal restore** option.
- b. The Bare Metal Restore page appears. Click the **start** button.

Figure 59 - Bare Metal Restore Page



3. The *Start BMR window* appears. Do the following:
  - a. In the **Backup Date** field, select the system image to use (date of that version) from the drop-down menu.
  - b. Click the **Start BMR** button. This locks and prepares the system image. Processing typically takes several minutes for the latest system image and increasingly longer for earlier versions. When the “Bare Metal Restore is ready for machine creation using the BMR CD” message appears, click the **OK** button to close the window.

Figure 60 - Start BMR Page

**Start Bare Metal Restore**

Server Name: 192.168.99.23  
 Server Address: 192.168.99.23

**Server Startup Options**

Backup Date:

This prepares the Bare Metal Restore backup. This may take from 5 minutes to 1 hour

## BMR Restore Configuration Page Fields and Definitions

Field	Description
Backup Job Status	Indicates whether there is a system image available: <ul style="list-style-type: none"> <li>If the image backup job has not run for the first time, the status is <b>Not Done</b>.</li> <li>If at least one version is available, the status is <b>Completed</b>.</li> </ul>
Date of Last Backup	Lists the finish time of the last image backup job. <b>Form</b> - mm/dd/yyyy - hh:mm:ss AM/PM <b>Example</b> - 03/20/2009 - 11:09:37 AM
Restore Status	Indicates whether a VM or BMR is active for this protected device: <ul style="list-style-type: none"> <li><b>Idle</b>—No active VM or BMR operation. (The image job is unlocked.)</li> <li><b>VM/BMR Starting</b>—The operation (failover VM, test VM, or BMR) is initializing.</li> <li><b>VM Running</b>—The failover or test VM is running.</li> <li><b>VM Pausing</b>—The failover or test VM is being shutdown. (All data is preserved.)</li> <li><b>VM Resuming</b>—A shutdown failover or test VM is being restarted.</li> <li><b>VM Starting BMR</b>—A BMR is started using the VM image. (The VM is shutdown before starting the BMR.)</li> <li><b>BMR Started</b>—A BMR is in progress. (The image job is locked, and a VM cannot run during this period.)</li> <li><b>BMR Stopping</b>—The BMR operation is stopped, and the image job resumes.</li> <li><b>BMR Starting VM</b>—The BMR operation is stopped, and the shutdown VM restarts. (This option applies only if the BMR was initiated through a <b>VM Starting BMR</b> command.)</li> </ul>
Start Button	Click this button to display the BMR Start window. <b>Note:</b> The image job is suspended when a BMR is started.
Stop Button	Click this button to stop the BMR operation and resume the image backup job (see <a href="#">Stop BMR</a> section). <b>Note:</b> If the BMR was initiated from a VM, that VM is discarded.
Restart VM Button	Click this button to stop the BMR operation and restart the VM (see <a href="#">Stop BMR</a> section).

### Start BMR Window Fields and Definitions

Field	Description
Server Name	Displays the alias name of the device. If no alias was specified when the device was added, displays the server address.
server Address	Displays the IP address or host name of the protected device.
Backup Date	Sets which system image to use. Select the target image (date of the desired version) from the pull-down list.

## Restore Device Using BMR Recovery Disk

To start the process, you can access one of the [BMR ISO versions](#) from the Axcient site:

- BMR AMD64 ISO
- BMR x86 ISO

When you have determined which BMR ISO is required, download the BMR ISO and burn it onto a bootable media compatible with the physical device.

When the BMR ISO has been burned onto a bootable media, connect it to the target device and boot from it.

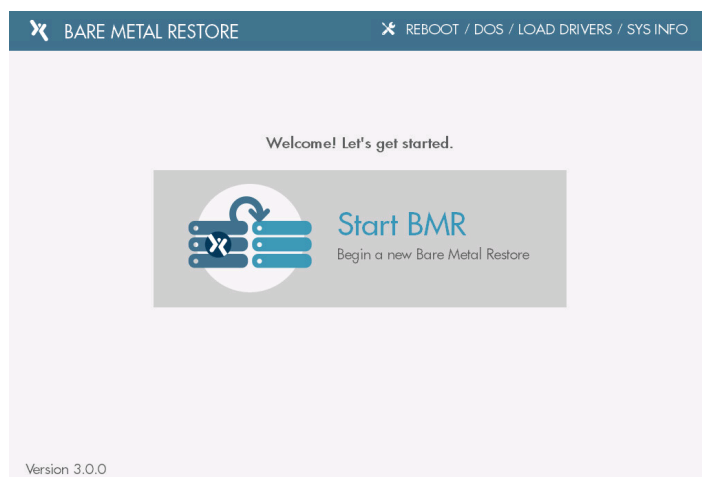
## Loading Additional Drivers

As part of the BMR process, common drivers are automatically loaded onto the target device. However, the target device might also require additional drivers to function properly. For example, you might need drivers that detect RAID devices.

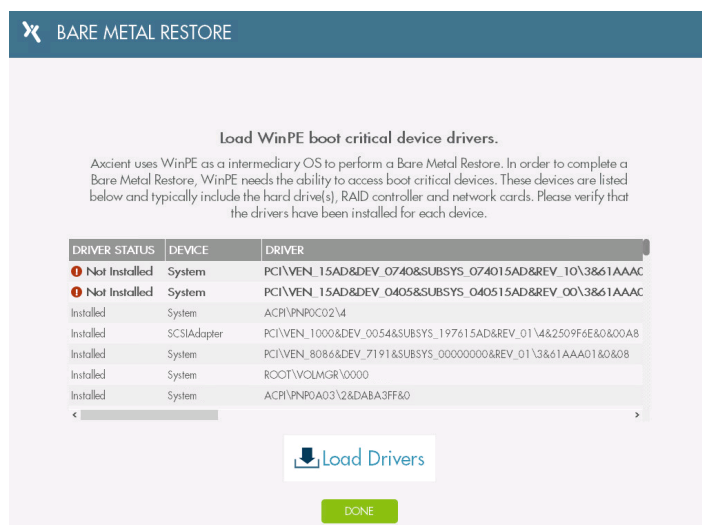
Before beginning the BMR process, you should determine if additional drivers need to be loaded onto the device.

1. When the device has booted from the bootable media, a *Start BMR* screen displays, prompting you to select from the following options:
  - **Reboot** allows you to reboot the device.
  - **DOS** opens a DOS window where you can issue commands such as `diskpart`, `chkdsk`, and so forth.
  - **Load Drivers** allows you to load drivers for the BMR ISO. For example, this can be used to load drivers to detect RAID devices on the target device.
  - **Sys Info** provides information used by Axcient Support to help troubleshoot problems.

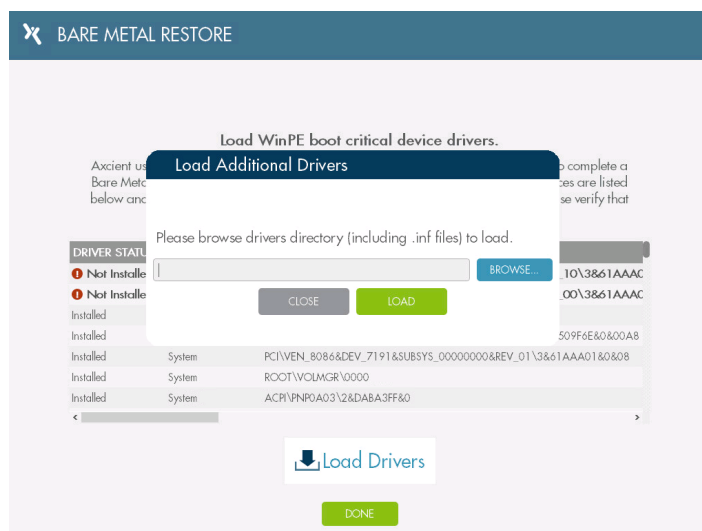
Select the **Load Drivers** option to load the drivers.



- In the next screen, you will be presented with a list of drivers that are required for the BMR process to complete successfully. To load drivers, click the **Load Drivers** button.

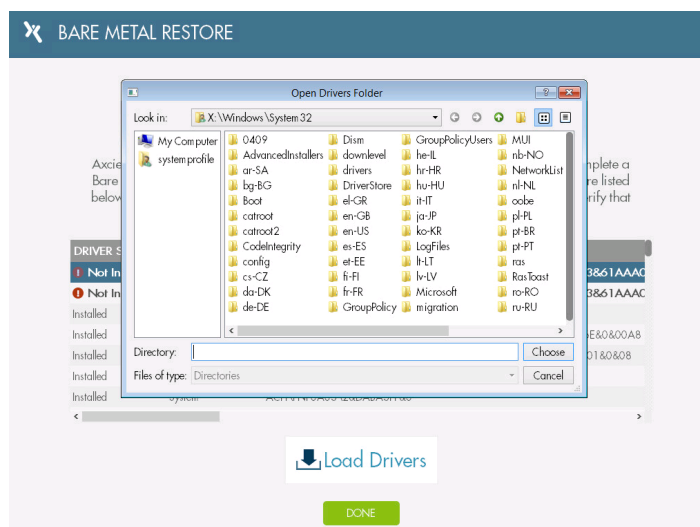


- In the *Load Additional Drivers* screen, click the **Browse** button to browse and select the folder containing the appropriate drivers.



- Click the **Choose** button to select a folder, and then click the **Load** button. The BMR ISO will automatically scan the folder and load any drivers available. Repeat this step as many times as necessary.

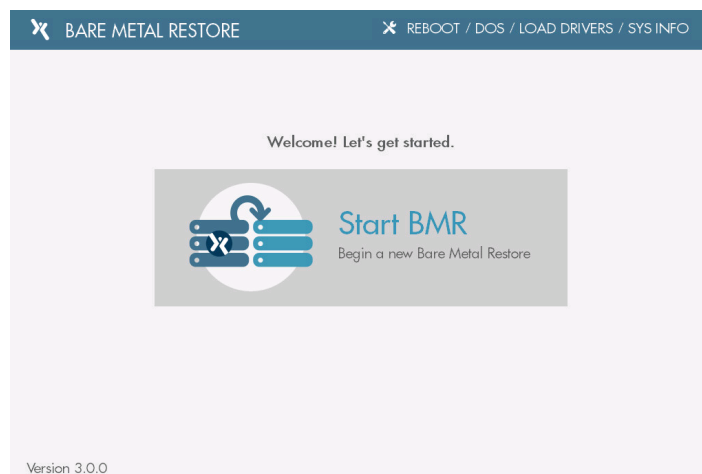




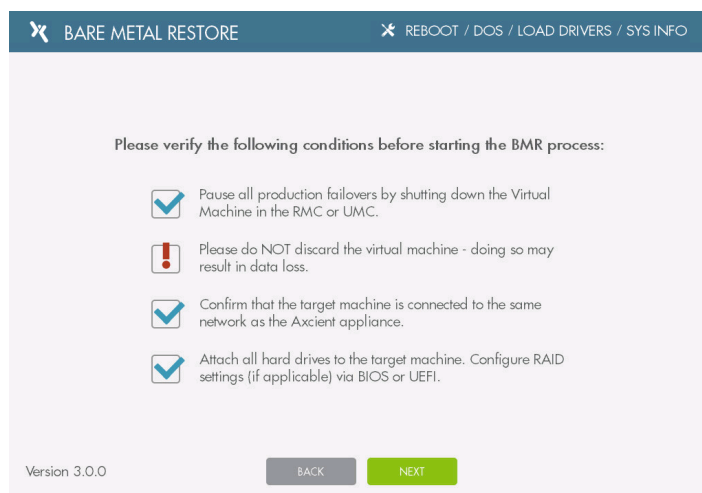
- When the necessary drivers have been selected, return to the initial *Start BMR* screen.

## Performing the BMR

- After all drivers have been loaded, and you have performed any required DOS commands, click the Start BMR button to begin the BMR process.

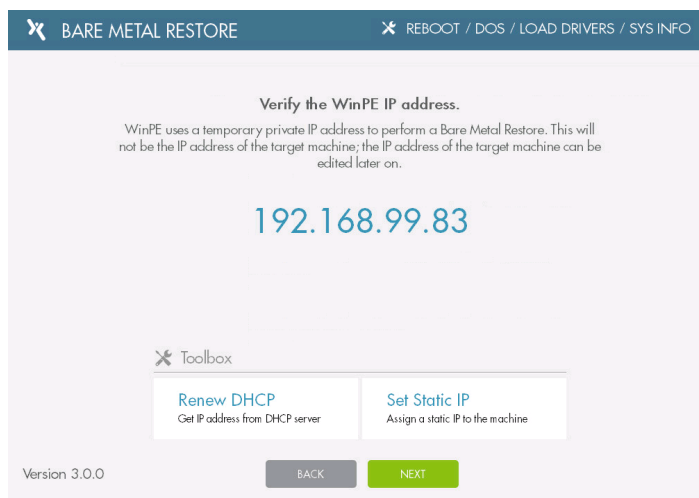


- In the next screen, you will be presented with a list of tasks that must be completed before beginning the BMR process. Failure to verify one or more of these conditions might cause the BMR process to fail. If performing a BMR from a production failover, do not discard the failover VMs. Instead, select the **Stop** button in the production failover VM to stop and not discard the VMs. Click the **Next** button to continue.



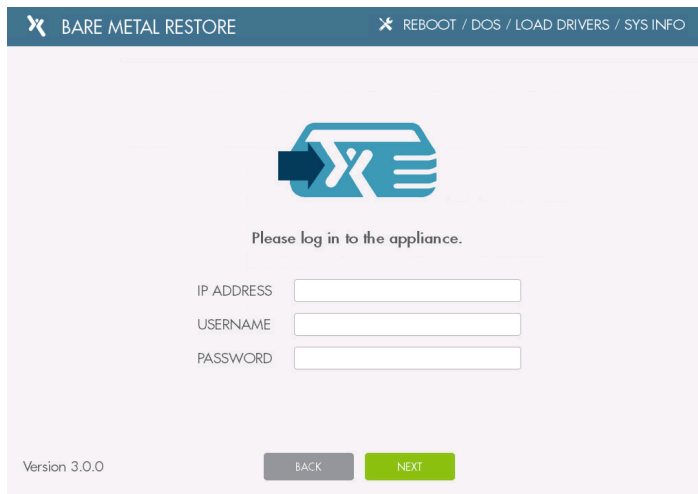
3. In the next screen, verify the WinPE IP address. The WinPE uses a temporary IP address to perform the BMR. This IP address is for the BMR only and will not be the final IP address of the device being restored. If you do not see an IP address on this screen, you will need to load the appropriate NIC drivers. When the IP address has been configured, click the Next button.

- Click the **Renew DHCP** button to automatically assign an IP address to the WinPE.
- Click the **Set Static IP** button to manually configure the IP address.



4. In the next screen, enter the following information for the appliance protecting the device being restore:
- IP Address of the appliance
  - Username
  - Password

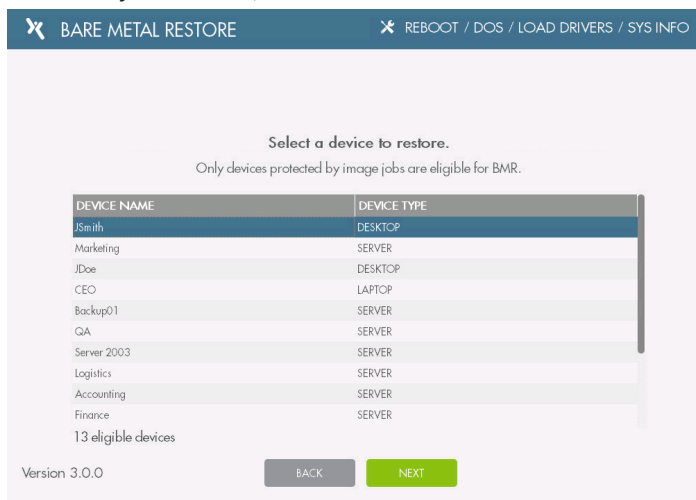
When you are finished, click the **Next** button.



The screenshot shows the 'BARE METAL RESTORE' login interface. At the top, there is a navigation bar with the Axcient logo and the text 'BARE METAL RESTORE' on the left, and 'REBOOT / DOS / LOAD DRIVERS / SYS INFO' on the right. The main area features a large blue Axcient logo with a play button icon. Below the logo, the text 'Please log in to the appliance.' is displayed. There are three input fields: 'IP ADDRESS', 'USERNAME', and 'PASSWORD'. At the bottom left, it says 'Version 3.0.0'. At the bottom right, there are two buttons: 'BACK' (grey) and 'NEXT' (green).

Version 3.0.0

5. In the next screen, select the device being recovered. Only one device can be selected. When are you finished, click the **Next** button.



The screenshot shows the 'BARE METAL RESTORE' device selection interface. At the top, there is a navigation bar with the Axcient logo and the text 'BARE METAL RESTORE' on the left, and 'REBOOT / DOS / LOAD DRIVERS / SYS INFO' on the right. The main area features the text 'Select a device to restore.' and a note 'Only devices protected by image jobs are eligible for BMR.'. Below this is a table with two columns: 'DEVICE NAME' and 'DEVICE TYPE'. The table lists 13 eligible devices. At the bottom left, it says 'Version 3.0.0'. At the bottom right, there are two buttons: 'BACK' (grey) and 'NEXT' (green).

DEVICE NAME	DEVICE TYPE
JSmith	DESKTOP
Marketing	SERVER
JDoe	DESKTOP
CEO	LAPTOP
Backup01	SERVER
QA	SERVER
Server 2003	SERVER
Logistics	SERVER
Accounting	SERVER
Finance	SERVER

13 eligible devices

6. In the next screen, select the date of the appropriate recovery point and click the **Choose** button.

Version 3.0.0

7. In the next screen, you will be presented with a list of the replicated drives from the selected device restore point. You can select to exclude one or more drives from the BMR process. *You cannot exclude the boot drive for the OS.* Click the **Next** button to continue.

Version 3.0.0

8. In the next screen, configure the disk partition schema. These fields are automatically populated with recommended settings.

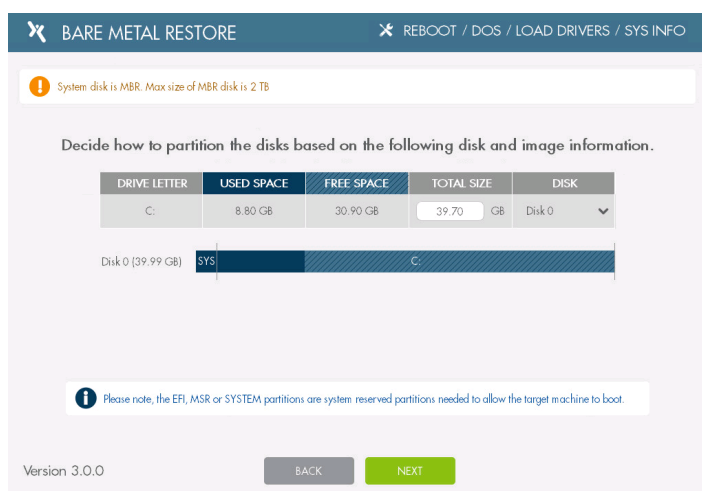
You might notice **SYS**, **MSR** or **EFI** in one or more of the partitions. These are reserved partitions needed to boot the target device.

The top section lists each detected volume. Use this section to update key settings:

- In the *Disk* column, use the drop-down menu to assign a **disk** to a specific driver letter.
- In the *Total Size* column, configure the **size of the partition**. Each partition, as well as the sum of all partitions, cannot be larger than the total disk size.

If you do not see any drives, or if a drive is missing, click the **Load Drivers** button to browse and load the appropriate drivers that will detect the missing drives.

When you are finished, click the **Next** button.

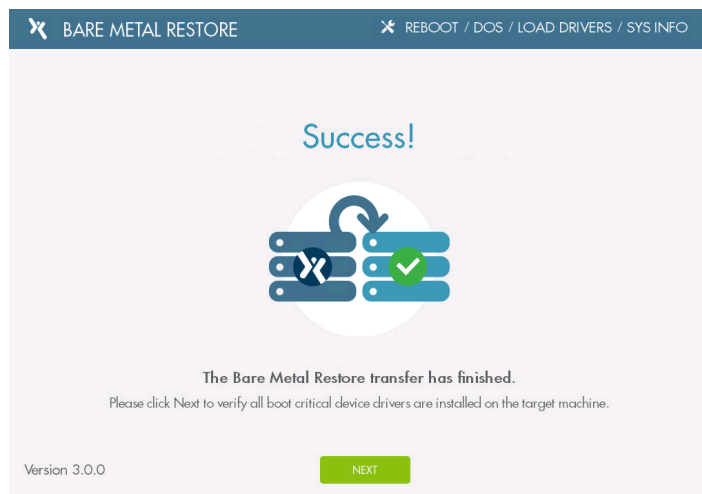


9. In the *Running BMR* screen, you can track the BMR process with:

- The progress bar,
- The total completion percentage,
- The drive currently being restored, and
- GB processed out of the total GB to be processed.



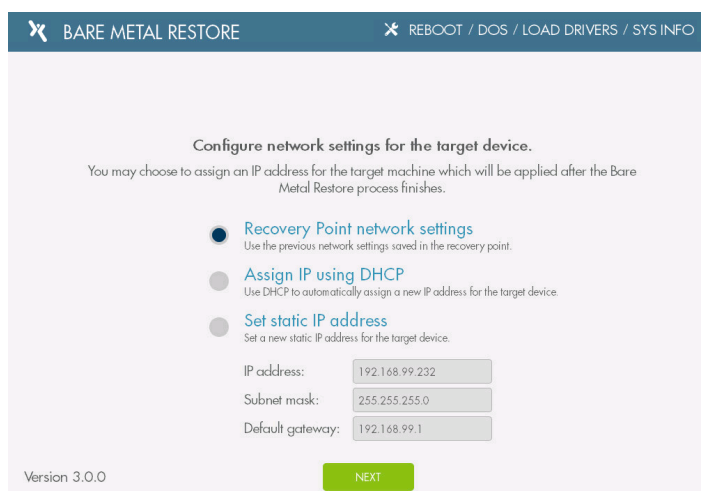
10. When the BMR process completes successfully, click the **Next** button.



11. In the next screen, configure the network information of the restored device. You can select from the following options:

- **Recovery Point network settings** allow you to use the network settings of the selected restore point.
- **Assign IP using DHCP** allows you to use a new IP address for the restored device after the BMR process completes and the device is rebooted.
- **Set static IP address** allows you to manually configure the network settings for the restored device.

Click the **Next** button when you are finished.

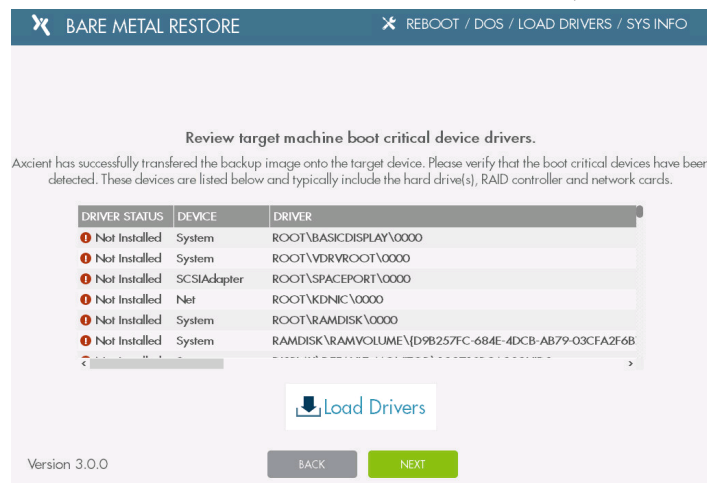


12. In the next screen, review the list of drivers for the target device. Click the **Load Drivers** button to browse and load the required drivers.

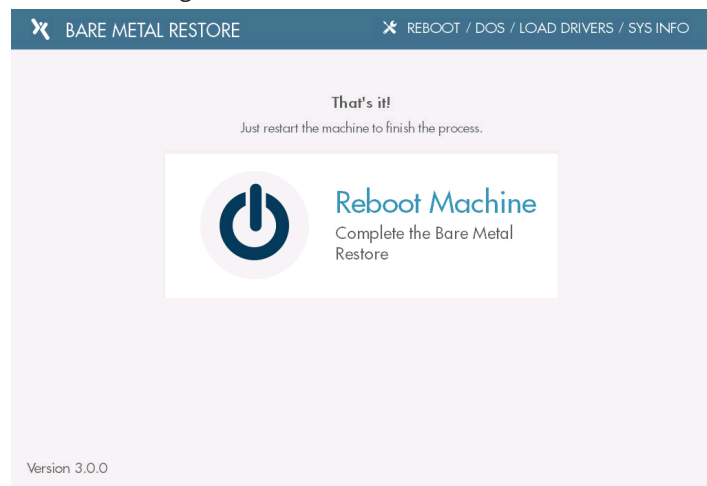
Please note that not all drivers are required to be downloaded in order to boot the device after the BMR process.

However, if you experience boot issues, please refer to the Troubleshooting Boot Errors section below.

When the boot-critical drivers have been installed, click the **Next** button.



- When the BMR process has completed successfully, click the **Reboot Machine** button to reboot the target device. Disconnect the bootable media containing the BMR ISO so that the device does not boot from the bootable media when restarting.



## Troubleshooting Boot Errors

If you are unable to start the target device after the BMR process completes, you should ensure that all necessary drivers have been added.

To confirm all necessary drivers have been added:

1. Reconnect the bootable media containing the BMR ISO to the target device and boot from the media.
2. In the **Start BMR** screen, click the **Load Drivers for Image Backup** option.
3. Follow the steps listed above to load any additional drivers needed for the device to function properly.



## Stop BMR

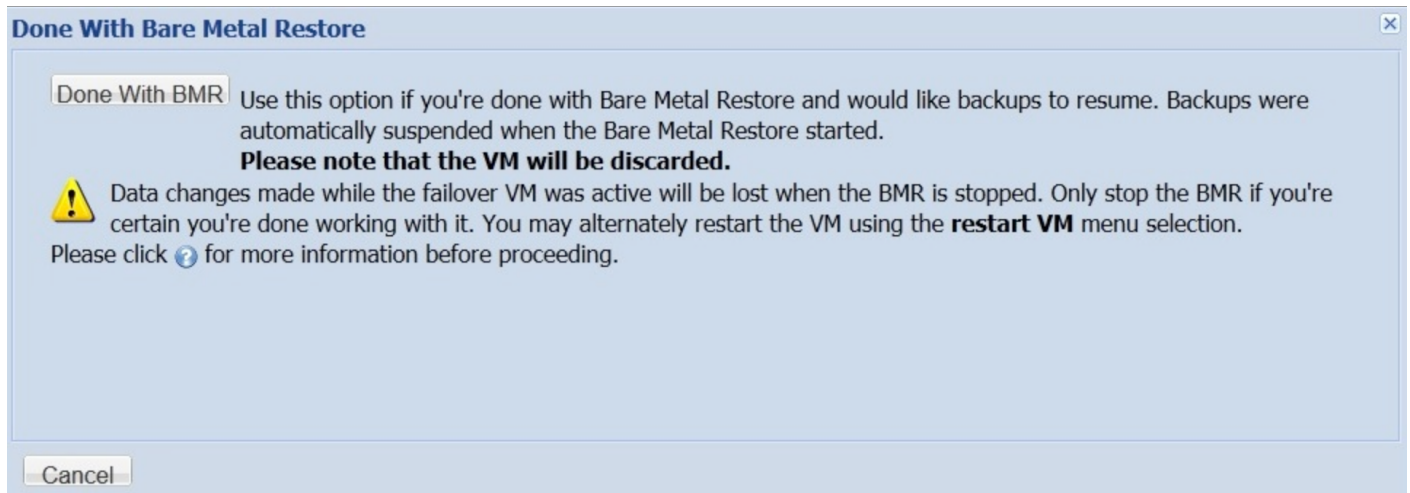
There are two options to complete a BMR operation:

- **Stop**—Stops the BMR process and restarts the image backup job. If the BMR was initiated from a VM, the VM is discarded.
- **Restart VM**—Stops the BMR process and restarts the VM. (The image backup job remains suspended.) This option applies only when the BMR was initiated from a running (or shutdown) VM.

## Stop BMR

To stop a BMR operation and resume the image backup job:

1. Follow the steps for either the dashboard or devices method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the **Virtual Machines & BMR** tab (see [Virtual Machine & BMR Tab](#) section).
    - b. Select the line for the target device, and click the **control** button.  
  
A VM/BMR window appears. Select the **bare metal restore** tab, and then select **stop** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** button, the icon of the target device, the image backup job, and the **bare metal restore** option.
    - b. The *Bare Metal Restore* page appears. Click the **stop** button.
2. The *BMR Done* window appears. Click the **Done With BMR** button. A status window appears while BMR is processing. When the “Bare Metal Restore processing is complete” message appears, click the **OK** button to close the window.

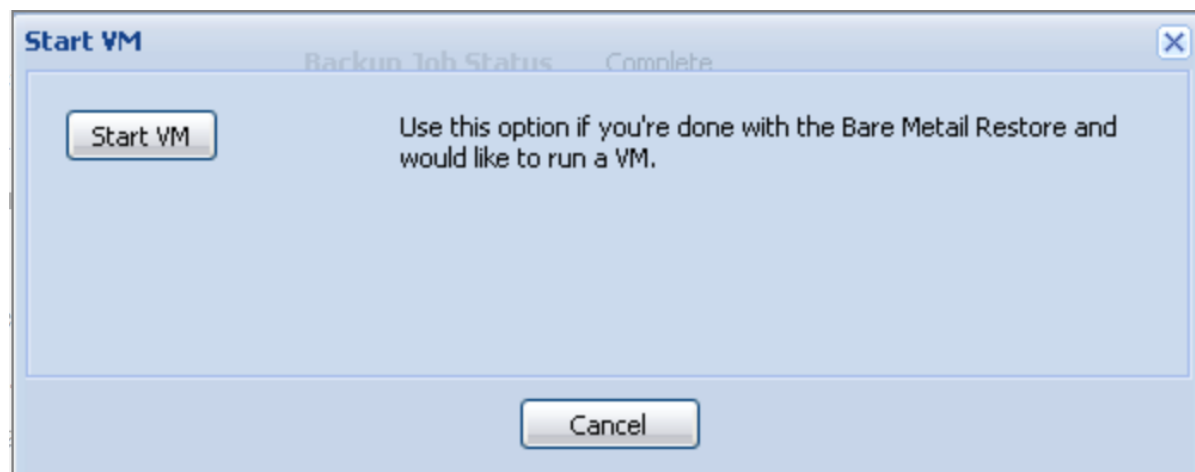
*Figure 61* - Done with BMR Window

## Restart BMR

To stop a BMR operation and restart a failover VM:

1. Follow the steps for either the dashboard or devices method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the **Virtual Machines & BMR** tab (see [Virtual Machine & BMR Tab](#) section).  
Select the line for the target device, and click the **control** button.
    - b. A VM/BMR window appears. Select the **bare metal restore** tab, and then select **restart VM** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** button, the icon of the target device, the image backup job, and the **bare metal restore** option.
    - b. The *Bare Metal Restore* page appears. Click the **restart VM** button.
2. The *Start VM* window appears. Click the **Start VM** button. A status window appears while the VM is restarted. When the “Failover VM has been started” message appears, click the **OK** button to close the window.

Figure 62 - Start VM Window



# Virtual Machine Overview

Axcient provides features designed to protect business continuity. These features allow you to recover when systems have problems or need maintenance. The first step is to create an image backup job (see “Back Up System Images ” section). You can then select a system image from the backup and invoke one or both of the following recovery services:

The Failover Virtual Machine feature allows you to failover a server on-demand and run a backup system image on the Axcient appliance as a “virtual machine” (VM). The failover VM can function as the server until the problem is fixed and the server comes back on line. It can work in conjunction with BMR by providing services until a new server is ready, at which point the VM image can be restored on the new hardware through BMR.

**NOTE:** The maximum number of supported image backup jobs and running VMs varies by the Axcient appliance model (see [Appliance Specifications](#) appendix).

You can BMR a device that runs any supported version of the Windows operating system, but failover VM support is limited to supported Windows Server and SBS versions. See the Axcient Release Notes for a list of the supported versions.

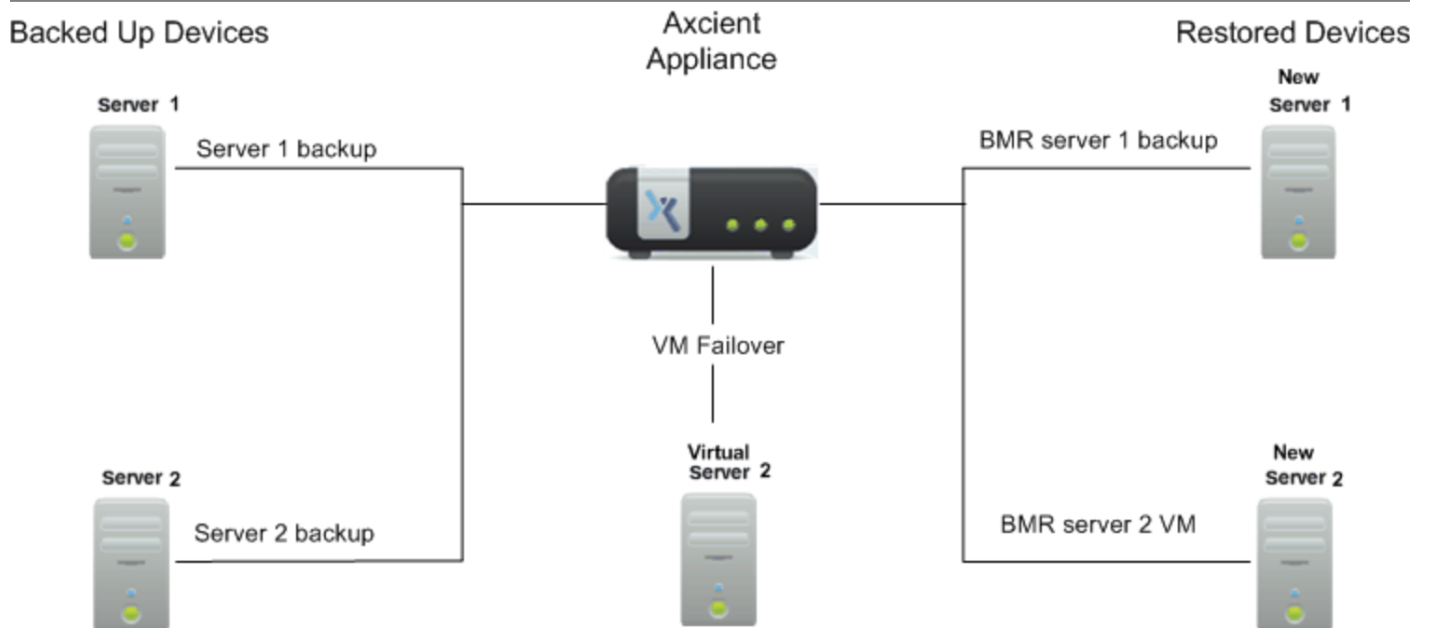
Although a failover VM can run indefinitely, it is not intended as a long-term replacement for a permanent server. The server functions should be transferred back to a server machine as soon as possible.

In the event of a site disaster where starting a VM on the local Axcient appliance is not feasible, you can start a “virtual office” in the cloud (that is, running in an Axcient data center). See the *Cloud Failover* chapter in the Axcient [Web Application User Guide](#) for more information.

The figure illustrates backing up and restoring two servers:

1. Server 1 functions properly but needs a hardware upgrade to accommodate increased demand. In this case, a BMR is performed on the new Server 1 hardware while the old Server 1 continues to run. A system image from the Server 1 backup job is restored into the new Server 1 hardware. After the new Server 1 is started, the latest file backups from the original Server 1 can be restored on the new Server 1. This ensures that any data changes made on the original server after the BMR system image was created are transferred to the new server. The original Server 1 is then shutdown, and the new Server 1 is brought online.
2. Server 2 has a catastrophic hardware failure. A failover VM image is started on the Axcient appliance when Server 2 goes down. The failover VM provides services to the organization while Server 2 is unavailable. When the new Server 2 hardware is ready, the VM is stopped. BMR is used to restore the latest VM image on the new hardware. The new device is started and takes over as Server 2. (File and mailbox jobs continue normally while a VM is running.)

Figure 63 - VM Failover and BMR Example



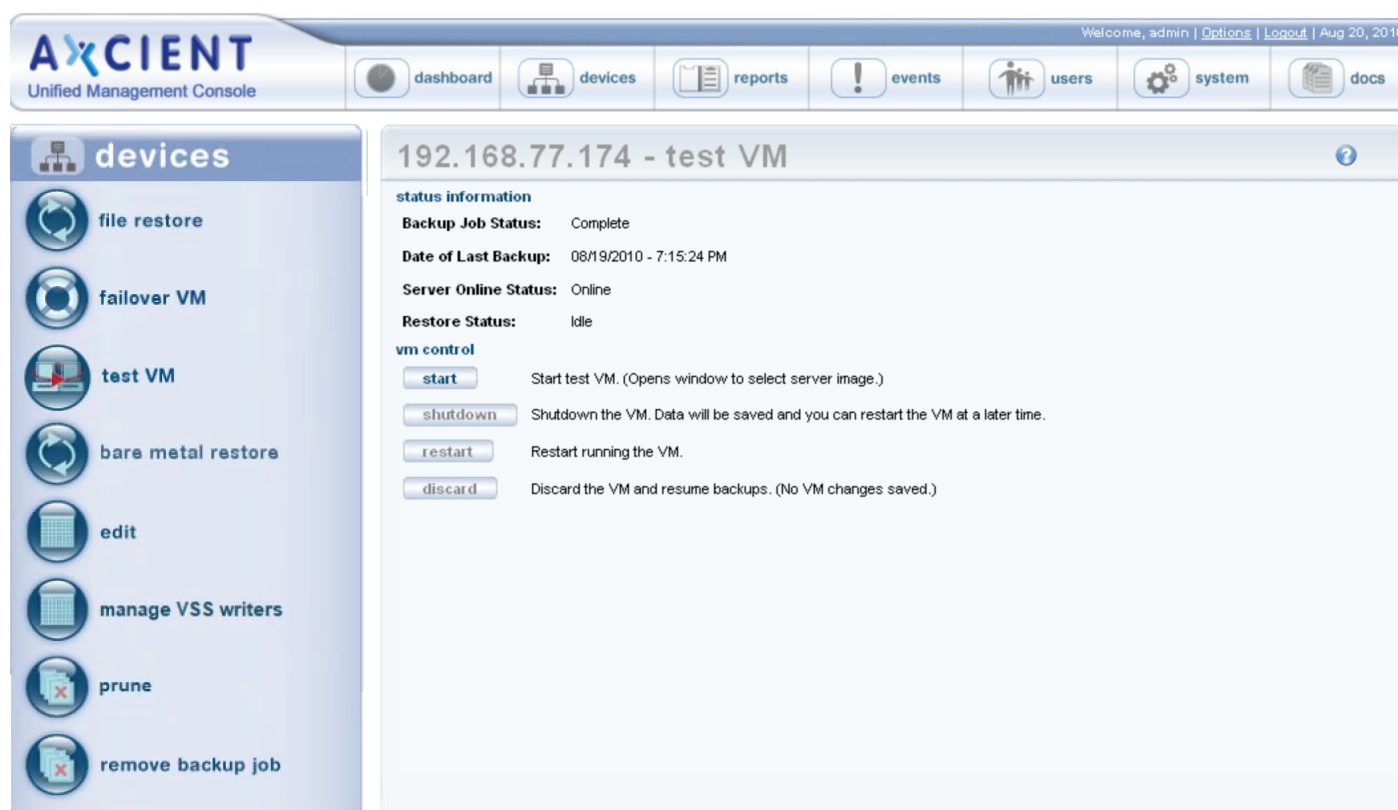
## Test Virtual Machine

After creating and running an image job, you can test whether a system image functions properly as a VM before using it as a live replacement for the protected server. This test is recommended after creating and running the image job for the first time. You can also periodically test and verify the VM as needed.

To test a VM image:

1. Navigate to the *Test VM Startup* window from the Dashboard or from a specific device.
  - For example, using the Dashboard method:
    - a. On the UMC, click the **dashboard** tab, and then click the **Virtual Machines & BMR** tab. The *Virtual Machines & BMR* table displays.
    - b. Click the **control** button for the desired target device. A *VM/BMR* window displays.
    - c. Click the **Test VM** tab, and then select **start** from the drop-down menu. The *Test VM Startup* window displays.
  - Alternatively, using the device method:
    - a. On the UMC, click the **devices** tab, and then click the **target device**.
    - b. On the left navigation menu, click the **image backup** option. The *Image backup* page displays.
    - c. On the left navigation menu, click the **test VM** option. The *Test VM* page displays.
    - d. On the *Test VM* page, click the **start** button. The *Test VM Startup* window displays.

Figure 64 - Test VM Page

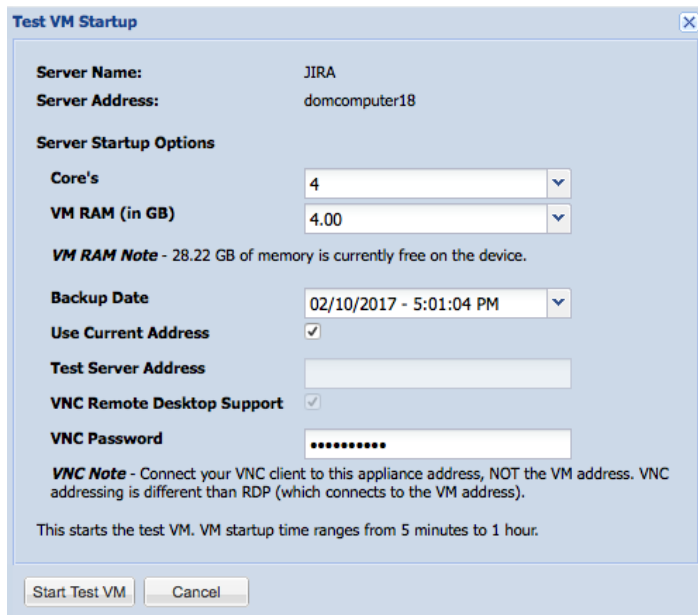


2. On the *Test VM Startup* window, update the following fields:
  - a. In the *Cores* drop-down menu, select the **number of virtual cores** to assign to the failover. Remember to leave at least 1 core for the appliance.
  - b. In the *VM RAM (in GB)* drop-down menu, select the amount of **RAM** to assign to the failover. Remember to leave at least 2GB for the appliance.
  - c. In the *Backup Date* drop-down menu, select the **date of the system image** to be used.
  - d. Select the **Use Current Address** checkbox to use the device IP address from the selected system image as the IP address of the failover VM. This allows you to test using the original address, but it disables the NIC on the test server so it cannot connect to the network. Instead, the test server is isolated to the test VM space on the Axcient appliance. It cannot communicate to devices on the real network or other test VMs.
  - e. In the *VNC Password* field, optionally configure a VNC password to be used when connecting to the VM. By default, this field is blank, meaning that a VNC password is not required.
3. When you are finished configuring settings, click the **Start Test VM** button, and then click the **OK** button to confirm. The test VM will start within 10-20 minutes on average, although you might need to wait a few hours depending on several factors, including image version, size, load, and network traffic. The most recent image will typically start more quickly than earlier versions. When the process is complete, the *Test VM Running* message displays in the *Restore Status* field.

Access the VM through the test address and verify the VM functions properly.

When the test is complete, shut down the test VM. For instructions, please reference the [Discard Virtual Machine](#) section.

*Figure 65 - Test VM Start Up Window*



The screenshot shows a window titled "Test VM Startup" with a close button in the top right corner. The window contains the following fields and options:

- Server Name:** JIRA
- Server Address:** domcomputer18
- Server Startup Options**
  - Core's:** 4 (dropdown menu)
  - VM RAM (in GB):** 4.00 (dropdown menu)
  - VM RAM Note:** 28.22 GB of memory is currently free on the device.
  - Backup Date:** 02/10/2017 - 5:01:04 PM (dropdown menu)
  - Use Current Address:** ☒
  - Test Server Address:** (empty text field)
  - VNC Remote Desktop Support:** ☒
  - VNC Password:** (password field with 8 dots)
- VNC Note:** Connect your VNC client to this appliance address, NOT the VM address. VNC addressing is different than RDP (which connects to the VM address).
- Footer text:** This starts the test VM. VM startup time ranges from 5 minutes to 1 hour.
- Buttons:** "Start Test VM" and "Cancel" at the bottom left.



## Important Test VM Notes

- You can safely run multiple test VMs set to the current address. Networking will be disabled for these VMs.
- You can log in to a current address test VM using local credentials only. Any attempt to log in using a domain account will fail because the NIC is disabled. Active Directory credentials cannot be used to log into a test VM because domain credentials are not recognized. This also applies to services that depend on Active Directory credentials. To work around this issue, enable domain credentials for the test VM. In addition, domain credentials must be enabled to shut down and restart a test VM. For more information, please reference the [Cannot Log Into Test VM](#) section of this guide.
- Set a domain controller test VM to current address only (so the NIC is disabled); do not use an alternate address for a domain controller.
- After starting a VM, it might be necessary to re-join the device to the domain.
- After starting a test VM using the current address, the **Shutdown** button in the UMC is disabled (appears gray). Such a test VM can only be shut down by issuing a shutdown command through a remote desktop connection (if RDP is enabled) or a VNC client.

## Start Virtual Machine

The Axcient appliance will not start a failover VM if the original server is still online, because it would cause a collision of IP addresses on the network.

To start a failover VM:

1. Follow the steps for either the dashboard or the device method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the **Virtual Machines & BMR** tab (see [Virtual Machine & BMR Tab](#) section).
    - b. Click the **control** button for the desired target device.
    - c. A VM/BMR Window appears. Select the *failover VM* tab and then select **start** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** option at the top of the UMC page, the icon of the target device, the image backup job, and the **failover VM** option.
    - b. The Failover VM page appears. Click the **start** button.

Figure 66 - Failover VM Page



2. The VM Startup window appears. Do the following in the indicated fields:
  - a. **Cores** - Select the number of virtual cores to assign to the failover. Remember to leave at least 1 core for the appliance.
  - b. **VM RAM (in GB)** - Select the amount of RAM to assign to the failover. Remember to leave at least 2GB for the appliance.
  - c. **Backup Date** - Select the system image to use (date of that version) from the drop-down menu.
  - d. **VNC Remote Desktop Support** - The Virtual Network Computing (VNC) feature is enabled by default. (To disable, uncheck the box.) If the device has Windows remote desktop (RDP) enabled, you can continue using it with the failover VM, and VNC support is optional. Otherwise, the only connection option is through VNC. VNC must be enabled here; it cannot be enabled after the VM is started.
  - e. **VNC Password** (optional) - To require a VNC viewer password when connecting to the VM, enter the password in this field. By default, it is blank, which means no VNC password is required.

Figure 67 - Failover VM Start Page

The screenshot shows a 'VM Startup' dialog box with the following fields and options:

- Server Name:** Server 2003
- Server Address:** domcomputer2003
- Server Startup Options**
  - Core's:** 4 (dropdown menu)
  - VM RAM (in GB):** 4.00 (dropdown menu)
  - VM RAM Note:** 28.22 GB of memory is currently free on the device.
  - Backup Date:** 03/04/2015 - 11:00:27 AM (dropdown menu)
  - VNC Remote Desktop Support:** ☒
  - VNC Password:** [Redacted with dots]
  - VNC Note:** Connect your VNC client to this appliance address, NOT the VM address. VNC addressing is different than RDP (which connects to the VM address).
- Footer text:** This starts the VM. VM startup time ranges from 5 minutes to 1 hour.
- Buttons:** Start VM, Cancel

## Important Failover VM Notes

- The IP address (or host name) to use when accessing the VM differs for RDP and VNC. Use the server IP address for RDP. Use the Axcient appliance IP address for VNC.
- Even after the VM status is listed as online, Windows performs hardware detection processing that can delay the server bring up for several more minutes. Network issues can delay this further. In addition, when accessing the VM through VNC, the mouse and keyboard drivers are loaded last, which can require several more minutes before you can use them through a VNC viewer.
- Windows treats a VM as new hardware. Therefore, when accessing the VM (through RDP or VNC), a Windows Product Activation message might appear indicating you must activate Windows on this hardware within a specified number of days. Click the Yes button to display an activation page and follow the instructions. (See the Windows documentation for more information.) If the VM will be stopped in less than the specified number of days, click the No button.
- If the server hosts Exchange, Exchange might not start properly when the VM starts, which requires that you manually start some Exchange services.
- After starting a VM, it might be necessary to re-join the device to the domain.
- When a VM is brought up for the first time, Windows might reinstall various drivers and prompt for a reboot. Do not reboot (or perform any other action) until the AxSvc service or process exits. Sometimes it is necessary to restart the VM to make the changes effective.

## Failover VM Configuration Fields and Descriptions

Field	Definition
Backup Status	Indicates whether there is a VM image available: <ul style="list-style-type: none"> <li>• If the image backup job has not run for the first time, the status is Not Done.</li> <li>• If at least one version is available, the status is Complete.</li> </ul>
Date of Last Backup	Lists the finish time of the last image backup job. <b>Form</b> - mm/dd/yyyy - hh:mm:ss AM/PM <b>Example</b> - 03/20/2009 - 11:09:37 AM
Server Online Status	Displays whether the protected device is online or offline. <b>Note</b> - The VM will not start if the device is alive (that is, Server Online Status is online).
Restore Status	Indicates whether a VM or BMR is active for this protected computer: <ul style="list-style-type: none"> <li>• <b>Idle</b>—No active VM or BMR operation. (The image job is unlocked.)</li> <li>• <b>VM/BMR Starting</b>—The operation (failover VM, test VM, or BMR) is initializing.</li> <li>• <b>VM Running</b>—The failover or test VM is running.</li> <li>• <b>VM Pausing</b>—The failover or test VM was shutdown. (All data is preserved.) The VM can be restarted.</li> <li>• <b>VM Resuming</b>—A shutdown failover or test VM is being restarted.</li> <li>• <b>VM Starting BMR</b>—A BMR is starting using the VM image. (The VM is shutdown while the BMR runs.)</li> <li>• <b>BMR Started</b>—A BMR is in progress. (The image job is locked, and a VM cannot run during this period.)</li> <li>• <b>BMR Stopping</b>—The BMR operation is stopped, and the image job resumes.</li> <li>• <b>BMR Starting VM</b>—The BMR operation is stopped, and the shutdown VM restarts. (This option applies only if the BMR was initiated through a VM Starting BMR action.)</li> </ul>
Start button	Click this button to display the VM Startup window (see the following entries in this tab).

Field	Definition
	<b>Note</b> Image jobs are suspended when a failover or test VM is started.
Shutdown button	Click this button to shutdown a running VM. This shuts down the VM but saves the data. The image job remains suspended. You can restart this VM as a later time (see <a href="#">Shutdown and Restart Virtual Machine</a> section).
Restart button	Click this button to restart a previously shutdown VM (see <a href="#">Shutdown and Restart Virtual Machine</a> section).
Discard button	Click this button to shutdown the VM and resume the image backup job. Data changes while the VM was active are discarded (see <a href="#">Discard Virtual Machine</a> section).
Bare Metal Restore button (Failover VM only)	Click this button to shutdown the running VM (saving the data) and start a BMR using the latest VM image (see <a href="#">BMR Virtual Machine</a> section).

### VM Start Window Fields and Definitions

Field	Description
Server Name	Displays the alias name of the device. If no alias was specified when the device was added, displays the server address.
Server Address	Displays the IP address or host name of the protected device.
VM Size	<p>Select the amount of memory to use for the VM. Running VMs compete with each other and active backup jobs for system memory. This field allows you to allocate how much of the available memory should be allocated to this VM while it is running. The available options are dynamically determined at run time starting at a minimal amount (512 MB) and going up in 256 MB increments to a maximum value. The available values vary by Axcient appliance model and the current memory usage.</p> <p>The allocated memory is reserved while the VM is active. When the VM is shutdown (shutdown or discard button), the memory is released. Several factors affect memory use (number/size of active backup jobs, additional VMs, other running services), so tuning for optimal performance might be necessary. If this will be the only running VM, the following memory is recommended:</p> <ul style="list-style-type: none"> <li>tower, 1-U, or 2-U appliance: 4096 (4 GB)</li> <li>set top appliance: 1536 (1.5 GB)</li> </ul>
Backup Date	Sets which system image to use. Select the target image (date of the desired version) from the pull-down list.
VNC Remote Desktop Support	<p>Enables Virtual Network Computing (VNC) support. If VNC remote desktop support is enabled, the newly started VM supports VNC client viewers. VNC is a remote protocol that provides similar functionality to the Microsoft Remote Desktop Protocol (RDP).</p> <p><b>Note:</b> When logging in to the VM through VNC, use the IP address or host name of the Axcient appliance, not the original server IP address. If multiple VMs are running, include the VNC port number in the IP address. The first VM uses the default VNC port number, which is 5900. Subsequent VMs increment the port number by one (5901, 5902, and so on). For example, if an Axcient appliance with an IP address of 192.168.77.26 is running two VMs, enter 192.168.77.26:5900 for the first VM and 192.168.77.26:5901 for the second VM.</p>
VNC Password	Sets a password when connecting to the VM through VNC. If this field is left blank (default value), the VNC client will not require a password.

## Discard Virtual Machine

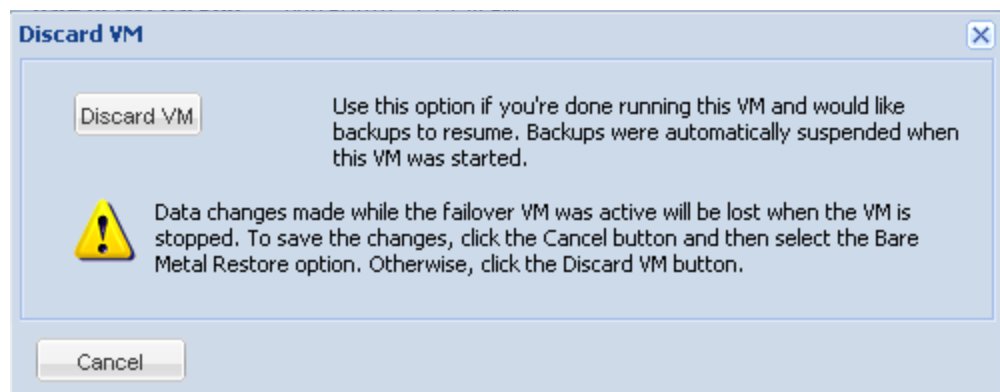
“Discarding” a VM means that the VM is shutdown and cannot be restarted. All data changes while the VM was running are discarded. (You can start a new VM, but the new VM will not reflect any changes made in the previous VM.) To discard a running or shutdown failover (or test) VM:

1. Follow the steps for either the dashboard or devices method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the Virtual Machines & BMR tab (see [Virtual Machine & BMR Tab](#) section).
    - b. Click the **control** button for the desired target device.
    - c. A VM/BMR window appears. Select the *failover VM* (or test VM) tab, and then select **discard** from the drop-down menu
  - Devices method:
    - a. Click the **devices** button, then the icon of the target device, then the desired image backup job, and finally the **failover VM** (or **test VM**) option.
    - b. The Failover VM or Test VM page appears. Click the **discard** button.
2. The Discard VM window appears. Click the **Discard VM** button. A status window appears while the VM is shutting down. When the “failover [test] VM has shutdown” message appears, click the **OK** button to close the window. The image backup job is restarted and runs normally again.

### Caution!

Data changes made while the failover VM was active will be lost when the VM is stopped. To save the changes, click the **Cancel** button and instead do a BMR of the VM (see [BMR Virtual Machine](#) section) or save the data in another way before discarding the VM (see [View Virtual Machine and BMR Status](#) section).

Figure 68 - Stop VM Window



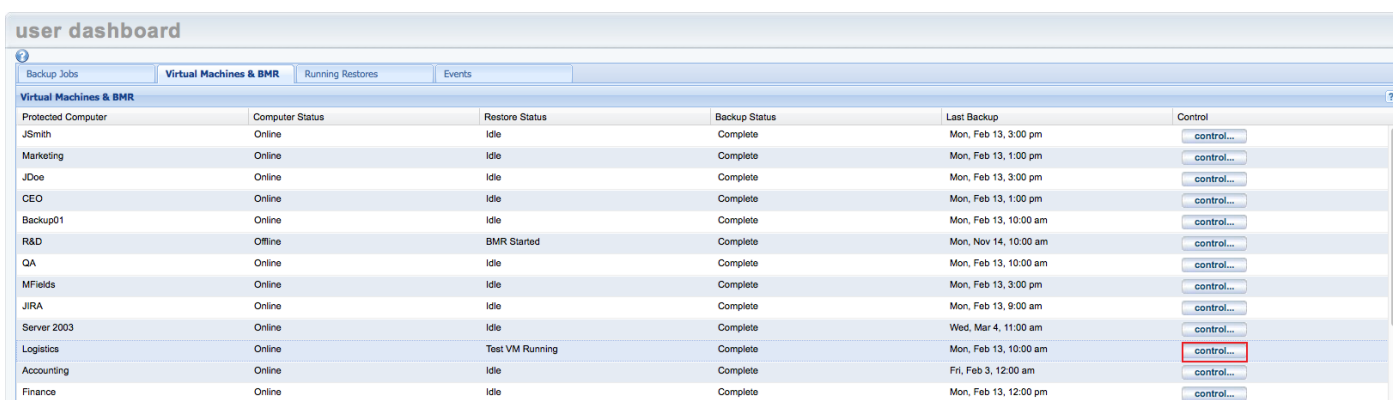
## Edit Running Failover

In some cases, you may need to edit the amount of resources allocated to either a test or production local failover. You can edit certain VM configuration settings without needing to discard and re-enable the VM. For example, you can increase or decrease VM resources, such as CPU cores and memory.

To edit the running failover:

1. On the UMC Dashboard, click the **Virtual Machines & BMR** tab and click the **Control** button for the running failover VM.

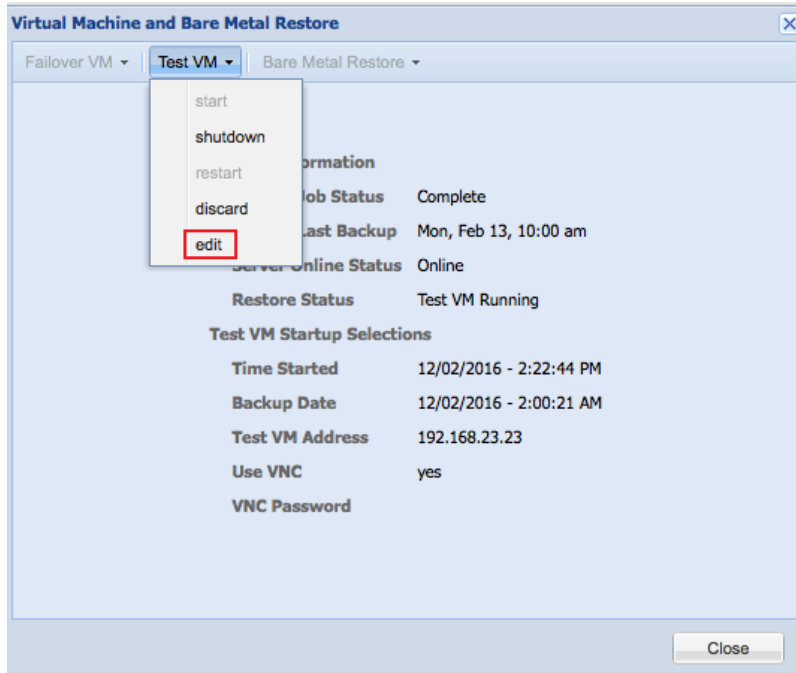
**Figure 69** - Press Control



Protected Computer	Computer Status	Restore Status	Backup Status	Last Backup	Control
JSmith	Online	Idle	Complete	Mon, Feb 13, 3:00 pm	control...
Marketing	Online	Idle	Complete	Mon, Feb 13, 1:00 pm	control...
JDoe	Online	Idle	Complete	Mon, Feb 13, 3:00 pm	control...
CEO	Online	Idle	Complete	Mon, Feb 13, 1:00 pm	control...
Backup01	Online	Idle	Complete	Mon, Feb 13, 10:00 am	control...
R&D	Offline	BMR Started	Complete	Mon, Nov 14, 10:00 am	control...
QA	Online	Idle	Complete	Mon, Feb 13, 10:00 am	control...
MFields	Online	Idle	Complete	Mon, Feb 13, 3:00 pm	control...
JIRA	Online	Idle	Complete	Mon, Feb 13, 9:00 am	control...
Server 2003	Online	Idle	Complete	Wed, Mar 4, 11:00 am	control...
Logistics	Online	Test VM Running	Complete	Mon, Feb 13, 10:00 am	control...
Accounting	Online	Idle	Complete	Fri, Feb 3, 12:00 am	control...
Finance	Online	Idle	Complete	Mon, Feb 13, 12:00 pm	control...

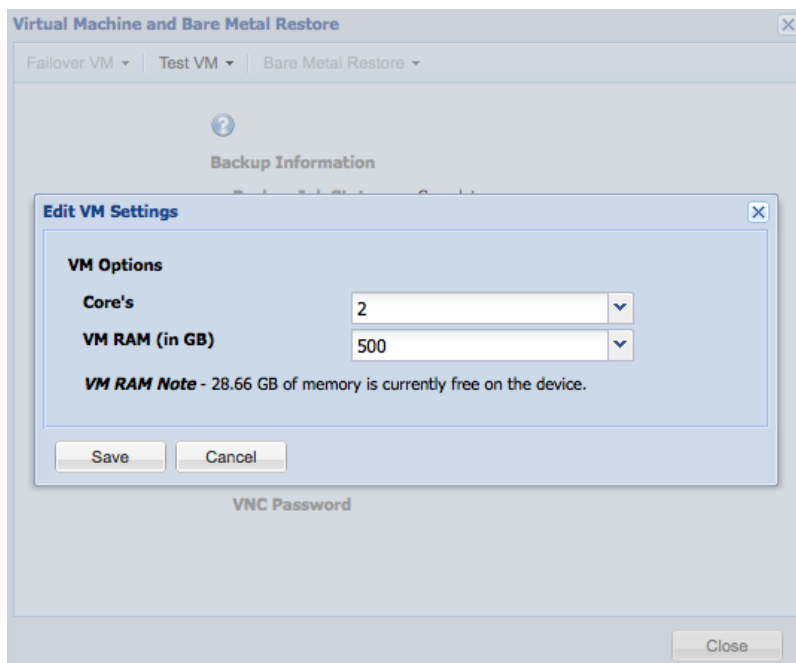
2. The *Virtual Machine and Bare Metal Restore* page will appear. Click the VM menu option in the top navigation menu (in this example, **Test VM**) and press the **Edit** option.

**Figure 70** - Press Edit



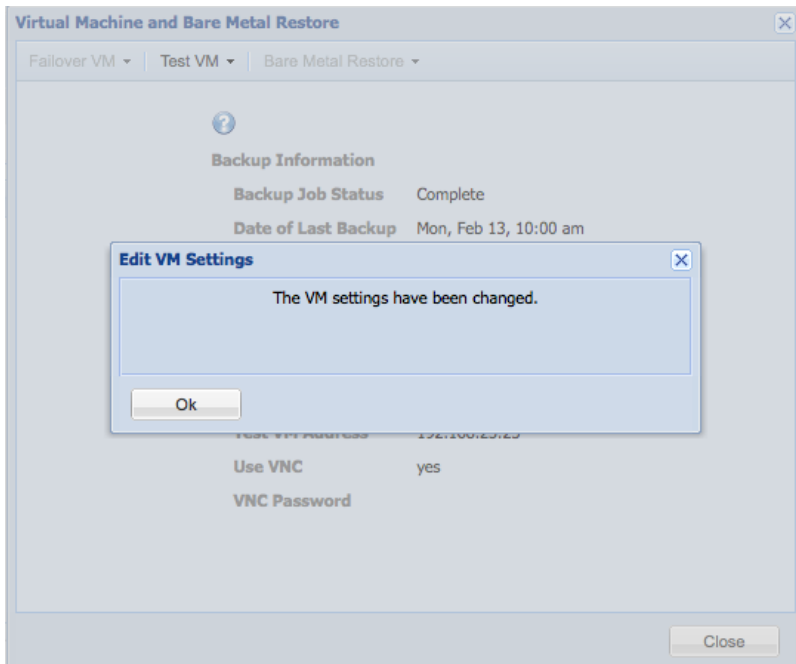
3. You will have the option to edit the *Core CPUs* field and the *VM RAM* field. Click the **Save** button when you are finished.

**Figure 71** - Edit VM Settings



4. You will be prompted with a notification stating the VM settings have been changed. Click **OK** to continue.



**Figure 72** - Backup Jobs Page

## BMR Virtual Machine

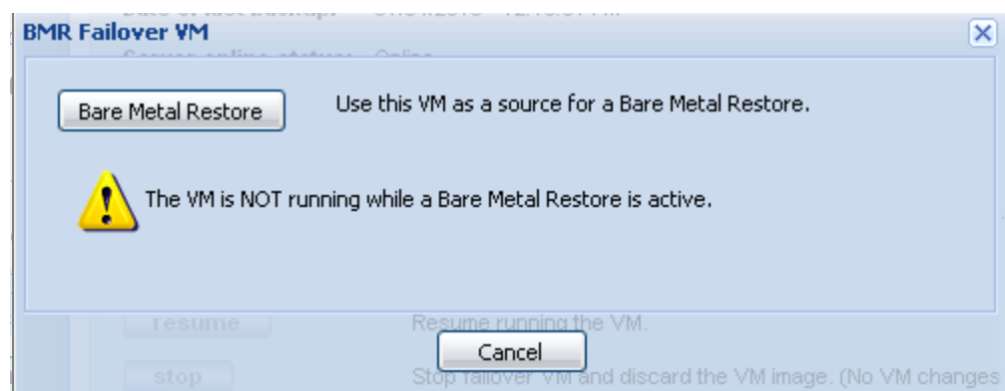
The VM can be restored on new hardware through BMR.

When a failover VM is started, revision files are stored in a folder named *axcient\_temp\_dir* that is located in the root folder of every volume (for example, *C:\axcient\_temp\_dir*). The size of an *axcient\_temp\_dir* folder can be substantial, and this folder is not needed for BMR. Therefore, it is recommended that you delete this folder in each volume before attempting a BMR. (While the VM is still running, open a window using either RDP or VNC, and delete the folder.) This will reduce the time required to download files from the Axcient appliance to the target device. If the *axcient\_temp\_dir* folders are not deleted prior to doing a BMR, it is recommended that you delete them from the target device after that device is up and running.

To BMR the latest VM image:

1. Follow the steps for either the dashboard or device method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the Virtual Machines & BMR tab (see [Virtual Machine & BMR Tab](#) section).  
  
Click the **control** button for the desired target device.
    - b. A VM/BMR window appears. Select the *failover VM* (or test VM) tab, and then select **bare metal restore** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** button, then the icon of the target device, then the desired image backup job, and finally the failover VM option.
    - b. The *Failover VM* page appears. Click the **bare metal restore** button.
2. The *BMR Failover VM* window appears. Click the **Bare Metal Restore** button. A status window appears while BMR is processing. (This step typically takes just a few minutes, but it could be 10 minutes or longer if the Windows shutdown that is part of this process takes a long time.) When the “Bare Metal Restore from VM has successfully completed” message appears, click the **OK** button to close the window.

Figure 73 - BMR Failover VM Window



3. Restore the VM image onto a new device (see [Restore Device Using BMR Recovery Disk](#) section).
4. Either discard or restart the VM (see [Stop BMR](#) section).

## Shutdown and Restart Virtual Machine

The VM sometimes shuts down and restarts as part of other actions (such as when doing a BMR from the VM), but you can manually shutdown or restart a VM at any time:

- **Shutdown**—Shuts down the running VM while preserving the data. This is equivalent to invoking the shutdown command from within the VM (through RDP or VNC).
- **Restart**—Restarts the VM and brings it back online. A restart is necessary after the VM was shutdown through the UMC or from within the VM. This is equivalent to rebooting the system.

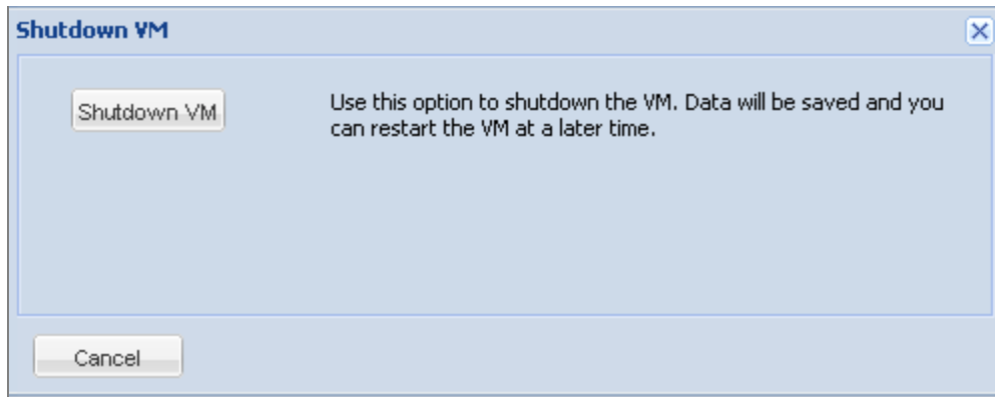
## Shutdown VM

To shutdown a failover (or test) VM:

1. Follow the steps for either the dashboard or devices method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the Virtual Machines & BMR tab (see [Virtual Machine & BMR Tab](#) section).
    - Click the **control** button for the desired target device.
    - A VM/BMR window appears. Select the *failover VM* (or *test VM*) tab, and then select **shutdown** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** button, then the icon of the target device, then the desired image backup job, and finally the **failover VM** (or **test VM**) option.
    - b. The Failover VM or Test VM page appears. Click the **shutdown** button.
2. The *Shutdown VM* window appears. Click the **Shutdown VM** button. A status window appears while the VM shuts down. When the “VM has been Shutdown” message appears, click the **OK** button to close the window.

The **Shutdown** button in the UMC is disabled (appears gray) for a test VM that is set to use the current IP address of the device. Such a test VM can only be shut down by issuing a shutdown command through a remote desktop connection (if RDP is enabled) or a VNC client (see [Virtual Network Computing \(VNC\) Usage](#) section).

*Figure 74* - Shutdown VM Window



## Restart VM

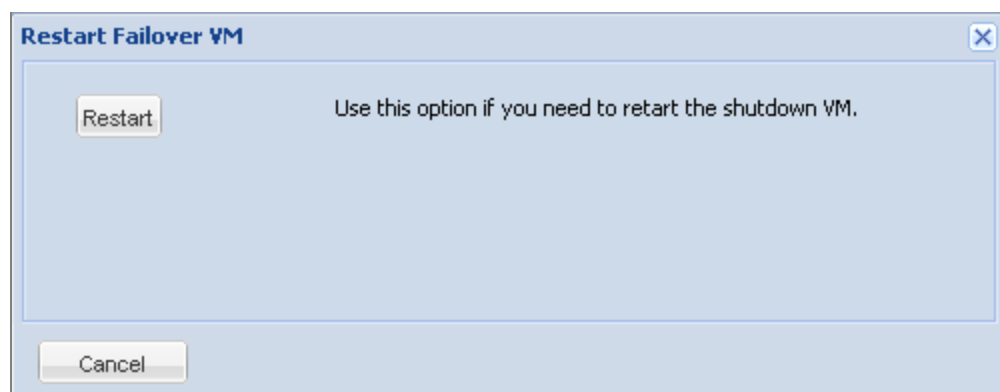
To restart a failover (or test) VM:

1. Follow the steps for either the dashboard or devices method:
  - Dashboard Method
    - a. Click the **dashboard** button at the top of the UMC page, and then select the Virtual Machines & BMR tab (see [Virtual Machine & BMR Tab](#) section).

Click the **control** button for the desired target device.

A VM/BMR window appears. Select the *failover VM* (or *test VM*) tab, and then select **restart** from the drop-down menu.
  - Devices Method
    - a. Click the **devices** button, then the icon of the target device, then the desired image backup job, and finally the **failover VM** (or **test VM**) option.
    - b. The Failover VM or Test VM page appears. Click the **shutdown** button.
2. The *Shutdown VM* window appears. Click the **Restart** button. A status window appears while the VM shuts down. When the “VM has been Shutdown” message appears, click the **OK** button to close the window.

Figure 75 - Restart VM Window



## View Virtual Machine and BMR Status

Image job, failover VM, test VM, and BMR status information is available through one of the following methods:

### Dashboard Method

1. Click the **dashboard** button at the top of the UMC page, and then select the Virtual Machines & BMR tab (see [Virtual Machine & BMR Tab](#) section).
2. Status information is displayed for each device with an image backup job, and additional information is displayed by clicking the associated **control** button.

### Devices Method

1. Click the **devices** button, then the icon of the target device, and then the desired image backup job.
2. Select the **failover VM**, **test VM**, or **bare metal restore** option to display the appropriate page. A *status information* section appears at the top of each page.

# System Management

## Set Networking Parameters

Network parameters were specified during installation. However, you can reset any of these parameters should the value change after installation.

To reset network parameters:

1. Click the **system** tab at the top of the UMC page and then click the **network settings** option in the left navigation menu.
2. The *Networking* page appears. To change a value, do the following in the indicated parameter fields. See the table below for detailed parameter descriptions.
  - **IP Address** - Enter the Axcient appliance IP address.
  - **Subnet Mask** - Enter the subnet mask value.
  - **Default Gateway** - Enter the IP address for the gateway.
  - **Domain** - Enter the domain name.
  - **Workgroup** - Enter the workgroup name.
  - **DNS Server** - Enter the IP address for the DNS server.
  - **Hostname** - Enter the Axcient appliance host name.
  - **Secondary DNS Server** - Enter the IP address of an alternate DNS server to be used when the primary one is not available.
  - **Tertiary DNS Server** - Enter the IP address of an alternate DNS server to be used when both the primary and secondary ones are not available.
3. When all parameter values are correct, click the **save** button.



Figure 76 - Networking Parameters Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system

**system**

- network settings
- quality of service
- date and time
- offsite configuration
- SNMP

## Networking

Settings for the network ?

IP address: 192.168.77.219 \*

Subnet mask: 255.255.255.0 \*

Default gateway: 192.168.77.1 \*

Domain: axcient.inc \*

Workgroup: WORKGROUP \*

Primary DNS Server: 192.168.44.22 \*

Hostname: ShravyaVAPP \*

Secondary DNS Server: 192.168.44.10 \*

Tertiary DNS Server: 192.168.44.10 \*

cancel save

## Networking Parameters Fields and Definitions

Field	Description
IP Address	Specifies the IP address for the Axcient appliance. (The default value is usually changed during installation.)
Subnet Mask	Specifies the mask value for the subnet on which the Axcient appliance resides.
Default Gateway	Specifies the IP address for the default gateway used by the Axcient appliance. (The default value is usually changed during installation.)
Domain	Specifies the name of the domain in which the Axcient appliance resides. (The default value is usually changed during installation.)
Workgroup	Specifies the name of the workgroup in which the Axcient appliance resides. (The default value is usually changed during installation.)
DNS Server	Specifies the IP address for the primary DNS server used by the Axcient appliance. (The default value is usually changed during installation.)
Hostname	Specifies the host name assigned to the Axcient appliance. (The default value is usually changed during installation.)
Secondary DNS Server	Specifies the IP address for an alternate DNS server for the Axcient appliance when the primary DNS server is not available.
Tertiary DNS Server	Specifies the IP address for an alternate DNS server for the Axcient appliance when both the primary and secondary DNS servers are not available.

## Set Bandwidth Usage (Quality of Service)

Network and system performance can be affected when the Axcient appliance is doing a backup or restore. Bandwidth used for backup or restore operations is not available for other business uses. As with all tuning issues, assess your business requirements to determine an optimal balance. It is common to enforce bandwidth throttling during regular business hours and then turn off throttling during off hours such as at night or on weekends. Another factor to consider is how time critical the operation. Backups are normally a part of routine maintenance and are rarely time critical. In contrast, restore operations are typically done on-demand to retrieve lost data. Such operations often have high priority and are time critical. As a result, you might choose to allocate higher bandwidth to restore operations than to backup operations.

To control the impact of backup and restore operations, you can configure the amount of bandwidth allocated to the Axcient appliance. You can specify separate bandwidth throttling speeds for the following operations:

- *Internet Connection*
  - **External Service Upload**—Sets the bandwidth limit from the Axcient appliance to the Axcient data center (backup operations).
- *Local Network Connection*
  - **Internal Service Download**—Sets the bandwidth limit from the Axcient appliance to a device (restore operations).
  - **Internal Service Upload**—Sets the bandwidth limit from a device to the Axcient appliance (backup operations).

By default, Axcient does not limit bandwidth throttling (unlimited). To change any setting:

1. Click the **system** tab at the top of the UMC page and then select the **quality of service** option.

The *Quality of Service* page displays.

2. To reset one or more rate limits, enter the desired speed in Mbps (see the table below for field descriptions). A value of zero (0.0) indicates that bandwidth throttling is disabled (no limit).
3. Click the **save** button.
4. A line for each day of the week displays under the *Business Hours* heading (lower portion of page). To specify business hours:
  - a. Select a **day** and specify the business hour **start** and **stop** times from the drop-down lists. Hour values are 1-23 (1am to 11pm), minutes 00-59. Select the blank value (no number) for both start and stop to indicate no business hours.
  - b. Click the **save** button.

### Caution!

If you create image replication jobs (see [Back Up System Images](#) section), setting the local network connections (internal service download and upload) below the default 1000 Mbps is not recommended. The image job will still run at a lower speed, but performance may be unacceptably slow.

#### Notes

If the start time is later than the stop time, then the stop time is the next day. For example, if Monday start time is 23:00 and the stop time is 5:00, then the business hours are considered to be from 11:00pm Monday until 5:00pm Tuesday.

You will get an error message if the start time of the following day is earlier than the stop time set for the previous day when the schedule spans midnight. For example, a Tuesday start time of 4:00pm produces an "invalid" message when attempting to save if the Monday stop time is 5:00pm on Tuesday (as in the previous bullet note).

Figure 77 - Quality of Service Page

## Quality of Service

Settings for network-bandwidth control.

**Maximum bandwidth allowed: 1000Mb/s**  
**Enter 0 to disable bandwidth control.**

External service upload rate limit business hours (Mbps):  \*

External service upload rate limit non-business hours (Mbps):  \*

Internal service download rate limit business hours (Mbps):  \*

Internal service download rate limit non-business hours (Mbps):  \*

Internal service upload rate limit business hours (Mbps):  \*

Internal service upload rate limit non-business hours (Mbps):  \*

### Business Hours

Select the start/stop time of your business hours.  
 Note: If you leave the selection blank, your non business hour bandwidth setting listed above will be used.

**Sun** Start:  :  :  Stop:  :  :

**Mon** Start:  :  :  Stop:  :  :

**Tue** Start:  :  :  Stop:  :  :

**Wed** Start:  :  :  Stop:  :  :

**Thu** Start:  :  :  Stop:  :  :

**Fri** Start:  :  :  Stop:  :  :

**Sat** Start:  :  :  Stop:  :  :

## Quality of Service Fields and Definitions

Field	Description
External Service Upload Rate Limit <i>Business Hours</i>	Sets the bandwidth from the Axcient appliance to the Axcient data center (backup operations) during business hours. Backup operations are typically not time critical, so consider balancing (reducing) this value with the other business interests that share the available external bandwidth. (A value of zero disables bandwidth throttling.)  <b>CAUTION:</b> If you have any image backup jobs (see <a href="#">Back Up System Images</a> section), do not set bandwidth throttling below the default of 1000 Mbps (1 Gbps). A lower setting will cause unacceptable performance degradation for an image backup job. This caution applies to all the bandwidth throttling parameters.
External Service Upload Rate Limit <i>Non-Business Hours</i>	Sets the bandwidth from the Axcient appliance to the Axcient data center (backup operations) during non-business hours. By default, bandwidth throttling is disabled (zero value) during non-business hours.
Internal Service Download Rate Limit <i>Business Hours</i>	Sets the bandwidth from the Axcient appliance to a device (restore operations) during business hours. Restore operations are often time critical, so consider allowing a large value for this operation at the possible expense of other business interests that share the local network bandwidth. (A value of zero disables bandwidth throttling.)
Internal Service Download Rate Limit	Sets the bandwidth from the Axcient appliance to a device (restore operations) during non-business hours. By default,

Field	Description
<i>Non-Business Hours</i>	bandwidth throttling is disabled (zero value) during non-business hours.
Internal Service Upload Rate Limit <i>Business Hours</i>	Sets the bandwidth from a device to the Axcient appliance (backup operations) during business hours. Backup operations are typically not time critical, so consider balancing (reducing) this value with the other business interests that share the local network bandwidth. (A value of zero disables bandwidth throttling.)
Internal Service Upload Rate Limit <i>Non-Business Hours</i>	Sets the bandwidth from a device to the Axcient appliance (backup operations) during non-business hours. By default, bandwidth throttling is disabled (zero value) during non-business hours.

## Set Time Zone

### Caution!

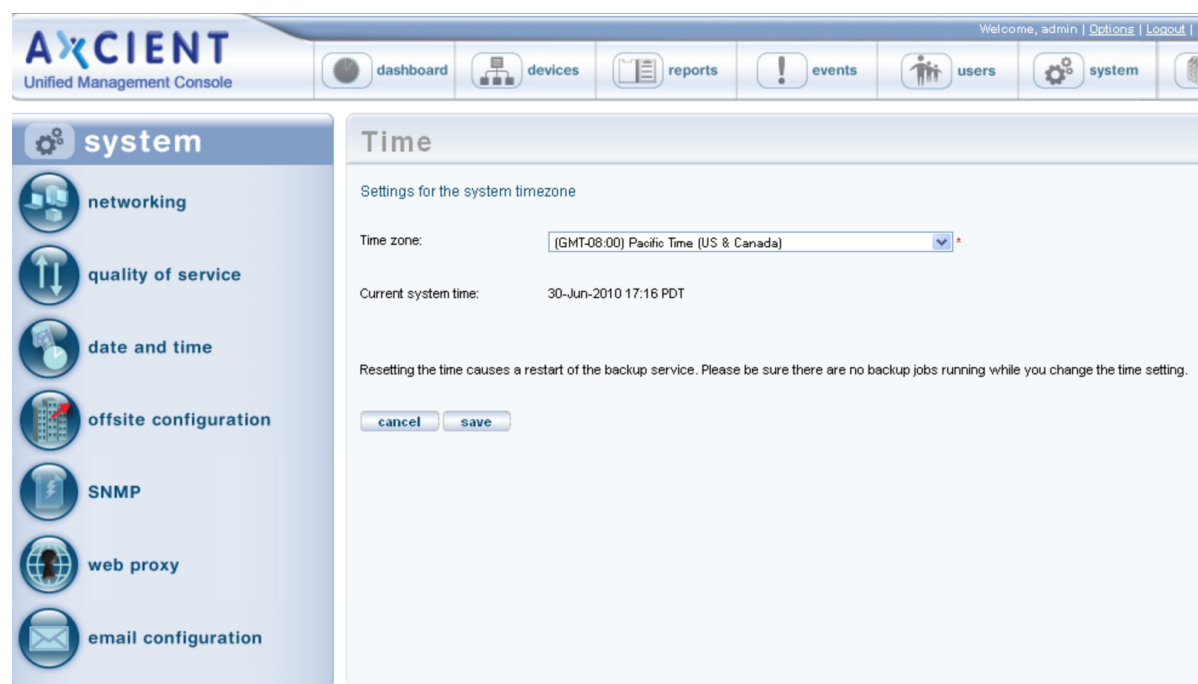
Resetting the time zone restarts the backup service. Do not change the time zone while any backup jobs are in progress, because this can could cause an active backup job to fail with unpredictable results and possible data corruption.

The Axcient appliance automatically sets its clock through an appropriate NTP server. However, you can specify what time zone to use. To set the time zone:

1. Click the **system** tab at the top of the UMC page and select the **date and time** option in the left navigation menu.
2. The *Time* page appears. Select the desired time zone from the drop-down menu in the *Time Zone* field.
3. Click the **save** button.

The current time appears directly below the Time Zone field. Use this to verify that the time zone changed correctly.

**Figure 78** - Time Page



## Configure SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. The Axcient appliance includes an SNMP agent that provides interoperability with industry standard SNMP manager systems. The Axcient SNMP agent includes support for two levels of information:

- Industry standard MIB-II support, which includes machine-level information such as network interfaces, machine temperature, and CPU information.
- Custom MIB support for Axcient-specific information, including Axcient version identifiers, backup job definitions, backup job results, and backup events or traps. The custom MIB (AXCIENT-BACKUP-MIB) includes the following fields within each group category:
  - *Version Information* fields identify Axcient revision levels. The fields are serial number, service ID, MAC address, software revision, IP address, subnet mask, gateway, and DNS server.
  - *Backup Jobs Information* fields describe the backup jobs and fall into two categories:
    - *Job Information* fields, which define the job, including name, type, schedule, offsite status, retention method, creator, user, and device information.
    - *Results Information* fields, which describe results from the last successful run of each backup job, including time, size, file (count, new, changed, deleted), and error statistics.
  - *Storage Statistic* - Fields in this category provide onsite and offsite storage usage information.
  - *SNMP Traps* - Trap types are sent by the Axcient appliance to indicate significant events. The most representative (and important) class of traps indicate the success or failure of backup jobs. The identifiers used for this subset of traps are *BACKUP\_STARTED*, *BACKUP\_WARNING*, *BACKUP\_SUCCEEDED*, and *BACKUP\_FAILED*.

Axcient implements the following MIBs:

- *AXCIENT-BACKUP-MIB* (custom)
- *MIB-II* (RFC 1213)
- *HOST-RESOURCES-MIB* (RFC 2790)

To configure SNMP for your Axcient appliance:

1. On the UMC, click the **system** tab. The *Configuration Summary* page displays.
2. Select the **SNMP** option on the left navigation menu.
3. On the *SNMP Settings* page, configure the following fields:
  - In the *Read Community* field, enter the SNMP community name, which allows read-only access (the default is *public*).
  - In the *Trap Sink* field, enter the trap receiver system IP address or name. If a port number is not specified, the standard SNMP manager port (162) is used. To specify an alternate port or an additional address, enter the IP address(es) in the following format:  
*xxx.yyy.zzz.aaa[:port#] [, ...]*
  - In the *Trap Sink Community* field, enter the community name to be included in trap messages sent by the SNMP agent (the default is *public*).
  - Select the **Use Inform Notifications** checkbox to use inform requests instead of traps as the SNMP notification method (the default is *traps*).
  - Select the **Use V1 Traps** checkbox to use SNMP version 1 (SNMPv1) instead of version 2 (the default is *SNMP Version 2*). This field is ignored if the *Use Inform Notifications* option is selected. Please reference the table below for more information.
  - Select the **Enable SNMP** checkbox to enable SNMP functionality (disabled by default).
4. Click the **save** button when you are finished.
5. Download the Axcient MIB. Right-click the *Axcient MIB link* and select **Save Link As** to download the Axcient MIB as a text file. The file name is *AXCIENT-BACKUP-MIB.txt*.
6. Copy the Axcient MIB (and the two standard MIBs if they are not already present) to the appropriate location on the SNMP manager system.

The SNMP page includes a table at the bottom that lists all defined jobs and their internal ID numbers. These values correspond to the *jobName* and *jobId* parameters in the Axcient MIB. Please reference the [Backup Jobs Information](#) section for more information.

The first three jobs listed in the table—*Offsite Backup*, *Alert Digest*, *Usage History*—are system jobs that always display. Any additional entries in the table are the jobs that you create. Please note that *Offsite Backup* only applies to scheduled offsite backup jobs and not offsite backup jobs performed through unbundled offsites.

If using unbundled offsites (i.e running an offsite replication immediately after the local job has completed), then there will be two internal IDs. One ID will be for the local job and the other ID will be for the offsite. These IDs are titled accordingly.



Figure 79 - SNMP Page

**system**

network settings

quality of service

date and time

offsite configuration

**SNMP**

web proxy

### SNMP Settings

Settings for the SNMP management agent. Download the [Axcient MIB](#)

Read community:

Trap sink:

Trap sink community:

Use inform notifications (trap is default): ☐

Use V1 traps (V2 is default): ☐

Enable SNMP: ☐

Schedule Name	Index
OffSite Backup	1
Alert Digest	2
Usage History	3
Image2003	4
Image2008r2	5

## SNMP Settings Fields and Definitions

Fields	Descriptions
Read Community	Sets the SNMP community name for read-only access. SNMP uses community names somewhat like passwords. They are exchanged in clear text in communications between the agent and its clients. All requests to the agent must contain a community name, which the agent compares against the one specified here to determine permissions and capabilities. By default, the SNMP agent sets up a single read-only community, named <i>public</i> , and all incoming requests must include <i>public</i> as the community name. These read-only requests can retrieve the values of variables only.
Trap Sink	<p>Specifies the IP address or system name of the client system to receive trap messages. This is normally the system on which the SNMP manager application resides. By default, Axcient assigns the standard port (162) for an SNMP manager, but you can specify an alternate port number by adding it to the end of the IP address. You can also specify additional addresses as a comma separated list.</p> <p><b>Format</b></p> <p><i>xxx.yyy.zzz.aaa[:port#] [, ...]</i></p> <p><b>Examples</b></p> <ul style="list-style-type: none"> <li>• <i>192.168.77.120</i> (uses default port 162)</li> <li>• <i>192.168.77.120:299</i> (uses alternate port 299)</li> </ul>
Trap Sink Community	<p>Sets the trap community name. This community name is used by the agent. It is included in trap messages that the agent sends.</p> <p>The Read Community value is sent by the clients and read by the agent, while the Trap Sink Community value is sent by the agent and read by the clients. Although both are set to the same value (<i>public</i>) by default, the two community values are independent and can be different.</p>
Use Inform Notifications	<p>Sets message passing to use inform notifications instead of traps. (The default is <i>traps</i>.)</p> <p>SNMP notifications can be sent as traps or inform requests. Traps are one-way transmissions; they do not require an acknowledgment from the receiver. Informs expect a response. If the sender never receives a response, the inform request can be sent again. Therefore, informs are more reliable than traps. However, informs consume more resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Additionally, traps are sent only once, while an inform may be retried several times. These retries increase traffic and add overhead on the network. Therefore, traps and inform requests provide a trade-off between reliability and resources.</p>
Use V1 Traps	<p>Sets SNMP support to version 1 (SNMPv1). The default is SNMP version 2 (SNMPv2). Use version 2 unless you have a specific need for version 1.</p> <p><b>Note:</b> This field is ignored if the <i>Use Inform Notifications</i> checkbox is selected.</p>
Enable SNMP	Enables SNMP functionality. This field is disabled by default.

## Configure Web Proxy

The Axcient appliance can work in conjunction with a web proxy. To configure the Axcient appliance for a web proxy server:

1. Click the **system** tab at the top of the UMC page and select the **web proxy** option in the left navigation menu.
2. The *Web Proxy* page appears. Do the following in the indicated fields:
  - **Web proxy host** - Enter the web proxy host IP address or name.
  - **Web proxy port** - Enter the port number used for the web proxy.
  - **Basic authentication** - Check the box to enable basic authentication. (Authentication is not enabled by default.)
  - **Username** - Enter a user name. (This applies only when Basic Authentication is checked).
  - **Password** - Enter the password for the user specified in the previous step.
  - **Use pre-backup ping** - This box is checked (on) by default. Do not change unless the **ping** command is explicitly blocked in your environment.
  - **Windows Default RPC Timeout (minutes)** - Do not change. (Default is 15 minutes.)
  - **Windows VShadow Timeout (minutes)** - Do not change. (Default is 90 minutes.)
3. When all fields are correct, click the **save** button.

After clicking **save**, the Axcient appliance attempts to connect to the Web Application as a test of Internet access using the web proxy settings. The message “Your settings have been saved” appears if the test is successful, but an error message appears if the Axcient appliance could not connect to the Web Application. If an error message appears, verify the web proxy settings are correct. If they are correct, check for other possible reasons the Web Application connection failed. See the [Axcient Error Messages Manual](#) for more information.

Figure 80 - Web Proxy Page

**Axcient**  
Unified Management Console

Welcome, admin | [Options](#) | [Logout](#)

**system**

- networking
- quality of service
- date and time
- offsite configuration
- SNMP
- web proxy**
- email configuration

### Web Proxy

Settings for a web proxy that is used for outgoing calls to RMC

Web proxy host:

Web proxy port:

Basic authentication: ☐

Username:

Password:

Use pre-backup ping: ☒

Windows Default RPC Timeout (minutes):

Windows VShadow Timeout (minutes):

### Web Proxy Fields and Definitions

Field	Descriptions
Web Proxy Host	Specifies the IP address or system name of the web proxy host server.
Web Proxy Port	Specifies the port number used for the web proxy on the host server.
Basic Authentication	Enables the basic authentication mechanism. By default, authentication is not enabled. The <b>Username</b> and <b>Password</b> fields are relevant (active) only when authentication is enabled.
Username	Specifies the user name to be authenticated by the web proxy server. (The proxy user has no relation to the administrative user entered when adding the device.)
Password	Specifies the password for the user in the <b>Username</b> fields.
Use Pre-backup Ping	<p>Sets an ICMP request (<b>ping</b> command) to occur prior to a backup job run. The <b>ping</b> test is used just before each backup job run to verify the target device is available. If this test fails, the backup job is aborted before it starts.</p> <p>This parameter should remain checked (on) in most cases. However, if the <b>ping</b> command is explicitly blocked in your environment, uncheck this box so the test will not occur before each backup job run.</p>
Windows Default RPC Timeout	This field is intended for Axcient internal use and should not be changed unless directed to do so by Axcient technical support.
Windows VShadow Timeout	This field is intended for Axcient internal use and should not be changed unless directed to do so by Axcient technical support.

## Configure E-Mail

The Axcient appliance sends e-mail alerts to designated recipients as configured through the alert mechanism (see [Configure Event Notification](#) section). You can specify the sender (Reply To) address and subject line that will appear on these e-mail alerts. To update the address and subject:

1. Click the **system** tab at the top of the UMC page and select the **email configuration** option in the left navigation menu.
2. The *E-mail Configuration* page appears. To change a value, do the following in the indicated fields:
  - a. **Reply-to address** - Enter the desired sender address for e-mail alert notifications. This is the address to which reply requests are sent. The default is *AxcientAppliance@axcient.net*.
  - b. **Default subject line** - Enter the desired subject line text for e-mail alert notifications. There is no default value.
  - c. **Set subject line mode** - Select the desired mode—**Append** or **Override**—for the subject line from the drop-down menu. The default is **Append**.
  - d. Select **Append** to append what is entered in the *Default subject line* to the standard subject text for that kind of message, which is “*client\_name - event\_description : job\_name*” for an alert e-mail and “*client\_name - Daily Alert Digest*” for a digest e-mail.
  - e. Select **Override** to display only what is entered in the *Default subject line* in the Subject line of any e-mail. (The standard subject text is not included.)
3. Click the (upper) **save** button.
4. When you configure alerts and select the **daily digest** option (see [Configure Event Notification](#) section), alerts that occurred during the preceding 24-hour period are emailed to the selected recipients at 6:00 AM each day by default. You can specify a different time by setting the hour (1-23) and minute (00-59) in the *Daily digest will be sent at* field to the desired time and then clicking the (lower) **save** button.

Figure 81 - E-mail Configuration Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system

**system**

network settings  
quality of service  
date and time  
offsite configuration

**email configuration**

Configure the email settings for sending alerts and messages.

Reply-to address: AxcientAppliance@axcient.net

Default subject line:

Set subject line mode: Append

cancel save

Daily digest will be sent at: 6 : 00

cancel save

## Configure PSA Settings

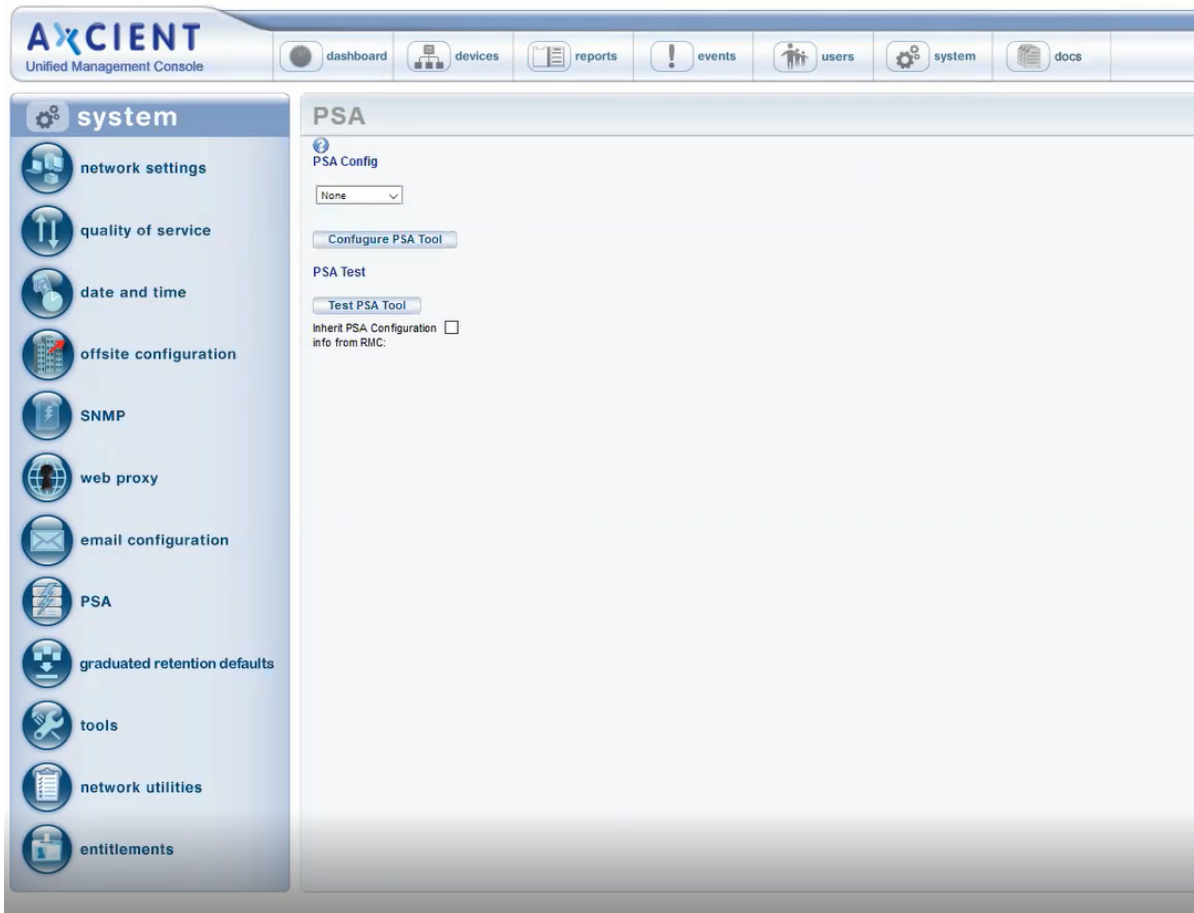
The Axcient appliance can be configured to automatically open a service ticket within a professional services automation (PSA) tool—such as ConnectWise or Autotask—when specific events occur, such as a backup failure. The UMC allows you to specify access credentials and triggering events for the PSA tool.

To configure the Axcient appliance for a PSA tool:

1. On the UMC, click the **system** tab. The *Configuration Summary* page displays.
2. On the *Configuration Summary* page, click the **psa settings** option on the left navigation menu. The *PSA* page displays.
3. Optionally, on the *PSA* page, click the **Inherit PSA Configuration Info from RMC** checkbox to inherit PSA settings already configured through the Axcient Web Application (RMC) . For more information, please reference the [Axcient Business Recovery Cloud Protection Guide](#).
4. Alternatively, use the *PSA Config* drop-down menu to select the appropriate **PSA tool**, and then click the **Configure PSA Tool** button.
5. Enter the appropriate information and then click the **Save** button.
  - If you are integrating with *ConnectWise*, please reference the [ConnectWise Configuration](#) section for configuration instructions.
  - If you are integrating with *Autotask*, please reference the [Autotask Configuration](#) section for configuration instructions.
6. Click the **Test PSA Tool** button to verify that the appliance can connect to that PSA tool. A success or error message will display below the button.
7. Select the events that should be reported to the PSA tool by clicking the **publish to psa tool** checkbox for each event type. For more information, please reference the [Configure Event Notification](#) section.

By default, no events are selected.

Figure 82 - PSA Settings Page



## Configure Graduated Retention Defaults

Graduated retention is the process of pruning older backup versions based on a progressive retention policy. Instead of a fixed retention period, in which each version of a job is saved for a specified interval and then pruned when it exceeds that amount of time, graduated retention rules save an expanding set of restore points that get progressively further apart in time as versions become older.

## Graduated Retention Requirements

In order for Graduation Retention to work properly, you will need to have consistent and regular backup jobs running. Additionally, you will need to give the appliance enough time to build enough recovery points for Graduation Retention to function.

If you miss a recovery point due to a backup job failing for any reason, the appliance will correct itself by applying the next successful backup job to the graduated retention order.

For example: if there are 24 hourly backup jobs scheduled and the 48th backup job fails, the 25th backup job will be used to complete the set of 24 backup jobs to complete a daily backup job as per the configured Graduated Retention Default settings. The same methodology applies for all daily, weekly and monthly backup jobs.

## Graduated Retention Limits

Graduated Retention does not apply retroactively. This means that Graduated Retention configuration changes will not apply to any previously created backups. This applies to when you initially enable Graduated Retention, and if you make any configuration changes to existing settings.

When reconfiguring the existing Graduated Retention settings, all configuration changes applied to the Graduated Retention policy will only apply to backup data created after the changes were committed. All backup data existing before changes to the Graduated Retention were made will be preserved using the Graduated Retention settings in place at the time.

### Methodology

Graduated retention involves two actions:

**Version Pruning** - Graduated retention works like a series of conveyor belts, one for each interval type (hourly, daily, weekly, and monthly). You can specify how long the interval should be for each type. (The defaults are 48 for hourly, 14 for daily, 5 for weekly, and 12 for monthly). A version (restore point) is added to the starting conveyor at each job run. When the conveyor fills up, the oldest one is pruned (deleted) at the next job run.

**Version Promotion** - Certain versions are promoted to the next higher interval type instead of being pruned. This process works as follows:



The job type (hourly, daily, weekly, or monthly) dictates the starting conveyor belt. When the starting conveyor belt fills for the first time, a base version is identified and a time interval (after completion) is set. The interval is 24 (one day) for an hourly type, 7 (one week) for a daily type, 5 (one month+) for a weekly type, and 12 (one year) for a monthly type.

The oldest version after the base is pruned at each new job run. This continues until *step c* applies.

When the base+interval version is reached, that version is promoted to the next higher type (instead of being pruned), the base is pruned, and the next version becomes the new base. For example, the 24th hourly version after the base is promoted to a daily version, and the 25th version becomes the new base for the next 24-hour period.

The same process is repeated in each succeeding (longer type) conveyor. The only difference is how fast each conveyor belt moves forward, because a succeeding conveyor does not move forward until a version is promoted from the previous (shorter type) conveyor belt.

The graduated retention flow operates as follows. This example uses Hourly and Daily backups and thresholds to illustrate how Gradual Retention works:

The first job run becomes the first saved version, indicated by a **black** bar on the far right of the time line (time is represented from right [newest] to left [oldest]). New backup jobs are added at the far right and previous backups are moved one to the left.

After 24 hours, the oldest backup point is tagged (indicated in **red**). The oldest backup of a 24 hour Hourly backup cycle will be replaced to make space for the newest Hourly backup point.

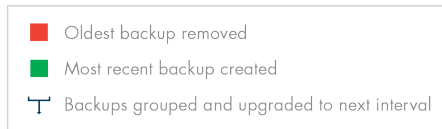
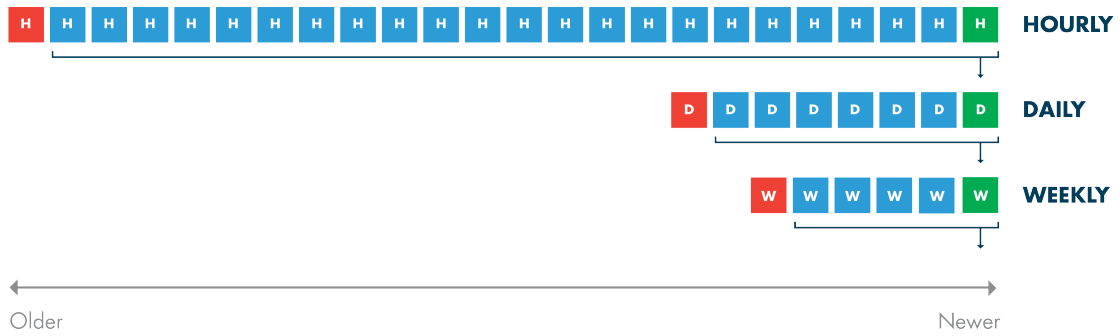
The 1st hourly (or 25th hour) hour backup job of the NEW hourly cycle is promoted as the newest backup point of the Daily backup cycle (indicated in **green** and associated arrows). This backup is also the first backup point of the new Hourly cycle. This process will repeat every 24 hours.

The net result is that each version is deleted after 24 hours except the **green** bar versions that are promoted to the Daily interval type.

The same process is repeated in the Daily category, except the cycle moves forward once a day when an Hourly version is promoted. A Daily backup point is not tagged until the oldest version in the Daily cycle is seven days old. The same methodology is repeated for the Weekly, and Monthly cycles as the aging and promotion cycle fills those categories.

When you restore a version, a list of dates (newest to oldest) is presented that match the remaining versions in the time line (right to left). Note that each version is a snapshot at a point in time, and the only difference from earlier to later versions is that the time intervals between snapshots increase as they get older.

**Figure 83** - Graduated Retention Time Line



## Ramifications

Note the following:

- Graduated retention is supported for file and image backup jobs, but not for mailbox backup jobs.
- Graduated retention has precedence over fixed retention. The *Keep Backups For* field in the backup job definition sets the fixed retention (how long a version should be saved before it is pruned). However, fixed retention is ignored when graduated retention is enabled.
- Graduated retention occurs before the backup run for a file job but after the backup run for an image job. The ramification is one more (older) restore point is retained for a file job than for an image job.
- Changing the Graduated Retention settings will not effect previous backup data which have had Graduated Retention settings applied. The only backup data that will be affected by a change to the Graduated Retention settings will be the backups created after the settings are saved.
- Disabling a backup job and then enabling it again later can also alter the set of available restore points because many restore points will be quickly pruned if they exceed the graduated retention period when the job is enabled.

## Procedure

Graduated retention is enabled in the job definition (see [Back Up Files](#) section or [Back Up System Images](#) section). To modify the default rule values:

Click the **system** tab at the top of the UMC page and select the **graduated retention** option in the left navigation menu.

The Graduated Retention Defaults page appears. The values in the four fields are the defaults that appear when setting graduated retention for a backup job. See the table below for a description of each field. To change a default, enter a new value in one or more of the fields.

When all four values are correct, click the **Save** button.

**Figure 84** - Graduated Retention Defaults Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system

**system**

network settings

quality of service

date and time

### Graduated Retention Defaults

?  
Default Settings for the rules used for graduated retention.

Default Hourly 48 \*

Default Daily 14 \*

Default Weekly 5 \*

Default Monthly 12 \*

cancel save

## Graduated Retention Defaults Fields and Definitions

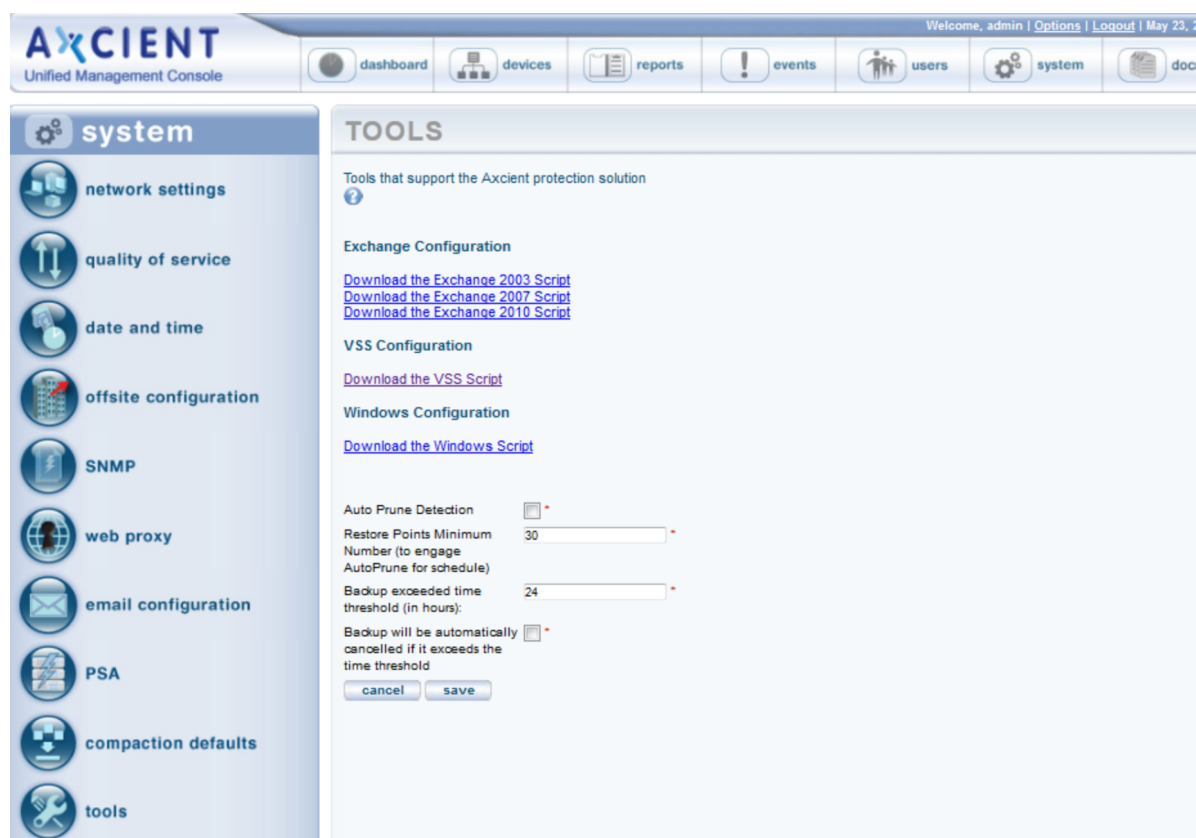
Field	Description
Default Hourly	Defines the retention period for the hourly rule, which is 48 hours by default.
Default Daily	Defines the retention period for the daily rule, which is 14 days by default.
Default Weekly	Defines the retention period for the weekly rule, which is 5 weeks by default.
Default Monthly	Defines the retention period for the monthly rule, which is 12 months by default.

## Use Configuration Tools

Axcient provides tools to help configure your Axcient protection solution. The table below describes the available tools and settings. To use a tool:

1. Click the **system** tab at the top of the UMC page and select the **tools** option in the left navigation menu.
2. The *Tools* page appears. Do one or more of the following:
  - **Download a configuration scrip** - To download a script, right-click on the link, select **Save Link As** (or the corresponding option for your browser), and save the file on the target device. (Clicking the link displays the script on the page.) The following scripts are available:
    - Exchange Configuration script (2003, 2007 and 2010)- **No longer required as EBR backups are no longer supported. For legacy users, consult the previous UMC Guide version for instructions.**
    - VSS Configuration script
    - Windows Configuration script
  - Check the **Auto Prune Detection** box to engage this feature, which automatically adjusts job retention when disk space is limited. The following field sets the minimal number of restore points (backup job runs) to engage the auto-pruning feature (see table below for more information).
  - Set how long a backup job can take before it generates an event message that it has not finished running. Enter the number of hours in the **Backup exceeded time threshold (in hours)** field. (The default is 24 hours.)
  - Set job runs to cancel automatically when they exceed the **Backup exceeded time threshold (in hours)** field value.

Figure 85 - Tools Page



## Tools and Descriptions

Tools	Description
Exchange 2010 Script	Links to a script that allows you to interactively configure an Exchange 2010 server to support a mailbox backup job. <b>No longer required as EBR backups are no longer supported. For legacy users, consult the previous UMC Guide version for instructions.</b>
Exchange 2007 Script	Links to a script that allows you to interactively configure an Exchange 2007 server to support a mailbox backup job. <b>No longer required as EBR backups are no longer supported. For legacy users, consult the previous UMC Guide version for instructions.</b>
Exchange 2003 Script	Links to a script that allows you to interactively configure an Exchange 2003 server to support a mailbox backup job . <b>No longer required as EBR backups are no longer supported. For legacy users, consult the previous UMC Guide version for instructions.</b>
VSS Script	Links to a script that allows you to interactively configure VSS to support image and file backup jobs on a Windows device. See the <a href="#">VSS Configuration Script</a> section for more information.
Windows Script	Links to a script that allows you to interactively configure a Windows device for the Axcient appliance. See the <a href="#">Windows Configuration Script</a> section for more information.
Auto Prune Detection	Enables the automatic pruning feature to adjust the job retention period when disk space is limited. Check the box to enable this feature (off by default). When a backup job is set to run, this feature does the following: <ol style="list-style-type: none"><li>1. Checks whether there is enough free disk space to store the new job run.</li></ol>

Tools	Description
	<ol style="list-style-type: none"> <li>If space is inadequate, the oldest backups are automatically deleted. The number of backups deleted is the minimal number to store the new job run.</li> <li>The <b>keep backups for</b> value in the job definition is reset to the new value. For example, if this is a daily backup job with a 30 day retention and 5 backups were deleted to store the new job run, the retention value is reset to 25 days.</li> </ol> <p><b>Note:</b> This feature applies to file and image backup jobs only; it does not affect mailbox backup jobs.</p>
Restore Points Minimum Number (to engage Auto Prune for schedule)	<p>Sets the minimum number of backup job runs (each of which represents a potential restore point) required for an individual job before Auto Prune Detection is engaged. This is a per-job global setting for the appliance, and it is set to 30 by default.</p> <p>Auto-pruning makes assumptions about how a job will grow. This requires enough runs to make a reasonable estimate of the average change per run. Otherwise, auto-pruning might not prevent the appliance from running out of space, or it might prune job runs that you want to keep as potential restore points.</p> <p><i>Do not set this value below 30 unless instructed to do so by Axcient technical support.</i></p>
Backup exceeded time threshold (in hours)	<p>Sets the duration before an event message is generated stating the backup job has not completed yet. The default is 24 hours. This can alert you to backup jobs that might be hung. Tune this value as needed (either larger or smaller) to accommodate the length of time your largest jobs typically take to run. Note: Unlike other event types, this type is not displayed in the log by default.</p> <p>To display such events and/or generate alerts when they occur, see <a href="#">Configure Event Notification</a> section.</p>
Backup will be automatically canceled if it exceeds the time threshold	Enables automatic job run cancellation when the run time exceeds the threshold value set in the previous field.



## Check Network Connections

The Axcient appliance requires network access to all protected devices and the Axcient data center. The UMC provides an interface to some common network utilities to check network access. See the table below for descriptions of the available utilities.

To check network connections:

1. Click the **system** tab at the top of the UMC page and select the **network utilities** option in the left navigation menu.
2. The *Network Utilities* page appears. Do one or more of the following:
  - a. **Ping command** - Enter an IP address or hostname in the ping address box and then click the **ping** button. The results appear in the box to the right.
  - b. **Traceroute command** - Enter an IP address or hostname in the traceroute address box and then click the **traceroute** button. The results appear in the box to the right.
  - c. **Nslookup command** - Enter an IP address or hostname in the nslookup address box and then click the **nslookup** button. The results appear in the box to the right.
  - d. **Offsite Bandwidth Check script** - Click the **Offsite Bandwidth Check** button, which executes a test data transfer through the Internet to an Axcient data center. The results appear in the box below the button. (This test can take some time for the larger data sizes; click the **Cancel** button to cancel a running test.) This test includes the following options:
    - **Run check using Data Center and current QoS** box - Leave this box unchecked to test your Internet speed. This tests the raw throughput from the appliance to an Axcient data center. Check this box to test both Internet speed and throughput in the data center. This test includes current quality-of-service (QoS) restrictions and any internal processing in the data center to store the data. By testing the options (unchecked, checked with current QoS settings, checked with QoS temporarily disabled), you can estimate the individual effects of the Internet speed, QoS restrictions, and data center processing when analyzing offsite backup performance issues.
    - **Megabytes of data to send** button - Select the size of the data packet to send (2, 8, or 32 MB). If you suspect traffic shaping is occurring, try both a small (2 MB) and large (32 MB) file. Traffic shaping is not occurring if the transmission speed for both is comparable, but it likely is occurring if the larger file transmission speed is slower.
  - e. **Connectivity Health script** - Click the **Connectivity Health** button, which executes a predetermined set of network connection tests (ping, nslookup, and Nmap commands). The results appear in the box below the button.

The results remain on the page (continue to display) until the test is re-run or cleared.

Figure 86 - Network Utilities Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system docs

**system**

- network settings
- quality of service
- date and time
- offsite configuration
- SNMP
- web proxy
- email configuration
- PSA
- graduated retention defaults
- tools
- network utilities
- entitlements

### network utilities

Tools for analyzing the network

Please enter the address (or hostname) and select a command button.

**ping** Address: 192.168.48.152 Output:

```
PING 192.168.48.152 (192.168.48.152) 56(84) bytes of data.
64 bytes from 192.168.48.152: icmp_seq=1 ttl=127 time=1.26 ms

--- 192.168.48.152 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.269/1.269/1.269/0.000 ms
```

**traceroute** Address: 192.168.48.152 Output:

```
traceroute to 192.168.48.152 (192.168.48.152), 30 hops max, 40 byte packets
 1 192.168.99.1 (192.168.99.1)  2.027 ms  2.085 ms  2.117 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

**nslookup** Address: 192.168.48.152 Output:

```
Server:      192.168.44.22
Address:     192.168.44.22#53

** server can't find 152.48.168.192.in-addr.arpa.: NXDOMAIN
```

**Offsite Bandwidth Check**  ☐ Run check using Data Center and current QOS Megabytes of data to send: ☒ 2 ☐ 8 ☐ 32

Offsite Bandwidth Check  
Testing raw upload speed (not involving Data Center).  
There was a problem running the Offsite Bandwidth Check:  
Checking Off-Site bandwidth WITHOUT QOS  
Warning: Permanently added 'rnc-qa02.axcient.inc,192.168.77.201' (RSA) to the list of known hosts.  
Permission denied, please try again.  
Permission denied, please try again.  
Permission denied (publickey,password).

Connectivity health command runs a set of tests that check network connectivity.

**Connectivity Health**

```
>>> Results for ping default gateway: <<<
PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data.
64 bytes from 192.168.99.1: icmp_seq=1 ttl=64 time=1.05 ms

--- 192.168.99.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.057/1.057/1.057/0.000 ms
>>> Results for ping primary dns server: <<<
PING 192.168.44.22 (192.168.44.22) 56(84) bytes of data.
64 bytes from 192.168.44.22: icmp_seq=1 ttl=127 time=0.236 ms

--- 192.168.44.22 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.236/0.236/0.236/0.000 ms
>>> Results for nslookup RMC host: <<<
Server:      192.168.44.22
Address:     192.168.44.22#53

Non-authoritative answer:
Name:   axcient.net
Address: 209.18.124.2
```

## Network Utilities Descriptions

Utility	Description
ping command	<p>Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.</p> <p>The following is sample output from a successful ping, which means the Axcient appliance can access this device:</p> <pre>PING 192.168.77.117 (192.168.77.117) 56(84) bytes of data. 64 bytes from 192.168.77.117: icmp_seq=1 ttl=128 time=0.342 ms --- 192.168.77.117 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.342/0.342/0.342/0.000 ms</pre>
tracert command	<p>Traces the network path that packets take as they are forwarded from the Axcient appliance to a destination address. The length of the network connection is indicated by the number of “hops” (forwarding from one router to another) in the tracert path. It lists all the routers it passes through until it reaches its destination, or fails to and is discarded. It also displays the time required for each hop from router to router. Traceroutes can be useful to diagnose slow network connections. For example, the tracert can expose a problem if one or more hops either take a long time or are marked with “*” indicating the time was really long.</p> <p>The following is sample output from a successful tracert with just one hop:</p> <pre>tracert to 192.168.77.117 (192.168.77.117), 30 hops max, 40 byte packets 1 (192.168.77.117) 0.370 ms 0.348 ms 0.341 ms</pre>
nslookup command	<p>Displays the IP address/domain name for the specified address. This command is often used as a reverse lookup to determine the domain name if you know the IP address or vice versa. In addition, the Domain Name System (DNS) server name and address used for the lookup is displayed.</p> <p>The following is sample output. DNS server information appears first, and lookup information follows:</p> <pre>Server: 192.168.44.22 Address: 192.168.44.22#53 117.77.168.192.in-addr.arpa name = admin-jmuench.axcient.inc.</pre>
Offsite Bandwidth Check	<p>Sends sample data offsite to an Axcient data center and displays the transmission results: number of records sent, total bytes copied, time of transmission in seconds, and transmission speed in KB per second. This provides a test of Internet throughput that you can use to estimate how long offsite backups might take and assess potential issues. There are options for specifying the path/bandwidth rate (QOS) and data size (MBs).</p> <p><b>Run check using Data Center and current QOS</b></p> <ul style="list-style-type: none"> <li>Check box to test transfer speed along the full path from the appliance to a storage server in the data center using the current bandwidth throttling.</li> <li>Check box and disable QOS during the test to check the full path performance with no bandwidth restriction (see <a href="#">Set Bandwidth Usage (Quality of Service)</a> section).</li> <li>Uncheck box to test using maximum available bandwidth. This checks Internet speed from the appliance to the data center (without going through the data center to a storage server).</li> </ul> <p><b>Megabytes of data to send</b></p> <ul style="list-style-type: none"> <li>Click <b>2</b> to send 2 MBs to the data center.</li> <li>Click <b>8</b> to send 8 MBs to the data center.</li> <li>Click <b>32</b> to send 32 MBs to the data center.</li> </ul> <p>One factor you can test for through multiple transmissions is traffic shaping. Traffic shaping is a process where a firewall, router, or IP service provider automatically throttles down throughput when sustained traffic flow is detected. To test for traffic shaping, send a small (2 MB) and large (32 MB) file and compare the transmission speeds. If they are comparable, traffic shaping is not an issue. However, if the larger file transmission speed is slower, traffic shaping might be enabled</p> <p>The following is sample output. In this example the 2 MB and QOS buttons were checked and the transmission speed was 117 KB per second.</p> <pre>&gt;&gt;&gt; Results for Offsite Bandwidth Check: &lt;&lt;&lt; Checking Off-Site bandwidth with current QOS</pre>

Utility	Description
	<p>0+69 records in</p> <p>0+69 records out</p> <p>2097152 bytes (2.1 MB) copied, 17.995 s, 117 kB/s</p>
connectivity health script	<p>Executes several network connectivity tests between the Axcient appliance and key systems. This script does the following:</p> <ol style="list-style-type: none"> <li>1. Pings the default gateway.</li> <li>2. Pings the DNS server.</li> <li>3. Pings and does an nslookup for the RMC host system in the Axcient data center.</li> <li>4. Checks the status of relevant ports (Nmap scan).</li> </ol> <p>If any of the ping tests fail, the Axcient appliance cannot function properly. The Nmap scan allows you to see whether one or more ports might need to be opened for the Axcient appliance. The following is sample output.</p> <pre>&gt;&gt;&gt; Results for ping default gateway: &lt;&lt;&lt; PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data. 64 bytes from 192.168.99.1: icmp_seq=1 ttl=255 time=1.02 ms --- 192.168.99.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 1.020/1.020/1.020/0.000 ms  &gt;&gt;&gt; Results for ping dns server: &lt;&lt;&lt; PING 192.168.44.22 (192.168.44.22) 56(84) bytes of data. 64 bytes from 192.168.44.22: icmp_seq=1 ttl=127 time=0.400 ms --- 192.168.44.22 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.400/0.400/0.400/0.000 ms  &gt;&gt;&gt; Results for nslookup RMC host: &lt;&lt;&lt; Server: 192.168.44.22 Address: 192.168.44.22#53 Non-authoritative answer: Name: axcient.net Address: 209.18.124.2  &gt;&gt;&gt; Results for ping RMC host: &lt;&lt;&lt; PING axcient.net (209.18.124.2) 56(84) bytes of data. 64 bytes from axcient.net (209.18.124.2): icmp_seq=1 ttl=51 time=10.3 ms --- axcient.net ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 10.398/10.398/10.398/0.000 ms  &gt;&gt;&gt;Verify that a connection can be made to port 22 of axcient.net: &lt;&lt;&lt; open  &gt;&gt;&gt; Detecting port status for Axcient relevant ports: &lt;&lt;&lt;</pre>

Utility	Description
	<i>Starting Nmap 5.61TEST2 ( <a href="http://nmap.org">http://nmap.org</a> ) at 2012-04-11 01:32 UTC</i> <i>Nmap scan report for localhost (127.0.0.1)</i> <i>Host is up (0.0000080s latency).</i> <i>PORT STATE SERVICE</i> <i>22/tcp open ssh</i> <i>53/tcp closed domain</i> <i>80/tcp open http</i> <i>123/tcp closed ntp</i> <i>.</i> <i>.</i> <i>.</i> <i>Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds</i>

## Check Entitlements

Each account comes with certain entitlements that are controlled through an enablement mechanism on the appliance:

- To view your current entitlements, click the **system** tab at the top of the UMC page and select the **entitlements** option in the left navigation menu. The *Entitlements* page appears. The top portion of the page lists entitlement information. The table below describes the information fields.
- The entitlements information is checked (and refreshed if needed) automatically every day. However, if you upgrade your entitlements and want to activate them immediately, click the **refresh** button. This gets the most current entitlements immediately from the RMC. The display section is then updated with the latest values.
- Some customers do not allow access to the Internet, which means the Axcient appliance cannot contact the RMC to download the entitlements information. In this case, you can manually enable the entitlements as follows:
  - Copy the contents of the entitlements e-mail you received from Axcient and paste it into the text box under the **Apply** button. Contact Axcient customer support if you have not received the e-mail.
  - Click the **Apply** button. The updated entitlements appear in the Display section.

Figure 87 - Entitlements Page

**Axcient**  
Unified Management Console

dashboard devices reports events users system docs

**system**

- network settings
- quality of service
- date and time
- offsite configuration
- SNMP
- web proxy
- email configuration
- PSA
- graduated retention defaults
- tools
- network utilities
- entitlements

### Entitlements

Display

Below are the entitlements for this appliance.

Entitlement Name	Entitlement Value
Service Id	f8wm
Onsite Storage (in GB)	2000
Offsite Storage (in GB)	123
Number of Servers	unlimited
Number of Workstations	unlimited
Package	WithoutProtectFlow
Local Failover	y
Bare Metal Restore	y
File Backup	y
Mailbox Backup	y
Image Backup	y
Maximum VMs for Local Failover	unlimited

**Refresh**

Click the Refresh button below to automatically retrieve entitlements for this appliance from Axcient (Internet connectivity is required).

Refresh

**Apply**

If you were e-mailed entitlements for this appliance from Axcient, paste them here and click the Apply button.

Apply

## Entitlements Terms and Definitions

Term	Description
Service ID	Displays the service ID for this customer.
Expiration Date	Displays the current expiration date for this account. This value represents how far into the future the entitlements are valid. This field does not appear if there is no expiration date, that is the entitlement is for an unlimited duration.
Manual Key	Indicates this account is set for manual enablement (see preceding bullet points). This field appears only when the manual key process has been approved.
Onsite Storage	Displays the amount of onsite storage capacity authorized for this account. Values are in Gigabytes.
Offsite Storage	Displays the amount of offsite storage capacity authorized for this account. Values are in Gigabytes.
Package	<p>Displays the marketing package name that applies to this account:</p> <ul style="list-style-type: none"> <li>• <b>Backup</b>—Enables file backup jobs.</li> <li>• <b>Protect</b>—Enables file backup jobs and mailbox backup jobs.</li> <li>• <b>Fortify</b>—Enables file backup jobs, mailbox backup jobs, and image backup jobs, which support both failover VM and BMR recovery options.</li> <li>• <b>Fortify-X</b>—Enables the same features as Fortify in a higher performance and capacity appliance.</li> <li>• <b>Cloud Continuity</b>—Enables the same features as Fortify plus cloud continuity.</li> <li>• <b>Cloud Continuity Plus</b>—Enables the same features as Cloud Continuity with additional compute resources in the cloud.</li> </ul>
Local Failover	Indicates this account is enabled to create failover (and test) VMs.
Bare Metal Restore	Indicates this account is enabled to perform bare metal restores (BMRs).
Mailbox Backup	Indicates this account is enabled for mailbox backup jobs on Exchange servers.
File Backup	Indicates this account is enabled for file backup jobs.
Image Backup	Indicates this account is enabled for image backup jobs.
Maximum VMs for Local Failover	Displays the number of simultaneous VMs allowed on this appliance. The value is either an integer or <b>unlimited</b> (meaning the only restriction is the physical capacity of the appliance).



## Set System Access and Availability

The top line of the UMC page includes logout and options links that support the following actions:

- To logout from the UMC, click **logout**.
- To access the *Options* page, click **options**. The *Options* page allows you to:
  - a. Change the password. See the *Change Password* section below for more information.
  - b. Copy job data to a DAS device for offsite backup at an Axcient data center. See the *Offsite Backup* chapter in the [Axcient DAS Transfer Guide](#) for more information.
  - c. Copy job data on to a DAS device as a separate archive drive. See the *Export Drive* chapter in the [Axcient DAS Transfer Guide](#) for more information.
  - d. Reboot or shutdown the Axcient appliance, or to restrict Axcient Technical Support access to the appliance. See the *Systems Options* section below for more information.
  - e. Reset the appliance to default factory settings (only appears when logged in as the administrator). See the *Factory Image Reset* section below for more information.

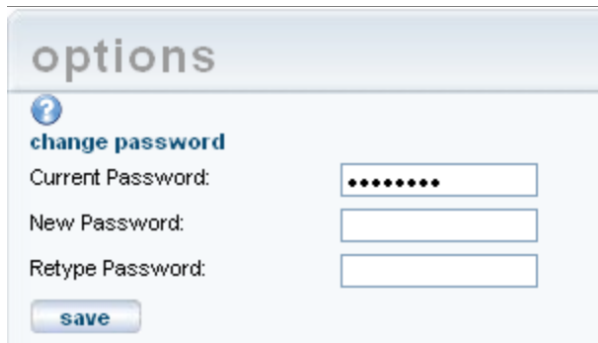
Figure 88 - Main Menu - Logout and Options



## Set System Access and Availability

To change the password of the currently logged in user:

1. To change the password of the currently logged in user:
  - a. **Current Password** - Enter the current password.
  - b. **New Password** - Enter the new password.
  - c. **Retype Password** - Re-enter (verify) the new password.
2. Click the **save** button.

*Figure 89* - Change Password Page

The image shows a web interface for changing a password. It features a light blue header with the word "options" in a bold, sans-serif font. Below the header, there is a section titled "change password" preceded by a blue circular icon containing a white question mark. The form consists of three rows of labels and input fields: "Current Password:" followed by a text box filled with ten black dots, "New Password:" followed by an empty text box, and "Retype Password:" followed by another empty text box. At the bottom left of the form is a blue button with the word "save" in white, lowercase letters.

**options**

**?**  
**change password**

Current Password:

New Password:

Retype Password:

**save**

## System Options

The System Options section allows you to reboot or shutdown the appliance. It also includes an option to restrict access to Axcient technical support personnel if you are logged in as the *restrictedadmin* user.

### Caution!

Do not reboot or shutdown if there are any running VMs, because this could leave the appliance in an unstable condition. Shutdown the VMs (see “Shutdown and Restart Virtual Machine ” section) before attempting to reboot or shutdown the appliance.

To reboot or shutdown the Axcient appliance:

1. Select one of the following:
  - Click the **reboot** button.
  - Click the **shutdown** button.
2. A pop-up window appears to verify the reboot or shutdown request. Click **OK**. A message appears indicating the reboot or shutdown is in progress. (A reboot can take several minutes.)

## Restrict Axcient Access

Axcient technical support personnel use a variety of tools to maintain the health of appliances in the field and to respond quickly if problems arise. This requires a certain level of remote access to the Axcient appliance through a secure connection to the Axcient data center. While this access is beneficial for many customers, the security policy in some organizations might preclude such access to Axcient employees. You have the option to restrict Axcient access to the appliances in your organization.

A special user, *restrictedadmin*, is provided so you can control outside access. The *restrictedadmin* user has the following characteristics:

- It has the same privileges as the *admin* user (see [Manage Users](#) section).
- It is an isolated account, so no other user (including admin) can modify this user. Only someone logged in as *restrictedadmin* can change any user parameters. This means that once you change the original password, no one else (including Axcient personnel) can log in as this user.
- The restrict access feature is accessible to the *restrictedadmin* user only.
- If you forget the password, admin or another user with administrator privileges can generate a temporary password sent to you (see [Modify a User](#) section).

To restrict Axcient access to this appliance:

1. Log in as the *restrictedadmin* user and click the **options** button.
2. Go to the *system options* section and do one or both of the following:
  - Check the **Restrict Axcient technical support access** box. This restricts Axcient customer support from accessing the appliance.
  - Check the **Restrict access from the RMC** box. This restricts access from the RMC to all users, not just Axcient technical support. When this feature is enabled, you will not be able to log into the UMC from the RMC, and the RMC file browse feature will be disabled. (Logging into the UMC directly through the local network is not affected.) When this box is checked, the other box is also checked (applied) automatically.

It can take up to 30 minutes after checking either box for the restriction to take effect.

Axcient technical support is limited without this access. If you encounter a problem, it might be necessary to grant access before Axcient technical support can resolve the issue. To grant access, clear (uncheck) the boxes. You can reapply the restriction when the support work is complete.

**Figure 90** - Options Page - System Options Selection

The screenshot shows a web interface titled 'options'. Below the title is a section with a question mark icon and the text 'change password'. There are three labels: 'Current Password:', 'New Password:', and 'Retype Password:'. Each label is followed by a text input field. The 'Current Password' field contains several dots, indicating masked text. At the bottom of the section is a 'save' button.

## Factory Image Reset

The Factory Image Reset section provides the option to reset the Axcient appliance to its default factory settings. You might choose this option if you are a reseller and have a customer return an appliance that you want to reuse for a different customer. In this case, it is important to remove any previous customer data and reconfigure the appliance to the default factory settings. This section appears only if you are **logged in as the administrator**.

### CAUTION!

Do not reset the appliance to the factory image unless you are certain nothing remains that you want to retain, because all remaining data is lost permanently.

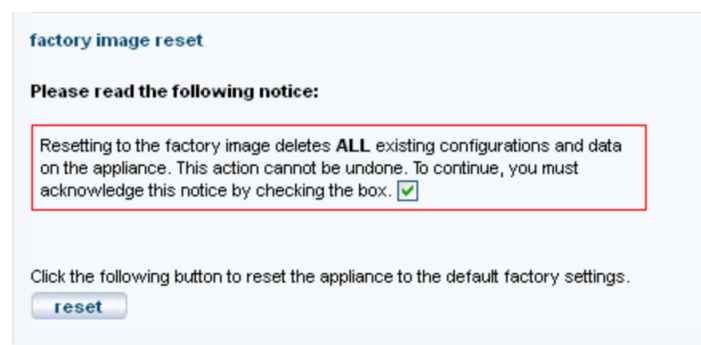
To reset an Axcient appliance to the factory default settings:

1. In the Factory Image Reset section (bottom of the **options** page), read the notice outlined in red and then check the acknowledgement box.
2. A **reset** button appears below the notice. Click the **reset** button.
3. A final confirmation box appears. Click the **Yes** button. You are then logged out of the UMC, and the reset process begins.

**CAUTION!**

The reset process might take up to 15 minutes. Do not log into the UMC while the appliance is being reset. Wait until after it reboots (which it does automatically after the reset is complete). Any interaction with the appliance prior to the reboot could leave it in an unstable or unusable state.

**Figure 91** - Option Page - Factory Image Reset Section



The screenshot shows a web interface for the 'factory image reset' section. At the top, the title 'factory image reset' is displayed in blue. Below it, a bold instruction reads 'Please read the following notice:'. A red rectangular box highlights a warning message: 'Resetting to the factory image deletes **ALL** existing configurations and data on the appliance. This action cannot be undone. To continue, you must acknowledge this notice by checking the box. ☒'. Below the red box, a line of text says 'Click the following button to reset the appliance to the default factory settings.' followed by a blue 'reset' button.

# User Management

You can add or modify user accounts and specify the set of permissions available to each user. The Axcient appliance comes with the following users by default:

- **admin**—May perform any operation on the Axcient appliance.
- **backupuser**—May create a backup job or restore data from a backup job.
- **limitedbackupuser**—May restore data from a backup job.
- **restrictedadmin**—May restrict access to the Axcient appliance (see “Set System Access and Availability” section).
- **bmr**—Used internally during a bare metal restore.

The permissions for a user are determined by that user's assigned role. The Axcient appliance comes with the following roles by default:

- **IT Admin**—Allows any operation. (The admin and restrictedadmin users are assigned this role.)
- **Events User**—Allows receiving e-mails and viewing event log and reports only.
- **Backup User**—Allows backup and restore operations only. (The backupuser is assigned this role.)
- **Limited Backup User**—Allows restore operations only. (The limitedbackupuser is assigned this role.)
- **Reseller**—Allows backup and restore operations, creating users, and viewing reports and event logs.

## Add a User

To add a new user:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Select the **create a user** option located on the left of the page.
3. The *Create a New User* page appears. Specify the following in the indicated fields:
  - **Email Address** - Enter an e-mail address. This becomes both the user name and the e-mail address for this user.
  - **Role** - Select a role for this user from the drop-down menu.
  - **Permissions** - Select the permissions (add a check mark in each box) for this user. The permissions allowed by the role are automatically checked, but you can add to or delete from this list.
4. When all the information is correct, click the **save** button. The new user now appears in the list of existing users with a message the user has been added but the account must be activated.
5. An e-mail that includes a temporary password is sent to the user e-mail address. You must log into the UMC using the temporary password (see [Logging in to the UMC](#) section). After logging in, you are prompted to change the password. After entering a new password (which becomes the permanent password) and clicking the **save** button, the UMC dashboard appears. You can now access the UMC and perform any action for which that user has permission.

Figure 92 - Create a New User Page

The screenshot displays the 'create a new user' interface within the Axcient Unified Management Console. The top navigation bar includes links for dashboard, devices, reports, events, users (highlighted), system, and docs. A sidebar on the left shows 'users' with sub-options: existing users, create a user (selected), and modify roles. The main content area is titled 'create a new user' and contains the following fields:

- Email address:** seller1@axcient.com
- Role:** Reseller (selected from a dropdown menu)
- Permissions:** A grid of checkboxes where several are checked:
 

<input checked="" type="checkbox"/> Create a Backup	<input checked="" type="checkbox"/> Restore from a Backup	<input checked="" type="checkbox"/> Create a User
<input checked="" type="checkbox"/> UMC User	<input checked="" type="checkbox"/> Configure an Uptiva	<input checked="" type="checkbox"/> Clear Alerts
<input checked="" type="checkbox"/> View Reports	<input checked="" type="checkbox"/> Receive Emails	<input checked="" type="checkbox"/> View Event Log
<input type="checkbox"/> Edit Limited Devices	<input type="checkbox"/> Edit All Devices	<input type="checkbox"/> Reboot the Uptiva
<input type="checkbox"/> Create Global Backup Templates	<input type="checkbox"/> Limited Restore from a Backup	

At the bottom of the form are 'cancel' and 'save' buttons. A link for 'Additional Email Addresses' is also present.

## Modify a User

### CAUTION!

Do not modify any of the default users (admin, bmr, backupuser, limitedbackupuser, and restrictedadmin). Modifying a default user can cause upgrades to fail.

To modify an existing user:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Click the **edit** field for the target user.

Figure 93 - Existing Users Page

Username	Role	Email	Active?	Edit	Account Status	Delete	Temp Password
admin	IT Admin	<a href="mailto:email1@axcient.com">email1@axcient.com</a>	Yes	<a href="#">Edit</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Send</a>
backupuser	Backup User	<a href="mailto:email2@axcient.com">email2@axcient.com</a>	Yes	<a href="#">Edit</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Send</a>
limitedbackupuser	Limited Backup User	<a href="mailto:email3@axcient.com">email3@axcient.com</a>	Yes	<a href="#">Edit</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Send</a>
bmr	Limited Backup User	<a href="mailto:email4@axcient.com">email4@axcient.com</a>	Yes	<a href="#">Edit</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Send</a>
reseller1@axcient.com	Reseller	<a href="mailto:reseller1@axcient.com">reseller1@axcient.com</a>	Yes	<a href="#">Edit</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Send</a>

3. The *Edit User* page appears. Update entries as desired in the indicated fields. You can add or change e-mail addresses, display name, password, role, and permissions. The table below describes each of the fields and options.
4. When all the information is correct, click the **save** button. The Existing Users page reappears with a message indicating the user was saved.

The *Temp Password* column allows you to generate a new temporary password. Clicking the **send** link automatically creates the new password and e-mails it to the user. (You are prompted to change it at the next login.) Because the password is changed, use this feature only if the current password has been lost or forgotten.



Figure 94 - Edit a User Page

The screenshot shows the 'edit user information' page in the Axcient Unified Management Console. The left sidebar has a 'users' section with options: 'existing users', 'create a user', and 'modify roles'. The main content area is titled 'edit user information' and contains the following fields and options:

- Username:** backupuser
- Email address:** email2@axcient.com (with a link to 'Additional Email Addresses')
- Full Name:** backupuser
- New Password:** (empty field)
- Retype Password:** (empty field)
- Role:** Backup User (dropdown menu)
- Permissions:**
  - ☒ Create a Backup
  - ☒ UMC User
  - ☐ View Reports
  - ☐ Edit Limited Devices
  - ☐ Create Global Backup Templates
  - ☒ Restore from a Backup
  - ☐ Configure an Uptiva
  - ☐ Receive Emails
  - ☐ Edit All Devices
  - ☐ Limited Restore from a Backup
  - ☐ Create a User
  - ☐ Clear Alerts
  - ☐ View Event Log
  - ☐ Reboot the Uptiva

At the bottom of the form are 'cancel' and 'save' buttons.

## Edit User Fields and Definitions

Field	Description
Username	Displays the user name. This value is set when the user account is created and cannot be changed.
Email address	<p>Sets the e-mail address to which relevant messages are sent by the Axcient appliance. The user name is the initial e-mail address, but you change this address at any time.</p> <p>To add additional addresses, click <b>Additional Email Addresses</b>. This displays additional rows to enter more addresses. e-mail messages will be sent to all the addresses in the list.</p>
Full Name	Sets the name that will appear in displays.
New Password	Sets a new login password.
Retype Password	Verifies the entry in <b>New Password</b> . If both entries are not identical, the password is not changed.
Role	Sets the assigned role. To change the role, select the new role from the drop-down menu.
Permissions	Sets the permissions (add or remove check mark in each box) for this user. The permissions allowed by the role are automatically checked, but you can add to or delete from this list.

## Deactivate a User

### CAUTION!

Do not delete any of the default users (admin, bmr, backupuser, limitedbackupuser, and restrictedadmin). Deleting a default user can cause upgrades to fail.

A UMC user account can be deactivated or deleted:

- Deactivating a user disables the user login but otherwise leaves that user account unaffected. Login attempts by that user are denied, but any backup jobs or other actions created by that user are retained and continue to function normally.
- Deleting a user removes all record of that user. However, you cannot delete a user if there are current backup jobs or other objects created by that user. All objects associated with that user must first be removed before deleting the user.

To deactivate (or reactivate) a user:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Do one of the following:
  - To deactivate the user account, Click **Deactivate** in the *Account Status* column for the target user. (Deactivate changes to Activate indicating the account is no longer active.)
  - To activate the user account, Click **Activate** in the *Account Status* column for the target user. (Activate changes to Deactivate indicating the account is now active.)

To delete an existing user:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Click the **Delete** button for that user.
3. You are prompted to verify the delete. Click the **delete** button. The user is removed from the existing users list and a message appears indicating the user was deleted.

Attempting to delete a user who has active backup jobs or other objects associated with that user generates an error message.

## Mange Roles and Permissions Overview

The permissions for a user are determined by the role assigned to that user. Each roles provides a set of allowed permissions. The Axcient appliance comes with the following roles by default:

- **IT Admin**—Allows any operation.
- **Backup User**—Allows backup and restore operations only.
- **Limited Backup User**—Allows restore operations only.
- **Reseller**—Allows backup and restore operations, creating users, receiving e-mails, and viewing reports and event log.
- **Events User**—Allows receiving e-mails and viewing reports and event log.

You can create additional roles and customize existing roles. The table below describes the available permissions and lists which ones apply for each of the default roles.

Do not change the permissions of the default roles. Instead, create a new role with a customized set of permissions.

### Permissions Categories

Permission	Description
Create a Backup	Allows the user to create a backup job (see <a href="#">Backup Jobs</a> chapter).
Restore from a Backup	Allows the user to restore data from a backup job.
Create a User	Allows the user to create other users (see <a href="#">Manage Users</a> section).
UMC User	Allows access to the UMC. This permission is required to login to the UMC, so all UMC users must have this permission.
Configure an Appliance	Allows the user to perform any of the tasks under the system tab.
Clear Alerts	Allows the user to clear (remove) an alert message from the log (see <a href="#">Event Logging</a> chapter).
View Reports	Allows the user to view reports.
Receive Emails	User is sent e-mails related to the user account, for example e-mail notification when a backup job created by that user fails.
View Event Log	Allows the user to view the event log (see <a href="#">Event Logging</a> chapter).
Edit Limited Devices	Allows the user to configure devices created by the logged in user (see <a href="#">Device Management</a> chapter).
Edit All Devices	Allows the user to configure any device (see <a href="#">Device Management</a> chapter).
Reboot the Appliance	Allows the user to reboot the Axcient appliance (see <a href="#">Set System Access and Availability</a> section).
Create Global Backup Templates	This feature is not currently supported.
Limited Restore from a Backup	Allows the user to do a limited set of restore options.
View All Devices	Allows the user to see the list of devices for that client.

## Add a Role

To add a new role:

Click the users button at the top of the UMC page.

The *Existing Users* page appears. Select the **modify roles** option located on the left of the page.

The *User Roles* page appears. Do the following in the indicated fields:

- **Role Name** - Enter a name for the role.
- **Permissions** - Select the permissions (add a check mark in each box) that apply to this role.

When all the information is correct, click the **save** button. A message appears indicating the role was saved, and the new role now appears in the list of existing roles.

Figure 95 - User Roles Page

The screenshot shows the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'users' menu with options for existing users, create a user, and modify roles. The main content area is titled 'user roles' and contains a table of existing roles.

Role Name	Edit	Delete
IT Admin	<a href="#">Edit</a>	<a href="#">Delete</a>
Reseller	<a href="#">Edit</a>	<a href="#">Delete</a>
Backup User	<a href="#">Edit</a>	<a href="#">Delete</a>
Limited Backup User	<a href="#">Edit</a>	<a href="#">Delete</a>
Events User	<a href="#">Edit</a>	<a href="#">Delete</a>

Below the table is the 'role details' section. It includes a 'Role name' input field and a 'Permissions' section with a grid of checkboxes:

<input type="checkbox"/> Create a Backup	<input type="checkbox"/> Restore from a Backup	<input type="checkbox"/> Create a User
<input type="checkbox"/> UMC User	<input type="checkbox"/> Configure an Uptiva	<input type="checkbox"/> Clear Alerts
<input type="checkbox"/> View Reports	<input type="checkbox"/> Receive Emails	<input type="checkbox"/> View Event Log
<input type="checkbox"/> Edit Limited Devices	<input type="checkbox"/> Edit All Devices	<input type="checkbox"/> Reboot the Appliance
<input type="checkbox"/> Create Global Backup Templates	<input type="checkbox"/> Limited Restore from a Backup	<input type="checkbox"/> View All Devices

A 'save' button is located at the bottom of the permissions section.

## Modify a Role

### CAUTION!

Do not modify any of the default roles (IT Admin, Backup User, Limited Backup User, Reseller, and Event User). Modifying a default role can cause upgrades to fail.

To modify (update the permission list of) an existing role:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Select the **modify roles** option located on the left of the page.
3. The *User Roles* page appears. Click the **edit** field for the target role and change the permissions (add or remove check marks) for this role.
4. Click the **save** button. A message appears indicating the role was saved.

Figure 96 - User Role Page - Edit

The screenshot shows the Axcient Unified Management Console (UMC) interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar shows the 'users' section with options for existing users, create a user, and modify roles. The main content area is titled 'user roles' and contains a table of existing roles. The 'IT Admin' role is highlighted with a red box, and its 'Edit' link is also highlighted. Below the table is the 'role details' section, which includes a 'Role name' field and a 'Permissions' section with various checkboxes.

Role Name	Edit	Delete
IT Admin	<a href="#">Edit</a>	<a href="#">Delete</a>
Reseller	<a href="#">Edit</a>	<a href="#">Delete</a>
Backup User	<a href="#">Edit</a>	<a href="#">Delete</a>
Limited Backup User	<a href="#">Edit</a>	<a href="#">Delete</a>
Events User	<a href="#">Edit</a>	<a href="#">Delete</a>

**role details**

Role name:

Permissions:

- ☐ Create a Backup
- ☐ UMC User
- ☐ View Reports
- ☐ Edit Limited Devices
- ☐ Create Global Backup Templates
- ☐ Restore from a Backup
- ☐ Configure an Uptiva
- ☐ Receive Emails
- ☐ Edit All Devices
- ☐ Limited Restore from a Backup
- ☐ Create a User
- ☐ Clear Alerts
- ☐ View Event Log
- ☐ Reboot the Appliance
- ☐ View All Devices

[save](#)

## Delete a Role

### CAUTION!

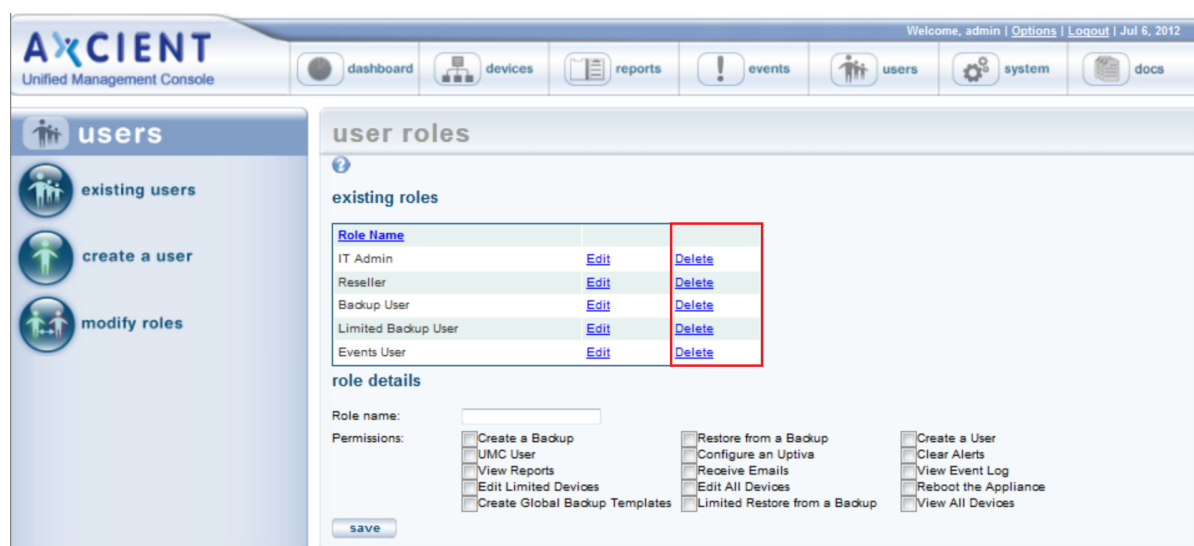
Do not delete any of the default roles (IT Admin, Backup User, Limited Backup User, Reseller, and Event User). Deleting a default role can cause upgrades to fail.

To delete an existing role:

1. Click the **users** button at the top of the UMC page.
2. The *Existing Users* page appears. Select the **modify roles** option located on the left of the page.
3. The *User Roles* page appears. Click the **delete** button for that role. The role is removed from the list.

A role cannot be deleted if it is currently used. An error message appears if the role is assigned to one or more users.

Figure 97 - User Role Page - Delete



# Reports

## View Reports

To view a report:

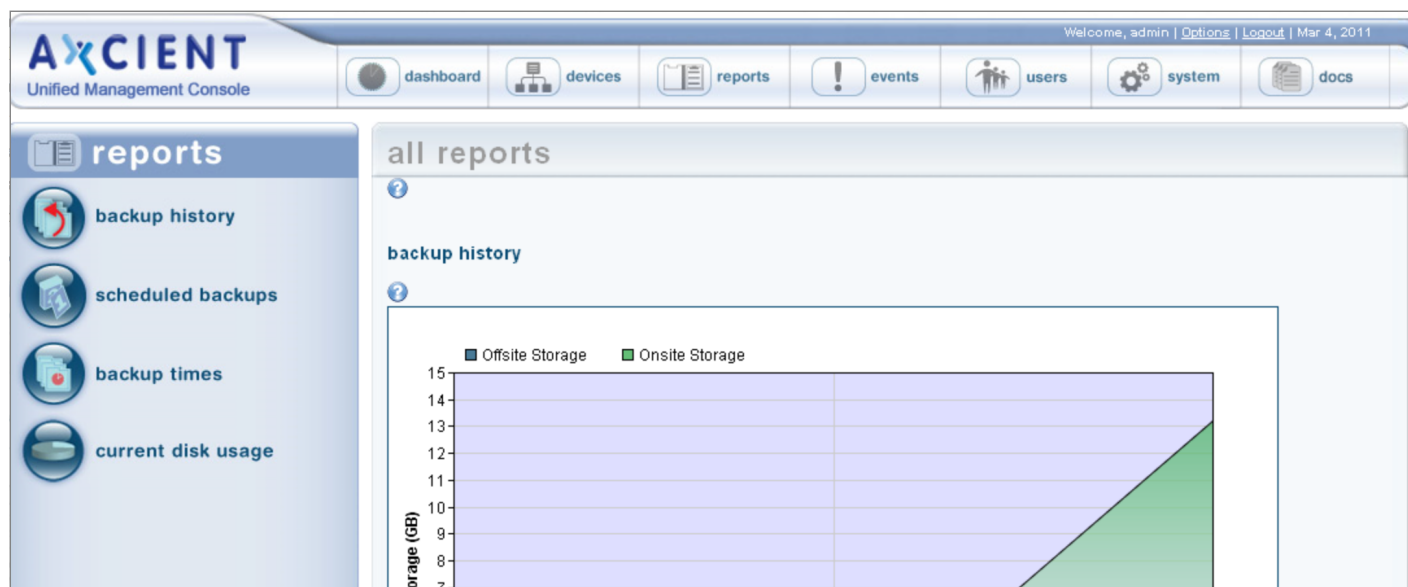
Click the **reports** button at the top of the UMC page. The *Reports* page displays the following set of predefined reports:

- Backup history**—Displays a history of storage space used for backups.
- Scheduled backups**—Displays information about each current backup job.
- Backup times**—Displays a history of every run of a backup job.
- **Current disk usage**—Displays a breakdown by backup job of current storage space used.

To view a report, do one of the following:

- For a static view of all four reports in a single display, scroll down the right side of the *reports* page.
- For a configurable view of an individual report, click on the report name (left side of the page), which displays a page for that report.

**Figure 98** - Reports Page



## Backup History Report

The data for this report is automatically updated once a day at 6:00 AM. The report does not reflect changes since 6:00 AM.

To display the *Backup History* report, click the **reports** tab in the main menu (top of the page) and then the **backup history** tab in the *Reports* menu (left of the page). The Backup (Storage) History report displays the following two graphs:

- The first graph displays the amount of onsite (Axcient appliance) and offsite (Axcient data center) storage used over time. The vertical axis is total storage amount and the horizontal axis is time.
- The second graph displays the amount of incremental data change over time. The vertical axis is incremental change storage amount and the horizontal axis is time.

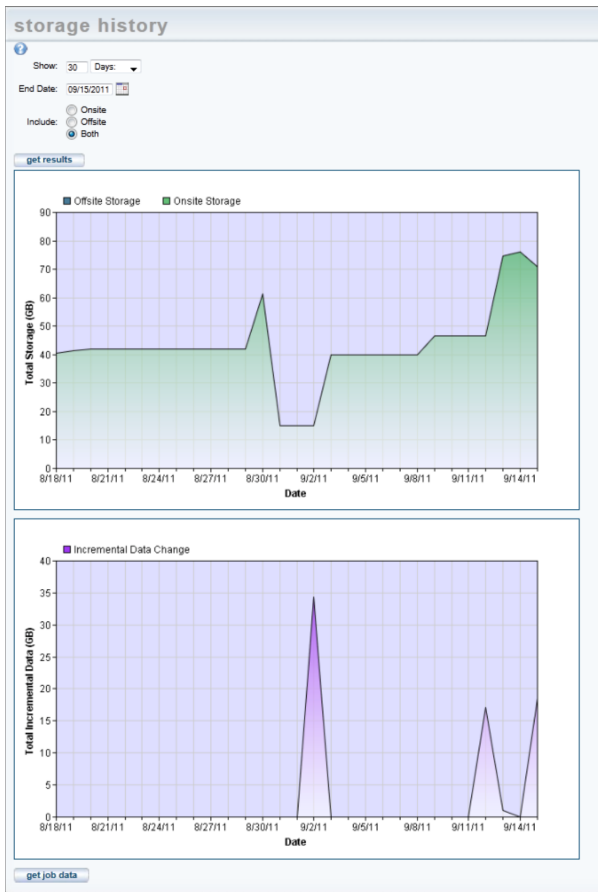
You can customize the report as follows:

- **Show**—Sets the duration of the report. Enter the number and select the unit (Days, Weeks, Months) from the drop-down menu.
- **End Date**—Sets the last day of the report. (The report start date is determined by moving back from this end date the interval specified in the *Show* field.) To set the date, click on the calendar, which opens a calendar pop-up window. Select the end date in the pop-up window and then click the **close** button.
- **Include**—Sets what data to include in the report. The options are onsite only, offsite only, or both. Select the button next to the desired choice.

To redisplay after customizing the report, click the **get results** button.

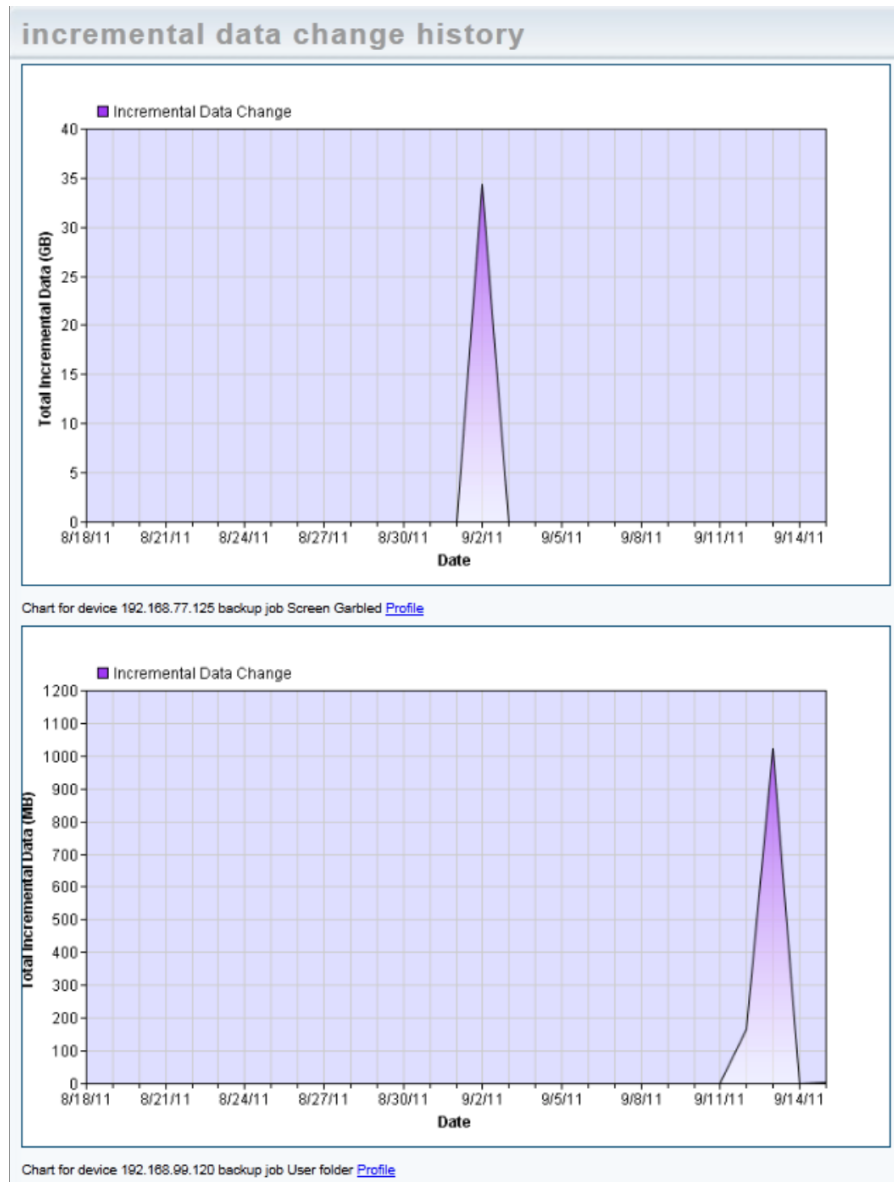


Figure 99 - Reports - Backup Storage History



The incremental change graph is cumulative across all jobs. To see the same graph broken down by job, click the **get job data** button. This displays a new page with a separate graph for each job. The device name (IP address or host name) and job name appear below each graph. Click the **Profile** link after the job name to display the profile report for that job (see “[Backup Job Profile Report](#)” section).

Figure 100 - Reports - Incremental Data Change



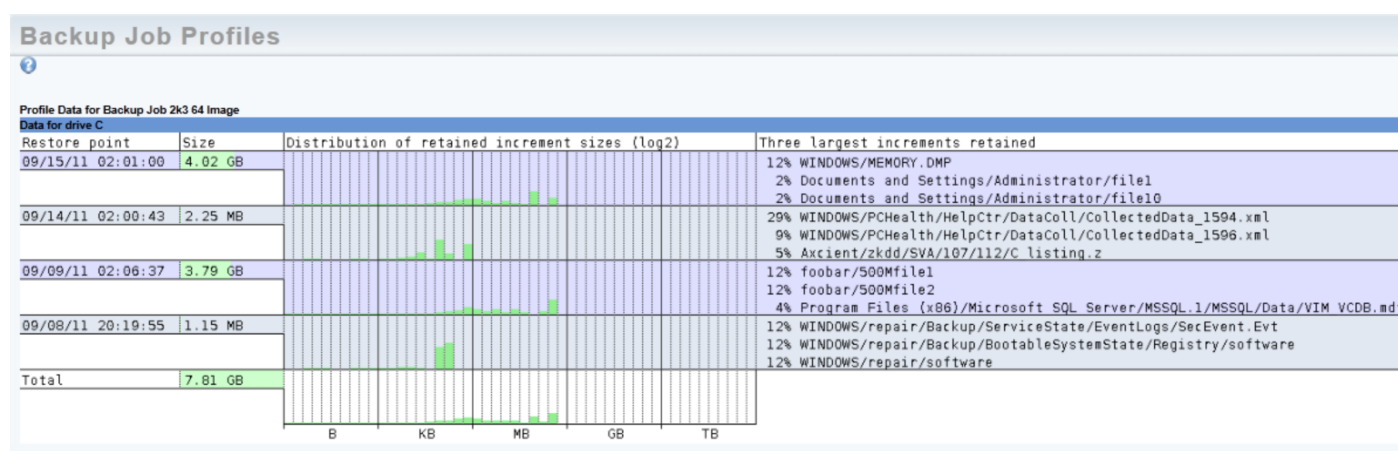
## Backup Job Profile Report

The Backup Job Profile report, which appears when you click the **Profile** link for a job on the Incremental Data Change History report, displays detailed information about each version (restore point) in that job. The table below describes the report contents.

The profile output displays one row per version in reverse chronological order with the latest shown at the top:

- The Size column shows the total size of the increments for a version.
- The distribution meters are a per-version histogram of increment sizes.
- The height of the distribution meters reflects the percentage of space relative to the respective restore points space consumed by increments falling within the respective size class.
- The three largest increments show the paths within the backup and the percentage of the restore points space consumed by the respective increment, ranked largest to smallest.

**Figure 101** - Reports - Backup Jobs Profile

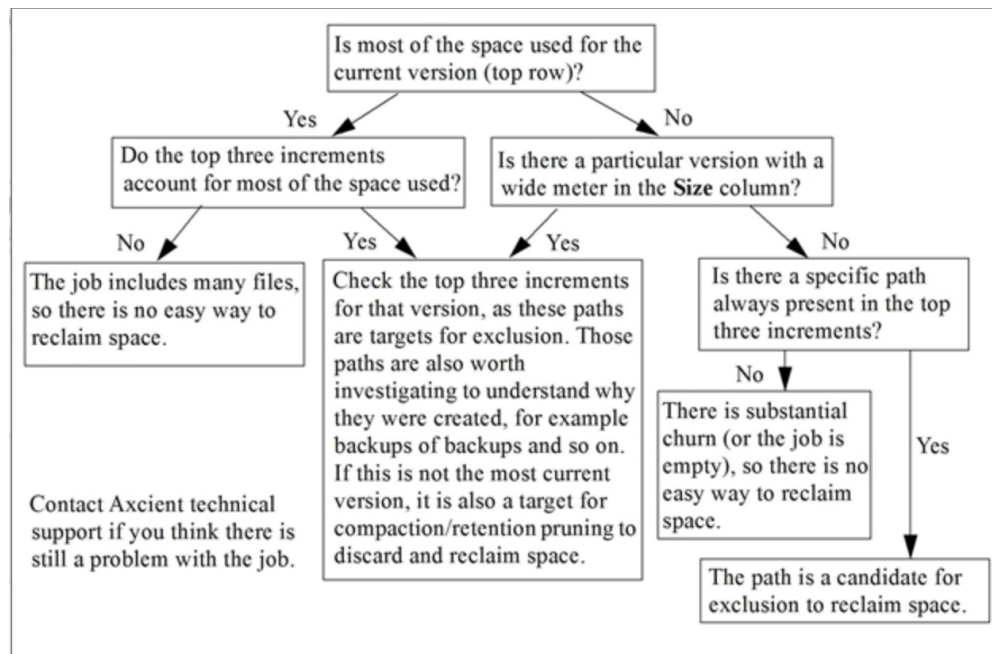


The following are guidelines for interpreting a profile:

1. The first row is the current version. Ideally, this version should contain at least 80% of the backups space. The profile warrants further investigation if the *Size* value is less than 80%. If it is less than 50%, this backup either has very large legitimate differentials or is snapshotting large files often (like a backup of a backup tends to do) and can be considered dysfunctional.
2. If all the meters within the distribution area occur on the left side of the area, there are no large increments to target for space reclamation. If the backup is large, it is achieving its size through large numbers of files, not large files.
3. Tall meters on the right side of the distribution area in any row except the top one (current version) indicate large increments that are ideal targets for space reclamation through retention/compaction tuning (see [Reduce Backup Job Size](#) ” section) as well as investigation as to why they are occurring.

4. Tall meters on the right side of the distribution area in the first row indicate large files in the current version. If there are no sizable increments below the first row for this file, there is a large file that does not change over time or changes very little. To reclaim space from this increment, you must exclude the path. You will not be reclaiming space by manipulating the retention period.
5. When you see tall meters within the distribution area towards the right side, these will likely be visible by name in the “Three largest increments” column, which identifies paths to exclude or investigate with the customer.

Use the following flowchart to quickly analyze a profile:



## Backup Jobs Profile Reports Fields and Descriptions

Field	Description
Restore Point	Displays the version date and time.
Size	Displays the size of that version (in MBs). The row background appears in a colored horizontal meter. The meter reflects the percentage of total job space used by that version. The bottom row is for the entire job (all versions combined).
Size distribution of differentials	<p>Displays an increment size histogram. The X axis categorizes increment occurrences by their size on a base-2 logarithmic scale. Each set of 10 sub-columns transitions to the next unit of size (Bytes, KB, MB, and so on). Within each 10-column set the sizes climb exponentially. The Bytes class columns are 1-2B, 2-4B, 4-8B, 8-16B, 16-32B, 32-64B, 64-128B, 128-256B, 256-512B, 512-1024B. The same progression is repeated for each size unit (KB, MB, and so on). This approach allows precise information about any size job (large or small) in a common display.</p> <p>A vertical meter appears within each histogram cell. The meter reflects the percentage of total version space used by that increment. This is effectively the same information for a single version that the Size column does for the entire job. The meters in the bottom row (Total) are computed relative to the entire backup size, not a single version.</p>
Three largest increments retained	<p>Displays the top three increments for each version ordered by size and includes the following information:</p> <ul style="list-style-type: none"> <li>Percentage of total version space used by that increment.</li> <li>Path of that increment (file) within the backup.</li> </ul>

## Schedule Backups Report

The Scheduled Backups report displays information about all defined backup jobs. Each line in the report represents a backup job. The table below describes the report contents. The report extends to multiple pages if necessary. You can get detailed profile information by clicking the **Profile** link for that job (see [Backup Job Profile Report](#) section).

- To change the number of jobs listed per page, enter the desired number in the **Rows Per Page** box and then press the **get results** button.
- Click on any column header (Schedule Name, Machine Address, Machine Description, OS Type, or Schedule Type) to order the entries alphabetically, alphanumerically, or by date as appropriate. Click the header to toggle the order: A-Z or Z-A alphabetically, 0 (zero)-Z or Z-0 alphanumerically, newest-to-oldest or oldest-to-newest by date.
- To export the report contents:
  - In the **Export options** line at the bottom of the report, click on the desired format (CSV, Excel, or XML).
  - A file download window appears. (This varies by operating system.) Save and download the file as directed.

**Figure 102** - Reports - Scheduled Backup Jobs

backup jobs						
<div> <div>?</div> <div>Rows per page: <input type="text" value="20"/></div> <div>get results</div> </div>						
Schedule Name	Machine Address	Machine Description	OS Type	Schedule Type	Next Backup	Show Profile
<a href="#">flockme</a>	<a href="#">192.168.44.224</a>	<a href="#">Tom's MAC</a>	Mac OS X	on-demand	(NA)	<a href="#">Profile</a>
<a href="#">backup on connect</a>	<a href="#">192.168.66.115</a>	<a href="#">backup on connect</a>	Windows	hourly	Wed, Jun 8, 3:00 PM	<a href="#">Profile</a>
<a href="#">2k3AD</a>	<a href="#">192.168.66.220</a>	<a href="#">2k3AD</a>	Windows	hourly	Wed, Jun 8, 3:00 PM	<a href="#">Profile</a>
<a href="#">asdf</a>	<a href="#">192.168.77.244</a>		Mac OS X	on-demand	(NA)	<a href="#">Profile</a>
<a href="#">Pictures</a>	<a href="#">192.168.77.244</a>		Mac OS X	on-demand	(NA)	<a href="#">Profile</a>
<a href="#">AD test</a>	<a href="#">192.168.99.11</a>	<a href="#">2k8 AD test</a>	Windows	on-demand	(NA)	<a href="#">Profile</a>
Export options: <a href="#">CSV</a>   <a href="#">Excel</a>   <a href="#">XML</a>						
Note*: Profiles are not supported for Mailbox Backups.						

### Schedule Backup Report Fields and Definitions

Field	Description
Schedule Name	Displays the name of the job. <ul style="list-style-type: none"> <li>Click the name to display the summary page for that job.</li> <li>Click <b>Schedule Name</b> to order the rows alphabetically by name. This is a toggle switch (A-Z, Z-A).</li> </ul>
Machine Address	Displays the IP address or machine name specified when the device was added. <ul style="list-style-type: none"> <li>Click the name or IP address to display the backup jobs summary page for that device.</li> <li>Click <b>Machine Address</b> to order the rows alphanumerically. This is a toggle switch (0-Z, Z-0).</li> </ul>
Machine Description	Displays the device alias specified when the device was added. (This field is blank if an alias was not specified.) <ul style="list-style-type: none"> <li>Click the description to display the backup jobs summary page for that device.</li> </ul>

Field	Description
	<ul style="list-style-type: none"><li>Click <b>Machine Description</b> to order the rows alphabetically by description. This is a toggle switch (A-Z, Z-A).</li></ul>
OS Type	Displays the operating system of the device. <ul style="list-style-type: none"><li>Click <b>OS Type</b> to order the rows alphabetically by operating system type. This is a toggle switch (A-Z, Z-A).</li></ul>
Schedule Type	Displays the type (frequency) of backup job. <ul style="list-style-type: none"><li>Click <b>Schedule Type</b> to order the rows alphabetically by schedule type. This is a toggle switch (A-Z, Z-A).</li></ul>
Next Backup	Displays when the next backup job run is scheduled.

## Backup Times Report

The Backup Times report displays a history of all backup job runs. This includes both local and Cloud backup jobs. (An offsite backup concatenates individual backup jobs into a single run at the specified time. See [Schedule Cloud Backup Job](#) section for more information. Each line in the report represents a backup job run. The report extends to multiple pages if necessary. The table below describes the report contents.

- To change the number of job runs listed per page, enter the desired number in the **Rows Per Page** box and then press the **get results** button.
- Click on any column header (Backup Name, Machine, Machine Description, User, Start Time, End Time, Elapsed Time, or Number of Files) to order the entries alphabetically, alphanumerically, or by date as appropriate. Click the header to toggle the order: A-Z or Z-A alphabetically, 0 (zero)-Z or Z-0 alphanumerically, newest-to-oldest or oldest-to-newest by date.
- To export the report contents:
  - In the **Export options** line at the bottom of the report, click on the desired format (CSV, Excel, or XML).
  - A file download window appears. (This varies by operating system.) Save and download the file as directed.



Figure 103 - Reports - Backup Times

backup times									
<div> <span>?</span> </div> <div>           Rows per page: <input type="text" value="20"/> </div> <div> <input type="button" value="get results"/> </div> <div>           503 results found         </div> <div> <a href="#">First</a>   <a href="#">Prev</a>   <a href="#">Page 7</a>, <a href="#">8</a>, <a href="#">9</a>, <a href="#">10</a>, <a href="#">11</a>, <a href="#">12</a>, <a href="#">13</a>, <a href="#">14</a>, <a href="#">15</a>, <a href="#">16</a>, <a href="#">17</a>, <a href="#">18</a>, <b>19</b>, <a href="#">20</a>, <a href="#">21</a>, <a href="#">22</a>, <a href="#">23</a>, <a href="#">24</a>, <a href="#">25</a>, <a href="#">26</a>   <a href="#">Next</a>   <a href="#">Last</a> </div>									
Backup Name	Machine	Machine Description	User	Start Time	End Time	Elapsed Time	Dirs & Files	Data	Failover Check
ExServer99201Ver001	192.168.99.201	server99201	admin	07/10/2012 - 2:00:14 PM	07/10/2012 - 2:00:49 PM	35 secs	250	512.15 MB	-
ExServer99201Ver001	192.168.99.201	server99201	admin	07/10/2012 - 3:00:14 PM	07/10/2012 - 3:00:48 PM	34 secs	250	512.15 MB	-
IMServ99201Ver001	192.168.99.201	server99201	admin	06/29/2012 - 4:23:53 PM	06/29/2012 - 4:31:15 PM	7 mins 22 secs	6	100.32 MB	<a href="#">View</a>
IMServ99201Ver001	192.168.99.201	server99201	admin	06/29/2012 - 4:47:12 PM	06/29/2012 - 5:39:00 PM	51 mins 48 secs	91523	15.63 GB	<a href="#">View</a>
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 11:56:09 AM	06/19/2012 - 11:58:09 AM	2 mins	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 12:56:57 PM	06/19/2012 - 12:57:02 PM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 1:57:01 PM	06/19/2012 - 1:57:05 PM	4 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 2:56:26 PM	06/19/2012 - 2:56:30 PM	4 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 3:57:02 PM	06/19/2012 - 3:57:06 PM	4 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 4:56:44 PM	06/19/2012 - 4:56:49 PM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 5:56:54 PM	06/19/2012 - 5:56:59 PM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 6:56:53 PM	06/19/2012 - 6:56:58 PM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/19/2012 - 7:56:53 PM	06/19/2012 - 7:56:58 PM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 9:56:56 AM	06/20/2012 - 9:57:01 AM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 10:56:53 AM	06/20/2012 - 10:56:58 AM	5 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 11:56:13 AM	06/20/2012 - 11:56:19 AM	6 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 12:56:17 PM	06/20/2012 - 12:56:24 PM	7 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 1:56:21 PM	06/20/2012 - 1:56:28 PM	7 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 2:56:15 PM	06/20/2012 - 2:56:23 PM	8 secs	68	1,000.00 MB	-
FFServ99221Ver001	192.168.99.221	server99221	admin	06/20/2012 - 3:56:44 PM	06/20/2012 - 3:56:51 PM	7 secs	68	1,000.00 MB	-
Export options: <a href="#">CSV</a>   <a href="#">Excel</a>   <a href="#">XML</a>									

## Backup Times Report Fields and Definitions

Field	Description
Backup Name	Displays the name of the job. <ul style="list-style-type: none"> <li>Click the name to display the summary page for that job.</li> <li>Click <b>Backup Name</b> to order the rows alphabetically by name. This is a toggle switch (A-Z, Z-A).</li> </ul>
Machine	Displays the IP address or machine name specified when the device was added. <ul style="list-style-type: none"> <li>Click the name or IP address to display the backup jobs summary page for that device.</li> <li>Click <b>Machine</b> to order the rows alphanumerically. This is a toggle switch (0-Z, Z-0).</li> </ul>
Machine Description	Displays the device alias specified when the device was added. (This field is blank if an alias was not specified.) <ul style="list-style-type: none"> <li>Click the description to display the backup jobs summary page for that device.</li> <li>Click <b>Machine Description</b> to order the rows alphabetically by description. This is a toggle switch (A-Z, Z-A).</li> </ul>
User	Displays the name of the user who created the backup job. <ul style="list-style-type: none"> <li>Click <b>User</b> to order the rows alphabetically by name. This is a toggle switch (A-Z, Z-A).</li> </ul> <p><b>Note:</b> Even if a different user invokes the job, for example clicks the start button in one of the dashboard tabs or the start</p>

Field	Description
	link in the job description, the name of the user who created the backup job is still displayed.
Start Time	Displays the time the backup job started. <ul style="list-style-type: none"> <li>Click <b>Start Time</b> to order the rows by start times. This is a toggle switch (newest-oldest, oldest-newest).</li> </ul>
End Time	Displays the time the backup job completed (or ended if it did not complete successfully). <ul style="list-style-type: none"> <li>Click <b>End Time</b> to order the rows by end times. This is a toggle switch (newest-oldest, oldest-newest).</li> </ul>
Elapsed Time	Displays the amount of time the backup job ran. <ul style="list-style-type: none"> <li>Click <b>Elapsed Time</b> to order the rows by duration. This is a toggle switch (shortest-longest, longest-shortest).</li> </ul>
Dirs & Files	Displays the number of files processed (backed up). <ul style="list-style-type: none"> <li>Click <b>Dirs &amp; Files</b> to order the rows by the number of files processed. This is a toggle switch (most-least, least-most).</li> </ul>
Data	Displays the amount of data processed. This value does not represent the complete size of the backup job (unless this is an on-demand or first time backup). It represents just the actual number of bytes processed during the run.
Validation Snapshot	For image backup jobs with <i>AutoVerify</i> enabled (see <a href="#">Configuring AutoVerify</a> section), displays a View link. (A dash is displayed in this field for all other entries.) Click View to display the VM desktop page shot for that image. The page shot appears in a separate window that includes the job name and start time. If the picture displays a normal desktop page shot, the VM booted successfully. If the picture displays a blue page (or other error condition), the VM did not boot successfully.

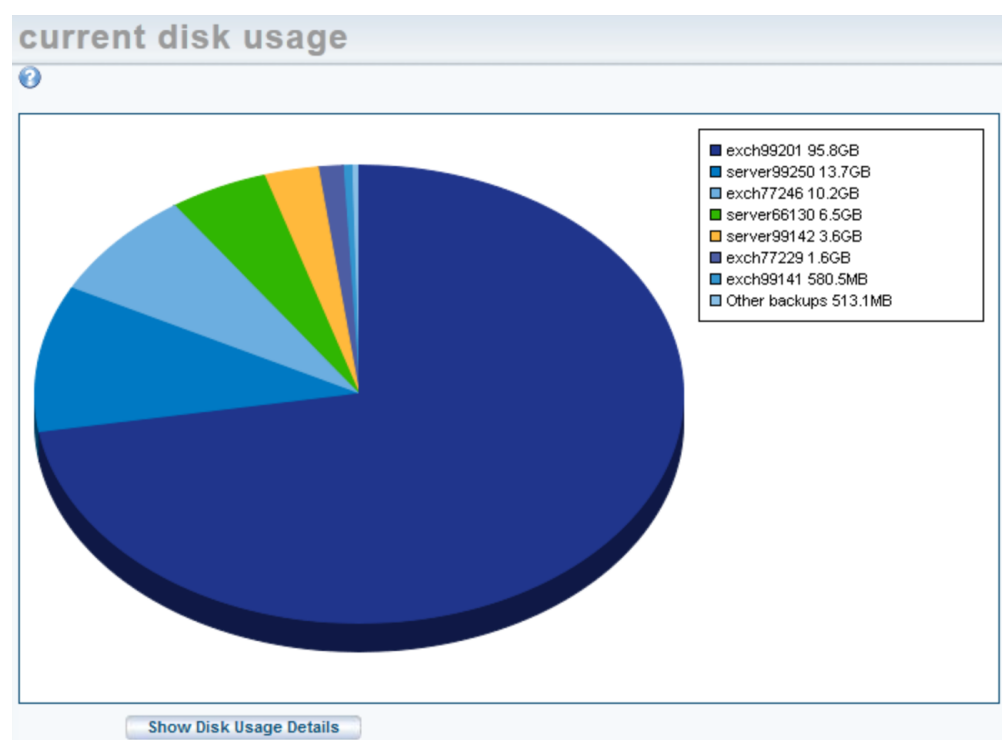
## Current Disk Usage Report

The current disk usage report displays the following information:

- **Disk usage per device chart** - This chart displays appliance disk space use broken down by device. The pie chart is subdivided by color codes with the following descriptive information on the right:
  - **device\_name** entry is the storage space used to back up that device. The seven devices that use the most space are listed individually by device name and size in descending order from largest to smallest. (All devices are listed this way if the total number of devices is eight or fewer.)
  - **Other backups** entry is the cumulative space used by all the additional devices (eighth and beyond) when there are more than seven devices. (This entry does not appear if the total number of devices is eight or fewer.)

The displayed numbers are approximations of the actual storage space used. This is the same information that is displayed in the user dashboard (see [Disk Utilization Panel](#) section).

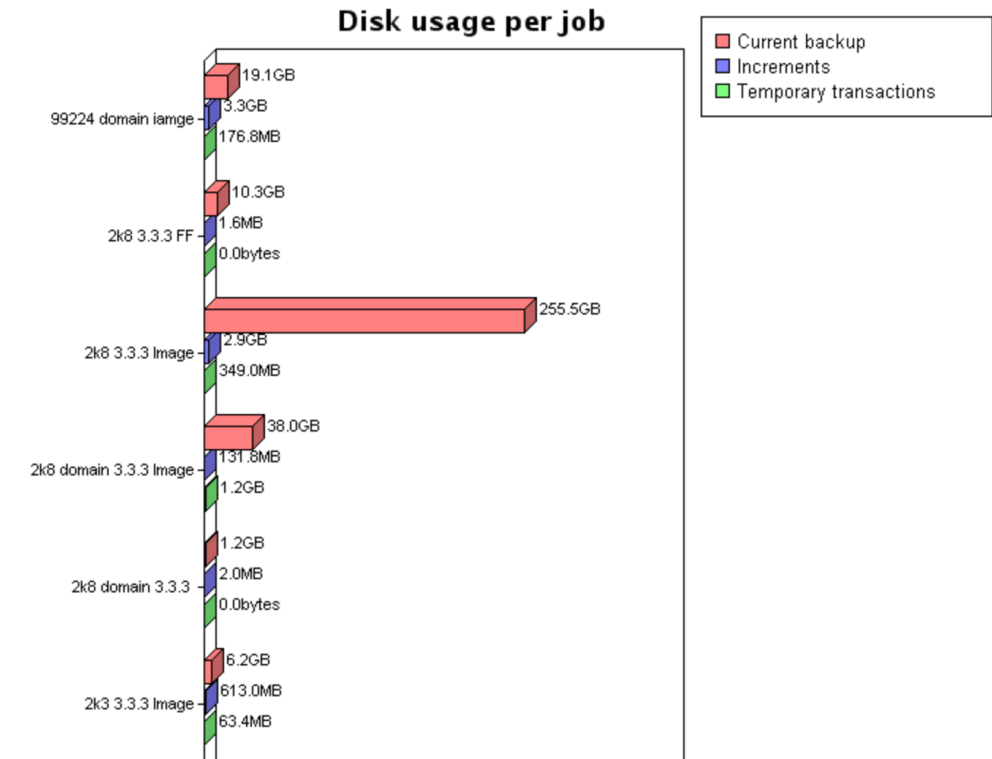
Figure 104 - Reports - Disk Usage Per Device



- **Disk usage per job chart** - When you click the Show Disk Usage Details button, a second chart appears that breaks down disk usage per job. All jobs on the appliance are listed, and loading this chart can take some time for appliances with many or large jobs. Three values are displayed for each job:
  - **Current Backup** - Displays the size of the current backup job. The current backup is a complete backup of all data needed to restore the current version.

- **Increments** - Displays the cumulative size of all older versions. Only the current backup includes all data in a backup job. Older versions save just the changed (delta) information, and the increments value is the total storage space needed for all the older versions combined.
- **Temporary Transactions** - A copy is created at each backup run and retained until the new snapshot is verified as valid and consistent. The temporary transaction is the space used for any copies while they are verified. (A copy is discarded after verification.)

Figure 105 - Reports - Disk Usage Per Job



# Event Logging

## View Log Messages

The Axcient appliance maintains an event log. The log displays messages about backup, restore, device, user, system and other types of events that occur on the Axcient appliance.


To view log messages, do one of the following:

- Click the **events** button at the top of the UMC page.
- Click the **Events** tab on the dashboard and then click the **See All Events** link.
- Select the event log option located on the left of the Events page.

By default, all events in the log are displayed, 20 per page, starting with the most recent. **First, Prev, Page#, Next, and Last** links are provided to move among the pages (when there are multiple pages). To configure the view:

- To order the entries, click on any column header (*Type, Date, Action, User*), which orders the entries alphabetically or by date as appropriate. Click the header to toggle the order (A-Z or Z-A alphabetically; newest-to-oldest or oldest-to-newest by date).
- The **Action** column displays up to 256 characters of a message. If “(truncated)” appears at the end of a message, there is more text to be displayed. To see the complete message in a pop-up window, click the **View** link for that message.
- To filter the list, do one of the following:
  - To filter by date, click the **Date** button, specify a date (click the calendar icon and select the day), and then click the **filter** button to display the events on that day.
  - To filter by user, click the **User** button, specify a user from the drop-down menu, and then click the **filter** button to display the events generated by that user.
  - To filter by event type(s), click the **Type** button, select one or more types from the scrollable list, and then click the **filter** button to display the events of those types.
    - To select a single type, click on that **type**.
    - To select a consecutive list, click the first type and then Shift-click the last.
    - To select a non-consecutive list, Ctrl-click each type.
  - To filter by backup job, click the **Schedule** button, select the job name from the pull-down list, and then click the **filter** button to display the events generated by that job.
  - To reset the number of rows displayed, enter the desired number of rows in the **Rows Per Page** box, and then click the **filter** button to reset the display to that number of rows. The default number of rows is 20 per page.

Figure 106 - Events Page



dashboard

devices

reports

events

users

system

docs

! events

event log

purge log

configure alerting

events

filtering ☒ None

Date: 07/10/2012

Onsite Backup Events

BACKUP\_WARNING

BACKUP\_FAILED

BACKUP\_ON\_CONNECT\_SET

BACKUP\_STARTED

BACKUP\_SUCCEEDED

BACKUP\_CANCELLED\_BY\_USER

BACKUP\_CANCELLED\_EXCEEDED\_TIME\_THRESHOLD

BACKUP\_SPACE\_EXCEEDED

BACKUP\_DATA\_CHANGE

Type: ☐

Schedule: ☐ -- Select a Schedule --

User: -- Select a User --

Rows per page: 7

filter

2,489 results found

First

Prev

Page 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

Next

Last

Type	Date	Action	User	Details
BACKUP_FAILED	07/10/2012 - 6:32:20 PM	[For corrective actions <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> ] Backup 'FFServ77117Ver001' on 192.168.77.117 Failed during pre-backup ping	admin	<a href="#">View</a>
BACKUP_STARTED	07/10/2012 - 6:32:20 PM	Backup Started: 'FFServ77117Ver001' on 192.168.77.117	admin	<a href="#">View</a>
USER_LOGIN	07/10/2012 - 6:29:16 PM	User: admin logged in	admin	<a href="#">View</a>
EBR_BACKUP_SUCCEEDED	07/10/2012 - 6:25:01 PM	Exchange Mailbox Backup (ExServer77229Ver001) on 192.168.77.229 succeeded	UBS	<a href="#">View</a>
BACKUP_DATA_CHANGE	07/10/2012 - 6:24:21 PM	Backup data for IMServ99201Ver001 on machine server99201 has changed by 83.5 KB	UBS	<a href="#">View</a>
SERVER_ALIVE_BACKUP_SUCCEEDED	07/10/2012 - 6:24:21 PM	Backup Hourly for IMServ99201Ver001 on 192.168.99.201 completed Successfully ( Included drives - C: )	admin	<a href="#">View</a>
SERVER_ALIVE_BACKUP_WARNING	07/10/2012 - 6:24:19 PM	Backup Hourly for IMServ99201Ver001 on 192.168.99.201 Warning - StdErr - Warning: Unable to open path "Windows/System32/LogFiles /WVRtBackup/EtwRTEventLog-System.etl". Cause: Permission denied Error: Unable to copy "Windows/System32/LogF ... (truncated)	admin	<a href="#">View</a>

Export options:

CSV

Excel

XML

© 2020 Axcient, Inc. All Rights Reserved.

193

## Log Messages Format and Types

The UMC uses a five-column display for a log messages. The tables below describes the fields in the display.

**Log Messages Fields and Definitions**

Field	Definition
Type	Displays the category type to which this event belongs.
Date	Displays the date and time the event occurred. <b>Form</b> - <i>mm/dd/yyyy - hh:mm:ss AM/PM</i> <b>Example</b> - <i>03/20/2009 - 11:09:37 AM</i>
Action	Displays the message text for this event.
User	Displays the name of the user that initiated the action. In addition to the three default users (admin, backupuser, and limitedbackupuser) and any created users, the system has the following internal users that might appear in this field: <ul style="list-style-type: none"> <li>• <b>UBS</b>—Processes associated with all backup actions.</li> <li>• <b>Off-site</b>—Process associated with offsite backup operations.</li> </ul>
Details	Clicking on the <b>View</b> link displays the complete message in a pop-up window.

The table below describes the event types within each of the event categories. The event categories are listed alphabetically in the table. Two names appear for each type. The name in upper case is the name that appears in the event messages. The name in parentheses is the name that appears in the Alerting page. The message flow for most events is as follows:

1. Generate a *STARTED* message when an event begins.
2. As the operation progresses, generate *INFO* (successful) or *WARNING* (unsuccessful or partially successful) messages when subactions complete.
3. Generate a *SUCCEEDED* or *FAILED* message when the event completes.

**Bare Metal Restore Lock Events**

Type	Description
<i>BMR_RESTORE_LOCK_STARTED</i> (BMR image-lock started)	Started a Bare Metal Restore lock image operation. These messages indicate normal operations.
<i>BMR_RESTORE_LOCK_SUCCEEDED</i> (BMR image-lock SUCCEEDED)	Bare Metal Restore lock image operation succeeded. These messages indicate the BMR locking process completed without any errors or qualifications. These messages indicate normal operations.
<i>BMR_RESTORE_LOCK_FAILED</i> (BMR image-lock FAILED)	Bare Metal Restore lock image operation failed. These messages indicate the lock process did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BMR_RESTORE_LOCK_WARNING</i> (BMR image-lock warning)	Warning generated when locking a Bare Metal Restore image. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BMR_RESTORE_LOCK_INFO</i> (BMR image-lock info)	Status information during an Bare Metal Restore lock operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.



## Bare Metal Restore Unlock Events

Field	Description
<i>BMR_RESTORE_UNLOCK_STARTED</i> (BMR image-unlock started)	Started a Bare Metal Restore unlock image operation. These messages indicate normal operations of starting the action.
<i>BMR_RESTORE_UNLOCK_SUCCEEDED</i> (BMR image-unlock SUCCEEDED)	Bare Metal Restore unlock image operation succeeded. These messages indicate the BMR unlocking process completed without any errors or qualifications. These messages indicate normal operations.
<i>BMR_RESTORE_UNLOCK_FAILED</i> (BMR image-unlock FAILED)	Bare Metal Restore unlock image operation failed. These messages indicate the unlock process did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BMR_RESTORE_UNLOCK_WARNING</i> (BMR image-unlock warning)	Warning generated when unlocking a Bare Metal Restore image. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BMR_RESTORE_UNLOCK_INFO</i> (BMR image-unlock info)	Status information during a Bare Metal Restore unlock operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.

## Device Events

Fields	Description
<i>BACKUP_JOB_ADDED</i> (Backup job added)	Added a backup job. These messages refer to creating a job, not running it (which are recorded in the <i>BACKUP_*</i> types). These messages indicate normal operations.
<i>BACKUP_JOB_DELETED</i> (Backup job deleted)	Deleted a backup job. These messages indicate normal operations.
<i>BACKUP_JOB_UPDATED</i> (Backup job updated)	Updated a backup job. These messages refer to updating the job definition, not running it. These messages indicate normal operations.
<i>DEVICE_ADDED</i> (Backup device added)	Added a device. These messages indicate normal operations.
<i>DEVICE_DELETED</i> (Backup device deleted)	Deleted a device. These messages indicate normal operations.
<i>DEVICE_MISSING</i> (Backup device has been missing for an extended period)	No successful backups for a laptop during the past two-week period.
<i>DEVICE_UPDATED</i> (Backup device updated)	Updated the settings for a device. These messages indicate normal operations.
<i>DEVICE_CREDENTIALS_UPDATED</i> (Backup device password updated)	Updated the administrative name or password for a device. These messages indicate normal operations.

## Exchange Mailbox Backup Events

Type	Description
<i>EBR_BACKUP_STARTED</i> (Exchange Mailbox Backup STARTED)	Started an Exchange mailbox backup operation. These messages indicate normal operations.
<i>EBR_BACKUP_SUCCEEDED</i> (Exchange Mailbox Backup SUCCEEDED)	Exchange mailbox backup operation succeeded. These messages indicate the Exchange mailbox backup process completed without any errors or qualifications. These messages indicate normal operations.
<i>EBR_DATA_MIGRATION_FAILED</i>	Exchange mailbox migration operation failed. These messages indicate the Exchange mailbox migration did not complete

Type	Description
(Exchange Mailbox Data Migration FAILED)	successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
EBR_BACKUP_WARNING (Exchange Mailbox Backup warning)	Warning generated when backing up an Exchange mailbox. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
EBR_BACKUP_FAILED (Exchange Mailbox Backup FAILED)	Exchange mailbox backup operation failed. These messages indicate the Exchange mailbox backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
EBR_RETENTION_FAILED (Exchange Mailbox Retention FAILED)	Exchange mailbox retention operation failed. These messages indicate the Exchange mailbox retention operation did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>

## Exchange Mailbox Restore Events

Type	Description
EBR_RESTORE_SUCCEEDED (Exchange Mailbox Restore SUCCEEDED)	Exchange mailbox restore operation succeeded. These messages indicate the Exchange mailbox restore process completed without any errors or qualifications. These messages indicate normal operations.
EBR_RESTORE_WARNING (Exchange Mailbox Restore warning)	Warning generated when restoring an Exchange mailbox. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
EBR_RESTORE_STARTED (Exchange Mailbox Restore started)	Started an Exchange mailbox restore operation. These messages indicate normal operations.
EBR_RESTORE_FAILED (Exchange Mailbox Restore FAILED)	Exchange mailbox restore operation failed. These messages indicate the Exchange mailbox restore operation did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>

## Export Copy Events

Field	Events
EXPORT_STARTED (Export started)	Started a backup operation to an export drive. These messages indicate normal operations.
EXPORT_SUCCEEDED (Export SUCCEEDED)	Backup operation to export drive succeeded. These messages indicate the backup completed without any errors or qualifications. These messages indicate normal operations.
EXPORT_FAILED (Export FAILED)	Backup operation to export drive failed. These messages indicate the backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
EXPORT_WARNING (Export warning)	Warning generated from a backup operation to an export drive. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
EXPORT_INFO (Export info)	Status information during a backup operation to an export drive. These messages usually record the successful completion of subtasks. These messages indicate normal operations.
EXPORT_CANCELLED_BY_USER (Export canceled by user)	Running backup operation to an export drive cancelled manually. These messages indicate the user intervened to cancel the job, usually by clicking the <b>cancel</b> button on the user dashboard.

## Network Events

Field	Description
<i>CANT_SEND_EMAIL</i> (Unable to send email)	Failed to send an e-mail alert notification. <b>It is recommended that alerting be configured for this type of message.</b>
<i>CANT_SEND_PSA_TICKET</i> (PSA integration FAILED)	Failed to send ticket information to a PSA tool. <b>It is recommended that alerting be configured for this type of message.</b>

## Offsite Backup or Verification Events

Field	Description
<i>OFFSITE_STARTED</i> (Offsite backup started)	Started an offsite backup operation. These messages indicate normal operations.
<i>OFFSITE_SUCCEEDED</i> (Offsite backup SUCCEEDED)	Offsite backup operation succeeded. These messages indicate the backup completed without any errors or qualifications. These messages indicate normal operations.
<i>OFFSITE_FAILED</i> (Offsite backup FAILED)	Offsite backup operation failed. These messages indicate the backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>OFFSITE_WARNING</i> (Offsite backup warning)	Warning generated from an offsite backup operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>OFFSITE_INFO</i> (Offsite backup info)	Status information during an offsite backup operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.
<i>OFFSITE_CANCELLED_BY_USER</i> (Backup cancelled by user)	Running offsite backup job cancelled manually. These messages indicate the user intervened to cancel the job, usually by clicking the <b>cancel</b> button on the user dashboard.
<i>OFFSITE_STORAGE_EXCEEDED</i> (Offsite storage exceeded)	These messages indicate the amount of space required to store the job at the Axcient data center exceeded the entitled amount allocated to this appliance. <b>It is recommended that alerting be configured for this type of message.</b>

## Offsite DAS Copy Events

Field	Description
<i>DAS_COPY_STARTED</i> (DAS drive copy started)	Started a DAS copy operation. These messages indicate normal operations.
<i>DAS_COPY_SUCCEEDED</i> (DAS drive copy SUCCEEDED)	DAS copy operation succeeded. These messages indicate the backup completed without any errors or qualifications. These messages indicate normal operations.
<i>DAS_COPY_FAILED</i> (DAS drive copy FAILED)	DAS copy operation failed. These messages indicate the backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>DAS_COPY_WARNING</i> (DAS drive copy warning)	Warning generated from a DAS copy operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>DAS_COPY_INFO</i> (DAS drive copy info)	Status information during a DAS copy operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations

## Onsite Backup Events

Field	Description
<i>BACKUP_STARTED</i> (Backup started)	Started an onsite backup operation. These messages indicate normal operations.
<i>BACKUP_SUCCEEDED</i> (Backup SUCCEEDED)	Onsite backup operation succeeded. These messages indicate the backup completed without any errors or qualifications. These messages indicate normal operations.
<i>BACKUP_FAILED</i> (Backup FAILED)	Onsite backup operation failed. These messages indicate the backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BACKUP_ON_CONNECT_SET</i> (Backup on connect SET)	Running a backup job with the "Backup on Connect" parameter set. This parameter is an option for laptops only.
<i>BACKUP_WARNING</i> (Backup warning)	Warning generated from an onsite backup operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BACKUP_CANCELLED_BY_USER</i> (Backup cancelled by user)	Running onsite backup job cancelled manually. These messages indicate the user intervened to cancel the job, usually by clicking the <b>cancel</b> button on the user dashboard.
<i>BACKUP_SPACE_EXCEEDED</i> (Backup failed because space on appliance exceeded entitlements)	The backup did not complete successfully because the space needed to complete the task exceeded the current entitlements for this user account. <b>It is recommended that alerting be configured for this type of message.</b>
<i>BACKUP_DATA_CHANGE</i> (Backup data has changed)	These messages list the amount a backup job changed in size after a job run.
<i>BACKUP_EXCEEDED_TIME_THRESHOLD</i> (Backup exceeded time threshold)	The backup job has not completed within the specified threshold interval (number of hours). These messages may or may not indicate a problem.

## Pruning Events

Type	Description
<i>SELECTIVE_PRUNING_SUCCEEDED</i> (Selective pruning SUCCEEDED)	Status information during a selective pruning operation. These messages usually record the successful completion of selective pruning. These messages indicate normal operations.
<i>SELECTIVE_PRUNING_STARTED</i> (Selective pruning started)	Started a selective pruning operation. These messages indicate normal operations.
<i>TEMPORAL_PRUNING_FAILED</i> (Temporal pruning FAILED)	Temporal pruning operation failed. These messages indicate the process did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SELECTIVE_PRUNING_FAILED</i> (Selective pruning FAILED)	Selective pruning operation failed. These messages indicate a subtask did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>TEMPORAL_PRUNING_STARTED</i> (Temporal pruning started)	Started a temporal pruning operation. These messages indicate normal operations.
<i>TEMPORAL_PRUNING_SUCCEEDED</i> (Temporal pruning SUCCEEDED)	Status information during a temporal pruning operation. These messages usually record the successful completion of temporal pruning. These messages indicate normal operations.

## Restore Events

Field	Description
<i>RESTORE_STARTED</i>	Started a restore operation. These messages indicate normal operations.

Field	Description
(Restore started)	
<i>RESTORE_SUCCEEDED</i> (Restore SUCCEEDED)	Restore operation succeeded. These messages indicate the restore completed without any errors or qualifications. These messages indicate normal operations.
<i>RESTORE_FAILED</i> (Restore FAILED)	Restore operation failed. These messages indicate the restore did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>RESTORE_WARNING</i> (Restore warning)	Warning generated from a restore operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>RESTORE_CANCELLED_BY_USER</i> (Restore canceled by user)	Running restore operation cancelled manually. These messages indicate the user intervened to cancel the restore, usually by clicking the <b>cancel</b> button on the user dashboard.

## Service Alive Backup Events

Field	Description
<i>SERVER_ALIVE_BACKUP_STARTED</i> (Server Alive Backup started)	Started a Server Alive backup operation. These messages indicate normal operations.
<i>SERVER_ALIVE_BACKUP_SUCCEEDED</i> (Server Alive Backup SUCCEEDED)	Server Alive backup operation succeeded. These messages indicate the backup completed without any errors or qualifications. These messages indicate normal operations.
<i>SERVER_ALIVE_BACKUP_FAILED</i> (Server Alive Backup FAILED)	Server Alive backup operation failed. These messages indicate the backup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_BACKUP_WARNING</i> (Server Alive Backup warning)	Warning generated from a Server Alive backup operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_BACKUP_INFO</i> (Server Alive Backup info)	Status information during a ServerAlive operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.

## Server Alive Validation Events

Field	Description
<i>SERVER_ALIVE_VALIDATION_STARTED</i> (Server Alive Validation started)	After running an image backup job, a validation check was started to ensure the latest version (restore point) can be used as a virtual machine image.
<i>SERVER_ALIVE_VALIDATION_COMPLETED</i> (Server Alive Validation COMPLETED)	The validation check to verify the latest image backup job version (restore point) can be used as a virtual machine image completed successfully.
<i>SERVER_ALIVE_VALIDATION_CANCELLED</i> (Server Alive Validation CANCELLED)	The validation check to verify the latest image backup job version (restore point) can be used as a virtual machine image was cancelled.
<i>SERVER_ALIVE_VALIDATION_FAILED</i> (Server Alive Validation FAILED)	The validation check to verify the latest image backup job version (restore point) can be used as a virtual machine image was canceled.

## Server Alive Virtual Machine Edit

Type	Description
<i>SERVER_ALIVE_EDIT_VM_FAILED</i>	Virtual Machine edit operation failed. These messages indicate the process did not complete successfully and provide

Type	Description
(Server Alive edit VM failed)	information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_EDIT_VM_SUCCEEDED</i> (Server Alive edit VM succeeded)	Virtual Machine edit operation succeeded. These messages indicate the process completed without any errors or qualifications. These messages indicate normal operations.

## Server Alive Virtual Machine Start

Field	Description
<i>SERVER_ALIVE_START_VM_STARTED</i> (Server Alive start VM started)	Starting a virtual machine (VM) on the Axcient appliance. These messages indicate normal operations. The “Start VM” category includes the following actions: start failover VM, resume failover VM, start failover VM from BMR, start test VM, and resume test VM.
<i>SERVER_ALIVE_START_VM_SUCCEEDED</i> (Server Alive start VM SUCCEEDED)	VM startup operation succeeded. These messages indicate the startup completed without any errors or qualifications. These messages indicate normal operations.
<i>SERVER_ALIVE_START_VM_FAILED</i> (Server Alive start VM FAILED)	VM startup operation failed. These messages indicate the startup did not complete successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_START_VM_WARNING</i> (Server Alive start VM warning)	Warning generated during VM startup operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_START_VM_INFO</i> (Server Alive start VM info)	Status information during a VM startup operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.

## Server Alive Virtual Machine Stop

Field	Description
<i>SERVER_ALIVE_STOP_VM_STARTED</i> (Server Alive Backup started)	Stopping a virtual machine (VM) on the Axcient appliance. These messages indicate normal operations when starting the action. The “Stop VM” category includes the following actions: stop failover VM, pause failover VM, start BMR from failover VM (which pauses the VM), stop test VM, and pause test VM.
<i>SERVER_ALIVE_STOP_VM_SUCCEEDED</i> (Server Alive Backup SUCCEEDED)	VM stop operation succeeded. These messages indicate the VM stopped without any errors or qualifications. These messages indicate normal operations.
<i>SERVER_ALIVE_STOP_VM_FAILED</i> (Server Alive Backup FAILED)	VM stop operation failed. These messages indicate the VM did not stop successfully and provide information about the problem. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_STOP_VM_WARNING</i> (Server Alive Backup warning)	Warning generated during VM stop operation. These messages indicate that a subtask did not complete successfully and should be investigated. <b>It is recommended that alerting be configured for this type of message.</b>
<i>SERVER_ALIVE_STOP_VM_INFO</i> (Server Alive Backup info)	Status information during a VM stop operation. These messages usually record the successful completion of subtasks. These messages indicate normal operations.

## System Events

Field	Description
<i>AUTO_PRUNING</i>	The auto pruning feature is active. These messages indicate the Auto Prune Detection feature has been enabled.
<i>REGISTRATION_SUCCEEDED</i> (Registration SUCCEEDED)	Registering the appliance with the RMC succeeded. This typically occurs during installation.
<i>REGISTRATION_FAILED</i> (Registration FAILED)	Registering the appliance with the RMC failed. This typically occurs during installation. <b>It is recommended that alerting be configured for this type of message.</b>

Field	Description
<p><i>LOW_DISK_SPACE_ALERT</i></p> <p><i>LOW_DISK_SPACE_ALERT_20_PCT</i></p> <p><i>LOW_DISK_SPACE_ALERT_10_PCT</i></p> <p>(Low disk space alert Low disk space alert 20% Low disk space alert 10%)</p>	Appliance disk space filled to near capacity. The 20% and 10 % messages indicate that only 20% or 10% of disk space is still available. This is a warning that you either need to increase the storage capacity of the appliance soon (upgrade to a larger model) or delete a substantial number of backup jobs. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>NO_DISK_SPACE_ALERT</i></p> <p>(No disk space left alert)</p>	The Axcient appliance has run out of available storage space, which means backup jobs cannot run successfully and could result in data corruption. This requires immediate attention to add capacity (upgrade appliance) or delete existing backup jobs. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>VSS_ISSUES_PRESENT_ON_DEVICE</i></p> <p>(VSS issues present on device)</p>	VSS is not configured properly to support the Axcient solution. These messages indicate what VSS-related problems are present. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>ONSITE_STORAGE_EXCEEDED</i></p> <p>(Onsite storage exceeded)</p>	Backup did not complete successfully because the space needed to complete the task exceeded the current entitlements for this user account. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>SYSTEM_SMART_DRIVE_CHECK_FAILED</i></p> <p>(SMART drive check FAILED)</p>	Disk drive health check operation failed. A failure here means there may be a problem with the disk drive, controller, or other component that affects disk access. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>SYSTEM_RAID_DRIVE_CHECK_FAILED</i></p> <p>(RAID drive check FAILED)</p>	The system could not complete the RAID implementation. These messages indicate either a disk or the RAID controller failed (although it could be due to a transient condition). <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>SYSTEM_RAID_DRIVE_CHECK_WARNING</i></p> <p>(RAID drive check WARNING)</p>	The RAID disks are re-syncing. These messages indicate the mirror is not available (potential single point of failure) until the sync operation is complete.
<p><i>SYSTEM_SHUTDOWN</i></p> <p>(System is shutting down)</p>	The system is shutting down. These messages indicate someone has initiated a shutdown.
<p><i>SYSTEM_ENABLE_ACCESS</i></p> <p>(System access is enabled)</p>	Axcient support employee access to the system is enabled. Axcient support personnel have special tools to maintain appliances, and these message indicate access is allowed.
<p><i>SYSTEM_DISABLE_ACCESS</i></p> <p>(System access is disabled)</p>	Axcient support employee access to the system is disabled. Axcient support personnel have special tools to maintain appliances, and these message indicate access has been blocked.
<p><i>ENTITLEMENTS_VALID</i></p> <p>(Entitlements valid)</p>	The appliance is authorized (entitled) to perform specified operations. These messages indicate normal operations.
<p><i>ENTITLEMENTS_INVALID</i></p> <p>(Entitlements invalid)</p>	The appliance could not authorize entitlements. These messages indicate either there is no entitlement information on the appliance or the information is invalid. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>EXTITLEMENTS_EXPIRED</i></p> <p>(Entitlements expired)</p>	These messages indicate the entitlements allowed to this account have expired. <b>It is recommended that alerting be configured for this type of message.</b>
<p><i>ENTITLEMENTS_REFRESHED</i></p> <p>(Entitlement refreshed)</p>	A new entitlement record was loaded into the Axcient appliance. These messages indicate normal operations.
<p><i>ENTITLEMENTS_WARNING</i></p> <p>(Entitlements warning)</p>	This message appears when the current account entitlements are about to expire.

## UI Update Events

Field	Description
<i>EVENT_LOG_PURGED</i>	Event log messages purged. These messages indicate normal operations.

Field	Description
(Event log purged)	
<i>QOS_BANDWIDTH_UPDATED</i> (QOS Bandwidth updated)	Bandwidth throttling settings changed. These are configured through the Quality of Service page. These messages indicate normal operations.
<i>SYSTEM_CONFIG_UPDATED</i> (System config updated)	One or more system configuration settings changed. These messages indicate normal operations.
<i>VOLUME_INTEGRITY_CHECK_ALERT</i> (Data integrity check)	A volume that was in a previous backup does not exist in the latest backup.

## User Events

Field	Description
<i>USER_LOGIN</i> (User login)	User logged into the UMC.
<i>USER_LOGOUT</i> (User logout)	User logged out of the UMC.
<i>USER_ADDED</i> (User account added)	UMC user added.
<i>USER_DELETED</i> (User account deleted)	UMC user deleted.
<i>USER_UPDATED</i> (User account updated)	UMC user profile changed.
<i>USER_LOCKED</i> (User account locked)	UMC user account locked, which prevents the user from logging into the UMC.
<i>USER_PASSWORD_CHANGED</i> (Password changed)	UMC user account password changed.

## Other Events

Field	Description
<i>VOLUME_INTEGRITY_CHECK_ALERT</i> (Volume integrity check)	Checks if all volumes in a previous backup exist in the latest backup.



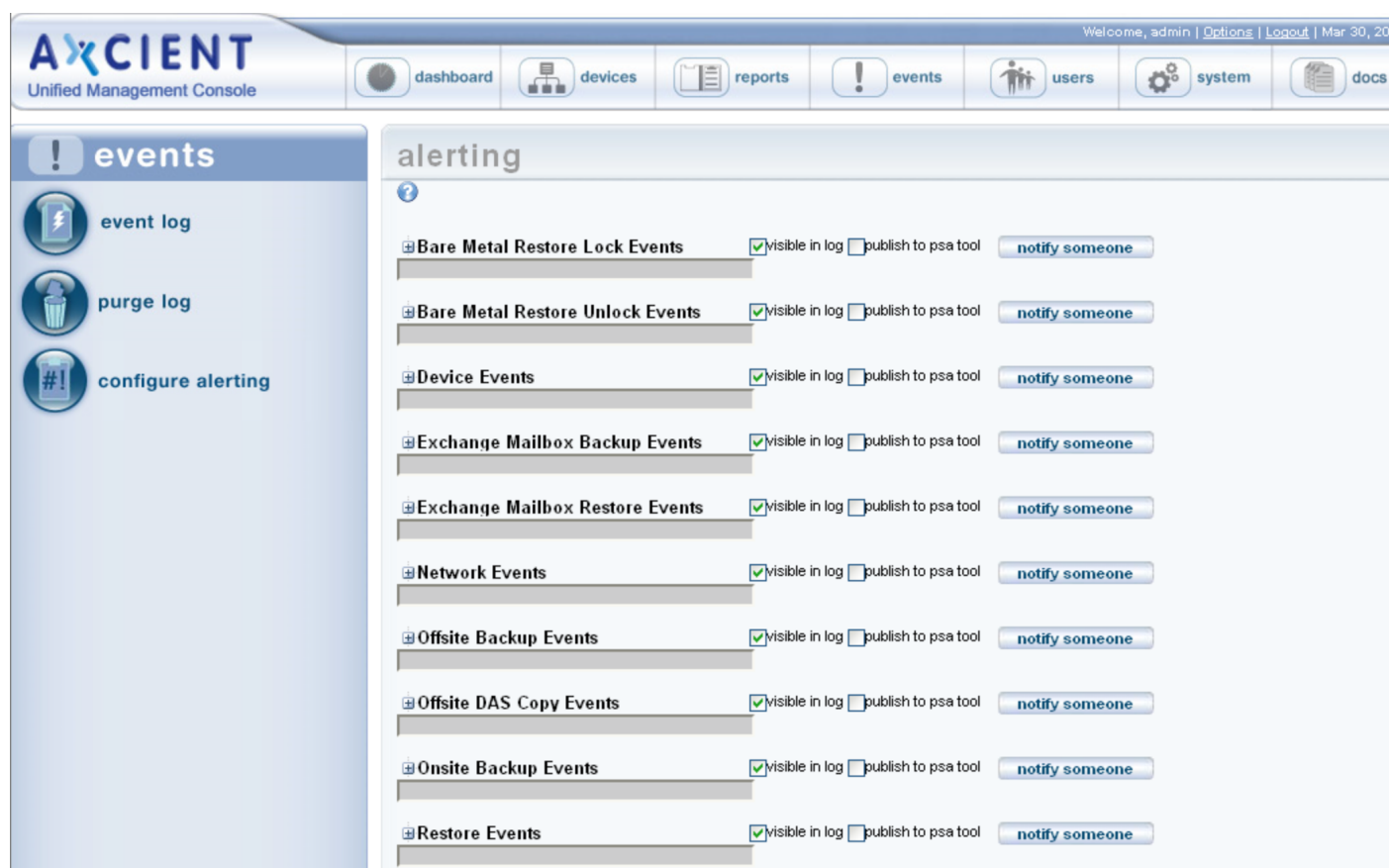
## Configure Event Notification

You can customize what messages are reported in the event log, what messages generate an e-mail alert, and who should be alerted for each type of event. By default, all types of messages are reported in the log, but no e-mail alerts are generated.

To customize event logging and alerting:

1. Click the **events** button at the top of the UMC page and select the **configure alerting** option in the left navigation menu.
2. The *Alerting* page appears. The event types are divided into various categories (Bare Metal Restore Lock Events, Bare Metal Restore Unlock Events, Device Events, and so on) in the middle of the page. To display the types within a category, click the plus mark (+) to the right of the category heading.

Figure 107 - Alerting Expanded Types



After clicking a plus mark (+), an expanded list of event types appears (Figure 118 ). Each type includes two check boxes:

**Visible in log box** - Checking this box writes event messages of this type to the log. All event types are checked by default, which means all are included in the log. To remove a message type from appearing in the log,

uncheck the box. (The box is a toggle that adds or removes the check mark on each click.)

- **Publish to psa tool box** - Checking this box sends event messages of this type to a configured Professional Services Automation (PSA) tool (see [Configure PSA Settings](#) section). This box is unchecked by default. (To be notified when PSA integration is not working, configure alerting for PSA integration Failed.)

Figure 108 - Alerting Expanded Types

The screenshot shows a web interface titled "alerting" with a help icon. It lists several event categories, each with a "notify someone" button. For each category, there are checkboxes for "visible in log" and "publish to psa tool".

Event Type	visible in log	publish to psa tool	notify someone
Bare Metal Restore Lock Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Bare Metal Restore Unlock Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Device Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Exchange Mailbox Backup Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">notify someone</a>
Exchange Mailbox Restore Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">notify someone</a>
Network Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite Backup Events	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite canceled by user	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite backup FAILED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">notify someone</a>
Offsite backup info	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite backup started	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite storage exceeded	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>
Offsite backup SUCCEEDED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">notify someone</a>
Offsite backup warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">notify someone</a>

To send an e-mail notification when an event of a particular type occurs, click the **notify someone** button to the right of that type. (To select an entire category, select the notify someone button to the right of that category.)

A dialog box appears to the right of the selected button. (It is a modal dialog box, which means you must complete this operation before continuing.) In this box do the following:

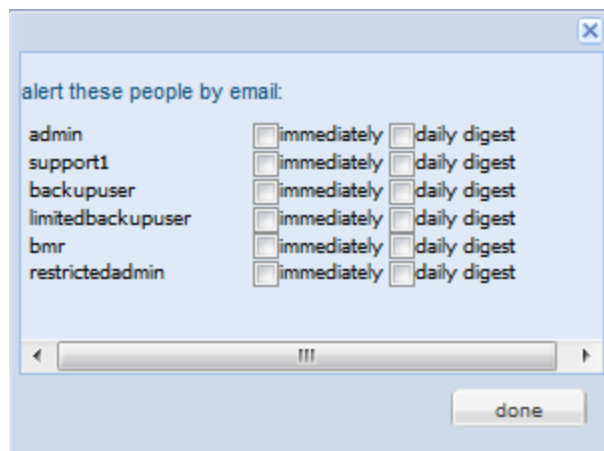
Under **alert these people by email**, a list of potential recipients appears. The displayed list includes all defined users. (To add a recipient to the list, first add that person as a user [see [Add a User](#) section] and then return to this step.) Check one or both of the following boxes for each recipient to be notified:

Check **immediately** to send an e-mail message whenever the event occurs.

- Check **daily digest** to send a cumulative list of these events once a day at 6:00 AM. The digest e-mail is a single cumulative list across all event types checked for this user.

When the list of recipients is correct, click the **done** button. The dialog box disappears, and the list of e-mail recipients appears in the gray box to the right of the *notify someone* button. (If the gray box is blank, no one is sent an e-mail when that type of event occurs.)

**Figure 109** - Selecting Alert Recipients



Repeat *Step 4* and *Step 5* for any type (or category) for which you want an e-mail notification sent.

Click the **save** button at the bottom of the Alerting page to apply the changes. (If you leave the page before clicking the **save** button, none of the changes will be saved. The **save** button can be clicked at any time to save changes made up to that point.)

Alerting e-mails use the following format:

*Subject: appliance\_alias\_name - message\_type [: job\_name]*

*(body) message\_text*

The *message\_type* is the name that appears in the Alerting page. The *job\_name* is appended to the *Subject* line if there is an associated job.

If the appliance alias name is not known (or is undefined) at the time the message is generated, the client name appears at the beginning of the *Subject* line. If neither is known, the appliance bar code appears at the beginning of the *Subject* line.

In addition to the selected alerts, the daily digest e-mail includes the *offsite storage* and *offsite backup progress* information displayed on the dashboard at the end of the e-mail (see [Disk Utilization Panel](#) section). This lets you monitor offsite progress at a glance.

## Save Log Messages

You can save the event log messages to a file and download the file to an appropriate location. You can download the complete log or a subset of messages specified by a filter.

To export the log contents:

1. Click the **events** button at the top of the UMC page.
2. (Optional) Set a filter to select the desired subset of messages (see [View Log Messages](#) section). Without a filter, all event messages in the log are selected.

In the *Export options* line at the bottom of the page, click on the desired format (CSV, Excel, or XML).

A file download window appears. (This varies by operating system.) Save and download the file as directed.

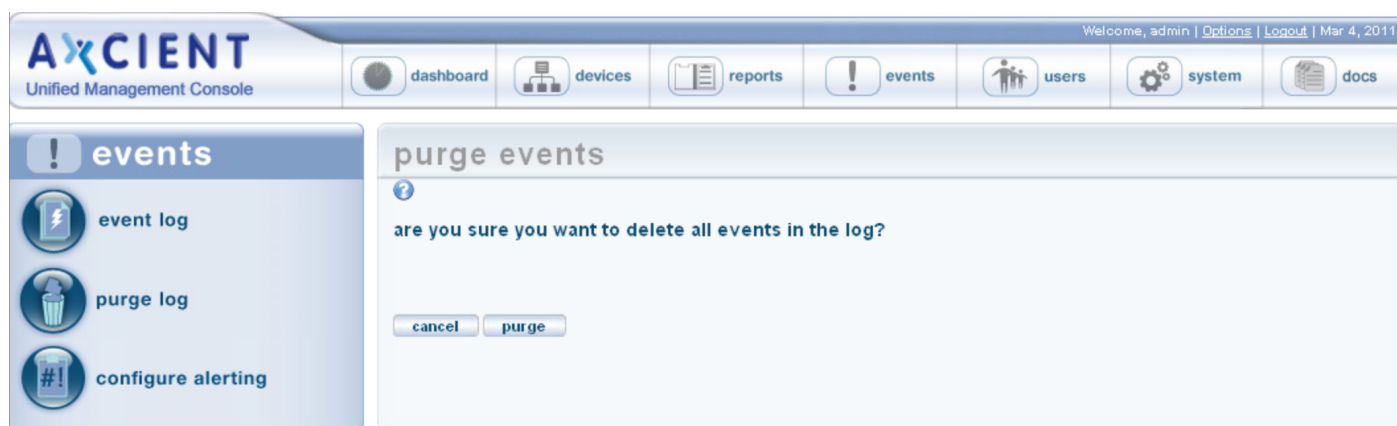
## Purge Log Messages

**CAUTION!** Purging the log deletes all messages in the event log. In order to save a history of events, download the messages to a separate file (see [Save Log Messages](#) section) before purging the log. Otherwise, all record of event messages is lost once the log is purged.

To purge (delete) all messages from the event log:

1. Click the **events** button at the top of the UMC page and select the **purge log** option in the left navigation menu.
2. The *Purge Events* page appears. Click the **purge** button.

**Figure 110** - Purge Log Page



# Event Messages

## Device Events

This section describes event messages that might appear when adding, modifying, deleting, or connecting to a device. (See the [Device Error Messages](#) section for page messages that might appear when attempting to add a device.)

### DEVICE\_ADDED

Message	Added Device: <i>deviceAddress</i>
Example	Added Device: 192.168.77.166 Added Device: admin-jsmith
Description	Device <i>deviceAddress</i> was added to the Axcient appliance. The example provides two devices naming conventions, IP address (192.168.77.166) and host name. (admin-jsmith). Adding a device allows the Axcient appliance to find that device on the network and log into the device. (To protect data stored on the device, you must create one or more backup jobs after adding the device.)
Action	Informational message (no action needed).

### DEVICE\_CREDENTIALS\_UPDATED

Message	Edited Device credentials: <i>deviceAddress</i>
Example	Edited Device: 192.168.77.166 Edited Device: admin-jsmith
Description	The user name and/or password were updated for device <i>deviceAddress</i> . The example provides two devices naming conventions, IP address (192.168.77.166) and host name. (admin-jsmith). This is necessary whenever the administrator account name or password is changed after adding the device. Otherwise, the Axcient appliance will no longer be able to access the device.
Action	Informational message (no action needed).

### DEVICE\_DELETED

Message	Deleted Device: <i>deviceAddress</i>
Example	Deleted Device: 192.168.77.166 Deleted Device: admin-jsmith
Description	Device <i>deviceAddress</i> was deleted from the Axcient appliance. The example provides two devices naming conventions, IP address (192.168.77.166) and host name. (admin-jsmith). Deleting a device removes any knowledge of that device from the Axcient appliance. (A device cannot be deleted if there are existing backup jobs for that device.)
Action	Informational message (no action needed).

## DEVICE\_MISSING

<b>Message</b>	Device <i>deviceAddress</i> has not been backed up for two weeks since backup failure
<b>Example</b>	Device 192.168.77.166 has not been backed up for two weeks since backup failure
<b>Description</b>	This message indicates that the device has not had a successful backup in the last two weeks. This message applies only to laptops and only to jobs in which the “Backup on Connect” field is set. The backup failure can be for any reason (laptop never connected, the backup job runs but fails, combination, other). The message is generated (but just once) for every two weeks (14 consecutive days) that the job does not complete a successful run.
<b>Action</b>	Check whether the laptop has been connected to the network during this period. If not, connect the laptop and leave it connected long enough to complete the backup. (Because “Backup on Connect” is set, the backup will start automatically after connecting to the network.) If the laptop was connected, check the log for other messages that identify why the backup job is failing.

## DEVICE\_UPDATED

<b>Message</b>	Edited Device: <i>deviceAddress</i>
<b>Example</b>	Edited Device: 192.168.77.166 Edited Device: admin-jsmith
<b>Description</b>	One or more of the parameters for device <i>deviceAddress</i> (such as device type or alias) were changed. The example provides two devices naming conventions, IP address (192.168.77.166) and host name. (admin-jsmith).
<b>Action</b>	Informational message (no action needed).



## Backup Job Definition Events

This section describes event messages that might appear when adding, modifying, or deleting a backup job. (Also see the [Image Job and Virtual Machine \(VM\) Events](#) section for image job events.)

### BACKUP\_JOB\_ADDED

Message	New Backup Job: <i>scheduleName</i>
Example	New Backup Job: 'Work Files'
Description	Backup job <i>scheduleName</i> was added to the Axcient appliance. This message is generated the first time a backup job is added.
Action	Informational message (no action needed).

### BACKUP\_JOB\_DELETED

Message	Backup job: <i>scheduleName</i> has been deleted.
Example	Backup job: 'Work Files' has been deleted.
Description	Backup <i>scheduleName</i> was deleted from the Axcient appliance. This message is generated whenever an existing backup job is deleted. When a backup job is deleted, all record of that job is deleted, including all the saved revisions.
Action	Informational message (no action needed).

### BACKUP\_JOB\_UPDATED

Message	Backup job: <i>scheduleName</i> has been deleted.
Example	Backup job: 'Work Files' has been deleted.
Description	One or more parameters of the backup job (for example, the contents or schedule type) for job <i>scheduleName</i> were updated. This message is generated whenever an existing backup job is modified.
Action	Informational message (no action needed).

### BACKUP\_JOB\_UPDATED\_RETENTION

Message	For job <i>scheduleName</i> , retention changed from: <i>oldRetentionLength oldRetentionMethod</i> to: <i>newRetentionLength newRetentionMethod</i>
Example	For job 'Work Files', retention changed from: 30 Days to 168 Hours
Description	In the backup job definition, the "Keep backups for" field (which specifies the amount of time to retain a backup instance) was changed. This message is generated whenever that field is modified.
Action	Informational message (no action needed).

## Onsite Backup Events

This section describes event messages that might appear when running an onsite backup job. (See the [Exchange Mailbox Events](#) section for events from running an Exchange mailbox job.)

### AUTO\_PRUNING

<b>Message</b>	Auto Freeing disk space due to low memory conditions
<b>Example</b>	(same)
<b>Description</b>	When attempting to do a backup, the auto-pruning feature detected there was not enough free disk space available, so the job retention period was automatically adjusted (reduced) and the older backup versions deleted to free up enough space to allow the backup job to continue. This message can also appear when doing a Cloud backup if the job definition is set for both local and Cloud.
<b>Action</b>	Informational message (no action needed).

### BACKUP\_CANCELED\_BY\_USER

<b>Message</b>	User <i>user_name</i> canceled <i>job_name</i> for machine <i>device_name</i> . Address of user's browser is <i>ip_address</i>
<b>Example</b>	User admin canceled Once for machine 2K3. Address of user's browser is 192.168.77.220
<b>Description</b>	A user canceled a job run, usually from the UMC dashboard.
<b>Action</b>	Informational message (no action needed).

### BACKUP\_DATA\_CHANGE

<b>Message</b>	User <i>user_name</i> canceled <i>job_name</i> for machine <i>device_name</i> . Address of user's browser is <i>ip_address</i>
<b>Example</b>	09/16/2011 - 8:51:46 AM Backup data for IMServ9921Ver345 on machine server9921 has changed by 5.1 GB
<b>Description</b>	The backup job changed in size by the indicated amount during that job run.
<b>Action</b>	Informational message (no action needed). A large change size indicates an offsite backup job run might take extended time If this job is also set for offsite backup.

### BACKUP\_EXCEEDED\_TIME\_THRESHOLD

<b>Message</b>	Backup <i>job_name</i> on machine <i>device_name</i> exceeds time threshold of number hours
<b>Example</b>	Backup IMServ77229Ver001 on machine server77229 exceeds time threshold of 3 hours
<b>Description</b>	The backup job has not completed within the allotted threshold interval. This might indicate the network is slow, there is an unusually large amount of data change, the backup job is hung, or the threshold interval is set too low.
<b>Action</b>	If you suspect the message indicates a problem, begin to investigate the problem by checking things such as network performance, device

health, and competing load issues. Also, check the log for other related error messages.

## BACKUP\_FAILED

<b>Message</b>	Backup <i>scheduleName</i> Failed --- Error - <i>systemMsg</i>
<b>Example</b>	Backup 'acl' Failed --- Error - could not mount or could not find any mounts for the device 192.168.77.194
<b>Description</b>	The backup failed due to the error described in <i>systemMsg</i> , which could describe a variety of conditions. In the example the backup failed because of a mount problem.
<b>Action</b>	The appropriate action varies by the cause of the failure. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> . If the message includes an “entitlement” comment (entitlement missing, expired, or not allowed), see the <a href="#">Check Entitlements</a> section for more information.

## BACKUP\_FAILED\_EXCEPTION

<b>Message</b>	Backup <i>scheduleName</i> on <i>deviceAddress</i> Failed --- Error - <i>exceptionMsgShort exceptionMsgStack</i>
<b>Example</b>	Backup 'testsh' on 192.168.77.194 Failed --- Error - Failed to create temporary file for jnidispatch library: java.io.IOException: No space left on device  java.lang.Error: Failed to create temporary file for jnidispatch library: java.io.IOException: No space left on device at com.sun.jna.Native.loadNativeLibraryFromJar(Native.java:600)  ...
<b>Description</b>	The backup failed because the system encountered a condition for which it was not prepared as described in <i>exceptionMsgShort</i> , which could describe a variety of conditions. In the example, the backup failed because the Axcient appliance ran out of space.
<b>Action</b>	The appropriate action varies by the cause of the failure. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

## BACKUP\_FAILED\_INTERRUPTED

<b>Message</b>	Backup <i>scheduleName</i> on <i>deviceAddress</i> was cancelled.
<b>Example</b>	Backup 'Work Files' on 192.168.77.194 was cancelled.
<b>Description</b>	A cancel request was initiated, which is usually due to the user pressing the <b>Cancel</b> button for the running job on the UMC dashboard. While this message usually appears because of a user cancel request, it could be generated from a system-initiated cancel operation.
<b>Action</b>	Informational message (no action needed) if the cancel request was initiated by the user. If a user did not request the cancel, check the log for other related event messages.

## BACKUP\_FAILED\_MOUNT

<b>Message</b>	Backup Failed: was unable to mount device <i>deviceDescription</i> <i>deviceAddress</i> , for schedule, <i>scheduleName</i>
----------------	---

<b>Example</b>	Backup Failed: was unable to mount device 'Joe laptop (admin-jsmith)', for schedule, "Documents and Settings"
<b>Description</b>	The device could not be mounted because there was a network problem, the mount was deleted, the mount password changed, or the device was too busy (100% CPU usage) to connect.
<b>Action</b>	Check each of the conditions identified in the explanation and correct as needed. If the mount password changed, update the password for that device in the UMC.

## BACKUP\_FAILED\_NO\_MOUNTS

<b>Message</b>	Backup Failed: could not mount or could not find any mounts for the device <i>deviceDescription</i> on <i>deviceAddress</i> , for schedule, <i>scheduleName</i>
<b>Example</b>	Backup Failed: could not mount or could not find any mounts for the device 'Joe laptop(admin-jsmith)', for schedule, "Documents and Settings"
<b>Description</b>	The device could not be mounted because there was a network problem (down or device unreachable), the mount was deleted, the mount password changed, or the device was too busy (100% CPU usage) to connect.
<b>Action</b>	Check each of the conditions identified in the explanation and correct as needed. If the mount password changed, update the password for that device in the UMC.

## BACKUP\_FAILED\_PRE\_PING

<b>Message</b>	Backup <i>scheduleName</i> on <i>deviceAddress</i> Failed during pre-backup ping
<b>Example</b>	Backup 'Work Files' on 192.168.77.194 Failed during pre-backup ping
<b>Description</b>	Before running a backup job, the Axcient appliance verifies it can access the device by running the <b>ping</b> command. In this case ping failed, so the backup job was canceled.
<b>Action</b>	The Axcient appliance cannot contact the device, so check the network connection. Possible causes include the device is shut down, the listed IP or other network address is not correct, or the network is down. When the connection issue is resolved (that is, you can ping the device), restart the backup job.

## BACKUP\_ON\_CONNECT\_SET

<b>Message</b>	Backup On Connect: <i>scheduleName</i> / <i>deviceDescription</i> <i>deviceAddress</i>
<b>Example</b>	Backup On Connect: 'Work Files' / 'Joe laptop (admin-jsmith)'
<b>Description</b>	This message is generated whenever a laptop device that has the "Backup on Connect" option set completes a backup. This message does not indicate whether the backup job run succeeded or failed, just that it completed for this laptop. Check the log for other events that indicated whether the job succeeded, completed with warnings, or failed.
<b>Action</b>	Informational message (no action needed).

## BACKUP\_STARTED

<b>Message</b>	Backup Started: <i>scheduleName</i> on <i>deviceAddress</i>
----------------	---

Example	Backup Started: 'Documents and Settings' on admin-jsmith
Description	A run of the backup job <i>scheduleName</i> was started.
Action	Informational message (no action needed).

## BACKUP\_SUCCEEDED

Message	Backup Completed: <i>scheduleName</i> Successfully on <i>deviceAddress</i>
Example	Backup Completed: 'Documents and Settings' on admin-jsmith
Description	Backup <i>scheduleName</i> completed successfully with no errors.
Action	Informational message (no action needed).

## BACKUP\_WARNING\_ALREADY\_RUNNING

Message	Backup <i>scheduleName</i> on <i>deviceAddress</i> is already running, ignoring request.
Example	Backup 'Documents and Settings' on admin-jsmith is already running, ignoring request.
Description	An instance of backup job <i>scheduleName</i> was running when the new run request was made. Therefore, the new request was ignored and discarded (not rescheduled).
Action	Informational message (no action needed). To restart immediately, cancel the running job and then start a new instance of the job. See the <a href="#">Backup Jobs Tab</a> section for instructions on how to cancel or start a backup job from the UMC dashboard.

## BACKUP\_WARNING\_EXCEPTION

Message	Backup <i>scheduleName</i> had a problem removing VSS volume, exception: <i>exceptionMsg</i>
Example	
Description	The VSS volume could not be unmounted (or encountered another problem) after the backup.
Action	See the <a href="#">Backup Fails Because of VSS Problem</a> section for corrective actions.

## BACKUP\_WARNING\_MOUNT\_EXCEPTION

Message	Could not mount: <i>deviceDescription</i> <i>deviceAddress</i> for schedule, <i>scheduleName</i> , because: <i>exceptionMsg</i>
Example	Could not mount: 'Joe laptop (admin-jsmith)' for schedule, 'Documents and Settings', because: There was a network problem: admin-jsmith/c\$, No route to host (return code: 113)
Description	This occurs if the volume specified in the schedule could not be mounted. This can occur if the system is or becomes off-line when the backup schedule is run. It can also occur if the sharing settings for the volume have been changed since the schedule was created.
Action	Make sure that the device to be backed up is connected to the network, that its file sharing settings are correct, and that there is not a

problem with the volume on the specified device.

## BACKUP\_WARNING\_MOUNT\_MAXTRIES

<b>Message</b>	Giving up trying to mount device: <i>deviceDescription deviceAddress</i> , for schedule: <i>scheduleName</i>
<b>Example</b>	Giving up trying to mount device: 'Joe laptop (admin-jsmith)', for schedule: 'Documents and Settings'.
<b>Description</b>	The Axcient appliance attempts to mount the volume specified in a schedule a certain number of times. After this, it give up and logs this message.
<b>Action</b>	Make sure the machine to be backed up is connected to the network, that its file sharing settings are correct and that there is not a problem with the volume on the specified machine.

## BACKUP\_WARNING\_MOUNT\_IN\_USE

<b>Message</b>	During setup of Open File Backup, the mount <i>mountPath</i> for Machine <i>deviceAddress</i> could not be unmounted because it was in use.
<b>Example</b>	
<b>Description</b>	The volume specified in the schedule could not be unmounted because it is still in use. This is not under end user control.
<b>Action</b>	Contact <a href="#">Axcient customer support</a> to investigate the issue.

## BACKUP\_WARNING\_NET\_SHARE\_NO\_REMOVE

<b>Message</b>	Could not remove sharing from the path <i>volumePath</i> on Machine <i>deviceAddress</i> : <i>systemMsg</i>
<b>Example</b>	
<b>Description</b>	The VSS Shadow volume exposed as a network share during the backup could not be removed.
<b>Action</b>	See the <a href="#">Backup Fails Because of VSS Problem</a> section for corrective actions.

## BACKUP\_WARNING\_NO\_DELETE\_STATS

<b>Message</b>	Unable to remove schedule statistics from the RMC while deleting Backup Job: <i>scheduleName</i>
<b>Example</b>	Unable to remove schedule statistics from the RMC while deleting Backup Job: 'Work Files'
<b>Description</b>	Statistical information about a backup job is sent to the RMC when the job is created, modified, or deleted. However, when <i>scheduleName</i> was deleted, the job statistics on the RMC were not updated. This is usually because the Axcient appliance connection to the RMC was lost, so the updated information could not be sent.
<b>Action</b>	Check the network connections and fix as necessary. A starting point is to determine whether the RMC is accessible ( <i>ping axcient.net</i> ). The specific error of not deleting the schedule statistics is benign and does not require any action.

**BACKUP\_WARNING\_NO\_INCLUSION**

<b>Message</b>	Backup <i>scheduleName</i> has no included files; note that 'pagefile.sys' cannot be backed up.
<b>Example</b>	Backup 'win pagefile.sys' has no included files; note that 'pagefile.sys' cannot be backed up.
<b>Description</b>	The folder(s) selected for backup do not include any files that can be backed up. (The pagefile.sys file is a system swap file that cannot be backed up, so the message will be generated even if the pagefile.sys file is in the backed up folder.)
<b>Action</b>	Review what files and folders are included in the job, and modify the job contents accordingly (or ignore the message if the selected files and folders are correct).

**BACKUP\_WARNING\_OPEN\_FILE\_EXCEPTION**

<b>Message</b>	Could not do Open File Backup for machine: <i>deviceAddress</i> for schedule, <i>scheduleName</i> : <i>exceptionMsg</i>
<b>Example</b>	Could not do Open File Backup for machine: 'server-9921' (for schedule, 'win2') : InterruptedException, sleep interrupted
<b>Description</b>	Several failure conditions when doing an open file backup can cause this exception. (An open file backup uses VSS.)
<b>Action</b>	See the <a href="#">Backup Fails Because of VSS Problem</a> and <a href="#">Open Files Not Backed Up</a> sections for corrective actions.

**BACKUP\_WARNING\_PRE\_PING\_EXCEPTION**

<b>Message</b>	Backup <i>scheduleName</i> on <i>deviceAddress</i> ping exception: <i>exceptionMsgShort</i>
<b>Example</b>	
<b>Description</b>	Before a backup is started, the Axcient appliance attempts to reach the machine specified in the schedule. The system had trouble issuing the <b>ping</b> command. This is an unusual error. Note the distinction between this message type and <i>BACKUP_FAILED_PRE_PING</i> , which is more likely.
<b>Action</b>	This can be a transient error that does not require any action. If this problem recurs, contact <a href="#">Axcient customer support</a> .

**BACKUP\_WARNING\_PRUNE**

<b>Message</b>	Backup <i>scheduleName</i> : Removing Old Retention had error: <i>systemMsg</i>
<b>Example</b>	Backup 'testsh': Removing Old Retention had error: errcode: 143; stderr: ; stdout:
<b>Description</b>	The appliance was unable to remove (prune) old job information. This is probably due to either a corruption problem or the appliance filling up to maximum capacity, which means there is insufficient available storage space to do the action.
<b>Action</b>	Check the available space on the UMC dashboard. If the appliance is completely full, free up some space (see the <a href="#">Reducing Backup Job Size</a> and <a href="#">Remove Backup Job</a> sections). If space is available, contact Axcient customer support.

**BACKUP\_WARNING\_PRUNE\_EXCEPTION**

Message	Backup <i>scheduleName</i> Warning -- Error in Retention Cleaning: <i>exceptionMsg</i>
Example	Backup 'x2' Warning --- Error in Retention Cleaning: sleep interrupted null
Description	This can occur if some unforeseen error condition exists during the removal of expired backups.
Action	Contact <a href="#">Axcient customer support</a> .

## BACKUP\_WARNING\_STAT\_CLEAN\_EXCEPTION

Message	Backup <i>scheduleName</i> Warning --- Error - Invalidating Old Statistics: <i>exceptionMsg</i>
Example	
Description	This can occur if some un for seen error condition exists during the removal of expired statistical data.
Action	Contact <a href="#">Axcient customer support</a> .

## BACKUP\_WARNING\_VDIFF

Message	Backup <i>scheduleName</i> Warning - StdErr from vdiff - <i>systemMsg</i>
Example	Backup 'testsh' Warning - StdErr from vdiff - Warning [digested_copy()] Failed to open source file: "/uptiva/mounts/192.168.77.194/4/lhamel/testshare/bad_a_e.txt"  ermo(#2 No such file or directory)  Warning [mirror_file()] Encountered problems copying from: "/uptiva/mounts/192.168.77.194/4/lhamel/testshare/bad_a_e.txt"  Warning [differential_copy_func()] Skipping would-be-added entry: "/uptiva/mounts/192.168.77.194/4/lhamel/testshare/bad_a_e.txt"
Description	Any number of warning conditions might be detected during the actual backup process. The message included with the warning provides more details. In the example there are warnings for a missing file.
Action	The appropriate action varies by the cause of the warning. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

## BACKUP\_WARNING\_VSHADOW\_ALREADY\_ACTIVE

Message	VSS collision with other backup jobs detected on <i>deviceAddress</i> so entering limited retry loop to await our turn...
Example	VSS collision with other backup jobs detected on 192.168.77.194 so entering limited retry loop to await our turn...
Description	VSS is being invoked by multiple jobs, but it cannot run in parallel. Therefore, the jobs are queued to run VSS.
Action	No action should be necessary, because the job will continue when VSS is available. However, if the job appears to be waiting indefinitely, cancel the job run and start it again later. If the condition is due to multiple jobs scheduled to run simultaneously, stagger the job schedule start times so they will not overlap when running.



## BACKUP\_WARNING\_VSHADOW\_NO\_CREATE

Message	Unable to create shadow volume for Machine <i>deviceAddress</i> <i>systemMsg</i>
Example	
Description	There was a problem creating or reaching the volume for the device.
Action	Be sure the target system has the proper credentials. For VSS-related corrective actions, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

## BACKUP\_WARNING\_VSHADOW\_NO\_DELETE

Message	Could not remove the Shadow Image for Machine <i>deviceAddress</i> <i>systemMsg</i>
Example	
Description	The shadow volume for this backup could not be deleted. A possible reason is that there are multiple backup jobs running on this machine and there is a temporary conflict.
Action	Wait and see if the warning repeats. If there are multiple jobs running concurrently on the same machine. Try staggering the jobs to avoid the overlap.

## BACKUP\_WARNING\_VSHADOW\_NO\_MOUNT

Message	Unable to create shadow volume for Machine <i>deviceAddress</i> because: <i>exceptionMsg</i>
Example	
Description	There was a problem mounting the volume, though the other steps, like creating the volume succeeded.
Action	Check all the sharing permissions for this job.

## BACKUP\_WARNING\_VSHADOW\_NO\_WRITER

Message	Please install the VSS writer for the <i>service_name</i> service. Unable to perform an Open File Backup without this writer.
Example	Please install the VSS writer for the Exchange service. Unable to perform an Open File Backup without this writer.
Description	The backup had a VSS-related problem. In the example the Exchange VSS writer is not installed or enabled.
Action	Install or enable the missing VSS writer. See the <a href="#">Backup Fails Because of VSS Problem</a> section for more information.

## BACKUP\_WARNING\_VSHADOW\_WRITER\_UNREADABLE

Message	Unable to read installed VSS writers
Example	(same)
Description	There is a problem with one or more of the VSS writers.

Action	See the <a href="#">Backup Fails Because of VSS Problem</a> section for more information.
--------	---

## BACKUP\_WARNING\_VSSPREP

Message	Unable to update Windows file system modification times with vssprep.exe for Machine <i>device_name: systemMsg</i>
Example	
Description	The backup had a VSS-related problem.
Action	See the <a href="#">Backup Fails Because of VSS Problem</a> section for more information.

## Offsite Backup Events

This section describes event messages that might appear when backing up (copying) data to the offsite Axcient data center.

### OFFSITE\_CANCELLED\_BY\_USER

Message	User <i>user_name</i> canceled the <i>job_name</i> job. Address of user's browser is <i>ip_address</i>
Example	User admin canceled the Off-Site job. Address of user's browser is 192.168.77.102
Description	A user canceled an offsite job, usually from the UMC dashboard.
Action	Informational message (no action needed).

### OFFSITE\_FAIL\_EBR\_EXCEPTION

Message	Off-Site Backup subtask for Exchange backup Failed with exception: <i>exceptionMsg</i>
Example	
Description	A subtask in an offsite mailbox backup job had a problem (generated an exception), which can be due to a variety of issues.
Action	The appropriate action varies by the cause of the failure. Read the <i>exceptionMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

### OFFSITE\_FAILED\_EXCEPTION

Message	Error occurred while running an off-site backup: <i>exceptionMsg</i>
Example	
Description	An offsite backup job had a problem (generated an exception), which can be due to a variety of issues
Action	The appropriate action varies by the cause of the failure. Read the <i>exceptionMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

### OFFSITE\_FAILED\_INTERRUPTED

Message	Off-site backup canceled
Example	(same)
Description	A cancel request was initiated, which is usually due to the user pressing the Cancel button for the running offsite job on the UMC dashboard.
Action	A cancel request was initiated, which is usually due to the user pressing the Cancel button for the running offsite job on the UMC dashboard.

### OFFSITE\_FAILED\_INTERRUPTED\_WITH\_ERRORS

<b>Message</b>	Off-site backup canceled
<b>Example</b>	(same)
<b>Description</b>	A cancel request was initiated, which is usually due to the user pressing the Cancel button for the running offsite job on the UMC dashboard.
<b>Action</b>	A cancel request was initiated, which is usually due to the user pressing the Cancel button for the running offsite job on the UMC dashboard.

## OFFSITE\_FAILED\_NO\_JOBS

<b>Message</b>	Off-Site Backup - no jobs to backup were found.
<b>Example</b>	(same)
<b>Description</b>	Individual offsite backup requests are queued in an offsite directory on the Axcient appliance. When an offsite job is initiated, the individual backup requests are run serially one by one. In this case, no individual backup requests were present in the offsite job queue, so the offsite backup job run was canceled.
<b>Action</b>	Informational message (no action needed). However, this could indicate there is a problem in getting the individual jobs queued up for offsite backup. Review the log for other messages about offsite job issues.

## OFFSITE\_FAILED\_NOMOUNT

<b>Message</b>	Off-Site Backup failed. Details: There was a problem mounting the Off-Site volume
<b>Example</b>	(same)
<b>Description</b>	An offsite backup job had a mount problem.
<b>Action</b>	See the <a href="#">Backup Fails Because of Mount Problem</a> section.

## OFFSITE\_FAILED\_OFFSITE\_DIR

<b>Message</b>	Off-Site Backup failed: No offsite directory found at: <i>srcPath</i>
<b>Example</b>	
<b>Description</b>	An offsite backup job failed because it could not find the offsite directory that contains the files to be backed up offsite
<b>Action</b>	Call <a href="#">Axcient customer support</a> .

## OFFSITE\_RETRY\_AXCIENT\_SYSTEM\_DATA

<b>Message</b>	There was a problem with offsite backup for axcient system data. Error Code: <i>errCode</i> . Will begin retry number <i>retryNumber</i> in <i>delaySeconds</i> seconds.
<b>Example</b>	
<b>Description</b>	This message appears because the relevant event could not be logged, which indicates a possible problem.

<b>Action</b>	No action is necessary, because the Axcient appliance will automatically retry the offsite backup. However, if the retry fails note the <i>errCode</i> and look for other relevant messages that identify the underlying problem.
---------------	---

## OFFSITE\_FAILED\_RMC\_SETTINGS

<b>Message</b>	Off-Site Backup failed. Details: There was a problem retrieving Off-Site settings
<b>Example</b>	(same)
<b>Description</b>	An offsite backup job failed to get needed information from the RMC. This typically is due to a network or Internet problem that prevented the Axcient appliance from connecting to the RMC.
<b>Action</b>	Check the network connections and firewall settings, and fix as necessary. A starting point is to determine whether the RMC is accessible ( <i>ping axcient.net</i> ).

## OFFSITE\_FAILED\_RSYNC\_WARNINGS

<b>Message</b>	Off-Site Backup completed with warnings: Please refer to previous subtask alerts for details. Subtask Summary: Errors: <i>errorCount</i> Warnings: <i>warningCount</i> Success: <i>successCount</i>
<b>Example</b>	Off-Site Backup completed with warnings: Please refer to previous subtask alerts for details. Subtask Summary: Errors: 0 Warnings: 1 Success: 3
<b>Description</b>	This is a summary message when at least one warning was generated by the offsite backup job.
<b>Action</b>	Check the log for other messages that describe the warning issues.

## OFFSITE\_FAILED\_SRC\_DIR\_EXCEPTION

<b>Message</b>	Off-Site Backup for machine: <i>deviceName</i> failed. Details: <i>exceptionMsg</i>
<b>Example</b>	
<b>Description</b>	An offsite backup job had a problem (generated an exception), which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Read the <i>exceptionMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

## OFFSITE\_RETRY\_EBR

<b>Message</b>	There was a problem with offsite backup for Exchange data. Error Code: <i>errCode</i> . Will begin retry number <i>retryNumber</i> in <i>delaySeconds</i> seconds.
<b>Example</b>	

<b>Description</b>	This message appears because the relevant event could not be logged, which indicates a possible problem.
<b>Action</b>	No action is necessary, because the Axcient appliance will automatically retry the offsite backup. However, if the retry fails note the <i>errCode</i> and look for other relevant messages that identify the underlying problem.

## OFFSITE\_RETRY\_DEVICE

<b>Message</b>	There was a problem with Offsite Backup for machine: <i>deviceDescription</i> <i>deviceAddress</i> , schedule: <i>scheduleName</i> . Error Code: <i>errCode</i> . Will begin retry number <i>retryNumber</i> in <i>delaySeconds</i> seconds.
<b>Example</b>	
<b>Description</b>	This message appears because the relevant event could not be logged, which indicates a possible problem.
<b>Action</b>	No action is necessary, because the Axcient appliance will automatically retry the offsite backup. However, if the retry fails note the <i>errCode</i> and look for other relevant messages that identify the underlying problem.

## OFFSITE\_STARTED

<b>Message</b>	Off-Site Backup has been started
<b>Example</b>	(same)
<b>Description</b>	An offsite backup job was started.
<b>Action</b>	Informational message (no action needed).

## OFFSITE\_SUBTASK\_SUCCEEDED\_INFO

<b>Message</b>	Off-Site Backup subtask for machine: <i>deviceAddress</i> , backup: <i>scheduleName</i> completed successfully.
<b>Example</b>	Off-Site Backup subtask for machine: 'systemdata', backup: 'System-Data-Transfer' completed successfully.
<b>Description</b>	An offsite backup job run can involve several steps. This message indicates one of the steps completed successfully.
<b>Action</b>	Informational message (no action needed).

## OFFSITE\_INIT\_TASK

<b>Message</b>	Off-Site Backup init task : <i>taskName</i> completed successfully.
<b>Example</b>	Off-Site Backup init task : ZIP_DATABASE completed successfully.
<b>Description</b>	All initialization tasks (prior to doing the offsite backup) completed successfully.
<b>Action</b>	Informational message (no action needed).

## OFFSITE\_SUCCEEDED

<b>Message</b>	Off-Site Backup completed successfully.
<b>Example</b>	(same)
<b>Description</b>	The offsite backup job run completed successfully without any errors or warnings.
<b>Action</b>	Informational message (no action needed).

## OFFSITE\_WARNING\_ALREADY\_RUNNING

<b>Message</b>	Previous Off-Site Backup still running.
<b>Example</b>	(same)
<b>Description</b>	An instance of the offsite backup job was running when the new run request was made. Therefore, the new request was ignored and discarded (not rescheduled).
<b>Action</b>	Informational message (no action needed). To restart immediately, cancel the running job and then start a new instance of the job. See the <a href="#">Backup Jobs Tab</a> section for instructions on how to cancel or start a backup job from the UMC dashboard.

## OFFSITE\_WARNING\_CLEAN\_TASK

<b>Message</b>	Off-Site Backup init task : <i>taskName</i> failed. Details: <i>systemMsg</i>
<b>Example</b>	
<b>Description</b>	An offsite backup job had an initialization problem (generated an exception or synchronization failure), which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Read the systemMsg for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .

## OFFSITE\_WARNING\_EXCHANGE\_RUNNING

<b>Message</b>	Off-Site Backup subtask for Exchange backup: <i>scheduleName</i> cannot be run while (onsite) EBR backup is running.
<b>Example</b>	Off-Site Backup subtask for Exchange backup: 'Exchange Mailboxes' cannot be run while (onsite) EBR backup is running.
<b>Description</b>	The Exchange mailbox backup job <i>scheduleName</i> was running when the offsite job started. Therefore, the offsite request was ignored and discarded (not rescheduled).
<b>Action</b>	Informational message (no action needed). Optionally, you can wait for the offsite backup job to complete (or cancel it prematurely) and then start it manually. See the <a href="#">Backup Jobs Tab</a> section for instructions on how to cancel or start a backup job from the UMC dashboard.

## OFFSITE\_WARNING\_INIT\_TASK

<b>Message</b>	Off-Site Backup init task : <i>taskName</i> failed. Details: <i>systemMsg</i>
<b>Example</b>	Off-Site Backup init task : ZIP_DATABASE failed. Details: (gzip:/uptiva/offsite/systemdata/mysqlbackup.sql.gz already exists; not

	overwritten)
<b>Description</b>	An offsite backup job had an initialization problem (generated an exception or synchronization failure), which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Read the <i>systemMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .

## OFFSITE\_WARNING\_INIT\_TASK\_EXCEPTION

<b>Message</b>	Off-Site Backup init task : <i>taskName</i> failed. Details: <i>exceptionMsg</i>
<b>Example</b>	Off-Site Backup init task : Remove any old schedule directories of machine: 23 failed. Details: errcode: 127; stderr:/mnt/ax/scratch/executor/uptiva-offsite-clean-64870.sh: line 51: [/mnt/ax/app/bin/offsite backup_wrapper; No such file or directory; stdout:
<b>Description</b>	An offsite backup job had an initialization problem (generated an exception or synchronization failure), which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Read the <i>exceptionMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .

## OFFSITE\_WARNING\_SERVER\_ALIVE\_EXCEPTION

<b>Message</b>	Off-Site Backup subtask for ServerAlive backup Failed with exception: <i>exceptionMsg</i>
<b>Example</b>	
<b>Description</b>	The appliance was unable to successfully transfer the data from one or more volumes to the Axcient data center. This is usually due to a network connectivity issue, or it may occur if the offsite backup is interrupted.
<b>Action</b>	Verify the network connectivity between the Axcient appliance and the Internet.

## OFFSITE\_WARNING\_SUBTASK\_RSYNC

<b>Message</b>	Off-Site Backup subtask for machine: <i>deviceAddress</i> , backup: <i>scheduleName</i> completed with warnings: <i>rsyncErrorLevelMsg</i> Error code: <i>rsyncErrorLevel</i> , stdout: <i>systemMsgrsyncErrorMsg</i>
<b>Example</b>	Off-Site Backup subtask for machine: 'systemdata', backup: 'System-Data-Transfer' completed with warnings: Partial transfer due to error (Error code: 23, stdout: IO error encountered -- skipping file deletion Number of files: 28 Number of files transferred: 9 Total file size: 8382651 bytes ...
<b>Description</b>	An offsite backup job had a subtask problem, which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Check <i>systemMsg</i> and <i>rsyncErrorMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .



## Restore Events

This section describes event messages that might appear when restoring data from a backup job. (See the [Exchange Mailbox Events](#) section for events from restoring mailboxes on an Exchange server.)

### RESTORE\_CANCELLED\_BY\_USER

Message	User <i>user_name</i> canceled restore of <i>device_name: job_name</i> . Address of user's browser is <i>ip_address</i>
Example	User admin canceled restore of 192.168.99.11 : 99.11 FF 1. Address of user's browser is 192.168.77.8
Description	A user canceled a restore operation, usually from the UMC dashboard.
Action	Informational message (no action needed).

### RESTORE\_FAILED

Message	Restore Failed for <i>scheduleName</i> , see previous warnings for specific cause
Example	Restore Failed for 'Work Files', see previous warnings for specific cause
Description	This is a general failure message that the Axcient appliance could not complete the restore operation. The cause of the failure is not indicated in this message.
Action	There should be additional (previous) messages in the event log about this restore operation. Review the other warning messages for information about the problem that caused the restore failure.

### RESTORE\_FAILED\_EXCEPTION

Message	Restore error for <i>scheduleName</i> because of error: <i>exceptionMsg</i>
Example	Restore Failed for 'foreign, acl' because of error: NullPointerException
Description	A restore attempt failed (generated an exception), which can be due to a variety of issues.
Action	The appropriate action varies by the cause of the failure. Check <i>exceptionMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

### RESTORE\_FAILED\_FILE\_CHECK

Message	Restore error for <i>scheduleName</i> : <i>filesMissing</i>
Example	Restore Failed for 'foreign, acl': could not copy: 'ulti_languages'; could not copy: 'CLS/attribReadOnly.txt'; could not copy: 'CLS';
Description	Could not verify that the files to be restored were copied correctly (not found, failed copy, corrupted file, or other issue), thus the restore attempt failed.
Action	Examine the <i>filesMissing</i> and determine if there is anything special about these files that would account for the problem. If necessary,

remove these files from the backup job (set to **Ignore** in the job definition).

## RESTORE\_FAILED\_INTERRUPTED

Message	Restore interrupted for <i>scheduleName</i>
Example	
Description	A cancel request was initiated, which is usually due to the user pressing the <b>Cancel</b> button for the running restore job on the UMC dashboard.
Action	Informational message (no action needed) if the cancel request was initiated by the user. If a user did not request the cancel, check the log for other related event messages

## RESTORE\_FAILED\_RDIFF

Message	Restore error for scheduleName: <i>rdiffMsg</i>
Example	
Description	A restore attempt failed, which can be due to a variety of issues.
Action	The appropriate action varies by the cause of the failure. Check <i>rdiffMsg</i> for clues to the problem. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .

## RESTORE\_STARTED

Message	Restore Started for Job <i>scheduleName</i>
Example	Restore Started for Job 'Work Files'
Description	A restore of the backup job <i>scheduleName</i> was started. This message does not indicate the scope of the restore (that is, which files in <i>scheduleName</i> are being restored), only that a restore has started.
Action	Informational message (no action needed).

## RESTORE\_SUCCEEDED

Message	Restore Completed: Backup Job <i>scheduleName</i>
Example	Restore Completed: Backup Job 'Work Files'
Description	A restore of the backup job <i>scheduleName</i> succeeded without errors. This message does not indicate the scope of the restore (that is, which files in <i>scheduleName</i> were restored), only that the restore succeeded.
Action	Informational message (no action needed).

**RESTORE\_WARNING\_ACL\_EXCEPTION**

<b>Message</b>	ACL exception encountered for job <i>scheduleName</i> , <i>exceptionMsg</i>
<b>Example</b>	
<b>Description</b>	A restore attempt failed (generated an exception) when copying ACL files, which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Check <i>exceptionMsg</i> for clues to the problem. Contact <a href="#">Axcient customer support</a> to debug the problem.

**RESTORE\_WARNING\_ACL\_FAILED**

<b>Message</b>	ACL restore warning for job <i>scheduleName</i> : <i>systemMsg</i>
<b>Example</b>	
<b>Description</b>	A restore attempt failed when copying ACL files, which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Check <i>systemMsg</i> for clues to the problem. Contact <a href="#">Axcient customer support</a> to debug the problem.

**RESTORE\_WARNING\_ACL\_MERGED**

<b>Message</b>	ACL merge error for job <i>scheduleName</i> : <i>mergeMsg</i>
<b>Example</b>	
<b>Description</b>	An error occurred when attempting to apply ACL files in a restore operation, which can be due to a variety of issues.
<b>Action</b>	The appropriate action varies by the cause of the failure. Check <i>mergeMsg</i> for clues to the problem. Contact <a href="#">Axcient customer support</a> to debug the problem.

**RESTORE\_WARNING\_ACL\_PATH\_NOCOPY**

<b>Message</b>	ACL copy error for job <i>scheduleName</i> , Cannot copy src: <i>sourceFile</i> to dest: <i>destinationFile</i>
<b>Example</b>	
<b>Description</b>	An error occurred when attempting to copy ACL files in a restore operation, which can be due to a variety of issues.
<b>Action</b>	Contact <a href="#">Axcient customer support</a> to debug the problem.

**RESTORE\_WARNING\_ACL\_PATH\_NOCOPY**

<b>Message</b>	cannot find time associated with backup ID: <i>backupStatisticsId</i> ; using 'now' for restore
<b>Example</b>	

<b>Description</b>	There is a problem restoring from the selected backup job version (date).
<b>Action</b>	Select an alternate date from the backup job list and restore from that version.

## RESTORE\_WARNING\_ILLEGAL\_FILENAME

<b>Message</b>	During restore of <i>scheduleName</i> , destination has a <i>osType</i> system, and a file or directory name from the backup, path, is not a legal filename on <i>osType</i> , so it will not be restored.
<b>Example</b>	During restore of 'testsh', destination has a WINDOWS system, and a file or directory name from the backup, 'lhamel/testshare/dir with space/dir with " quote', is not a legal filename on WINDOWS, so it will not be restored.
<b>Description</b>	One or more files to be restored have file names that are illegal in the target operating system. This can occur when the target device operating system is different from the source device. For example, if you backed up a device running Linux or another UNIX-based operating system and attempt to restore those files on a Windows device, the restore will fail if one or more files have illegal Windows names. (UNIX allows certain characters in file names, such as a quote or colon, that are illegal in Windows file names.)
<b>Action</b>	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Remove any files with illegal names from the list of files to restore, and then repeat the restore job.</li> <li>2. Restore the files with illegal characters to a target device with the same operating system.</li> <li>3. Rename the files (removing the illegal characters), and then move them to the original target device.</li> </ol>

# Exchange Mailbox Events

This section describes event messages that might appear when backing up or restoring mailboxes on an Exchange server.

## EBR\_BACKUP\_EXCEPTION

Message	Exchange Mailbox Backup <i>scheduleName</i> failed with exception: <i>exceptionMsg</i>
Example	Exchange Mailbox Backup (Folder to be deleted) failed with exception: EBR command timed out.
Description	The Exchange mailbox backup ailed due to the error described in <i>exceptionMsg</i> , which could describe a variety of conditions. In the example the backup failed because it timed out during execution.
Action	Review the details in <i>exceptionMsg</i> to determine what action is needed. For corrective actions to some typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> . If the message includes an “entitlement” comment (entitlement missing, exceeded, expired, or not allowed), see the <a href="#">Check Entitlements</a> section for more information.

## EBR\_BACKUP\_FAILED\_RESTORE\_RUNNING

Message	Exchange Backup cannot progress while restore is active
Example	(same)
Description	The Exchange mailbox job was being restored when the backup run request was made. Therefore, the backup run request was ignored and discarded (not rescheduled).
Action	Informational message (no action needed). Optionally, wait for the restore to complete and then manually start the backup job. See the <a href="#">Backup Jobs Tab</a> section for instructions on how to start a backup job from the UMC dashboard.

## EBR\_BACKUP\_STARTED

Message	Exchange Backup Started: <i>scheduleName</i> on <i>deviceAddress</i>
Example	Exchange Backup Started: ‘Exchange Mailboxes’ on 192.168.77.246
Description	A run of the Exchange mailbox backup job <i>scheduleName</i> was started.
Action	Informational message (no action needed).

## EBR\_SUCCEEDED

Message	Exchange Mailbox Backup <i>scheduleName</i> succeeded
Example	Exchange Mailbox Backup (Exchange Mailboxes) succeeded: Mailboxes processed: 6 Mailboxes backed up: 6 Mailbox backup failures: 0

	Warnings issued: 0 Messages backed up: 0 Bytes backed up: 0
<b>Description</b>	Exchange mailbox backup <i>scheduleName</i> completed successfully with no errors. Summary information about the backup job run is included.
<b>Action</b>	Informational message (no action needed).

## EBR\_BACKUP\_SUCCEEDED\_WITH\_WARNINGS

<b>Message</b>	Exchange Mailbox Backup <i>scheduleName</i> succeeded with warnings
<b>Example</b>	Exchange Mailbox Backup 'Exchange Mailboxes' succeeded with warnings
<b>Description</b>	Exchange mailbox backup <i>scheduleName</i> completed but not without errors. Additional warning messages were generated that describe the errors.
<b>Action</b>	Check for other warning messages related to this job run.

## EBR\_BACKUP\_WARNING\_MAILITEM

<b>Message</b>	Exchange processing message: <i>itemMsg</i>
<b>Example</b>	
<b>Description</b>	The Exchange mailbox backup process encountered issues that could have made backing up certain mail item fail.
<b>Action</b>	Informational message (no action needed).

## EBR\_DATA\_MIGRATION\_FAILED

<b>Message</b>	Exchange Backup data migration failed for Exchange Mailbox Backup ( <i>job_name</i> ) Caused by: Problem <i>description</i> . Apparent cause: <i>description</i>
<b>Example</b>	Exchange Backup data migration failed for Exchange Mailbox Backup (ExServ77229Ver002) Caused by: Problem connecting to AD server. Apparent cause: Invalid Credentials
<b>Description</b>	The attempt to migrate an existing mailbox job to the new format that supports multiple restore points failed. Earlier versions of the Exchange mailbox backup feature supported a single blob representation of the Exchange database. Now, multiple blob instances representing different dates can be saved. However, to accommodate this change, existing mailbox jobs must be migrated to a new format. This is a one-time migration is required of all older mailbox jobs.
<b>Action</b>	Check the problem and cause descriptions for information. In this example, the credentials used to log into the AD server were invalid, so the job needs to be re-run with proper credentials.

## EBR\_RESTORE\_CANCELLED

<b>Message</b>	Exchange Mailbox Restore was cancelled.
<b>Example</b>	(same)
<b>Description</b>	User initiated cancellation.
<b>Action</b>	Informational message (no action needed).

## EBR\_RESTORE\_FAILED\_BUSY\_BACKUP

<b>Message</b>	Mailbox restore could not be run because a mailbox backup was in progress.
<b>Example</b>	(same)
<b>Description</b>	An instance of the Exchange mailbox backup job was running when the new run request was made. Therefore, the new request was ignored and discarded (not rescheduled).
<b>Action</b>	Informational message (no action needed). To restart immediately, cancel the running job and then start a new instance of the job. See the <a href="#">Backup Jobs Tab</a> section for instructions on how to cancel or start a backup job from the UMC dashboard.

## EBR\_RESTORE\_FAILED\_BUSY\_RESTORE

<b>Message</b>	Mail box restore could not be run because a mailbox restore was in progress.
<b>Example</b>	(same)
<b>Description</b>	The Exchange mailbox job was being restored when the new restore request was made. Therefore, the new request was ignored.
<b>Action</b>	Wait for the current restore to complete and then restart the new restore request.

## EBR\_RESTORE\_FAILED\_EXCEPTION

<b>Message</b>	Exchange Mailbox Restore failed, caused by: <i>exceptionMsg</i>
<b>Example</b>	
<b>Description</b>	The mailbox restore failed due to the error described in <i>exceptionMsg</i> , which could describe a variety of conditions.
<b>Action</b>	The appropriate action varies by the cause of the failure. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> .

## EBR\_RESTORE\_STARTED

<b>Message</b>	Exchange Restore Started: <i>scheduleName</i> on <i>deviceAddress</i>
<b>Example</b>	Exchange Restore Started: 'Exchange Mailboxes' on 192.168.77.246
<b>Description</b>	A restore of the Exchange mailbox backup job <i>scheduleName</i> was started. This message does not indicate the scope of the restore (that is, which mailboxes in <i>scheduleName</i> are being restored), only that a restore has started.

<b>Action</b>	Informational message (no action needed).
---------------	---

## EBR\_RESTORE\_SUCCEEDED

<b>Message</b>	Exchange Restore Succeeded.
<b>Example</b>	(same)
<b>Description</b>	A restore of the Exchange mailbox backup job succeeded without errors. This message does not indicate the scope of the restore (that is, which mailboxes were restored), only that the restore succeeded.
<b>Action</b>	Informational message (no action needed).

## EBR\_RESTORE\_WARNING\_MAILITEM

<b>Message</b>	Exchange processing message: <i>itemMsg</i>
<b>Example</b>	
<b>Description</b>	The Exchange mailbox restore process encountered issues that could have made restoring certain mail item fail.
<b>Action</b>	Review the details in itemMsg to determine if any action is needed.

## EBR\_RESTORE\_FAILED

<b>Message</b>	Exchange Backup retention failed for Exchange Mailbox Backup ( <i>mailbox_job_name</i> ) on <i>device_addr</i> Cused by: <i>error_msg</i>
<b>Example</b>	Exchange Backup retention failed for Exchange Mailbox Backup (EBRServ99201Ver001) on 192.168.99.201 Caused by: EBR failure: RETENTION_CHECK_COMPLETED_WITH_ERRORS
<b>Description</b>	The Exchange mailbox restore process encountered issues that could have made restoring certain mail item fail.
<b>Action</b>	Review the details in itemMsg to determine if any action is needed.



## Image Job and Virtual Machine (VM) Events

This section describes event messages that might appear when adding, updating, or deleting an image backup job and when starting or stopping a virtual machine (VM).

### SERVER\_ALIVE\_BACKUP\_FAILED

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> Failed --- Error - <i>systemMsg</i>
<b>Example</b>	Backup Server Alive on 192.168.99.23 Failed --- Error - /mnt/ax/scratch/executor/uptiva-slave-1-4-6823.sh: line 48: /mnt/ax/app/SVA/axvmi.sh: Permission denied
<b>Description</b>	The image backup failed due to the error described in <i>systemMsg</i> , which could describe a variety of conditions. In the example the backup failed because of a permission denied problem.
<b>Action</b>	The appropriate action varies by the cause of the failure. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a> . If the message includes an “entitlement” comment (entitlement missing, expired, or not allowed), see the <a href="#">Check Entitlements</a> section for more information.

### SERVER\_ALIVE\_BACKUP\_STARTED

<b>Message</b>	Backup <i>firstTimePrefix</i> Started for <i>scheduleName</i> on <i>deviceAddress</i>
<b>Example</b>	Backup Started for ‘240-to-241-SVA-9927’ on 192.168.99.27
<b>Description</b>	A run of the image backup job <i>scheduleName</i> for the device <i>deviceAddress</i> was started. The <i>firstTimePrefix</i> value is “First-Time” if this is the first run of the backup job, blank if this is a regularly scheduled (or manually initiated) run, and “Refresh” if this is a refresh of the “current” image (set by the “Refresh Interval” field in the image job definition.)
<b>Action</b>	Informational message (no action needed).

### SERVER\_ALIVE\_BACKUP\_SUCCEEDED

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> completed Successfully
<b>Example</b>	Backup [Refresh] for ‘Server Alive’ on 192.168.99.120 completed Successfully.
<b>Description</b>	A run of the image backup job <i>scheduleName</i> for the device <i>deviceAddress</i> completed successfully. The <i>firstTimePrefix</i> value is “First-Time” if this is the first run of the backup job, blank if this is a regularly scheduled (or manually initiated) run, and “Refresh” if this is a refresh of the “current” image (set by the “Refresh Interval” field in the image job definition.)
<b>Action</b>	Informational message (no action needed).

### SERVER\_ALIVE\_BACKUP\_WARNING

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> Warning - StdErr - <i>systemMsg</i>
----------------	---

<b>Example</b>	
<b>Description</b>	An image backup was unable to transfer some files from the protected machine to the Axcient appliance. This may occur if the credentials configured on the Axcient appliance do not have permission to transfer all files. The user through which the backup is occurring should have administrative privileges and be part of the Backup Operators group. Additionally, there are some operating system-specific files (such as System Volume Information or Java Runtime Files) which are intentionally configured by each respective application to be inaccessible by all user accounts.
<b>Action</b>	Those files that cannot be backed up may be excluded from the backup job. See the <a href="#">Back Up System Images</a> section for instructions on how to exclude files from an image backup job. (A warning about a permission denied error from vdiff-backup being unable to lstat the \$BitMap, \$MFT, \$MFTMirr, \$LogFile, or \$Volume files can be ignored.)

## SERVER\_ALIVE\_BACKUP\_WARNING\_POST\_PRUNE\_INTERRUPTED

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> was cancelled during post-backup retention pruning, so that sub-task was cancelled also.
<b>Example</b>	Backup 'Server Alive' on 192.168.99.23 was cancelled during post-backup retention pruning, so that sub-task was cancelled also.
<b>Description</b>	The backup job was canceled, so any subtasks associated with the job were also canceled.
<b>Action</b>	Informational message (no action needed).

## SERVER\_ALIVE\_BACKUP\_WARNING\_PRUNE

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> Warning - retention pruning failed: <i>systemMsg</i>
<b>Example</b>	Backup [Refresh] 'Server Alive' on 192.168.99.23 Warning - retention pruning failed: /mnt/ax/scratch/executor/uptiva-slave-1-4-6818.sh: line 48: /mnt/ax/app/SVA/axvmi.sh: Permission denied
<b>Description</b>	One or more files could not be pruned from the Axcient appliance storage.
<b>Action</b>	Allow one backup to complete successfully. This issue is usually resolved automatically.

## SERVER\_ALIVE\_BACKUP\_WARNING\_PRUNE\_EXCEPTION

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> Warning - retention pruning failed: <i>exceptionMsg</i>
<b>Example</b>	
<b>Description</b>	One or more files could not be pruned from the Axcient appliance storage.
<b>Action</b>	Allow one backup to complete successfully. This issue is usually resolved automatically.

## SERVER\_ALIVE\_BACKUP\_WARNING\_STATS\_EMPTY

<b>Message</b>	Backup <i>firstTimePrefix</i> for <i>scheduleName</i> on <i>deviceAddress</i> vdiff statistics empty. See: <i>statsFilePath</i>
----------------	---

Example	
Description	Internal error.
Action	Contact <a href="#">Axcient customer support</a> .

## SERVER\_ALIVE\_VM\_BACKUP\_CANCELLED

Message	Backup job cancelled to fulfill <i>failoverType</i> request for: <i>scheduleName</i> on: <i>deviceAddress</i>
Example	Backup job cancelled to fulfill VM Failover request for: 'Server Alive' on: 192.168.99.120
Description	An image backup job run for job <i>scheduleName</i> on device <i>deviceAddress</i> was cancelled (and not rescheduled) because it conflicted with a current VM failoverType action. The <i>failoverType</i> is one of the following: VM Failover, VM Shutdown, VM Pause, Bare Metal Lock, Bare Metal Unlock.
Action	Informational message (no action needed). Optionally, manually start the image job run after the <i>failoverType</i> completes.

## SERVER\_ALIVE\_VM\_FAILED

Message	<i>failoverType</i> for: <i>scheduleName</i> on: <i>deviceAddress</i> for backup date: <i>backupDate</i> stderr: <i>systemMsg</i>
Example	
Description	The Axcient appliance was unable to start a VM successfully.
Action	If this issue continues, contact <a href="#">Axcient customer support</a> .

## SERVER\_ALIVE\_VM

Message	<i>failoverType</i> for: <i>scheduleName</i> on: <i>deviceAddress</i> stderr: <i>systemMsg</i>
Example	VM Failover for: 'Server Alive' on: 192.168.99.120
Description	A VM successfully started on the Axcient appliance.
Action	Informational message (no action needed).

## SERVER\_ALIVE\_VM\_STARTED

Message	<i>failoverType</i> Started for: <i>scheduleName</i> on: <i>deviceAddress</i>
Example	VM Failover Started for: 'Server Alive' on: 192.168.99.120
Description	A <i>failoverType</i> condition was started on the Axcient appliance for the device <i>deviceAddress</i> . The <i>failoverType</i> is one of the following: VM Failover, VM Shutdown, VM Pause, Bare Metal Lock, Bare Metal Unlock. Every STARTED message has a corresponding outcome message, so watch the log for the corresponding SUCCEEDED or FAILED message.
Action	Informational message (no action needed).

**SERVER\_ALIVE\_VM\_STOPPED**

<b>Message</b>	<i>failoverType</i> stopped for: <i>scheduleName</i> on: <i>deviceAddress</i>
<b>Example</b>	VM Failover stopped for: 'Server Alive' on: 192.168.99.120
<b>Description</b>	A failover (or test) VM for the device <i>deviceAddress</i> was stopped on the Axcient appliance.
<b>Action</b>	Informational message (no action needed).

**SERVER\_ALIVE\_VM\_SUCCEEDED**

<b>Message</b>	<i>failoverType</i> succeeded for: <i>scheduleName</i> on: <i>deviceAddress</i> for backup date: <i>backupDate</i>
<b>Example</b>	VM Failover succeeded for: 'Server Alive' on: 192.168.99.120 for backup date: 05/05/2010 - 7:49:48 PM
<b>Description</b>	A VM <i>failoverType</i> based on the system image dated <i>backupDate</i> for the device <i>deviceAddress</i> was started successfully on the Axcient appliance. The <i>failoverType</i> is one of the following: VM Failover, VM Shutdown, VM Pause, Bare Metal Lock, Bare Metal Unlock.
<b>Action</b>	Informational message (no action needed).

## Bare Metal Restore (BMR) Events

This section describes event messages that might appear when doing a BMR.

### BMR\_RESTORE\_FAILED

Message	Restore has failed for <i>deviceAddress</i>
Example	Restore has failed for 192.168.77.104
Description	The bare metal restore failed for an unspecified reason.
Action	The appropriate action varies by the cause of the failure. For corrective actions to typical problems, see <a href="http://www.axcient.com/log-actions">www.axcient.com/log-actions</a>

### BMR\_RESTORE\_INFO

Message	The restore is <i>restoredPercent</i> complete for <i>deviceAddress</i>
Example	The restore is 50% complete for 192.168.99.23
Description	Progress message during the restore process.
Action	Informational message (no action needed).

### BMR\_RESTORE\_STARTED

Message	Restore has started for <i>deviceAddress</i>
Example	Restore has started for 192.168.99.23
Description	The system image for 192.168.99.23 has been locked and prepared to be restored on a new device.
Action	Informational message (no action needed).

### BMR\_RESTORE\_SUCCEEDED

Message	Restore has succeeded for <i>deviceAddress</i>
Example	Restore has succeeded for 192.168.99.23
Description	The system image for 192.168.99.23 has been restored successfully on a new device.
Action	Informational message (no action needed).

## System Events

This section describes event messages that might appear about the Axcient appliance (hardware, configuration, and network status).

### CANT\_SEND\_MAIL

Message	error attempting to send mail: exceptionMsg
Example	
Description	E-mail from the Axcient appliance is sent through a security tunnel to the Axcient data center where it is processed and sent to the recipient from a mail server in the data center. This error message means an e-mail could not be sent. The primary causes for this error are an issue in the data center (not likely) and a problem with the tunnel connection (most likely). There are a variety of reasons the tunnel would not be connected such as firewall rules or an Internet problem.
Action	Check your firewall settings to make sure the Axcient appliance is not blocked from sending an e-mail to the RMC. If this is not the problem, contact <a href="#">Axcient customer support</a> .

### CANT\_SEND\_PSA\_TICKET

Message	Trying to send PSA ticket to <i>psa_tool</i> failed with the following error: <i>error_msg</i>
Example	Trying to send PSA ticket to ConnectWise failed with the following error: Server returned HTTP response code 500 for URL: <a href="https://test.connectwise.com/v4_6_release/services/system_io/integration_io/processclientaction.rails">https://test.connectwise.com/v4_6_release/services/system_io/integration_io/processclientaction.rails</a>
Description	There was a problem when trying to send ticket information from the Axcient appliance to the target PSA tool. This could result from a number of issues. In the example, a ConnectWise ticket failed because of an HTTP 500 (internal server) error.
Action	Review the <i>error_msg</i> for clues as to the problem and proceed accordingly. If you cannot determine and correct the underlying problem yourself, contact Axcient customer support.

### CHECK\_SMART\_DRIVE

Message	SMART: Please check drive health on <i>driveId</i>
Example	SMART: Please check drive health on /dev/md0
Description	One of the hard drives is beginning to fail. It is likely the drive will need to be replaced.
Action	Contact <a href="#">Axcient customer support</a> to arrange for a replacement drive.

### INFORMATION\_TASK\_FAILED

Message	The following <i>errorCt</i> UBS tasks failed to complete: Check Storage Space <i>CHECKSTORAGESPACE</i>
---------	--

	Contact RMC <i>CONTACTRMC</i> Check SMART status <i>CHECKSMARTSTATUS</i> Get Storage Space <i>GETSTORAGESPACE</i> Send Events <i>SENDEVENTS</i> Send Stats <i>SENDSTATS</i> Send Statistics <i>SENDSTATISTICS</i>
<b>Example</b>	The following (1) UBS tasks failed to complete: Check Storage Space [Succeed] Contact RMC [Fail] Check SMART status [Succeed] Get Storage Space [Succeed] Send Events [Succeed] Send Stats [Succeed] Send Statistics [Succeed]
<b>Description</b>	<p>The Axcient appliance does a periodic set of status checks and reports. This message reports the status (succeed or fail) of those status checks. In the example, the Axcient appliance was not able to contact the RMC. A “Fail” status indicates the following:</p> <ul style="list-style-type: none"> <li>• Check Storage Space: Storage capacity on the Axcient appliance is nearly full; more free space is needed.</li> <li>• Contact RMC: There was a connection error at either the Axcient appliance end or the RMC end. This could be due to a connection being down or to a connection being prevented, such as a firewall block.</li> <li>• Check SMART Status: A disk health test failed or disk health status was not available.</li> <li>• Get Storage Space: The required space exceeds the available space. This is due to exceeding either the entitled space or the physical capacity.</li> <li>• Send Events: A daily report of relevant failure and recovery events was not sent to the RMC.</li> <li>• Send Stats: Statistics about backup jobs was not sent to the RMC.</li> <li>• Send Statistics: Statistics about the Axcient appliance was not sent to the RMC.</li> </ul>
<b>Action</b>	<p>Select the appropriate action:</p> <ul style="list-style-type: none"> <li>• Check Storage Space: There are several options to free up disk space, such as enabling the <b>auto prune detection</b> feature, manually reducing the retention period, or excluding unneeded data from one or more backup jobs. See the <a href="#">Reduce Backup Job Size</a> section for more information.</li> <li>• Contact RMC: Check the network connections and firewall settings, and fix as necessary. A starting point is to determine whether the RMC is accessible (ping axcient.net).</li> <li>• Check SMART Space: Check for a “Please check drive health...” message in the log, and if one is present, contact Axcient customer support to arrange for a replacement drive.</li> <li>• Get Storage Space: If the Check Storage Space test also failed, the problem is probably not enough free disk space. Otherwise, check entitlements (see the <a href="#">Check Entitlements</a> section).</li> <li>• Send Events: See Contact RMC action.</li> <li>• Send Stats: See Contact RMC action.</li> <li>• Send Statistics: See Contact RMC action.</li> </ul>

## LOW\_DISK\_SPACE\_ALERT\_10\_PCT

<b>Message</b>	Less than 10% of Axcient Appliance storage remaining! Backup jobs may not have sufficient overhead to complete successfully. Reduce
----------------	---

	backup retention to conserve space.
<b>Example</b>	(same)
<b>Description</b>	The Axcient appliance is dangerously low on storage space, which could lead to failed backups and even data corruption if the appliance runs out of disk space.
<b>Action</b>	Analyze your storage requirements and do one (or both) of the following: <ul style="list-style-type: none"> <li>• Reduce the space currently used. This can be done by (1) reducing the retention period of selected jobs, (2) reducing the schedule frequency of selected jobs, or (3) deleting jobs. See the <a href="#">Reduce Backup Job Size</a> section for more information.</li> <li>• Contact <a href="#">Axcient customer support</a> to get a larger capacity Axcient appliance that better fits your needs.</li> </ul>

## LOW\_DISK\_SPACE\_ALERT\_20\_PCT

<b>Message</b>	Less than 20% of Axcient Appliance storage remaining! If space utilization grows too much further, backup jobs may fail. Consider reducing backup retention to conserve space.
<b>Example</b>	(same)
<b>Description</b>	The Axcient appliance is dangerously low on storage space, which could lead to failed backups and even data corruption if the appliance runs out of disk space.
<b>Action</b>	Analyze your storage requirements and do one (or both) of the following: <ul style="list-style-type: none"> <li>• Reduce the space currently used. This can be done by (1) reducing the retention period of selected jobs, (2) reducing the schedule frequency of selected jobs, or (3) deleting jobs. See the <a href="#">Reduce Backup Job Size</a> section for more information.</li> <li>• Contact <a href="#">Axcient customer support</a> to get a larger capacity Axcient appliance that better fits your needs.</li> </ul>

## NO\_DISK\_SPACE\_ALERT

<b>Message</b>	There is no storage remaining on the Axcient Appliance! Backup jobs cannot execute. Reduce backup retention to conserve space.
<b>Example</b>	(same)
<b>Description</b>	The Axcient appliance has run out of available storage space, which means backup jobs cannot run successfully and could result in data corruption.
<b>Action</b>	Analyze your storage requirements and do one (or both) of the following: <ul style="list-style-type: none"> <li>• Reduce the space currently used. This can be done by (1) reducing the retention period of selected jobs, (2) reducing the schedule frequency of selected jobs, or (3) deleting jobs. See the <a href="#">Reduce Backup Job Size</a> section for more information.</li> <li>• Contact <a href="#">Axcient customer support</a> to get a larger capacity Axcient appliance that better fits your needs.</li> </ul>

## PURGE\_EVENT\_LOG

<b>Message</b>	The event log was truncated
<b>Example</b>	(same)



<b>Description</b>	The event log was purged. Purging deletes all existing messages from the log. However, logging remains active, and all new events will be recorded in the log.
<b>Action</b>	Informational message (no action needed).

## QOS\_BANDWIDTH\_CHANGE

<b>Message</b>	QOS Bandwidth Changed from <i>oldQosSettingList</i> QOS Bandwidth Changed to <i>newQosSettingList</i>
<b>Example</b>	(QOS Bandwidth Changed from External service download rate limit:: 1000000 External Service Upload Rate Limit:: 100000 Internal service download rate limit:: 1000000 Internal service upload rate limit:: 1000000  QOS Bandwidth Changed to External service download rate limit:: 1000000 External Service Upload Rate Limit:: 500 Internal service download rate limit:: 1000000 Internal service upload rate limit:: 1000000)
<b>Description</b>	The bandwidth setting (quality of service) was changed for one or more of the adjustable rate limits: external upload rate, internal download rate, internal upload rate. (In the example the external upload rate was changed to 500 Kbit/sec from 1 Gbit/sec.)
<b>Action</b>	Informational message (no action needed). See the <a href="#">Set Bandwidth Usage (Quality of Service)</a> section for more information.

## QOS\_BANDWIDTH\_INITIALIZED

<b>Message</b>	QOS Bandwidth Schedule Initialized as <i>newQosSettingList</i>
<b>Example</b>	QOS Bandwidth Schedule Initialized as External service download rate limit:: 1000000 External Service Upload Rate Limit:: 100000 Internal service download rate limit:: 1000000 Internal service upload rate limit:: 1000000
<b>Description</b>	The bandwidth settings (quality of service) were enabled for the first time.
<b>Action</b>	Informational message (no action needed). See the <a href="#">Set Bandwidth Usage (Quality of Service)</a> section for more information.

## REGISTRATION\_FAILED

<b>Message</b>	Failed Registration for Axcient appliance: <i>serialNumber</i>
<b>Example</b>	Failed Registration for Axcient appliance: a5xl
<b>Description</b>	Axcient appliance <i>serialNumber</i> was not registered. Typically, this is because either there is no network connection to the RMC (where registration occurs) or Axcient has not yet added this appliance to the RMC.
<b>Action</b>	Verify that you can reach the RMC (ping axcient.net). If not, check your network connections. If you can reach the RMC, contact Axcient customer support and verify the appliance has been added to the RMC.

## REGISTRATION\_SUCCEEDED

<b>Message</b>	Succeeded Registration for Axcient appliance: <i>serialNumber</i>
----------------	---

Example	Succeeded Registration for Axcient appliance: a5xl
Description	The Axcient appliance <i>serialNumber</i> was registered successfully with the RMC.
Action	Informational message (no action needed).

## REGISTRATION\_TRIAL\_MODE

Message	Did not fully register Appliance, registered in trial mode Appliance: <i>serialNumber</i>
Example	Did not fully register Appliance, registered in trial mode Appliance: a5xl
Description	Axcient appliance <i>serialNumber</i> was not registered and, therefore, started in trial mode. (In this case <i>serialNumber</i> could appear as “TRIAL”.) Typically, this is because either there is no network connection to the RMC (where registration occurs) or Axcient has not yet added this appliance to the RMC.
Action	Verify that you can reach the RMC ( <i>ping axcient.net</i> ). If not, check your network connections. If you can reach the RMC, contact Axcient customer support and verify the appliance has been added to the RMC. When in trial mode, the UMC dashboard displays a trial message at the bottom of the page. Register the appliance using the <b>Register Now</b> link provided on the UMC dashboard.

## SYSTEM\_CONFIG\_UPDATED

Message	System update was performed for <i>systemSettingsType</i>
Example	
Description	The system setting <i>systemSettingsType</i> was updated (changed).
Action	Informational message (no action needed).

## SYSTEM\_DISABLE\_ACCESS

Message	Disable Axcient technical support access
Example	(same)
Description	Access to the appliance through special tools available to Axcient technical support personnel has been disabled. This is a configurable option for customers who wish to maintain strict access security.
Action	Informational message (no action needed).

## SYSTEM\_ENABLE\_ACCESS

Message	Enable Axcient technical support access
Example	(same)
Description	Access to the appliance through special tools available to Axcient technical support personnel has been enabled.

<b>Action</b>	Informational message (no action needed).
---------------	---

## SYSTEM\_RAID\_DRIVE\_CHECK\_FAILED

<b>Message</b>	RAID drive check FAILED. RAID: Drive status for <i>driveId</i> is: <i>driveStatus</i>
<b>Example</b>	RAID drive check FAILED. RAID: Drive status for RAID 5 is: Recovering, 16% complete Alert time: Thu May 05 16:10:37 PDT 2011
<b>Description</b>	The system could not complete the RAID implementation. This could be a transient event, in which case the RAID can recover. However, if this condition persists, it is likely because either a disk or the RAID controller failed.
<b>Action</b>	Wait to see if the RAID recovers. If it does not in a reasonable amount of time, contact Axcient customer support to replace the bad disk or controller.

## SYSTEM\_RAID\_DRIVE\_CHECK\_WARNING

<b>Message</b>	RAID drive check WARNING. RAID: Drive status for <i>driveId</i> is: <i>driveStatus</i>
<b>Example</b>	
<b>Description</b>	The RAID implementation is in the process of recovery. Some event occurred that required the RAID array to rebuild. This message indicates the RAID array is being rebuilt currently.
<b>Action</b>	Informational message (no action needed). However, if the RAID array does not rebuild successfully in a reasonable amount of time, there might be another problem that does require attention.

## SYSTEM\_SHUTDOWN

<b>Message</b>	The system is shutting down. All running jobs and other processes will be stopped.
<b>Example</b>	(same)
<b>Description</b>	A manual or system shutdown was initiated, and the system is shutting down.
<b>Action</b>	Informational message (no action needed).

## User Events

This section describes event messages that might appear when users access the UMC and when adding, modifying, or deleting user accounts.

### USER\_ADDED

Message	Add User: <i>username</i>
Example	Add User: jsmith@axcient.com
Description	The user account <i>username</i> was added to the UMC
Action	Informational message (no action needed).

### USER\_DELETED

Message	User: <i>username</i> has been deleted
Example	User: jsmith@axcient.com has been deleted
Description	The user account <i>username</i> was deleted from the UMC
Action	Informational message (no action needed).

### USER\_LOCKED

Message	User account: <i>username</i> has been locked, too many login failures. Wait 30 minutes before logging in again.
Example	User account: jsmith@axcient.com has been locked, too many login failures. Wait 30 minutes before logging in again.
Description	If there are several failed login attempts, the system locks out additional attempts. (The most common causes of login failures are forgetting or misspelling the password.) The lock is released after 30 minutes.
Action	Wait 30 minutes for the lock to clear and try again.

### USER\_LOGIN

Message	User: <i>username</i> logged in
Example	User: jsmith@axcient.com logged in
Description	The user <i>username</i> logged in to the UMC.
Action	Informational message (no action needed).

**USER\_LOGOUT**

<b>Message</b>	User: <i>username</i> logged out
<b>Example</b>	User: jsmith@axcient.com logged out
<b>Description</b>	The user <i>username</i> logged out of the UMC.
<b>Action</b>	Informational message (no action needed).

**USER\_PASSWORD\_CHANGED**

<b>Message</b>	Password change for user: <i>username</i>
<b>Example</b>	Password change for user: jsmith@axcient.com
<b>Description</b>	The password for user account <i>username</i> was updated on the UMC
<b>Action</b>	Informational message (no action needed).

**USER\_UPDATED**

<b>Message</b>	Edit User: <i>username</i>
<b>Example</b>	Edit User: smith@axcient.com
<b>Description</b>	The user account <i>username</i> was updated on the UMC
<b>Action</b>	Informational message (no action needed).

## DAS Events

This section describes event messages that might appear when transferring files from the Axcient appliance to a direct attach storage (DAS) device for transfer to an Axcient data center.

### DAS\_COPY\_ALREADY\_COPYING

<b>Message</b>	OffsiteCopy in progress, but called again. Ignoring.
<b>Example</b>	(same)
<b>Description</b>	The data is already being copied to the DAS device, so it is unnecessary to start it again.
<b>Action</b>	Informational message (no action needed).

### DAS\_COPY\_CONNECTED\_ON\_REBOOT

<b>Message</b>	OffsiteCopy: Axcient appliance is rebooted with DAS connected
<b>Example</b>	(same)
<b>Description</b>	A DAS device was connected to the Axcient appliance when the appliance was rebooted.
<b>Action</b>	Informational message (no action needed).

### DAS\_COPY\_DISCONNECTED

<b>Message</b>	OffsiteCopy: DAS device has been abruptly removed after start of DAS copy
<b>Example</b>	(same)
<b>Description</b>	The connection to the DAS device was broken during an offsite backup job run. This could be due to someone physically disconnecting the drive or to a hardware problem that caused the signal to fail.
<b>Action</b>	Verify the DAS device is connected to the Axcient appliance. If it is disconnected, reconnect the DAS and restart the DAS download. If it is connected, unplug and then reconnect the DAS. If the Axcient appliance still cannot see the DAS, contact Axcient customer support.

### DAS\_COPY\_ERROR

<b>Message</b>	OffsiteCopy unable to mount das: <i>systemMsg</i>
<b>Example</b>	
<b>Description</b>	The system was unable to mount and/or copy the data to the DAS device. This can be caused because the DAS device is not connected properly, there is a hardware failure in the DAS device, or there was an intermittent error.
<b>Action</b>	Disconnect and reconnect the DAS device and retry the copy operation. If it fails again, call <a href="#">Axcient customer support</a> .

**DAS\_COPY\_EXCEPTION**

<b>Message</b>	Error occurred while running an Offsite DAS Drive Copy, exception: exceptionMsg
<b>Example</b>	
<b>Description</b>	An error condition (exception) was encountered during the DAS operation. This error can come from various conditions, but it most likely was generated because of a mount issue or a file copying issue.
<b>Action</b>	Disconnect and reconnect the DAS device and retry the copy operation. If it fails again, call <a href="#">Axcient customer support</a> .

**DAS\_COPY\_INFO**

<b>Message</b>	OffsiteCopy: offsite DAS copy has starting...
<b>Example</b>	(same)
<b>Description</b>	An offsite backup job run has started to the DAS device (i
<b>Action</b>	Informational message (no action needed).

**DAS\_COPY\_MOUNTED**

<b>Message</b>	OffsiteCopy: Copy button is enabled and DAS is mounted
<b>Example</b>	(same)
<b>Description</b>	The DAS device is recognized by the Axcient appliance and is ready for use.
<b>Action</b>	Informational message (no action needed).

**DAS\_COPY\_NOMOUNTED**

<b>Message</b>	OffsiteCopy: Unable to mount
<b>Example</b>	(same)
<b>Description</b>	The DAS device could not be mounted, which means the DAS cannot be used as the target device for an offsite backup job.
<b>Action</b>	Disconnect and reconnect the DAS device to see if that solves the problem.

**DAS\_COPY\_STARTED**

<b>Message</b>	OffsiteCopy: Beginning copy process...
<b>Example</b>	(same)

<b>Description</b>	An offsite backup job run has started. This backup is to the DAS device (instead of directly to the Axcient data center through the Internet).
<b>Action</b>	Informational message (no action needed).

## DAS\_COPY\_STARTING

<b>Message</b>	OffsiteCopy: Beginning copy process...
<b>Example</b>	(same)
<b>Description</b>	An offsite backup job run has started. This backup is to the DAS device (instead of directly to the Axcient data center through the Internet).
<b>Action</b>	Informational message (no action needed).

## DAS\_COPY\_SUCCEEDED

<b>Message</b>	OffsiteCopy: Offsite files have been copied to DAS device
<b>Example</b>	(same)
<b>Description</b>	The offsite backup job was copied successfully to the DAS device.
<b>Action</b>	Informational message (no action needed). After a successful backup, follow the return instructions in the <a href="#">Axcient DAS Transfer Guide</a> .

## DAS\_COPY\_UNMOUNTED

<b>Message</b>	OffsiteCopy: DAS device has been unmounted
<b>Example</b>	(same)
<b>Description</b>	The DAS device was unmounted. This happens automatically after a successful backup.
<b>Action</b>	Informational message (no action needed).

## DAS\_COPY\_UNMOUNTING\_ERROR

<b>Message</b>	Unable to unmount the DAS device after copying offsite error: <i>systemMsg</i>
<b>Example</b>	
<b>Description</b>	The DAS device could not be unmounted, which could be due to a number of issues.
<b>Action</b>	Contact <a href="#">Axcient customer support</a> . Do NOT disconnect the DAS device. It is important to ensure the data is synced properly to the DAS before disconnecting to avoid corruption.

## DAS\_COPY\_UNMOUNTING\_EXCEPTION

<b>Message</b>	Unable to unmount the DAS device after copying offsite exception: <i>exceptionMsg</i>
----------------	---



**Example****Description**

The DAS device could not be unmounted, which could be due to a number of issues.

**Action**

Contact [Axcient customer support](#). Do NOT disconnect the DAS device. It is important to ensure the data is synced properly to the DAS before disconnecting to avoid corruption.

**DAS\_COPY\_UNMOUNTING****Message**

OffsiteCopy: Ummounting DAS device

**Example**

(same)

**Description**

The DAS device is being unmounted. This happens automatically after a successful backup.

**Action**

Informational message (no action needed).

## Export Copy Events

This section describes event messages that might appear when transferring files from the Axcient appliance to a direct attach storage (DAS) device used as an external backup archive.

### EXPORT\_CANCELLED\_BY\_USER

Message	Export Copy: Copy to drive canceled by user
Example	(same)
Description	A user canceled an export copy to a DAS device.
Action	Informational message (no action needed).

### EXPORT\_FAILED

Message	Export Copy failed: <i>message</i>
Example	
Description	An export copy to a DAS device failed.
Action	Review the message to assess the problem and then attempt to export again. See the <a href="#">Axcient DAS Transfer Guide</a> for more information.

### EXPORT\_INFO

Message	Export Copy: <i>message</i>
Example	Export Copy: message
Description	These are information messages displayed as an export copy to a DAS device is performed.
Action	Informational message (no action needed).

### EXPORT\_STARTED

Message	Export Copy: Started...
Example	(same)
Description	An export copy to a DAS device has started.
Action	Informational message (no action needed).

### EXPORT\_SUCCEEDED

<b>Message</b>	Export Copy completed successfully. Succeeded: <i>number_of_jobs</i> <i>device_name: job_name</i> ...
<b>Example</b>	Export Copy completed successfully. Succeeded: 3 192.168.99.11 : 99.11 FF 1 192.168.77.85 : twaxdev test-file1 192.168.99.11 : 99.11 foobar
<b>Description</b>	An export copy to a DAS device completed successfully. The message indicates how many jobs were copied and lists those jobs.
<b>Action</b>	Informational message (no action needed).

## EXPORT\_WARNING

<b>Message</b>	Export Copy: <i>warning_message</i>
<b>Example</b>	Export Copy: Unable to unmount the drive after completing copy. Exception: java.lang.InterruptedException: sleep interrupted
<b>Description</b>	A problem occurred during an export copy operation that generated a warning. In the example, the appliance was unable to unmount the DAS device after completing the export copy.
<b>Action</b>	Contact <a href="#">Axcient customer support</a> . Do NOT disconnect the DAS device. It is important to ensure the data is synced properly to the DAS before disconnecting to avoid corruption.

## Entitlement Events

This section describes event messages that might appear during entitlement-related actions (entitlements granted to this user account).

### ENTITLEMENT\_EXPIRED

<b>Message</b>	Entitlement expired for appliance <i>serviceld</i> . Contacting RMC to update it.
<b>Example</b>	Entitlement expired for appliance '2tej'. Contacting RMC to update it.
<b>Description</b>	The entitlements allowed to this account have expired. The Axcient appliance will attempt to contact the RMC to get the latest entitlement information.
<b>Action</b>	Wait a few minutes and then check the current entitlements (see the <a href="#">Check Entitlements</a> section).

### ENTITLEMENT\_INVALID

<b>Message</b>	Entitlement is invalid for appliance <i>serviceld</i> .
<b>Example</b>	Entitlement is invalid for appliance '2tej'.
<b>Description</b>	The Axcient appliance could not validate entitlements, either because no entitlement information is available or the information is not correct for this appliance.
<b>Action</b>	Wait a few minutes and then check the current entitlements (see the <a href="#">Check Entitlements</a> section).

### ENTITLEMENT\_INVALID

<b>Message</b>	Entitlement is valid for appliance <i>serviceld</i> .
<b>Example</b>	Entitlement is valid for appliance '2tej'.
<b>Description</b>	The Axcient appliance is authorized (entitled) to perform specified actions.
<b>Action</b>	Informational message (no action needed).

### ENTITLEMENT\_UPGRADED

<b>Message</b>	Entitlement was upgraded for appliance <i>serviceld</i> .
<b>Example</b>	Entitlement was upgraded for appliance '2tej'.
<b>Description</b>	A new entitlement record was loaded into the Axcient appliance. This can occur when new information is downloaded from the RMC or when a user manually pastes in new information in the Entitlements page of the UMC (in authorized accounts).
<b>Action</b>	Informational message (no action needed).



**OFFSITE\_STORAGE\_EXCEEDED**

<b>Message</b>	Offsite storage used is: <i>offsiteUsed</i> which is more than the offsite storage allowed: <i>offsiteAllowed</i> for this appliance.
<b>Example</b>	Offsite storage used is: '550 GB' which is more than the offsite storage allowed: '500 GB' for this appliance.
<b>Description</b>	The amount of offsite storage used to store the backup jobs from this Axcient appliance exceeds the entitled amount allocated to this appliance.
<b>Action</b>	Wait a few minutes and then check the current entitlements (see the <a href="#">Check Entitlements</a> section).

**ONSITE\_STORAGE\_EXCEEDED**

<b>Message</b>	Onsite storage used is: <i>onsiteUsed</i> which is more than the onsite storage allowed: <i>onsiteAllowed</i> for this appliance.
<b>Example</b>	Onsite storage used is: '1100 GB' which is more than the onsite storage allowed: '1000 GB' for this appliance.
<b>Description</b>	The amount of onsite storage used to store the backup jobs exceeds the entitled amount allocated to this account.
<b>Action</b>	Wait a few minutes and then check the current entitlements (see the <a href="#">Check Entitlements</a> section).

## Device Error Messages

This section describes error messages that might appear when adding or modifying a device.

<b>Message</b>	An error occurred in retrieving your shares.
<b>Example</b>	(same)
<b>Description</b>	The device was not reachable because it was shutdown, it was not addressable though the network (no response to ping), the network was down, or the administrative password was changed after the device was added.
<b>Action</b>	Check each of the conditions identified in the explanation and correct as needed. If the administrative password changed, update the specified password for the device.

<b>Message</b>	Could not connect to device: <i>device-name</i>
<b>Example</b>	Could not connect to device: Sam laptop
<b>Description</b>	During the discovery phase when adding multiple devices, one or more of the device parameters (name, IP address, user name, password) were wrong for the listed device.
<b>Action</b>	Verify that all the entered information for the specified device is correct (e.g., misspelling, incorrect IP address, missing domain\username) and then try again to add the device.

<b>Message</b>	Devices that failed to add: Could not connect to device: <i>device1-name</i> Could not connect to device: <i>device2-name</i> (and so on)
<b>Example</b>	Devices that failed to add: Could not connect to device: 192.168.77.36 Could not connect to device: EBR Server1
<b>Description</b>	During the discovery phase when adding multiple devices, one or more of the device parameters (name, IP address, user name, password) were wrong for the listed devices.
<b>Action</b>	Verify that all the entered information for the specified devices is correct (e.g., misspelling, incorrect IP address, missing domain\username) and then try again to add the device.

<b>Message</b>	This address is already in use.
<b>Example</b>	(same)
<b>Description</b>	Credentials for a device already in use were entered.
<b>Action</b>	Verify that all the entered information for the device is correct (e.g., misspelling, incorrect IP address, missing domain\username) and then try again to add the device.

<b>Message</b>	Unable to connect to machine.
<b>Example</b>	(same)
<b>Description</b>	One or more of the device parameters (name, IP address, user name, password) were wrong.
<b>Action</b>	Verify that all the entered information for the device is correct (e.g., misspelling, incorrect IP address, missing domain\username) and then try again to add the device.



## BMR Error Messages

This section describes error messages that might appear on the target machine console when doing a BMR.

<b>Message</b>	BMR failed - No Server is locked for Bare Metal Restore. Use the Bare Metal Restore button on the page at Devices/Server/Job Name.
<b>Example</b>	(same)
<b>Description</b>	A BMR image for the source device is not prepared for download on the Axcient appliance.
<b>Action</b>	Select and prepare the image through the UMC. See the <a href="#">Start BMR</a> section for more information.

<b>Message</b>	Cannot enable network interface. Please load appropriate driver.
<b>Example</b>	(same)
<b>Description</b>	The network is not enabled. One possible reason is that none of the default drivers is appropriate for this device.
<b>Action</b>	Download the appropriate driver. You can do this through the <b>Load Driver</b> option on the BMR login page. To identify unknown components, see the <a href="#">Unknown Device Identifier Utility</a> section.

<b>Message</b>	Not enough space on disk 0 - required: <i>required_size</i> , actual: <i>actual_size</i>
<b>Example</b>	Not enough space on disk 0 - required: 315 GB, actual: 223 GB
<b>Description</b>	The size of the target device disk is too small to hold the source device BMR image.
<b>Action</b>	Use a target device with sufficient capacity to hold the source device image.

<b>Message</b>	The current machine has less number of disks than the backed-up server.
<b>Example</b>	(same)
<b>Description</b>	A BMR cannot be performed because the target device has fewer disks than the source device.
<b>Action</b>	Change to a different target device that has as least as many (or more) hard disks as the source device.

<b>Message</b>	The existing partition table doesn't have drive <i>letter</i>
<b>Example</b>	The existing partition table doesn't have drive C:
<b>Description</b>	This happens only when if "use existing partition table" is selected and the existing partitions do not include the specified drive (C: in the example).
<b>Action</b>	Either create the partition for the specified drive or uncheck "use existing partition table" and then try again.

<b>Message</b>	BMR aborted: The target drive <i>letter</i> is smaller than disk usage of the source drive (target.size= <i>val1</i> , source.usage= <i>val2</i> ). Try BMR with manual partition on larger drives.
<b>Example</b>	BMR aborted: The target drive C: is smaller than disk usage of the source drive (target.size= <i>size_in_bytes</i> , source.usage= <i>size_in_bytes</i> ). Try BMR with manual partition on larger drives.
<b>Description</b>	The target device disk is too small to copy the source device image. This can happen when performing a BMR from a running VM whose disk consumption is now larger than the original configured disk.
<b>Action</b>	Partition the target drive to be larger than <i>val2</i> , and then retry the BMR with the “use existing partition table” box checked.

<b>Message</b>	Network interface cable unplugged.
<b>Example</b>	(same)
<b>Description</b>	The network cable is not plugged in to the BMR target device.
<b>Action</b>	Plug a network cable into the target device.

<b>Message</b>	Can not get a valid IP address.
<b>Example</b>	(same)
<b>Description</b>	The BMR target device cannot acquire a valid IP address.
<b>Action</b>	Verify your DHCP server is serving the subnet of the BMR target device, or assign a static IP to the target device.

<b>Message</b>	No available backup.
<b>Example</b>	(same)
<b>Description</b>	The Axcient appliance has been locked for a BMR, but there is no available BMR image (internal error).
<b>Action</b>	Contact <a href="#">Axcient customer support</a> .

<b>Message</b>	One of the following: <ul style="list-style-type: none"> <li>• Unable to load restored system information.</li> <li>• Unable to load restored system disk information.</li> <li>• Unable to load restored operating system version.</li> </ul>
<b>Example</b>	(same)
<b>Description</b>	Cannot load source system information from the prepared image, or the information is corrupted (internal error).
<b>Action</b>	Contact <a href="#">Axcient customer support</a> .

<b>Message</b>	One of the following: <ul style="list-style-type: none"> <li>• Unable to retrieve disk information.</li> <li>• Unable to detect any hard disks. Please make sure necessary storage device drivers are loaded, and cable/power for hard disks are connected.</li> <li>• Unable to retrieve volume information.</li> </ul>
<b>Example</b>	(same)
<b>Description</b>	Cannot detect any hard disk on the BMR target device.
<b>Action</b>	Verify that the necessary storage device drivers are loaded on the BMR target device, and that cable and power for the hard disks are connected.

<b>Message</b>	One of the following: <ul style="list-style-type: none"> <li>• Unable to connect to Axcient Appliance.</li> <li>• Not a valid Axcient Appliance.</li> </ul>
<b>Example</b>	(same)
<b>Description</b>	The BMR boot CD cannot find or connect to the Axcient appliance. It is likely the entered hostname or IP address is not valid.
<b>Action</b>	Verify that you have the correct hostname or IP address for the Axcient appliance and then enter it in the “IP Address of Axcient Appliance” field of the BMR boot CD login page.

<b>Message</b>	One of the following: <ul style="list-style-type: none"> <li>• No network interface found. Please load network driver.</li> <li>• Failed to set static IP - invalid IP address/subnet mask.</li> <li>• Failed to set static IP - invalid gateway.</li> </ul>
<b>Example</b>	(same)
<b>Description</b>	The provided static IP address is not valid for one of the stated reasons. These issues can result if a static IP is specified in the BMR boot CD login page.
<b>Action</b>	Verify you have the correct network address information and (based on the message) do one of the following from the BMR boot CD login page: <ul style="list-style-type: none"> <li>• Select the <b>Load Driver</b> option and load the correct network driver.</li> <li>• Select the <b>Set Static IP</b> option and enter a valid IP address, subnet, and gateway.</li> </ul>

# Optimizing

## Setup Summary

There are several steps to configure and maintain an Axcient data protection solution:

1. **Analyze protection needs** - You need to determine how much backup storage space is required and what protection services you want. Consider the following:
  - **Number and size of devices to protect** - Determine the number and size (disk space) of devices to protect. This dictates how big an appliance you will need to protect those devices. It is common to underestimate the amount of backup storage space required. While the Axcient solution is designed to grow as your needs grow, making a better estimate up front reduces the need and hassle of upgrading in the future.
  - **Type of protection** - Axcient can provide basic backup protection for nearly any type of device, but it can also provide business continuity protection for most Windows-based devices and an application-aware mailbox backup option for Exchange servers. The number, scope, and type of backup jobs all affect the capacity and performance requirements needed from the Axcient appliance.
2. **Offsite backup requirements** - Backing up everything to the cloud ensures complete disaster and cloud virtual office protection, but it also means transferring significant amounts of data to the cloud on a regular basis. Part of analyzing your protection needs is determining your offsite requirements.
3. **Install appliance** - The first task is to install an Axcient appliance at your site. [Installation Guidelines](#) section covers steps that make the installation go smoothly.
4. **Add devices** - Target device addresses and credentials must be entered so the appliance can log into and back up the data on those devices. [Device Guidelines](#) section provides guidelines for ensuring device connections work properly.
5. **Add backup jobs** - The single most important setup task is to define one or more backup jobs for each device. [Backup Job Guidelines](#) section describes factors to consider when creating backup jobs.
6. **Configure appliance** - The appliance can run using all default settings, but it is likely you will want to customize some settings. [Appliance Configuration Guidelines](#) section describes some configuration options.
7. **Monitor progress** - When your solution is configured and running, monitoring operations is an ongoing need. [Monitoring Guidelines](#) section describes options available to simplify the monitoring process.

## Installation Guidelines

Installing an Axcient appliance (see the [Axcient Installation Guide](#)) is usually a simple task if your network is set up properly. Consider the following before you install:

1. The Axcient appliance comes with predetermined network settings, some of which must be updated for your environment. Before you get to the installation network settings page, be sure you have the correct values for IP address, subnet mask, gateway, domain, workgroup, DNS server, and hostname. If any of the values entered on this page are incorrect, the appliance will not work properly.

**Figure 111** - Installation Network Setting Page

**Axcient**  
Unified Management Console

### initial setup: step 1 - network settings

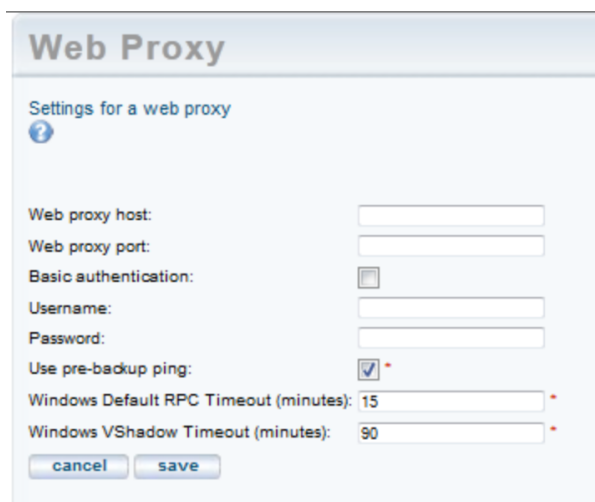
Thank you for choosing Axcient!

The first step in configuring your new Axcient appliance data replication management system is to reconfigure the network settings for your environment.

IP address:	192.168.100.1
Subnet mask:	255.255.255.0
Default gateway:	192.168.100.254
Domain:	change.me
Workgroup:	WORKGROUP
Primary DNS Server:	4.2.2.1
Hostname:	axcient
Secondary DNS Server:	4.2.2.2
Tertiary DNS Server:	4.2.2.3
MAC address::	00:9c:02:99:38:08
Serial #::	BE1012A0211220058

[next](#) [cancel](#)

The Axcient appliance requires access through your internal network to the target devices and Internet access to an Axcient data center in order to provide protection. Check your firewall setting to make sure the Axcient appliance has such access. If you use a web proxy, configure the Axcient appliance for that proxy server. See the [Configure Web Proxy](#) section for instructions.

**Figure 112** - Web Proxy PageThe image shows a web-based configuration page titled "Web Proxy". Below the title is a subtitle "Settings for a web proxy" with a help icon. The page contains several input fields: "Web proxy host:" and "Web proxy port:" are text boxes; "Basic authentication:" is a checkbox; "Username:" and "Password:" are text boxes; "Use pre-backup ping:" is a checked checkbox; "Windows Default RPC Timeout (minutes):" is a text box with the value "15"; and "Windows VShadow Timeout (minutes):" is a text box with the value "90". At the bottom are "cancel" and "save" buttons.

Web Proxy

Settings for a web proxy

Web proxy host:

Web proxy port:

Basic authentication: ☐

Username:

Password:

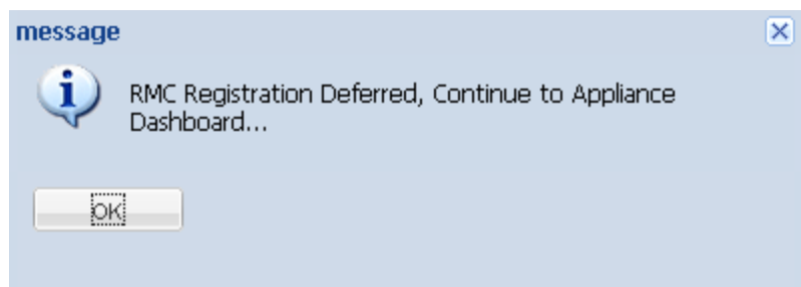
Use pre-backup ping: ☒

Windows Default RPC Timeout (minutes):

Windows VShadow Timeout (minutes):

The Axcient appliance uses a number of ports at various times. Be sure to open ports 8, 22, 53, 80, 123, 443, and 4015 to 4030 for the appliance.

In order to complete registration, the Axcient appliance must be able to access the RMC, which runs in an Axcient data center. If you get a registration deferred message during installation, see [Cannot Register Appliance](#) section for possible causes and corrective actions.

**Figure 113** - Deferred Registration Method

The Integrated Lights Out (ILO) feature can be configured at any time, but it is recommended that you do it when you install an appliance, because enabling ILO requires physical access to the appliance (see [Remote Hardware Maintenance](#) section).

## Device Guidelines

The Axcient appliance must have proper access to a device in order to protect that device. Note the following guidelines when preparing, adding, or updating a device.

- **Enter device credentials** - When adding or updating a device, consider the following when entering values into the indicated fields:
  - **Hostname or IP** - If you use DHCP, it is generally better to enter a host name rather than an IP address, because if the IP address changes, you must manually update this field or the Axcient appliance will no longer be able to access the device. Also, enter a fully qualified host name (as illustrated below) if the device is not on the same domain as the appliance; otherwise, just the host name is sufficient. Example:  
*hostname.subdomain.domain.com*
  - **Device Type** - Choosing server or desktop does not affect the backup options. However, choosing laptop causes a “backup on connect” field to appear when you create a backup job. See [Laptop Backup Strategy](#) section for more information.
  - **Administrative username** - For Exchange servers and some other devices, the entered name must include the domain in the following form: *domain\name*
  - **Administrative password** - It is common that administrator passwords are changed periodically, and when this occurs, you must update the password in this field or the Axcient appliance will no longer be able to access the device.

**Figure 114** - Device Page

The screenshot shows a web form titled "add a device". It contains the following fields and controls:

- Hostname or IP:** A text input field.
- Operating system:** A dropdown menu with "AUTODETECT" selected.
- Device type:** A dropdown menu with "-- Select a Type --" selected.
- Administrative username:** A text input field containing "admin". Below it, a note reads: "(Domain name required for Exchange Server. Format: domain\username)".
- Administrative password:** A text input field with masked characters (dots).
- Device alias:** A text input field.
- Additional user assigned:** A dropdown menu with "-- Select a User --" selected.
- At the bottom left are "cancel" and "save" buttons.

- **Enable file sharing** - The file sharing service must be enabled on a device before the Axcient appliance can back up data. To turn on file sharing, see the appropriate file sharing section for your operating system in [Cannot Add Device](#) section.

- *Configure Windows device* - Because Axcient uses special features of the Windows operating system to support business continuity and other advanced features, it is necessary that each Windows device be properly configured to work with an Axcient appliance. The best way to do this is to run the Windows and VSS configuration scripts on each Windows device. The scripts can be downloaded from the UMC tools page. See the [Use Configuration Tools](#) section for more information.
- *Verify connectivity* - After a device is added, it is a good practice to verify the connection. On the UMC click on the target device and then select the test access option. Connectivity access, data access, and control access tests are automatically performed and the results—OK or failure—are displayed. You can do this test at any time to verify device access. See the [Test Device Access](#) section for more information.



## Initial Backup Strategy

The single most important setup task is to define one or more backup jobs on each device that address your protection needs. The following sections highlight factors to consider when creating or updating a backup job.

- [Image File Job Considerations](#)
- [File Job Considerations](#)
- [Additional Job Considerations](#)
- [Initial Backup Strategy](#)
- [Laptop Backup Strategy](#)

## Image Job Considerations

Creating an image backup job is a fairly simple task (Figure 127 ), but the following bullet points are factors to consider. See the [Back Up System Images](#) section for more information.

- **Schedule type** - The first factor is the schedule. The default is an hourly type that actually runs just twice a day, at 8am and again at 6pm. From experience this is an appropriate schedule for many customers. However, you need to judge whether it fits your business needs. Changing to a more frequent schedule means your storage and performance overhead increases, while decreasing the frequency does the opposite.
- **Image refresh** - A related question is whether to engage the refresh mechanism, which is off by default. This creates a “current” backup image that is updated regularly without the overhead of saving each version, because the “current” version is simply overwritten at each refresh. Enabling refresh is a good strategy if you want to keep an up-to-date version during business hours.
- **Retention method** - The next consideration is retention, that is how long to keep old versions. Because image jobs back up everything on the device, retention is usually kept short, as in the default of just one week. File jobs are often added for data that should be saved for longer periods. However, if storage space is not a big issue, you can save image jobs much longer. This also relates to the question of whether to have a fixed retention period or instead use graduated retention. See [Additional Job Considerations](#) section for a discussion of the fixed retention versus graduated retention issue.
- **Pre-backup log flushing** - The pre-backup log flushing is on by default. This is a good idea when relevant and a non-factor when not relevant, so you can safely leave this field enabled.



Figure 115 - Image Backup Job

### 192.168.99.201 - create image backup

Image level backup maintains an up-to-date replica of your system for failover and/or restore

Schedule name:

Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Disk drives:  C:   
☒  E:

Backup schedule type:

Backup Offsite: ☐

Refresh interval:

Run initial backup now: ☒

Start time:  :  (8:00 AM)

Start a backup every:  hours

Keep starting backups until:  :  (6:00 PM)

On these days: ☒ Monday  
☒ Tuesday  
☒ Wednesday  
☒ Thursday  
☒ Friday  
☐ Saturday  
☐ Sunday

Keep backups for:  hours (about 7.0 days)

Turn on Compaction ☐ (Allows for restore points to be compacted over time.)

Turn on Log Flushing (Pre Backup): ☒ (e.g., MS Exchange Server, MS SQLServer)

Reminder\* If Quality of Service (bandwidth throttling) is on, make sure the internal service download and upload rate limits are set to 1 Gbit/sec (default value). A lower setting will cause unacceptable performance degradation for an image backup job.

[Advanced Options](#)

**Summary**

Your backup will run on Monday, Tuesday, Wednesday, Thursday, Friday, every 10 hours, between the hours of 8:00 AM and 6:00 PM.

Backups will be retained for 168 hours (about 7.0 days)

## File Job Considerations

When creating a new File Job, you must consider the following:

- **Schedule Name** - The name for the file replication job as it appears through the UMC.
- **Enabled** - Whether or not the job is enabled, which determines whether or not it will run.
- **Relative Offsite Priority** - Set an integer priority level for the offsite replication. The larger the number, the higher priority of the offsite replication job. If unbundled offsites are enabled, this setting is ignored. This setting is only applied when bundled offsites are enabled.
- **Backup schedule type**- Determine the frequency of the replication schedule. You can select from the following options:
  - On Demand
  - Hourly
  - Daily
  - Weekly
  - Monthly
  - Yearly

Because files can be restored from a system image, file backup jobs are not needed for devices protected by an image job. However, the retention period for image jobs is typically short, so add a file job for data you want to save for a longer period.

**Figure 116** - File Backup Job

domcomputer11 - backup schedule

Create a schedule for your backup job. Select a backup schedule type and complete the corresponding details. An explanation of your schedule configuration is given in the summary below.

Schedule name:

Enabled: ☒ (If disabled, the schedule will not be run but data will be retained indefinitely.)

Relative Offsite Priority:  (Enter any integer to raise this schedule's offsite priority relative to others. Larger value means higher priority.)

Backup schedule type:

---

**The following directories/files will be saved on the Axcient appliance:**

**The following directories/files will be saved on the Axcient appliance and Offsite Storage:**

C:

**The following directories/files will be explicitly excluded:**

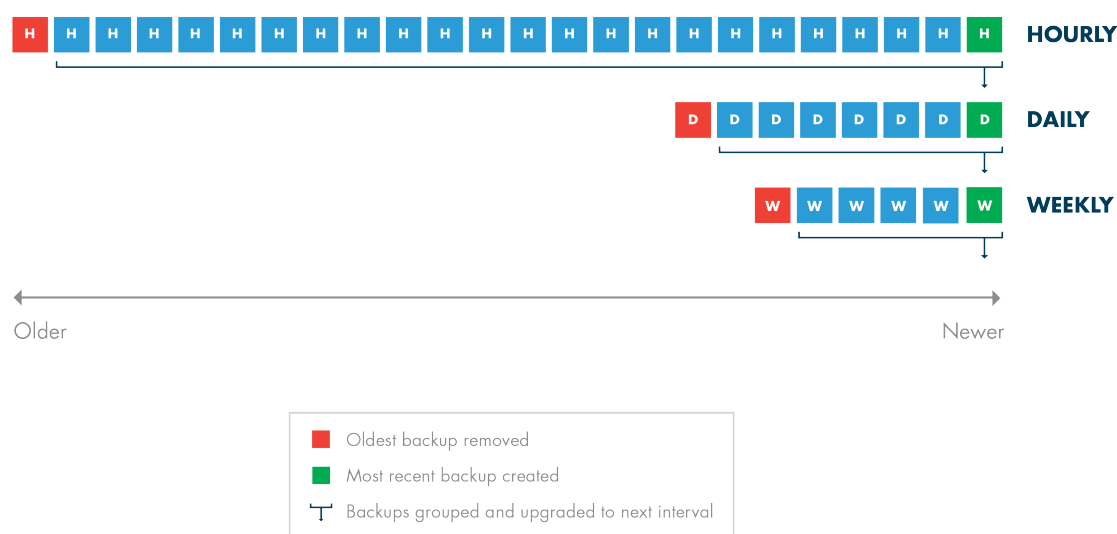
---

## Additional Job Considerations

### Fixed Retention vs. Graduated Retention

A factor for image and file backup jobs is whether to retain backup versions for a set period of time or use graduated retention to retain backup versions for long periods. (Mailbox jobs can only use fixed retention.) Fixed retention is fine for short to medium durations, but consider graduated retention if you want to keep records for an extended period. The figure below illustrates how graduated retention works. A backup version is retained for a period of time and then is either discarded or promoted to the next higher type, for example from hourly to daily, based on a sliding schedule. Older versions are retained indefinitely but the time interval between versions grows as they are promoted to higher types. Note that the job size will continue to grow until each applicable type is filled (defaults: 48 hourly + 14 daily + 5 weekly + 12 monthly = 79 versions). You can use fixed retention for some jobs and graduated retention for others depending on your needs. See the [Configure Graduated Retention Defaults](#) section for a detailed description of graduated retention.

**Figure 117** - Graduated Retention Time Line



## Data Exclusions

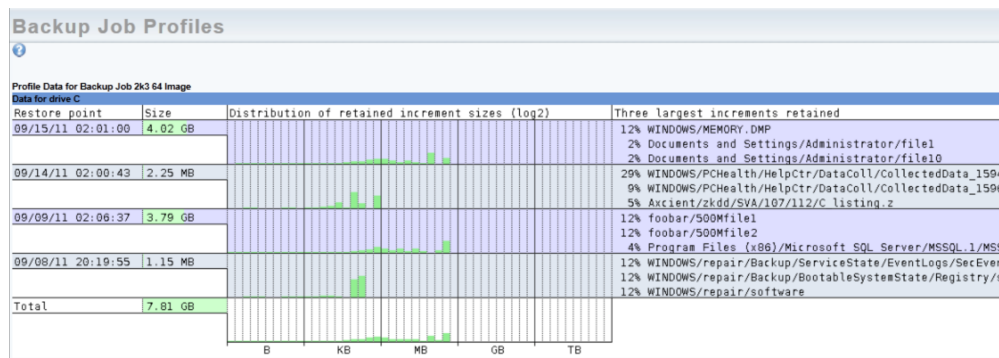
You might choose to exclude some data from an image or file backup job if (but only if) that data is not needed (see the [Modify Backup Job](#) section). This can substantially reduce the size of a backup job.

- **Exclude disk** - You might exclude a disk that is dedicated to temporary or log files that do not need to be backed up. Also, exclude external USB drives because the drive number is part of the identification, and when an external drive is unplugged and then plugged in again, the Axcient appliance will not find it if it is assigned a new letter. In addition, the bare metal restore feature reserves the X and Z drive labels, so BMR will not work with any X or Z drives; such drives should be renamed or excluded if BMR protection is needed.
- **Exclude files** - A more common scenario is excluding certain folders within a drive that are not needed, such as a directory for temporary files.

## Analyze Job Profile

When a backup job has been running for some time and the size seems too large (or small), you can analyze that job in more detail. You can run a profile report that displays detailed information about each version in the job, which allows you to analyze whether any files should be excluded to reclaim space. See the “[Backup Job Profile Report](#)” section for more information.

Figure 118 - Job Profile Report

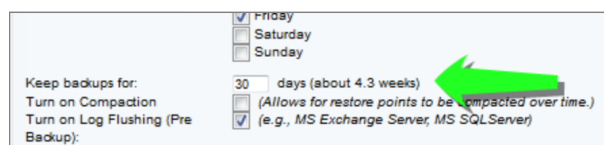


## Reduce Retention

If it becomes necessary to reclaim space on the appliance, there are several ways to reduce backup job size. Two have already been discussed, proactively excluding data from the job and running a job profile to identify suspect files that can also be excluded. Another method is to reduce the retention period. There are three ways to reduce retention:

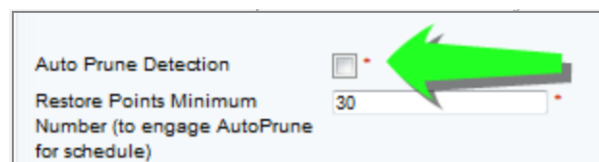
- **Manually reduce retention** - You can manually reduce the retention period for one or more jobs. For example, changing the Keep backups for value from 30 to 15 days will remove half the retained versions going forward (see the [Modify Backup Job](#) section).

Figure 119 - Manually Reduce Retention



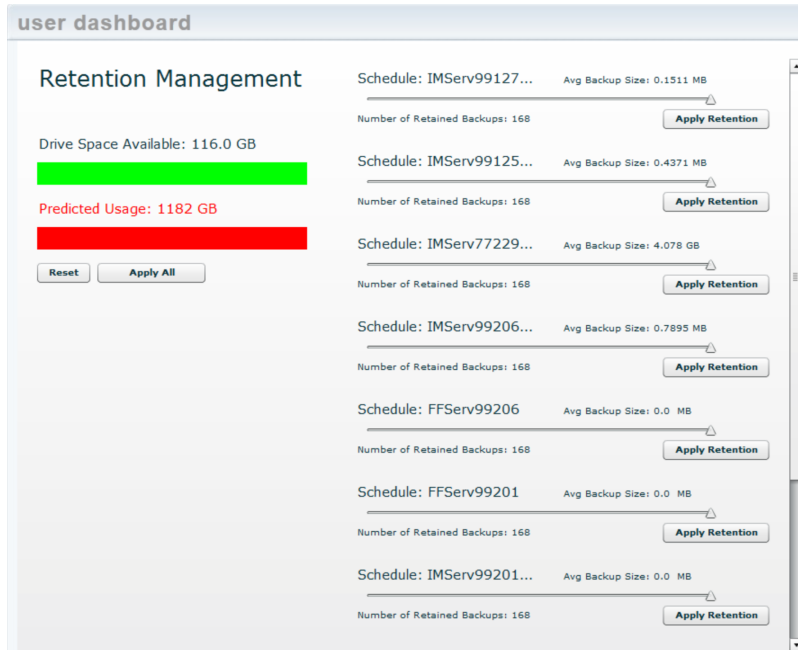
- **Auto prune retention** - You can enable auto pruning, which checks for free space and automatically deletes the oldest backups if space is inadequate. See the [Use Configuration Tools](#) section for more information.

Figure 120 - Auto Prune Detection



- **Set retention management** - The UMC dashboard includes a retention management link that opens a page from which you can quickly change the retention setting for your largest jobs. See the [Reduce Backup Job Size](#) section for more information.

**Figure 121** - Retention Management





## Initial Backup Strategy

The time it takes to run a backup job is directly related to the available network bandwidth, and backup jobs compete with other network traffic. If unchecked, the Axcient appliance will use all available bandwidth when running a backup job. You can adjust the amount of bandwidth the Axcient appliance can use through three parameters, two that control the upload and download rates on the internal network and one that controls the upload rate to the Internet. See the [Set Bandwidth Usage \(Quality of Service\)](#) section for more information.

The initial run for each backup job can be lengthy because all the data must be copied. (Subsequent runs only copy new and changed data.) When you add a device, it is common to create an image job and/or large file. The initial device backup could take days depending on the amount of data to save and the speed of the network.

Consider the following in your initial backup planning:

1. **Onsite Backups (internal network)** - Bandwidth throttling is on continuously and set at 1 Gbit/second for both the internal upload and download rates by default.
  - a. If you create an image job, do not set the internal throttling rates below 1 Gbit/second. Image jobs require a minimum of 1 Gbit/second for the internal download and upload rates. (Image jobs will run at lower rates, but the performance is quite slow.)
  - b. If you do not have an image job and are concerned that the 1 Gbit/second rate might adversely affect normal internal network traffic, restrict the rate during peak business hours. If normal Monday-Friday business hours apply, consider restricting the bandwidth to something less than 1 Gb/second during the week such as 100 Mbit/second (or if you have a slow network perhaps half the available bandwidth).
  - c. Turn off bandwidth throttling during the first weekend (or first non-business days) and set the backup jobs to start that Friday evening, so the initial backup can run without throttling from Friday night through Monday morning. Also, determine the slow hours for your business (typically late evening through early morning), and consider turning off throttling during those hours to provide time for backups that does not impact normal business.
2. **Offsite Backups (Internet)** - Offsite backup is limited by your Internet connection. Bandwidth throttling is on continuously and set at 1 Gbit/second for external upload (Internet) by default.
  - a. Internet connections are typically much slower than the corporate network. If you have a slow Internet connection, consider resetting the external upload rate to an appropriate figure (perhaps half the available bandwidth) during business hours.
  - b. All offsite backup jobs are placed in a queue and run sequentially (some parallel processing) at a set time each day (see the [Schedule Cloud Backup Job](#) section). Set the start time to minimize the impact on other business traffic through the Internet. This typically means setting the start to a time after the close of regular business.
  - c. Determine the slow hours for your business (typically late evening through early morning), and consider turning off external throttling during those hours. Typically, the start of this period would coincide with the offsite job start time set in *step b*.

- d. Determine the amount of data to be backed up offsite. If the amount of data to transfer will take more than 14 days to transfer through your Internet connection (see following calculation), call Axcient technical support and request a direct attach storage (DAS) transfer. A DAS device is connected directly to the Axcient appliance, the data is copied to the DAS device, and then the DAS device is shipped to an Axcient data center. See the Axcient [DAS Transfer Guide](#) for more information about a DAS transfer.

Offsite upload time can be calculated as follows:

1. Determine the actual upload speed of the Internet connection in Mbps. One way to do this is to perform a Web search on “connection speed test,” which will return a number of convenient online tools for measuring the Internet upload speed. Use the smaller of upload speed or QoS external upload rate in the following calculation.
2. Determine the amount of data in GBs to be uploaded. For an initial backup where all jobs are to be backed up off site, this is the total amount of data on the appliance.
3. Calculate the upload time as follows:

$$Time = ((Data * 1024 * 8) / Speed) / 86400$$

where *Time* is in days, *Data* is in GBs, and *Speed* is the upload speed in Mbps.

## Laptop Backup Strategy

Axcient requires that a device be connected to the network in order to back up its data. However, laptop computers are often not connected to the network. If you back up laptop computers that are seldom connected to the network, consider using one or both of the following backup strategies:

- **Set Backup on Connect Feature** - When creating a backup job for a laptop device (see the [Back Up Files](#) section), check the Backup on connect box, which causes the Axcient appliance to monitor offline laptops and immediately begin a backup as soon as a laptop connects if that laptop missed the last scheduled backup run.

On a Windows laptop, a pop-up window appears when the backup begins notifying the user that a backup is in progress and cautioning the user not to disconnect until the backup is complete. (By default, no such message appears on non-Windows laptops.)

- To implement a pop-up window message for Linux or Mac OS X laptops using the **xedit** application to display the message, add the following *message* command line to the *smb.conf* file  
`message command = csh -c 'xedit %s;rm %s' &`  
 The *%s* argument resolves to the file name containing the message.

- **Create a UMC account for each laptop user** - Add laptop users as UMC users with permission to back up their respective laptops. The users (or you) can then create an on-demand backup job that they can execute whenever they log into the UMC, which gives them control to back up their data whenever it is convenient for them. This is recommended only if other (automatic) options are infeasible, because it requires that you train users on how to create a backup job and leaves the backup responsibility to the users. When using this strategy, write a procedure that describes precisely how to create and execute the on-demand job, and give that procedure to each user for reference. To implement this strategy:
  - a. Add the laptop owner as a new user (see the [Add a User](#) section) with the following permissions: **Create a Backup, Restore from a Backup, UMC User**. (Grant additional permissions as desired.)
  - b. Add the laptop as a device and set the **Additional user assigned** field to the new user (see the [Add a Device](#) section).

## Appliance Configuration Guidelines

The Axcient appliance can be configured in a number of ways. This section describes some of those options.

- [System Settings](#)
- [Third-Party Support](#)
- [Remote Hardware Maintenance](#)

## System Settings

The Axcient appliance comes with default settings that should work in most situations, but some features must be enabled and others should be configured for optimal performance. The following (and most) appliance settings are configured through the UMC system tab.

## Quality of Service

The Quality of Service (QoS) settings determine when and how much bandwidth throttling to enforce. If QoS is turned off completely—that is a value of zero in a field—the Axcient appliance will use all available bandwidth as needed. This is usually a good strategy during off hours, which is why the default values disable throttling during non-work hours.

If throttling during business hours is needed to reduce contention, remember that image backup jobs are processing intensive, so you should not reduce the internal upload or download rate below the 1000 Mbps default value if you have image jobs. Without image jobs, reducing these values might not adversely affect performance, but monitor backup job speed after adjusting the value to assess the impact.

The external upload rate sets Internet bandwidth throttling. Contention for Internet bandwidth during business hours is common, so reducing the Axcient appliance rate might be appropriate. However, this will limit the speed of offsite backups during those hours, so monitor whether the offsite backup speed is acceptable after reducing this value.

See the [Set Bandwidth Usage \(Quality of Service\)](#) section for more information.

Figure 122 - Quality of Service Setting

## Quality of Service

Settings for network-bandwidth control.

**Maximum bandwidth allowed: 1000Mb/s**  
**Enter 0 to disable bandwidth control.**

External service upload rate limit business hours (Mbps):

External service upload rate limit non-business hours (Mbps):

Internal service download rate limit business hours (Mbps):

Internal service download rate limit non-business hours (Mbps):

Internal service upload rate limit business hours (Mbps):

Internal service upload rate limit non-business hours (Mbps):

### Business Hours

Select the start/stop time of your business hours.  
 Note: If you leave the selection blank, your non business hour bandwidth setting listed above will be used.

**Sun** Start:  :  Stop:  :

**Mon** Start:  :  Stop:  :

**Tue** Start:  :  Stop:  :

**Wed** Start:  :  Stop:  :

**Thu** Start:  :  Stop:  :

**Fri** Start:  :  Stop:  :

**Sat** Start:  :  Stop:  :

## Offsite Backup

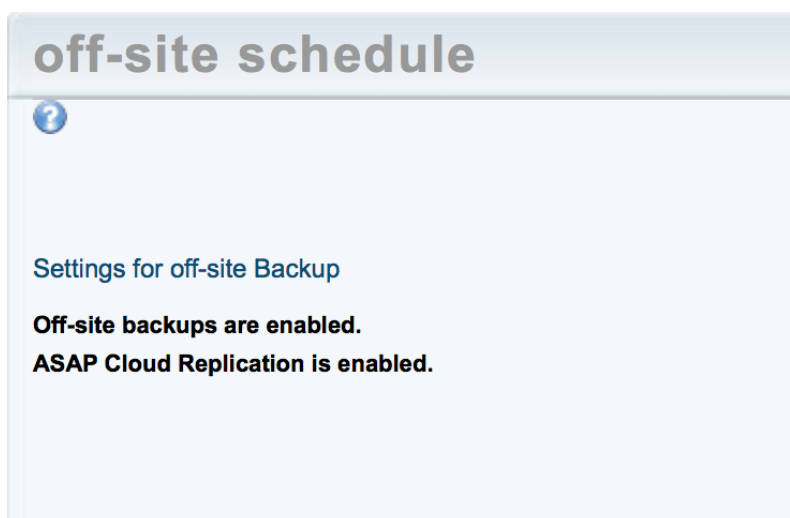
When creating a backup job, you specify what data should be saved offsite (as well as onsite). When a backup job runs, the offsite data is put in a queue in an offsite staging area in the Axcient appliance, but the data is not immediately transmitted to an Axcient data center. There are two methods of performing an offsite backup:

### Unbundled Offsites

In the Axcient Web Application, you can enable the Unbundled Offsites feature for Cloud backups. This makes it so that individual device backups will automatically begin replicating to the Axcient Cloud as soon as the local backup for the device completes. Rather than the entire Axcient appliance being replicated at one time, this allows individual devices to be backed up to the Axcient Cloud independently of one another and the Axcient appliance. This results in overall less network demand when replicating data to the Cloud.

When enabled in the Web Application, you will see the following page in the *Offsite Schedule* page. To enable or disable the Unbundled Offsites feature, please refer to the [Axcient Web Application User Guide](#).

Figure 123 - Unbundled Offsite Backup Setting

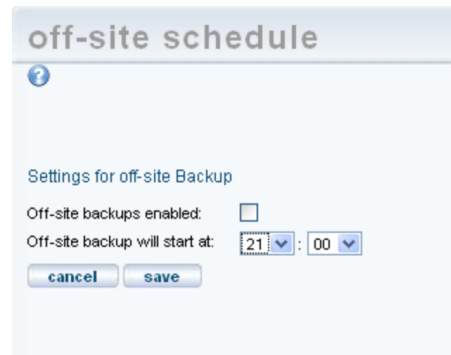


### Manual Offsite Backup

Transmission to the Axcient data center begins at a set time, and all the pending offsite backup jobs are transmitted in order (some parallel processing). Transmission continues until all queued jobs have been sent.

Offsite backups are not scheduled to run by default. You must first activate offsite backups and set the offsite backup start time. See the [Schedule Offsite Backup Job](#) section for more information.

**Figure 124** - Manual Offsite Backup Settings



off-site schedule

Settings for off-site Backup

Off-site backups enabled: ☐

Off-site backup will start at: 21:00

[cancel](#) [save](#)

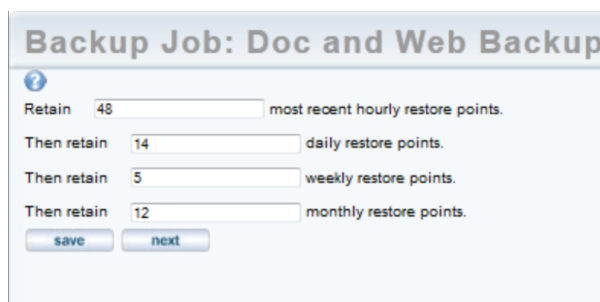


## Graduated Retention

If you use graduated retention for some or all jobs, review the settings for appropriateness. The settings determine the time intervals before backup versions are either discarded or promoted to the next longer type. The default values are two days for hourly (versions), two weeks for daily, a month for weekly, and a year for monthly. If any of these defaults are not desirable, change the value to the desired duration. See the [Configure Graduated Retention Defaults](#) section for more information.

You have the option to set alternate graduated retention values for a specific job. See the [Set Local Graduated Retention Rules](#) section for more information.

**Figure 125** - Local Gradual Retention Rules



The screenshot shows a configuration window titled "Backup Job: Doc and Web Backup". It contains a list of retention rules for different backup types. The first rule is "Retain 48 most recent hourly restore points." followed by "Then retain 14 daily restore points.", "Then retain 5 weekly restore points.", and "Then retain 12 monthly restore points." At the bottom of the window are two buttons: "save" and "next".

Retention Rule	Value
Retain	48
most recent hourly restore points.	
Then retain	14
daily restore points.	
Then retain	5
weekly restore points.	
Then retain	12
monthly restore points.	

## Ports

As noted in the [Installation Guidelines](#) section, the Axcient appliance uses several ports that must be open. The installation guidelines list common ports that are used, but it is not a complete list. See the [Appliance Specifications](#) section for a complete description of port usage.

## Third-Party Support

Axcient provides features to support some third-party tools.

### SNMP

Axcient supports SNMP and provides a custom Axcient MIB. To use SNMP enter the appropriate information and download the Axcient MIB from the link. See the [Configure SNMP](#) section for more information.

Figure 126 - SNMP Settings

Schedule Name	Index
OffSite Backup	1
Alert Digest	2
Usage History	3
Image2003	4
Image2008r2	5

## Professional Services Automation Tools

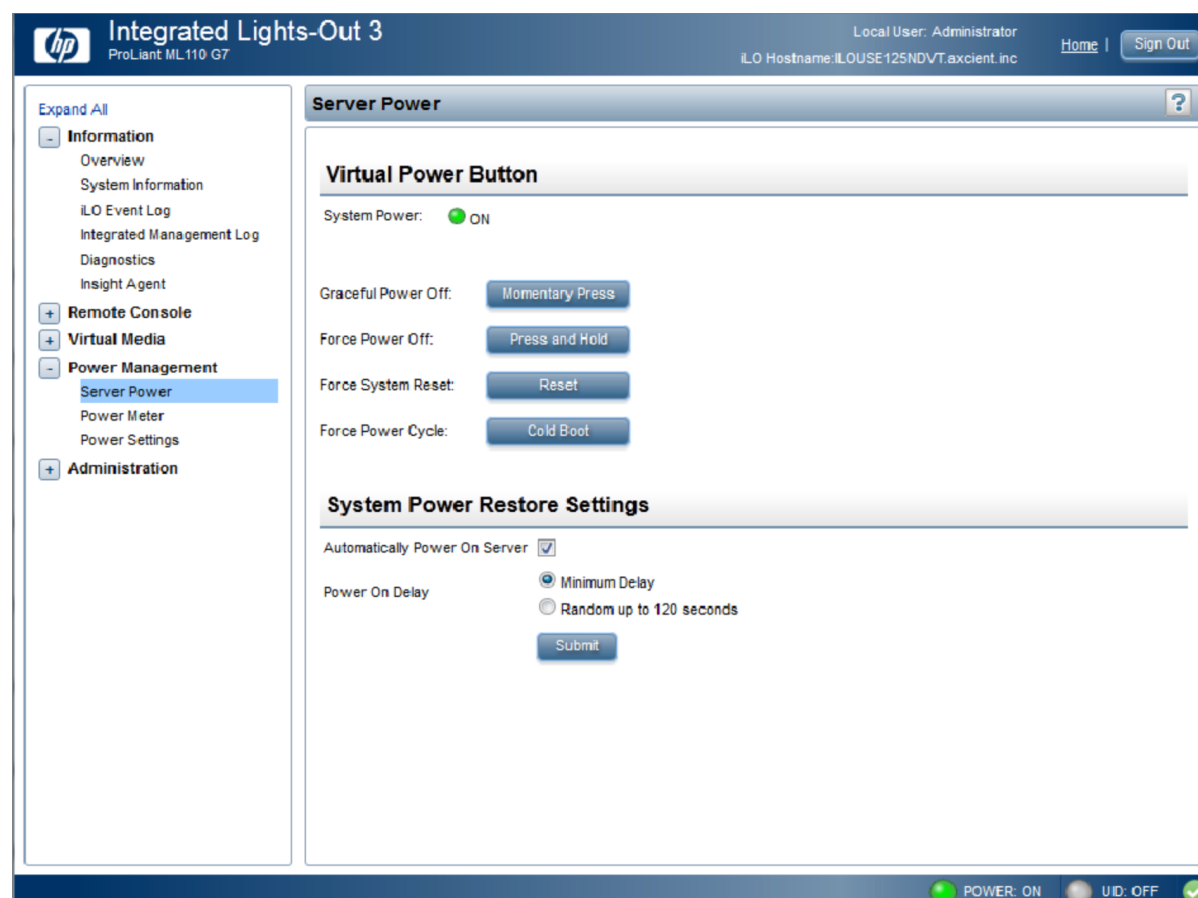
Axcient supports selected professional services automation (PSA) tools. If you use either ConnectWise or Autotask, you can integrate those PSA tools with the Axcient alert mechanism to generate tickets in the PSA tool. Axcient provides a custom configuration page for each supported PSA, but the integration also requires some configuration on the PSA side. See the [Configure PSA Settings](#) section for more information.

## Remote Hardware Maintenance

An integrated lights out (ILO) feature is built into the hardware that allows you to remotely reboot, power off, or power on an Axcient appliance. This capability can be valuable when managing an Axcient appliance from a remote site, because it is not feasible to physically check the appliance if there is a hardware problem.

The appliance firmware must be configured to enable the ILO functionality. See the “iLO Configuration and Use” appendix for this procedure

Figure 127 - iLO User Interface



## Backup Fails Because of Windows VSS Problem

On Windows-based devices, the Axcient appliance uses the Microsoft Volume Shadow Service (VSS) for image backup jobs (always) and file backup jobs (when *Open File Manager* is set). The table below lists several potential issues when using VSS.

VSS Problems

Problem	Solution
Another backup solution is preventing the Axcient appliance from properly using VSS.	If another backup solution is installed on the protected server, adjust your backup schedule appropriately so that the Axcient backup job schedule and the other third-party backup schedule do not overlap.
If an error message refers to a disabled VSS writer, register that writer as described in the following procedure.	If an error message refers to a disabled VSS writer, register that writer as described in the following procedure.
VSS is not enabled for this device.	Axcient provides a VSS configuration script that you can run on a device. This script enables VSS, registers application writers, and identifies potential issues. See the <a href="#">VSS Configuration</a> appendix for instructions on how to download and use this script.
VSS is not enabled for this device.	Allocate adequate space as described in the procedure at the end of this section.

Before executing a job run, the Axcient appliance checks whether the VSS writer is enabled for certain applications on the protected device. If one of these applications is present and the VSS writer is not registered correctly, the image job aborts and a failure message appears in the event log. The following applications are checked:

- Microsoft Exchange
- Microsoft SQL
- Microsoft SharePoint
- Microsoft Active Domain (NTDS)

In most supported system configurations the VSS writers are enabled by default, but in Windows SBS 2003 they are disabled by default. If the device is running Windows SBS 2003 or a VSS writer failed to register, use the following procedures to manually register the VSS writers for the applications in question.

## Exchange Server VSS Writer

1. Run *regedit*.
2. Locate the following key:  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem`
3. Double-click the **Disable Exchange Writer** value.
4. Change the value to 0 (from 1).
5. Quit *regedit*.
6. Do one of the following:
  - Stop and then restart the Exchange Information Store service.
  - Reboot the Windows server.

## SQL Server VSS Writer

1. Run *services.msc*. This opens the service Microsoft Management Console (MMC).
2. Locate the SQL Server VSS Writer service.
3. Right-click and select the **Properties** menu item.
4. Set the Startup type to *Automatic* (if it is not already set to automatic).
5. Start the service (if it is not already started).

## SharePoint VSS Writer

1. Run *services.msc*. This opens the service Microsoft Management Console (MMC).
2. Locate the Windows SharePoint Services VSS Writer (for SharePoint 2003 or 2007) or SharePoint 2010 VSS Writer service.
3. Right-click and select the **Properties** menu item.
4. Set the Startup type to *Automatic* (if it is not already set to automatic).
5. Start the service (if it is not already started).
6. Register SharePoint from a command window by (1) changing to the directory  
`%COMMONPROGRAMFILES%\Microsoft shared\web server extensions\<#>\bin`, where <#> is 12, 14, or other (higher) number, and (2) entering the following command:  
`STSADM -o registerwsswriter`

## Active Domain (NTDS) VSS Writer

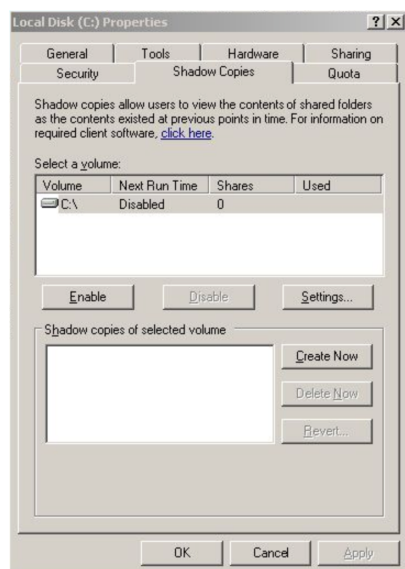
The VSS writer is a built-in function in Windows 2003 and later versions. There is no manual way to enable (or disable) it.

## Allocate Shadow Copy Space Procedure

To allocate additional shadow copy space:

1. Open a Windows Explorer window, select the target drive, and then right click and select Properties from the menu.
2. Select the Shadow Copies (Windows 2003 Server) or Configure Shadow Copies (Windows 2008 Server) tab, select the target volume, and click the **Settings** button.

**Figure 128** - Shadow Copies Tab

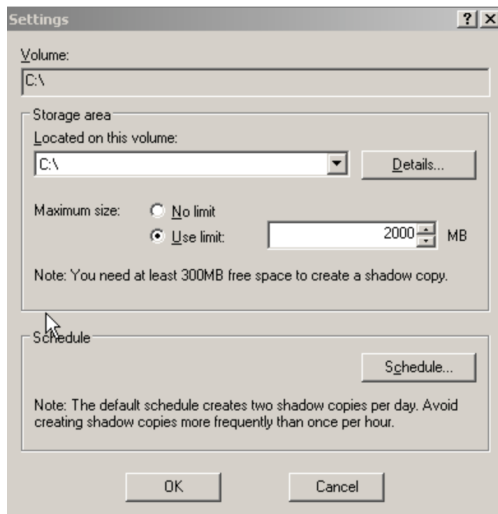


In the *Maximum Size* field (under Storage Area), do one of the following and then click **OK** to close the window:

- Click **No Limit** (recommended).

Click **Use Limit** and enter the size. A rule of thumb is to set this at 25% of the size of the disk. (The example is 2000 MB, which is appropriate for an 80 GB disk.)

In the *Properties* window, click **OK** to save and close.

*Figure 129 - Settings Window*

## Backup Fails Because of Permission Problem

A permission problem can cause a job run to fail. The table below lists potential permission problems.

### Permission Problem

Problem	Solution
The backup job does not have permission to back up some or all of the target files because either the user credentials or file permissions do not allow the backup to run successfully.	If the user credentials or permissions are incorrect, change them accordingly. If specific files deny access to the user, either change the permissions on those files to allow access or exclude those files from the backup job. Consider setting proper permissions at the highest level possible and then working your way down to the subdirectories to ensure they inherit the correct permissions.
Windows file redirection is enabled, and the backup job does not have permission to back up the redirected files.	The default permission for Windows folder redirection is the grant the user exclusive rights, which means an administrator does not have read access to the redirected folders to back them up. The solution is to change the default permissions. See <a href="#">Backup Fails Because of Windows Redirection</a> section for more information.

**Figure 130** - Permission Denied Error Message

Type	Date	Action	User	Details
BACKUP_WARNING	05/21/2012 - 11:44:14 AM	Backup Completed with WARNING: 'Doc-Training Backup' on axcient-jmue2 with warning: Warning: Unable to open path "c\$/Users/gmasters/Documents/Courseware Button Sets/Blue-Buttons/___MACOSX/._blue-forward-off.png". Cause: Permission denied Error: Unable to copy "c\$/Users/gmasters/Documents/Courseware Button Sets/Blue-Buttons/___MACOSX/._blue-forward-off.png". Skipping.. Cause: Permission denied Warning: Unable to open path "c\$/Users/gmasters/Documents/Courseware Button Sets/Blue-Buttons/___MACOSX/._blue-forward-on.png". Cause: Permission denied	UBS	<a href="#">View</a>

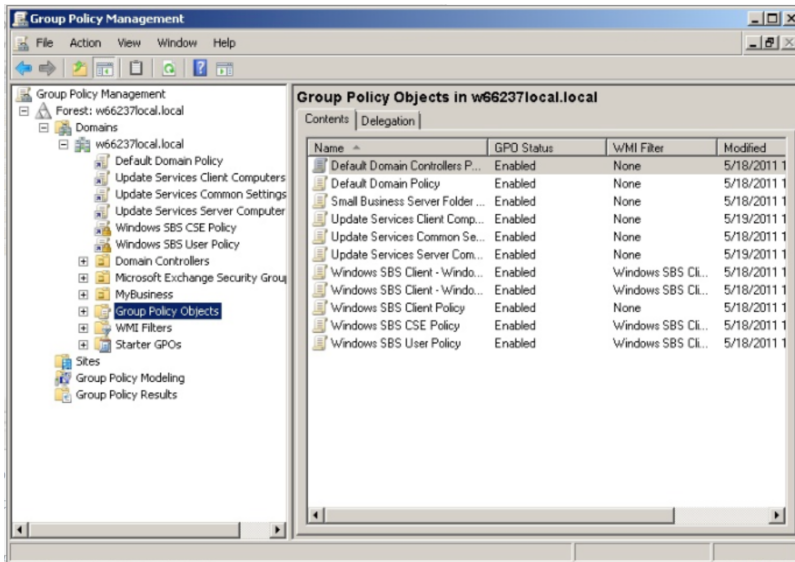


## Backup Fails Because of Windows Redirection

If you employ Windows redirection, the redirected files may not be backed up. This is because the default permission for Windows folder redirection is to grant the user exclusive rights, which means an administrator does not have read access to the redirected folders to back them up. To set the permissions so Axcient can back up the folders:

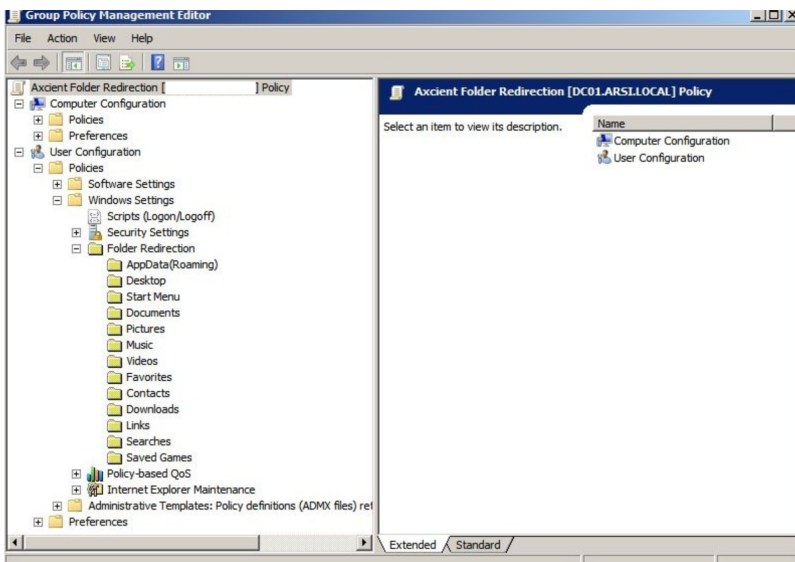
1. Create a share folder as the root of all redirected folders on the server hosting the redirected folders. Set the permissions as follows:
  - a. *Share Permissions:*
    - Everyone - Full Control
    - Administrators - Full Control
    - System - Full Control
  - b. *NTFS Permissions* (In all cases except for general note #1)
    - Everyone - Create Folder/Append Data (This Folder Only)
    - Everyone - List Folder/Read Data (This Folder Only)
    - Everyone - Read Attributes (This Folder Only)
    - Everyone Traverse Folder/Execute File (This Folder Only)
    - CREATOR OWNER - Full Control (Subfolder and Files Only)
    - System - Full Control (This Folder, Subfolder and Files)
    - Domain Admins - Full Control (This Folder, Subfolder and Files)
2. Start the Group Policy Manager (*Start > Control Panel > Administration Tools > Group Policy Manager*).
3. Create a new Group Policy Object (GPO) called *Axcient Folder Redirection*:
  - a. Open the tree to the target domain.
  - b. Right-click on **Group Policy Objects** and select **New**.
  - c. Enter the name *Axcient Folder Redirection* and click **OK**.

Figure 131 - Folder Redirection - Group Policy Manager



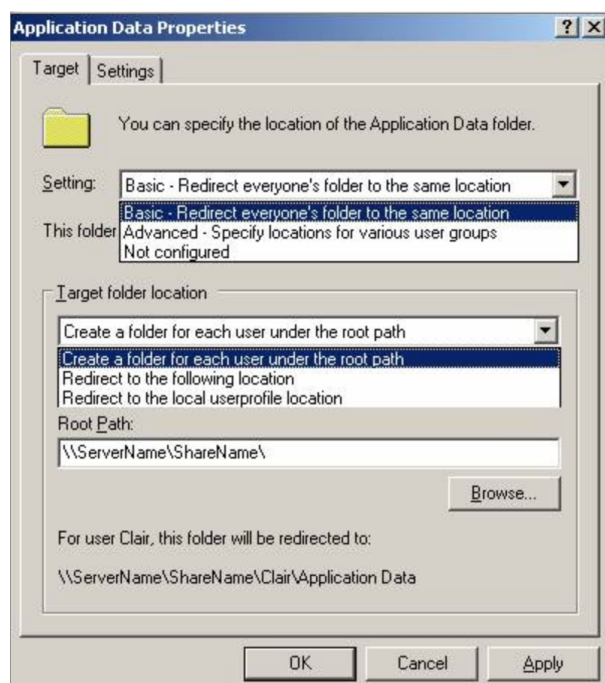
- Expand the *Group Policy Objects* folder, right-click on the newly created *Axcient Folder Redirection* entry, and select **Edit**.
- The *Group Policy Management Editor* window appears, and *Axcient Folder Redirection* appears at the top of the tree. Expand the tree to *User Configuration > Policies > Windows Settings > Folder Redirection*.

Figure 132 - Folder Redirection - Group Policy Management Editor



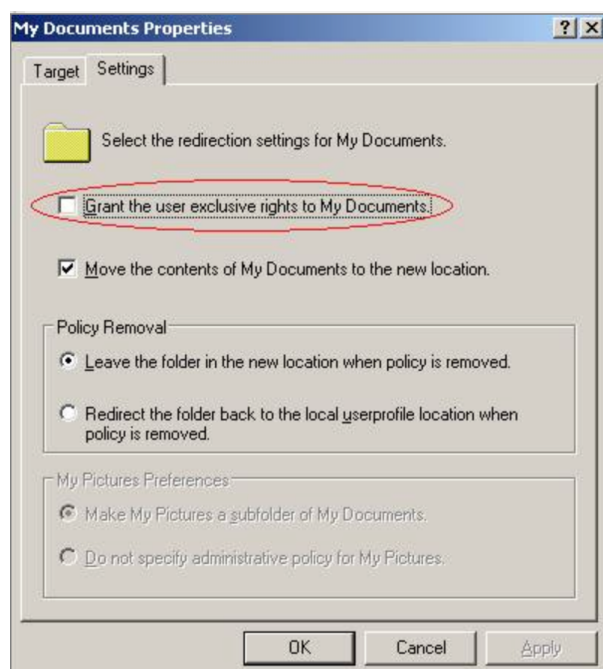
6. Enable folder redirection for a desired target (such as *Desktop* or *Documents*):
  - a. Select the target, right-click, and select **Properties** to display the properties window for that target.
  - b. Click the **Target** tab. In the *Setting* field, select **Basic - Redirect everyone's folder to the same location**.
  - c. In the Root Path field, enter `\\server_name\share_name\` where *server\_name* is the name of the server and *share\_name* is the name of the share folder you created in *step 1*.

**Figure 133** - Folder Redirection - Properties Target Tab



7.
  - a. Click the **Settings** tab. Uncheck the box next to *Grant the user exclusive rights to My Documents*.
  - b. When both the *Target* and *Settings* tab fields are correct, click the **OK** button.

Figure 134 - Folder Redirection - Properties Settings Tab



8. Repeat *step 6* for each desired target (Desktop, Documents, Pictures, and so on).
9. When all settings are configured, link the GPO to the appropriate target (the root level domain, child domain, or any organizational unit):
  - a. For the root level domain, return to the Group Policy Management window and right-click on the domain. (Adjust accordingly for other targets.)
  - b. Select **Link an Existing GPO**.
  - c. A link window appears. Select the newly created Folder Redirection GPO, and click **OK**.
10. To test that the configuration is correct, reboot the client machine and then log in as a user. If folder redirection is successful, the follow event appears in the application log:
 

*Event ID: 1-1*

*User: <name>*

*Computer: <name>*

*Description:*

*Failed to perform redirection of folder <name>.*

*The folder is configured to be redirected to <path>.*

*The following error occurred: Access is denied.*

## SBS 2008 and 2011

This section applies to devices running Windows Small Business Server (SBS) 2008 or 2011. The Console for SBS 2008 and 2011 (a) does not expose the capability to turn off the “exclusive” bit in the folder redirection GPO, and (b) may overwrite an existing folder redirection GPO named “Small Business Server Folder Redirection Policy.” Therefore, the following is recommended:

1. If you need to turn off the exclusive bit for folder redirection GPO, do not invoke the SBS Console. Instead, create a new folder redirection GPO, and set its scope properly. (Link it to the proper OU and optionally filter by the proper user group.) In addition, use the Group Policy Management directly and turn off the “exclusive” bit in the folder redirection GPO.
2. Files and folders created before the “exclusive” bit in folder redirection GPO is turned off retain the original exclusive ACL, which prevents Axcient from backing them up. To fix this:
  - a. Download `psexec.exe` from the following URL:  
<http://technet.microsoft.com/en-us/sysinternals/bb897553>
  - b. Copy `psexec.exe` to the file server hosting the redirected folder.
  - c. Running under “Local System” credentials, enter the following command:  
`psexec -s -i -d cmd.exe`
  - d. In the newly created `cmd.exe` running as local system, grant the proper ACL at the root of the redirected folder recursively to `BUILTIN\Administrators`:  
`icacls C:\users\FolderRedirections /t /c /grant "BUILTIN\Administrators":(OI)(CI)(F)`
  - e. Repeat *Step d* for any additional redirected folder root levels.

Files and folders created after *Step 2* (and after the “exclusive” bit in folder redirection GPO is turned off) should have proper permissions and require no additional steps.

Group policy propagation from the DC to client machines can take time, and may require a user to login multiple times before the folder redirection GPO takes effect. To verify the new GPO policy is in effect:

Log into a client device as administrator, and run the following command:

```
gpupdate /force
```

2. Reboot the device.

Login as a regular user and go to a redirected folder.

Enter the following command:

```
gpreult /scope user /v
```

Check the section under *Folder Redirection*. The first time folder redirection takes effect, a system event with event ID 501 source “Folder Redirection” should appear.

Repeat procedure for each client device.

## Backup Fails Because of Mount Problem

A mount problem can cause a job run to fail. The table below lists potential mount problems.

Mount Error Message	
Problem	Solution
The device could not be mounted because there was a network problem (down or device unreadable), the mount was deleted, the mount password changed, or the device was too busy (100% CPU usage) to connect.	Check each of the conditions identified in the problem explanation and correct as needed. If the mount password changed, log into the UMC and update the password for that device.

**Figure 135** - Mount Error Message

Type	Date	Action	User	Details
BACKUP_WARNING	05/10/2012 - 3:37:28 PM	Backup Completed with WARNING: 'FFServ99201' on 192.168.99.201 with warning: mount(//192.168.99.201/c\$): Cannot allocate memory Unable to mount //192.168.99.201/c\$ on remote host.	UBS	<a href="#">View</a>
BACKUP_WARNING	05/10/2012 - 9:41:31 AM	Backup Completed with WARNING: 'FFServ99201' on 192.168.99.201 with warning: Warning: Unable to read remaining contents of directory "c\$/", skipping. Cause: Permission denied copy_file(): open(/uptiva/mounts/32/105/c\$/Axcient/afba/FILE/32/105/ax-complete.log): Permission denied	UBS	<a href="#">View</a>

## Backup Fails Using Samba

On a Linux (or other UNIX) system running an older (pre-3.3.1) version of Samba, backups might fail if some of the backed up files are symbolic links. To work around this limitation, upgrade Samba to 3.3.1 or later, or identify and remove the symbolic links from the directories to be backed up.

## Backup Fails Due to Symbolic Links (Windows 7)

On a Windows 7 system, attempting to backup a directory with symbolic links will cause the backup to fail. To work around this problem, remove symbolic links (or the folders that include them) from the backup job (see the [Modify Backup Job](#) section). Windows 7 automatically adds symbolic links to the *All Users* folder (in *C:\Users*), so if this folder is included in the backup job (which it would be if the disk drive is selected for backup), deselect (set to **Ignore**) the *All Users* folder from the backup job.



## Backup Hangs After Lost Connection

When a network outage occurs that breaks the connection between a protected device and the Axcient appliance while a backup job is in progress, the backup job can hang indefinitely. To resolve this problem, simply cancel and restart the backup job. Restarting the job whenever a network outage occurs is a recommended practice, because it is not always apparent that the job is hanging indefinitely.

When the connection between a device and the Axcient appliance is lost for any reason while a backup job is in progress, the Axcient appliance will go into a loop and retry to connect up to 180 times before giving up. Thus, the backup job run might appear hung, because it could be 45 minutes or more before it gives up and logs a failure event. While in this loop, the *File Count* field for that job in the Running Jobs panel on the dashboard will display “(Retry #)” in front of the current file name as in the following example:

*(Retry #87) Windows/foo/bar.txt*

## Open Files Not Backed Up

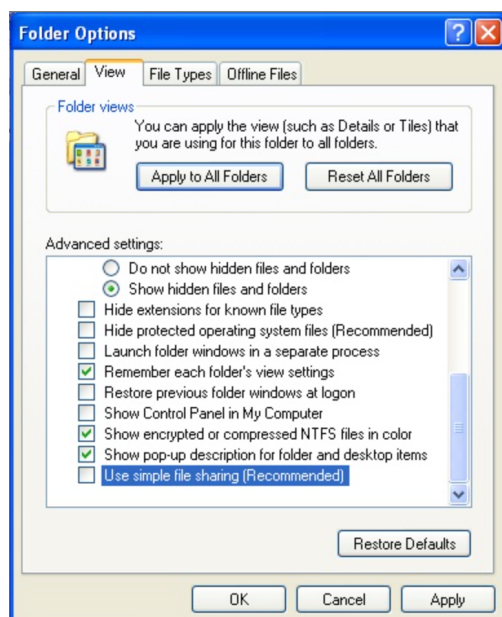
In a file backup job, some files might not be backed up because they were being used (open and locked) at the time the backup job ran. If this is a Windows device, click the “Use Open File Manager” box in the job definition, which invokes VSS so the Axcient appliance can back up any files regardless of whether they are open. For non-Windows devices, remove (set to **Ignore**) the open files from the job definition if this situation persists.

## Files Missing When Creating Backup (XP)

If Simple File Sharing is enabled when creating a backup job for an XP device, no files will appear after selecting the plus sign (+) to display the file tree for a disk. To fix this problem, disable Simple File Sharing as follows:

1. From *My Computer*, select **Tools > Folder Options**.
2. The Folder Options page appears. Select the **View** tab and uncheck (disable) the *Use simple file sharing [Recommended]* box .

**Figure 136** - Folder Options Page



## Cannot Backup Windows Encrypted Files

Windows includes an option to encrypt a file or folder. When this encryption method is used, the Axcient appliance does not have read access. As a result it cannot back up or restore any files and folders that are encrypted using this method. A different encryption method must be used if you want the Axcient appliance to back up encrypted files.

## Cannot Set "On Demand" Job Retention Period

Unlike interval based jobs (hourly, daily, monthly, yearly), on-demand jobs do not have retention periods:

- Only the latest version of a file on-demand job is saved. That version is kept indefinitely until it is deleted or replaced by a new on-demand request.
- All versions of an image on-demand job are saved indefinitely and can be selected for use in a VM or BMR.

## Not All "Active" Backup Jobs Running

You can schedule any number of backup jobs to run at any time, but the Axcient appliance runs a maximum of five backup jobs simultaneously. If more than five are scheduled concurrently, the sixth and subsequent jobs are put in a queue. When a job completes, the next job in the queue starts running. This continues until there are no jobs left in the queue. There are three possible states for an active job:

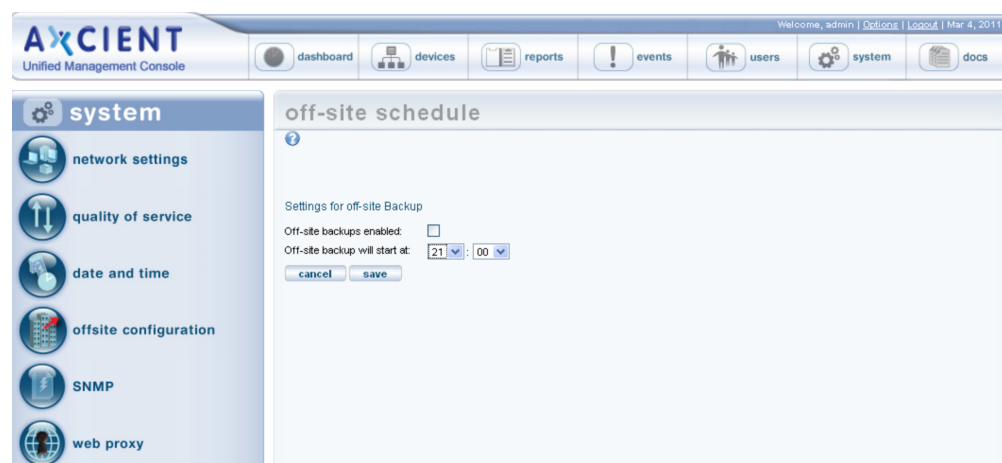
- **Initializing**—Indicates the job is being configured to run.
- **Waiting to run**—Indicates the job was initialized but is waiting in the queue to run.
- **In progress**—Indicates the job is currently running.

## Offsite Backups are Slow

Offsite backup performance can be affected by a number of factors. First, if offsite backup jobs are not running, make sure the **off-site backups enabled box** is checked in the *Offsite Configuration* page under the UMC system tab. This is not enabled by default, so you must check the box before any offsite backups will run.

When an offsite backup is running, check the status in the UMC dashboard. This provides dynamic information about offsite backup progress. See the [Disk Utilization Panel](#) section for more information about monitoring offsite progress.

**Figure 137** - Offsite Backup Enable Box



If progress seems too slow, check your transmission speed. There are two steps:

1. Determine the actual upload speed of your Internet connection and the time it should take to upload the data. See [Initial Backup Strategy](#) section for this procedure.
2. Click the UMC **system** tab and then **network utilities**. The offsite bandwidth check sends a 2, 8, or 32 MB file from the appliance to and through the data center, which tests both raw throughput across the Internet and processing time within the data center for small and large files. See the [Check Network Connections](#) section for more information about running and interpreting this test.

### Offsite Performance Problems

Problem	Solution
Bandwidth throttling is on too high.	Review the QoS settings and assess whether they should be changed. See the <a href="#">Set Bandwidth Usage (Quality of Service)</a> section for more information.
Firewall traffic shaping is on. This is a process where a firewall, router, or IP service provider automatically throttles down throughput when sustained traffic flow is detected, which can be an issue for large offsite backup jobs.	<p>Run the offsite bandwidth check with 2 and 32 MB files:</p> <ul style="list-style-type: none"> <li>• If throughput is comparable for small and large files, then there is no traffic shaping.</li> <li>• If the small file throughput is greater than the large file, then traffic shaping is likely impeding your offsite backup.</li> </ul> <p>Determine where the shaping is occurring (firewall, router, or IP provider) and adjust settings accordingly if traffic shaping is on.</p>
Rolling backup files cause duplicated data backup.	Rolling files, such as log files that repeat each day with a date stamp, are targeted as new files, even though most of the data is repeated in each file. To fix this, reconfigure applications so they do not create rolling files.

Problem	Solution
Moving data among devices causes duplicated data backup.	Any backup job will treat data moved from one device to another as new data and copy all of it. Avoid this practice if possible.
Offsite mailbox and image jobs use duplicated data backup.	While having both a mailbox job and an image backup job is a good protection strategy, backing up both offsite might not be worth the overhead because in the case of a disaster, it is likely the Exchange server would need to be restored as a whole, making the offsite mailbox job redundant for disaster recovery and expensive overhead to back up.
Problem files (dysfunctional or unnecessary) are being copied offsite.	Backing up problem files slows both onsite and offsite backups, but it has a greater influence on offsite backups because of the slower Internet speed. For any offsite job that runs slowly, run the Job Profile report on that job to determine if there are problem files (see <a href="#">Additional Job Considerations</a> section). This allows you to see if some files should be deleted or the retention/pruning settings changed to reclaim space, which should improve offsite backup performance.



## Restoring UNIX Files on Windows Device Fails

If you backed up a device running Linux or another UNIX-based operating system and attempt to restore those files on a Windows device, the restore will fail if one or more files have illegal Windows names. UNIX allows certain characters in file names, such as a quote or colon, that are illegal in Windows file names. Therefore, it is not possible to restore such files on a Windows system. In addition, the entire restore job fails when such a file name is encountered. To work around this limitation:

1. Remove any files with illegal names from the list of files to restore, and then repeat the restore job to the target Windows system.
2. Restore the files with illegal Windows characters to a UNIX system. Rename the files (removing the illegal characters), and then move them to the target Windows system.

Windows rejects file names with any of the following characters:

`| / : * ? " ' < > |`

## Restore Fails Using Samba on MAC OS X

If a restore operation fails for a Mac OS X device running Samba, it might be due to a symbolic link problem. The default Samba configuration on Mac OS X enables symbolic linking in a way that causes a problem for the Axcient appliance.

To correct this problem, open the Samba configuration file (**smb.conf**) and change the **follow symlinks** parameter as follows:

- Default setting:  
*follow symlinks = yes*
- Change to (or add this line if it does not appear in the Samba configuration file):  
*follow symlinks = no*

## Cannot Restore to Target Location

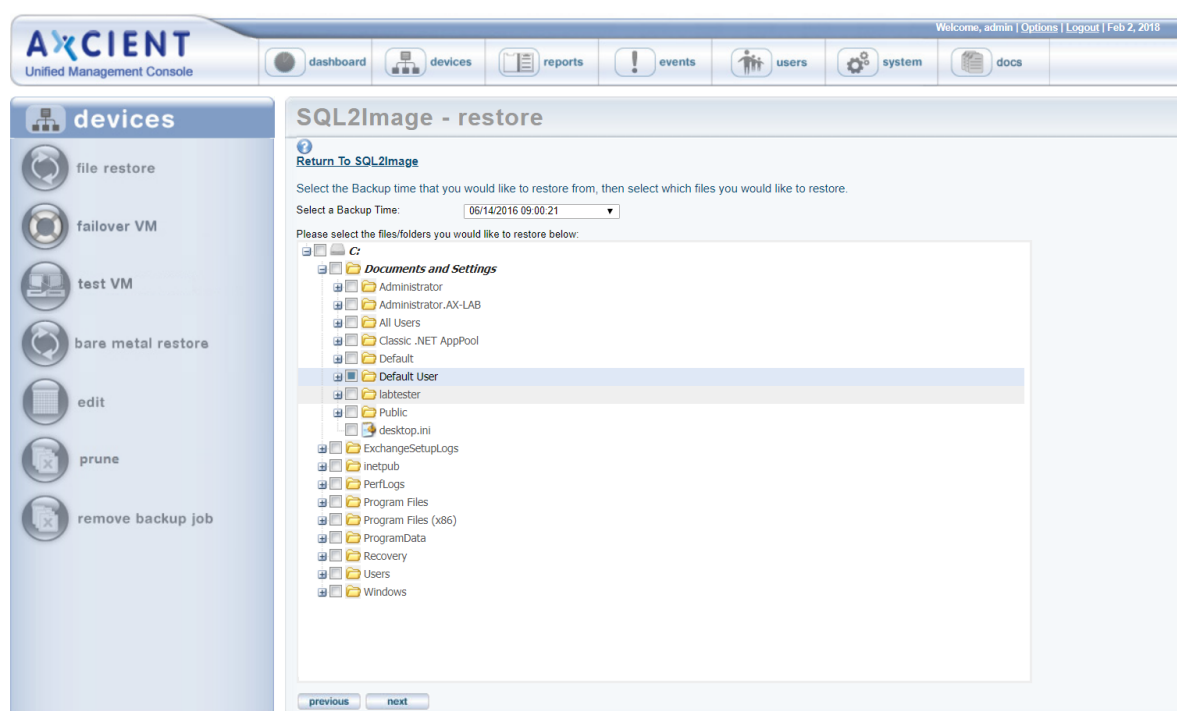
It is possible to choose a target directory to restore files for which the user does not have write permission. In this case, even though you were allowed to select the target directory, the Axcient appliance could not write to that directory, so the restore failed. To avoid this problem, make sure the user has write permission before attempting the restore operation or choose an alternative target location for which the user does have permission.

## Cannot Restore Files (Tree View Does Not Expand)

Normally when restoring files from an image or file backup job, you select the files to restore from a tree view of the device contents. However, there are occasions when clicking on the icon does not open the tree view. This is typically due to one of the following:

- You are using Internet Explorer (IE), and the browser hangs when trying to display the content tree. You can usually solve this problem by either switching to the Firefox browser or run IE in compatibility mode.
- There is a permission problem that prevents the browser from displaying the tree. Check that you have proper (read) permission for content on that device.

**Figure 138** - File Restore Tree View



## Cannot Restore Exchange Mailbox (Account Deleted)

If an administrator deletes an Exchange user or mailbox, that user account and/or mailbox no longer exists. A mailbox backup job includes credential tied to that account, so a restore attempt will fail because the credentials are no longer valid. To work around this limitation and restore the mailbox from a backup job:

1. If the user account was deleted, recreate the user in Active Directory with the same name as the deleted user.
2. Send an e-mail to the user or have that user log into Outlook. This step is necessary to create a new mailbox for that user.
3. Outlook has a set of default folders including Inbox, Drafts, Calendar, Contacts, and Tasks. These are automatically added when the new mailbox is created. If the restore specified the original location, messages from the default folders are not restored to the new default folders. Instead, they are restored to folders titled **folder\_name (restored)** such as **Inbox (restored)**. Optionally, move the messages from the restored folders to the corresponding default folders and then delete the restored folders.

## BMR Fails at Final Boot (Windows 2003)

It is possible after completing the BMR process for a device which runs Windows 2003 that the device fails to boot and instead displays a blue page (BSOD). Windows 2003 is not as sophisticated as Windows 2008 in detecting hardware and loading the appropriate drivers, and under a rare set of circumstances can result in this failed boot problem.

To resolve the problem, boot the device using the original Windows Server 2003 CD, and run the Windows Setup. Windows Setup searches for a previous installation. Select the previous installation, which is the BMR image, and follow the instructions of the Windows Server 2003 CD to complete the installation. (If a previous installation is not found, there might be a hardware problem.) See the documentation that is included with your computer, or contact your computer manufacturer, for more information.

## BMR Fails at Final Boot (Active Directory Server)

When doing a BMR of a system with Active Directory installed, the device might fail to boot and instead display a blue page (BSOD). This problem is due to a permission issue with Active Directory; specifically, the permissions are not set correctly for the `C:\Windows\NTDS` directory. To recover from this problem:

1. Click the **F8** key when the machine is booting to go to the *Advanced Boot Options* page.
2. Select **Directory Services Restore Mode**.
3. Log in using the local Admin credentials.
4. Add full permissions for the local *SYSTEM* account to the `C:\Windows\NTDS` directory.
5. Reboot into normal mode.

You should now be able to log in using domain user credentials.

## Failover VM Pause Shut Down Server

A failover VM should never run while the original server is still online, because both use the same IP address causing a collision of IP addresses on the network. (This is also true of a test VM if you enter the IP address of an online device.) The Axcient appliance checks for this when you attempt to start a failover VM, and it prevents the VM from starting if the original server is still online. However, after the VM starts, it is possible to bring the original server online. This could lead to several problems. One can occur if you issue a subsequent pause command to the VM. Instead of pausing the VM, it might shut down the original server. (The VM pause command is the same as issuing a **shutdown** command.) If this occurs:

1. Submit a second pause command to pause the VM.
2. Determine what you really want to do:
  - If the original server is not viable, leave it shut down, and continue working with the VM as desired.
  - If the original server is viable, stop the VM, and restart the original server.



## Exchange Not Working in VM

After starting a failover VM that is hosting Exchange, make sure that Exchange has successfully started. In some situations, required Exchange services do not start at boot-up. Do the following:

1. Go to the MMC services manager snap-in and check to see if all *Microsoft Exchange ...* services with a startup type of **automatic** have actually started.
2. If any have not, right-click on the service and select **start**.

## Cannot Access Running VM

You can access a running VM through either Windows remote desktop (RPC) or a VNC viewer. However, if you cannot access the VM through one of these options, you might be entering the wrong IP address (or host name). RPC and VNC access the VM through different IP addresses:

- RPC requires the original server IP address or host name.
- VNC requires the Axcient appliance IP address or host name.

## Cannot Log in to Test VM

When a test VM is first started, Active Directory credentials cannot be used to log into the test VM. (Local user credentials may be used.) This is true for both RDP and VNC connections. This will also cause any services that depend on Active Directory credentials to fail to authenticate users.

You can explicitly add domain support that a test VM will recognize. To use domain credentials with a test VM:

1. Add the host name *axcient-test-vm* to the Active Directory database.
2. Take the test VM out of the domain and then add it back into the domain. (This step can be performed either before or after the test VM has started.) Follow the steps for your version of Windows (2003 or 2008):

### *Windows 2003*

- a. Right-click on My Computer and select the **Change ...** button.
- b. Under the **Member of** check box, select the **workgroup** radio-button option, enter a name for the workgroup to join, and click **OK**. You might be asked to authenticate in order to proceed. Enter domain account credentials with authority to remove a host from a domain.
- c. A welcome to the workgroup message appears. Click **OK**.
- d. A message to reboot appears. Click **OK** but do not reboot.
- e. Select (again) the **Change ...** button.
- f. Under the **Member of** check box, select the **Domain** radio-button option, enter the name of your domain, and click **OK**. You might be asked (again) to authenticate in order to proceed. Enter domain account credentials with authority to add a host to a domain.
- g. A welcome to the domain message appears. Click **OK**.
- h. A message to reboot appears (again). Click **OK** and this time reboot.

### 3. *Windows 2008*

- a. Right-click on **Computer** and under the *Computer name, domain and workgroup settings* section, click **Change Settings**.
- b. The *System Properties* window appears. Under the Computer name tab, click **Change...**
- c. Under the **Member of** check box, select the **Workgroup** radio-button.
- d. Enter a name for the workgroup to join and then click **OK**.
- e. A message appears about knowing the administrator password in order to log in. Ensure that you have access to the local (non-domain) credentials, then click **OK**.
- f. A welcome to the workgroup message appears. Click **OK**.
- g. A message about restarting computer to apply changes appears. Click **OK**.
- h. Click the **Close** button on the *System Properties* window.

- i. A message about restarting computer to apply changes appears (again). Click **Restart Later**.
  - j. Repeat *steps a* through *c*, but this time under the **Member of** check box, select the **Domain** (instead of Workgroup) radio-button.
  - k. Enter a name for the workgroup to join and then click **OK**.
  - l. A Windows Security window appears. Enter a user name and password with domain administrator credentials, and then click **OK**.
  - m. Repeat *Steps f* through *i*, but this time click **Restart Now** (instead of Restart Later).
4. Domain credentials can now be used to log into the Test VM. If domain credentials still do not work, reboot the test VM.

## Restored Device Cannot Join Domain (Password Problem)

Windows requires that machine account passwords be changed every 30 days by default, and the passwords saved on the device and on the domain controller must match for a device to join a domain. If you restore (VM or BMR) a device image from an earlier date than the most recent password changes, the passwords might not match. In this case the restored device will not be allowed to join the domain.

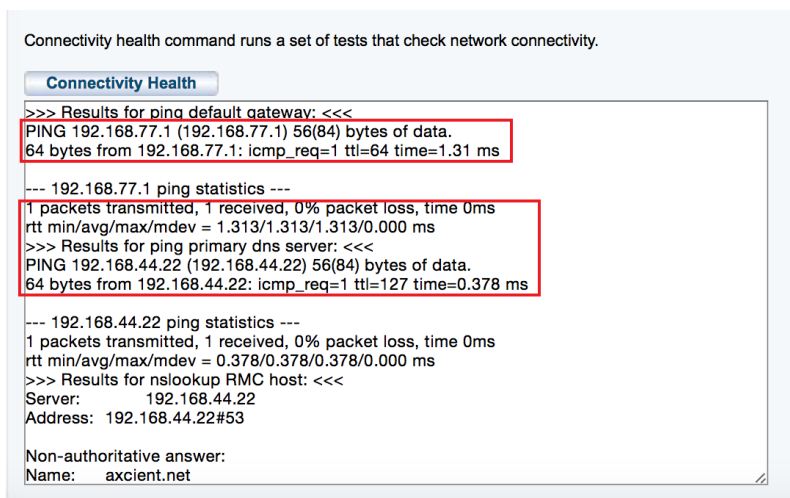
To correct this problem, remove the device from the domain and then join it back. (You need a privileged domain account to do this.)

To avoid the problem in the future, you can increase the machine account password age or disable machine account password changes altogether, but these options have security implications and are not recommended.

## Cannot Connect to Web Application

A number of conditions can prevent access to the Axcient Web Application. To check connectivity between the Axcient appliance and the Web Application, click the **system** tab and then select the **network utilities** option. Click the **Connectivity Health** button, which automatically tests access to the Web Application (and gateway, DNS lookup, and port 22). See the [Check Network Connections](#) section for more information about this test.

**Figure 139** - Web Application Connectivity Health



## Web Application Connectivity Problems

Problem	Solution
One or more appliance network settings are not correct.	Click the UMC <b>system</b> tab and then the <b>network settings</b> option to verify that the IP address, gateway, domain, workgroup, and DNS server are all correct, or update them as needed.
A needed port is not open.	The appliance communicates with the Web Application at various times through ports 22, 443, and 4015 to 4030. Check UMC Guide for latest appliance specifications in terms of ports that must be open. Verify these ports are open to the appliance, or open them if they are not.
A web proxy is blocking access.	Configure the Axcient appliance for the proxy server. See the <a href="#">Configure Web Proxy</a> section for this procedure. If you are running the Microsoft ISA firewall and configuring the proxy server does not fix the problem, you can turn off the web proxy as follows: <ol style="list-style-type: none"> <li>1. On the ISA Server Management console, click on the <b>Firewall Policy</b> node.</li> <li>2. On the <b>Toolbox</b> tab, click <b>Protocols</b>.</li> <li>3. Expand <i>All Protocols</i>, right-click <b>HTTP</b>, and then click <b>Properties</b>.</li> <li>4. Click the <b>Parameters</b> tab. In the <i>Application Filters</i>, clear <i>Web Proxy Filter</i> and then click <b>OK</b>.</li> <li>5. Click <b>Apply</b> to update the firewall policy.</li> </ol>
Network access to the appliance or the Internet is down.	The problem is often a transient network issue, but it will require more depth analysis of your network if the problem persists.
Appliance has not been registered.	Register the appliance using the <b>Register Now</b> link provided on the UMC dashboard.

## System Performance Slows

The most likely cause of a performance issue is that the backup or restore process is taking too much of the available network bandwidth. See the [Set Bandwidth Usage \(Quality of Service\)](#) section for instructions on how to control this.

## System Time Incorrect

The Axcient appliance uses NTP to set the system clock. If the time listed for events is not correct, the system might not have access to an NTP server. This can occur if the firewall policy denies access to the targeted NTP servers. To ensure the Axcient appliance has access to an appropriate NTP server, allow access through the firewall to the following IP address:

*91.189.94.4:123*

Port 123 is the standard NTP port, and *ntp.ubuntu.com* (91.189.94.4) is one of the NTP servers that the Axcient appliance uses to set the clock.



## Cannot Register Appliance

After installing an Axcient appliance, the registration process with the RMC can fail for a variety of reasons. The table below describes possible reasons (and corrective actions) for registration failing.

Troubleshooting Registration Problems

Problem	Solution
Registration failed because it is blocked by a web proxy server.	Configure the Axcient appliance for the proxy server. See the “Configure Web Proxy” section for this procedure.
Registration failed because the RMC did not find the appliance at the specified IP address.	If the Axcient appliance has been up since you changed the IP from 192.168.100.1 to the new IP address, the first IP might be cached on the router/switch. Reboot the appliance, which should register the NIC card's MAC address on the router/switch with the new IP.
Registration failed because of a browser-related problem when using Internet Explorer (version 8 or 9).	Try one of the following: <ul style="list-style-type: none"> <li>Register using Firefox instead of Internet Explorer.</li> <li>In Internet Explorer use Compatibility mode for all sites. In addition, clear out the browser cache for ALL items. (Past failed pages get cached and used, so it is important to completely clear the cache.)</li> </ul>
Registration failed because either the specified DNS name is not correct or the DNS server is not forwarding/answering.	Change the <i>DNS Server</i> entry to a public DNS address: 4.2.2.1, 4.2.2.2, or 8.8.8.8
Registration failed because port 22 (ssh) is blocked.	Registration requires a secure channel using port 22, so open port 22.

To check the network connections:

1. Click the **system** button at the top of the UMC page and select the **network utilities** option in the left navigation menu.
2. The *Network Utilities* page appears. Click the **Connectivity Health** button. This tests access to the gateway, DNS lookup, RMC, and port 22 (checks whether it is open). The results appear in the box below the button.

The following is sample Connectivity Health output from a working system:

>>>Results for ping default gateway: <<<

PING 10.0.3.1 (10.0.3.1) 56(84) bytes of data.

64 bytes from 10.0.3.1: icmp\_seq=1 ttl=255 time=0.441 ms

--- 10.0.3.1 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.441/0.441/0.441/0.000 ms

>>>Results for ping dns server: <<<

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

64 bytes from 8.8.8.8: icmp\_seq=1 ttl=52 time=56.6 ms

--- 8.8.8.8 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 56.626/56.626/56.626/0.000 ms

>>>Results for nslookup RMC host: <<<

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: axcient.net

Address: 209.18.124.2

>>>Results for ping RMC host: <<<

PING axcient.net (209.18.124.2) 56(84) bytes of data.

64 bytes from axcient.net (209.18.124.2): icmp\_seq=1 ttl=54 time=38.3 ms

--- axcient.net ping statistics ---

*1 packets transmitted, 1 received, 0% packet loss, time 0ms*

*rtt min/avg/max/mdev = 38.347/38.347/38.347/0.000 ms*

*>>>Verify that a connection can be made to port 22 of axcient.net: <<<*

*open*

## Offsite Progress Bars Do Not Update

Browsers cache pages to improve performance by redisplaying the cached page instead of downloading a fresh version. However, information on a cached page can become stale if it changes quicker than the cached page is updated. This problem can occur in the UMC when tracking the progress of offsite backup jobs. If the offsite backup progress bars on the dashboard do not update regularly (see the [Disk Utilization Panel](#) section), use the following procedures to force Firefox and Internet Explorer to check for a new version every time a page is loaded.

### Firefox: Reset Refresh Rate

To change the Firefox refresh rate:

1. Start Firefox and open a new tab.
2. Enter `about:config` in the location bar and approve the warning that appears.
3. Enter `browser.cache.check_doc_frequency` in the search bar below the location bar.
4. Double-click the preference name value (**`browser.cache.check_doc_frequency`**) and change the value from 3 (default) to 1. This sets Firefox to refresh a page every time it is loaded.
5. Close the tab.
6. When you no longer need to refresh pages every time they are loaded, repeat this procedure and reset to the default value of 3.

### Internet Explorer: Reset Refresh Rate

To change the Internet Explorer refresh rate:

1. Start Internet Explorer and go to **Tools > Internet Options**.
2. On the *General* tab, click the **Settings** button in the *Browsing History* section.
3. A *Temporary Internet Files and History Settings* window appears. Under *Check for newer versions of stored pages*, click the **Every time I visit the webpage** button. (The default is *Automatically*.) This sets IE to refresh a page every time it is loaded.
4. Click the **OK** button.
5. When you no longer need to refresh pages every time they are loaded, repeat this procedure and reset to the default value by clicking the **Automatically** button.

## Appliance Running out of Space

Warning messages appear in the event log when the appliance is 80%, 90%, and 100% full. Whenever you see one of these messages, the Axcient appliance is dangerously low on storage space, which could lead to failed backups and even data corruption if the appliance runs out of disk space. In this situation analyze your storage requirements and do one (or both) of the following:

- Reduce the space currently used. This can be done by (1) reducing the retention period of selected jobs, (2) reducing the schedule frequency of selected jobs, or (3) deleting jobs. See the [Reduce Backup Job Size](#) section for more information.
- Contact [Axcient customer support](#) to get a larger capacity Axcient appliance that better fits your needs.

## Cannot Access Device

The Axcient appliance stores the administrative credentials entered when the device was added. If the administrator password is changed, the Axcient appliance will no longer be able to access the device. To fix this:

1. Click the **devices** button at the top of the UMC page.
2. Click the icon of the target device.
3. Click the **edit device** option.
4. Enter the new password in the *Administrative Password* field and then click the **save** button.

See the [Modify a Device](#) section for more information.

## Cannot Add Device Overview

The following sections describe possible reasons why an Axcient appliance fails to add a device.

- [Incorrect Device Credentials](#)
- [Firewall Blocking Access \(Windows and Vista\)](#)
- [Local Workgroup Credentials Not Accepted \(Vista\)](#)
- [Local User Not Authenticated \(Windows XP\)](#)
- File Sharing Not Enabled: [\(XP\)](#) [\(Vista\)](#) [\(Windows 7\)](#) [\(MAC OS X\)](#) [\(Samba\)](#)

## Incorrect Device Credentials

Devices are added or updated from the *devices* tab in the UMC. Several fields can cause problems if the information is not entered or updated properly, as described in the table below.

**Figure 140** - Add Device Page

The screenshot shows the Axcient Unified Management Console interface. The top navigation bar includes links for dashboard, devices, reports, events, users, system, and docs. The left sidebar is titled 'devices' and contains icons for adding, removing, and changing credentials for devices. The main content area is titled 'add a device' and contains the following fields:

- Hostname or IP: 192.168.77.151
- Operating system: AUTODETECT
- Device type: DESKTOP
- Administrative username: admin
- Administrative password: (masked with asterisks)
- Device alias: Joe desktop
- Additional user assigned: (dropdown menu)

Buttons for 'cancel' and 'save' are located at the bottom of the form.

### Device Credential Problem

Problem	Solution
Hostname or IP address not found.	<p>Consider the following:</p> <ul style="list-style-type: none"> <li>When entering a host name, you can enter just the name if the device is in the same domain as the appliance. However, if the device is in a subdomain, enter the fully qualified domain name: <i>hostname.subdomain.domain.com</i></li> <li>If you enter an IP address and use DHCP, the device will no longer be found if DHCP changes the IP address. In this case the IP address must be updated in the device page.</li> </ul>
Administrative name not accepted.	<p>Consider the following:</p> <ul style="list-style-type: none"> <li>The user must have full administrator privilege on the device.</li> <li>For Exchange servers and some other devices, the entered name must include the domain in the following form: <i>domain\name</i> (for example <i>axcient\admin</i>)</li> </ul> <p>In addition, the domain name must be in the Windows domain format, not the DNS format (for example, <i>axcient\admin</i> instead of <i>axcient.com\admin</i>).</p>
Administrative password not accepted.	If the password was changed, the password must be updated in the device page.



## Firewall Blocking Access (Windows and Vista)

The Axcient appliance requires that files on a device are shared. If the firewall setting denies file sharing, the Axcient appliance cannot add the device. To allow file sharing in Windows or Vista:

1. Select **Start > Control Panel > Security Center** and then **Windows Firewall**. (Getting to the Windows Firewall display varies depending on the Windows version and view setting.)
2. Select the **Exceptions** tab.
3. Click the **File and Printer Sharing** box so a check mark appears.
4. Click the **OK** button.

## Local Workgroup Credentials Not Accepted (Vista)

Vista's administrative shares (*c\$*, *d\$*, and so on) are not visible or accessible on the network by default, which might prevent the Axcient appliance from adding the device. To enable administrative shares:

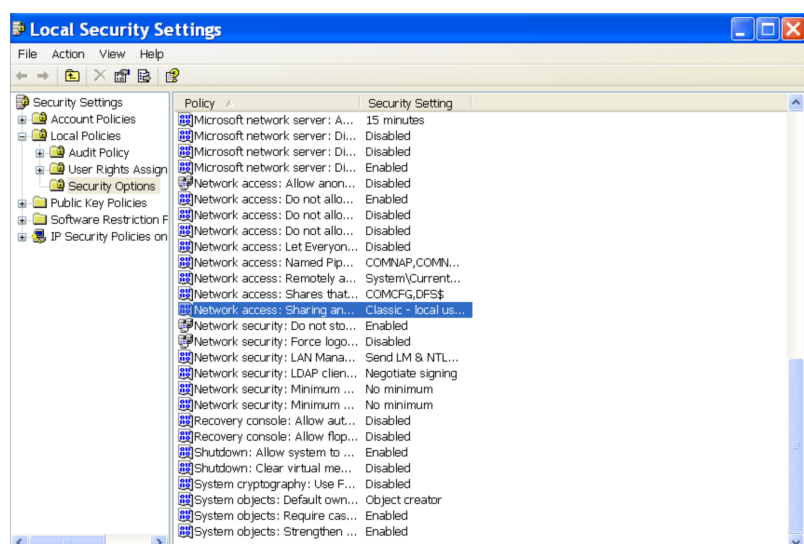
1. Launch the registry editor, To do this, enter the following command:  
*regedit*
2. Go to the following location:  
*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System*
3. Set the following key to the value 1 (one):  
*LocalAccountTokenFilterPolicy DWORD*

## Local User Not Authenticated (Windows XP)

If the local policies security option is set to Classic, network logins that use local account credentials authenticate by using those credentials. If this is set to Guest only, network logins that use local accounts are automatically mapped to the Guest account instead of their actual accounts. To change this:

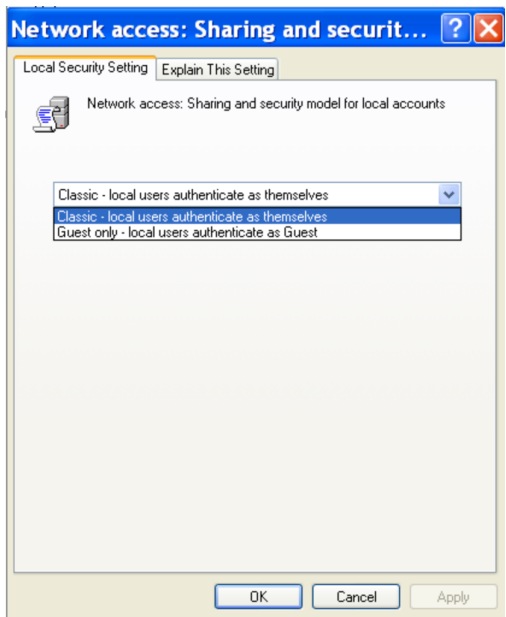
1. Go to the following location: **Start > Control Panel > Administrative Tools > Local Security Policy > Security Setting > Local Policies > Security Options**
2. Select (double click) the following policy:  
*Network access: Sharing and security model for local accounts*

Figure 141 - Local Security Settings Page



3. A dialog box appears. Select the **Local Security Settings** tab. From the drop-down menu, select **Classic - local users authenticate as themselves** and then click **OK**.

**Figure 142** - Local Security Settings Tab

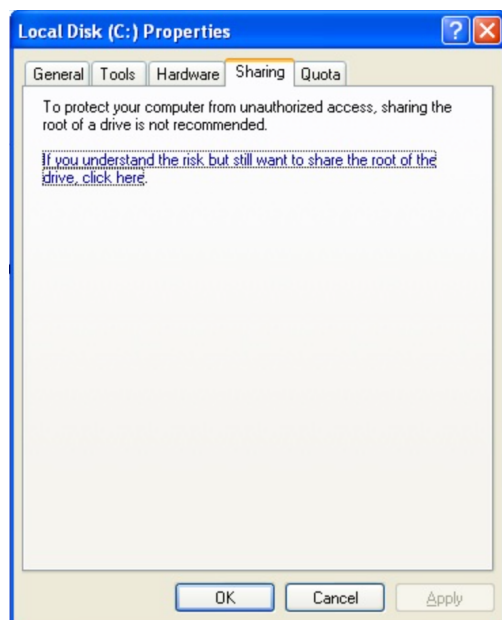


## File Sharing Not Enabled (XP)

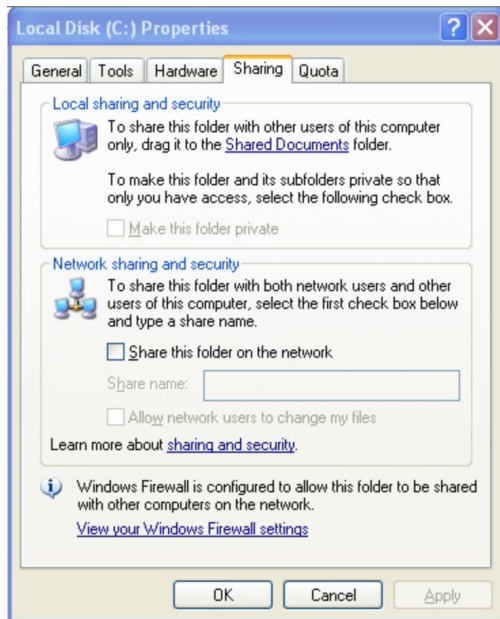
File sharing is not enabled by default. Activate it as follows:

1. From *My Computer*, select the system disk (typically C:), right-click the mouse, and choose **Properties**.
2. The *Properties* window appears. Select the **Sharing** tab.
3. If file sharing is not enabled, the sentence “If you understand the risk but still want to share the root of the drive, click here” appears. Click on this sentence.

**Figure 143** - Properties Sharing Page 1



4. The *Sharing* tab reappears with new text. Click the **OK** button. (Do not change any setting on the page.)

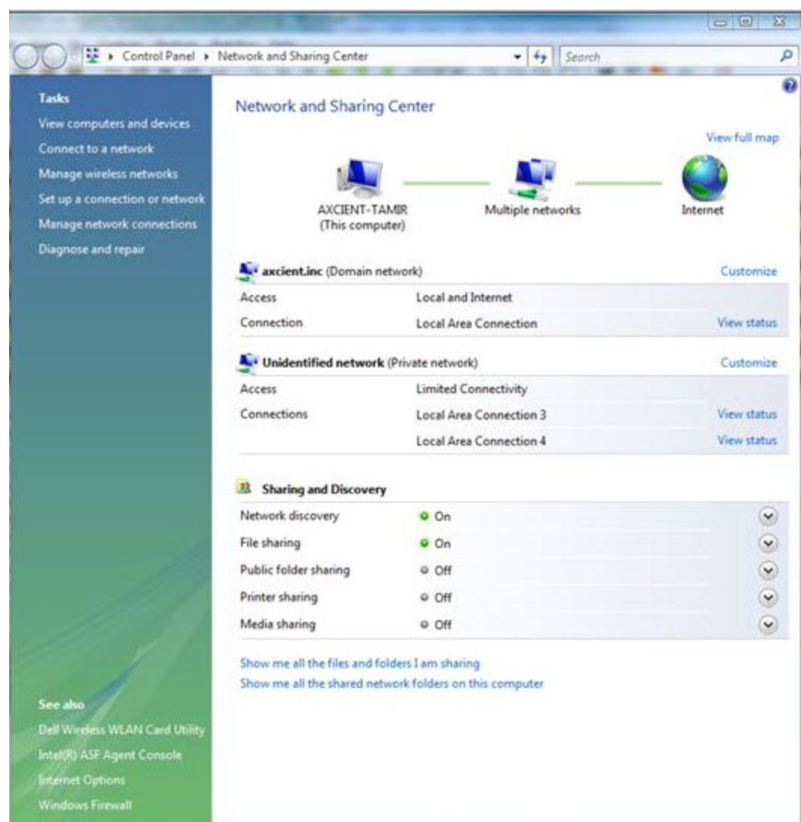
**Figure 144** - Properties Sharing Page

## File Sharing Not Enabled (Vista)

Delete this text and replace it with your own content. Network discovery and file sharing are not enabled by default. Activate them as follows:

1. Select **Start > Control Panel > Network and Sharing Center**.
2. In the Sharing and Discovery section, click the **On** button for **Network discovery** and **File sharing**.

Figure 145 - Network and Sharing Center Page



## File Sharing Not Enabled (MAC OS X)

The Axcient appliance cannot access a device until file sharing is enabled. To enable file sharing when running Mac OS X:

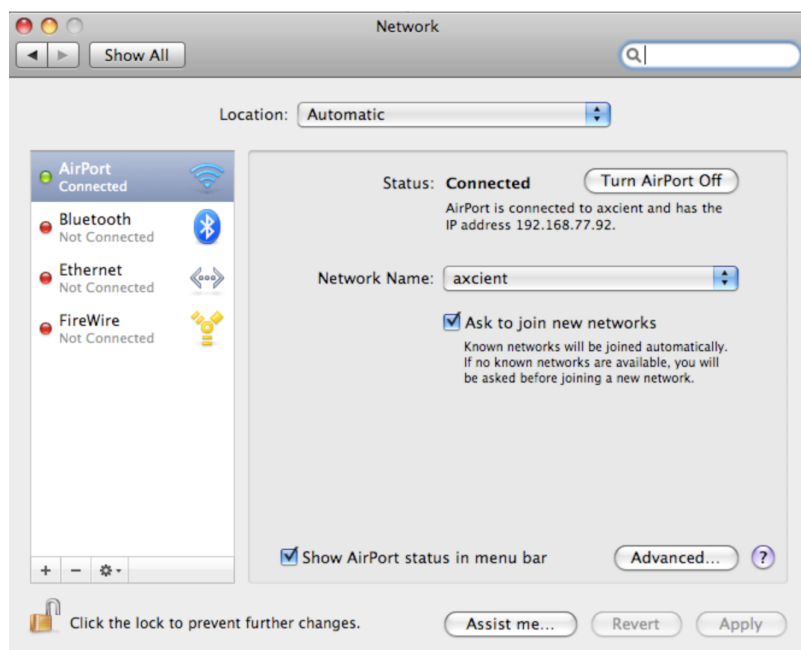
1. Go to *System Preferences* and click on **Network** under *Internet & Network*.

**Figure 146** - MAC OS X System Preferences



2. Select a network card from the list on the left and then click **Advanced**.

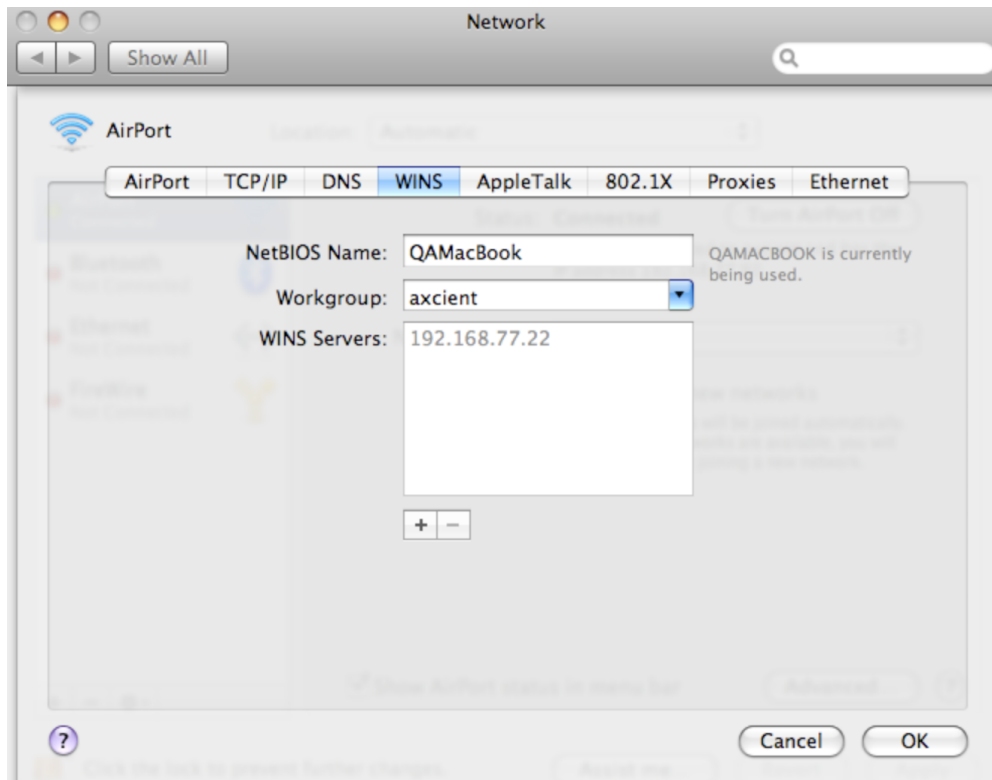
**Figure 132:** MAC PS X Network (Main) Page





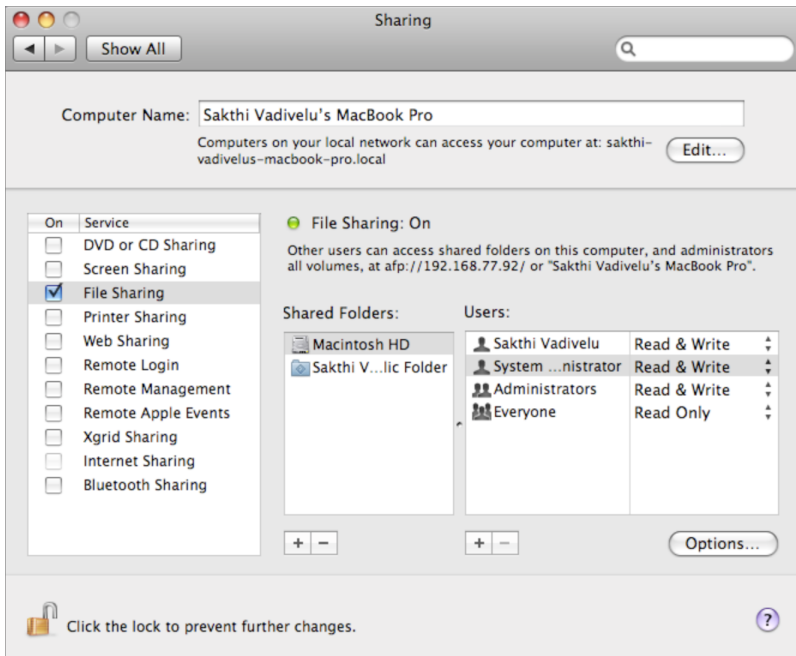
3. Select **WINS** from the horizontal menu list near the top. In the *WINS* display, enter the name (if the displayed name is not correct), select a workgroup from the drop-down menu, and then click **OK**.

Figure 147 - MAC OS X Network (Advanced) Page



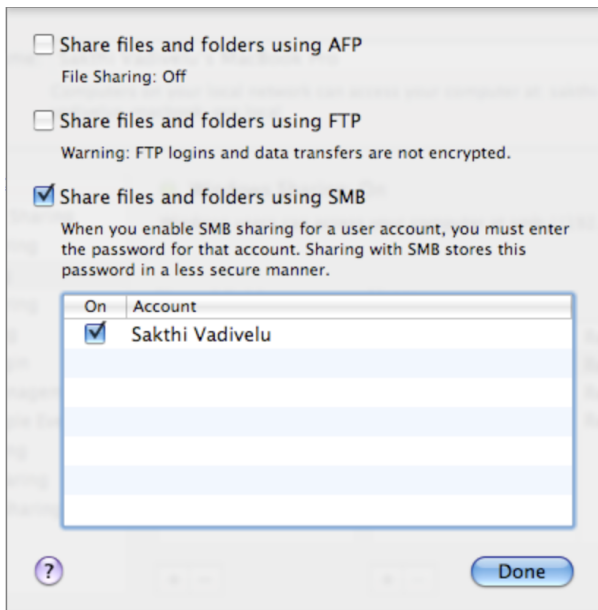
4. The main network page reappears. Click **Apply** and then select the back arrow button at the top.
5. The *System Preference* window reappears. Click on **Sharing** under *Internet & Network*.
6. In the *Sharing* window do the following:
  - a. Select the **File Sharing** box in the left pane.
  - b. Select the folders to share from the middle pane. Click the **plus (+)** button to open a window to select folders and files. After making your selection, click **Add**. The middle pane lists the selected files. Use the **minus (-)** button to remove files from the list.
  - c. Select the user from the right pane. Click the **plus (+)** button to open a window to select a user (or add a new user). After making your selection, click **Select**. The right pane lists the allowed users and their permissions. Use the **minus (-)** button to remove users from the list.

Figure 148 - MAC OS X Sharing (Main) Page



- Click the **Options** button, which displays another window. Select the box for Share Files and folders using SMB and then click **Done**. (It does not matter to the Axcient appliance whether the other two boxes are checked, only that the SMB is checked.)

Figure 149 - MAC OS X Sharing (Options) Page



## File Sharing Not Enabled (Samba)

The Axcient appliance cannot access a device until file sharing is enabled. Please note that the command syntax in the following steps vary by operating system. Check the documentation for your operating system (Linux, Solaris, and so on). The following example is for Ubuntu.

To enable file sharing when running Samba in a UNIX-based operating system, do the following

1. Verify you are running the latest version of Samba as follows:
  - a. Check for the latest version of installed applications (which includes Samba). To do this, enter  
*sudo apt-get install update*
  - b. Install the latest version of Samba. To do this, enter  
*sudo apt-get install samba*

If the latest version is already installed, a message to that effect will appear. Otherwise, installation begins. A message appears when the installation is complete.

2. Go to the */etc/samba* director by entering:  
*cd /etc/samba*
3. Edit the *smb.conf* file. For example, to use *vi* as the editor, enter:  
*vi smb.conf*
4. The *smb.conf* file is the Samba configuration file. The file includes instructions about how to define a share area, and it allows you to configure a variety of options. The Axcient appliance requires that the following three share parameters be set for any area that you want to back up.
  - The *path* parameter is set to the starting point. Include the full path to the share location. For example, to be able to back up all user directories in */home*, enter:  
*path = /home*
  - The *browseable* parameter must be set to *yes* as follows:  
*browseable = yes*
  - The *read only* parameter must be set to *no* as follows:  
*read only = no*
  - The *security* parameter must be set to *user* as follows:  
*security = user*
  - Do not comment out the default *[homes]* share section as that is required in some cases. The following four lines should not be commented out:  
*[homes]*  
*comment = Home Directories*  
*browseable = no*  
*writable = yes*

The Axcient appliance can back up data even if *read only* is set to *yes*, but it cannot restore data because it will not have write permission.

Create as many share entries as necessary to allow the desired access. The following example configures a *rootshare* that sets the entire device (starting at root) as a sharable area:

```
[rootshare]
comment = root share to backup on device1
path = /
browseable = yes
read only = no
security = user
```

5. Change the Samba user password by entering the following command (and the subsequent prompts):

```
sudo smbpasswd -a user_name
```

## File Sharing Not Enabled (Windows 7)

The Axcient appliance cannot access a device until file sharing is enabled. Enabling a Windows 7 system requires the following changes from the default settings:

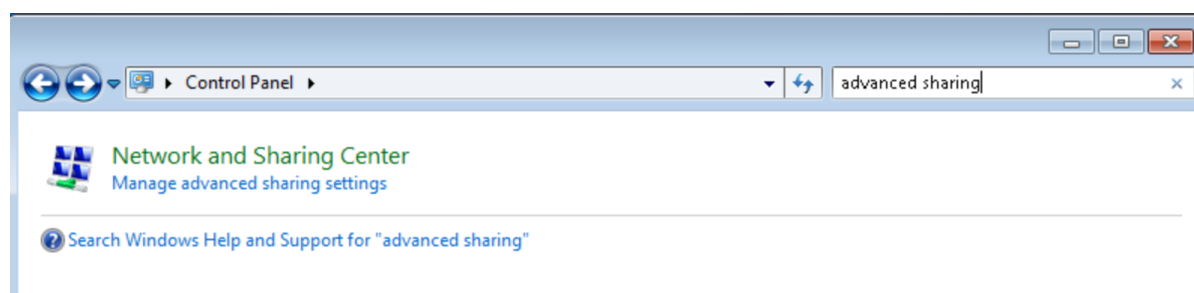
1. Enable file sharing
2. Enable the built-in Administrator user

## Enable File Sharing

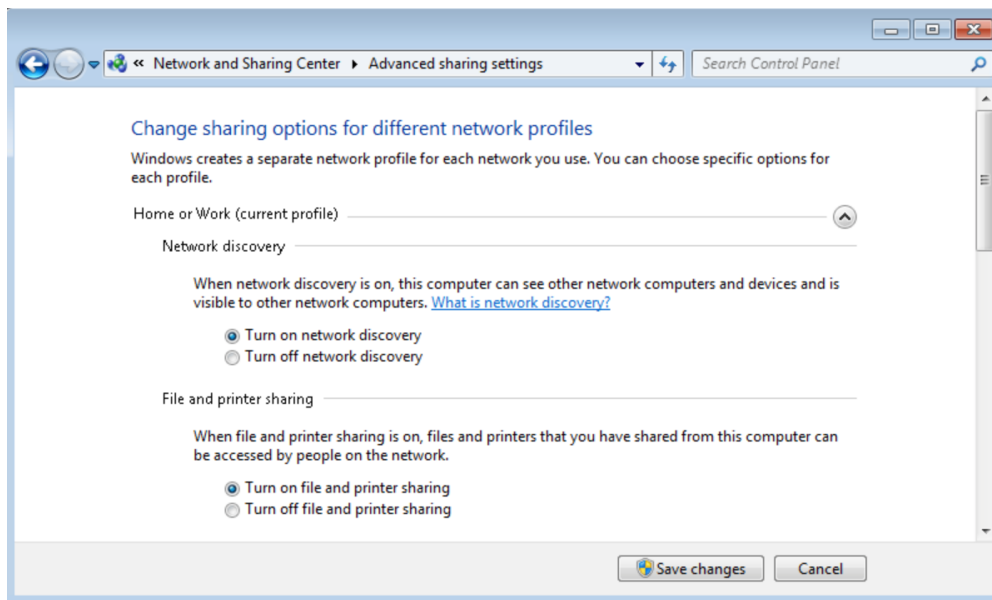
File sharing is disabled by default. To enable file sharing:

1. Select the **Start** menu, open the *Control Panel*, enter *advanced sharing* in the search box (upper right of page), and then click **manage advanced sharing settings**.

**Figure 150** - Control Panel Search (Advanced Sharing)



2. A Change Sharing Options display appears. Do the following:
  - a. Turn on network discovery (click the radio button for **Turn on network discovery** under *Network discovery*).
  - b. Turn on file sharing (click the radio button for **Turn on file and printer sharing** under *File and printer sharing*).
  - c. Click the **Save changes** button.

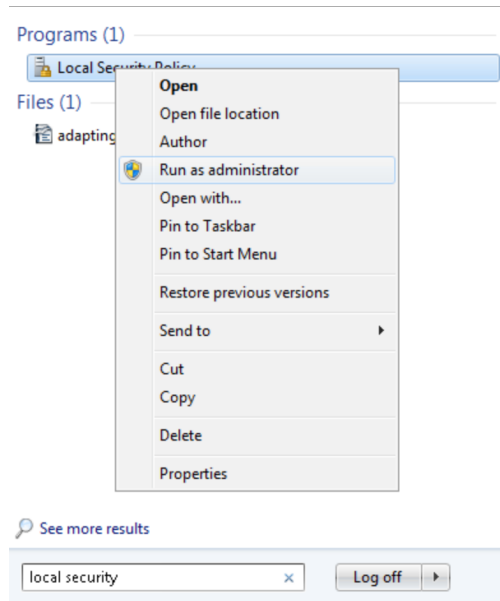
**Figure 151** - Advances Sharing Settings

## Enable Administrator

The built-in administrator user account is disabled by default. To enable the administrator:

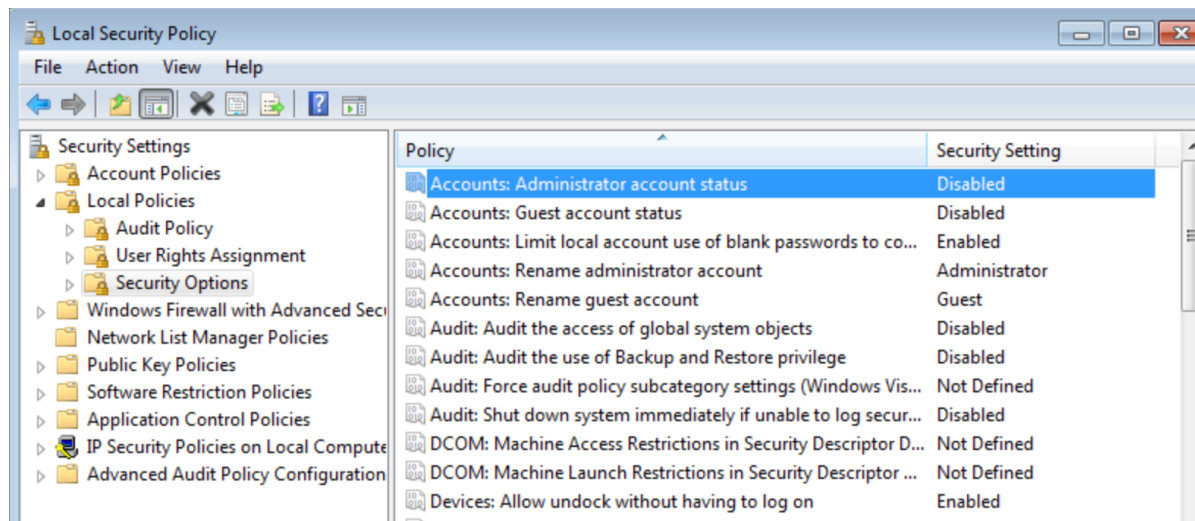
1. Select the **Start** menu and enter *local security* in the search field.
2. Select **Local Security Policy**, right-click to display a drop-down menu, and select **Run as administrator**.

Figure 152 - Local Security Policy Menu

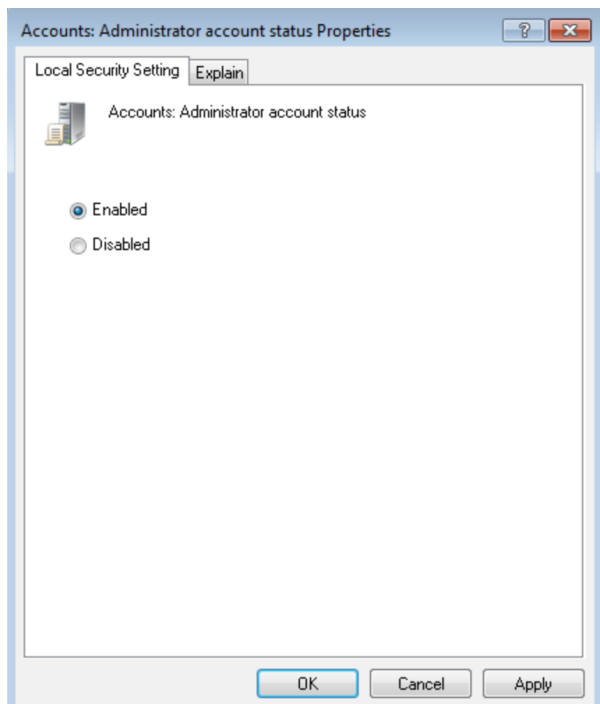


3. The Local Security Policy window appears. In the left pane select **Local Policies > Security Options**. The security options appear in the right pane. Double-click on **Accounts: Administrator account status**.

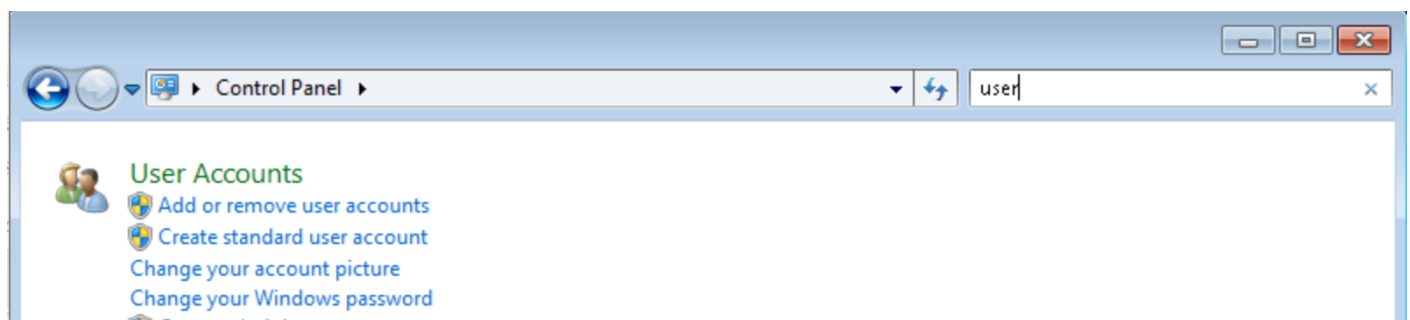
Figure 153 - Security Options - Administrator Account Status



4. The *Administrator account properties* window appears. Select the **Enabled** radio button and then click the **OK** button.

*Figure 154* - Enable Administrator Window

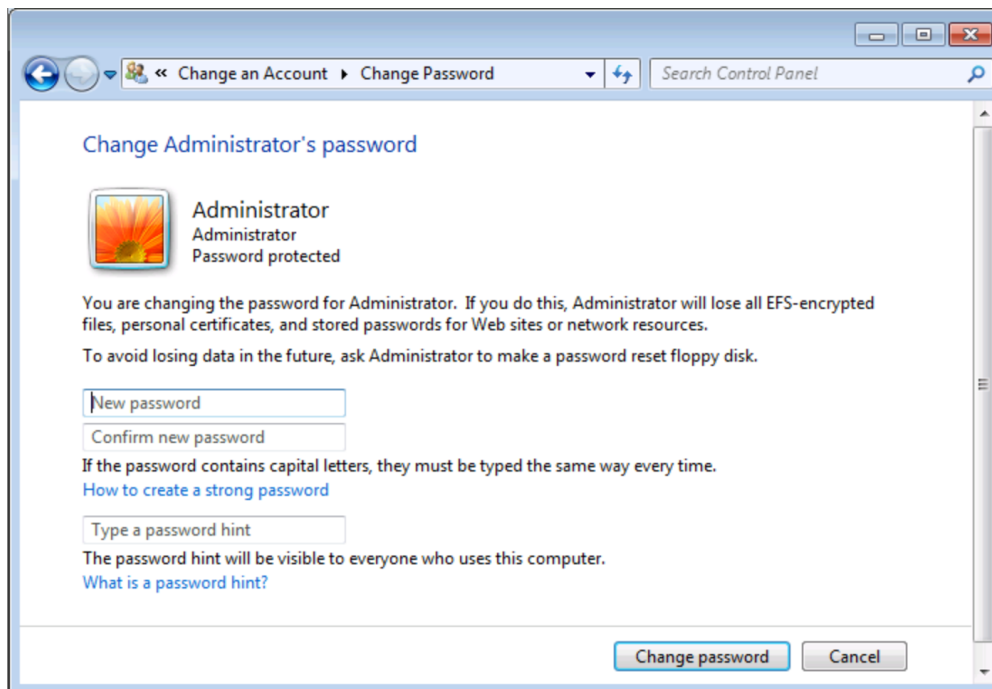
5. Select the **Start** menu, open the **Control Panel**, enter *user* in the search box (upper right of page), and then click **User Accounts**.

*Figure 155* - Control Panel Search (Users)

6. Select **Manage** another account from the selection list.
7. Select **Administrator** from the list of accounts.
8. Select **Create password** from the list of actions.
9. Enter (and confirm) the new password, optionally enter a password hint, and then click the **change password** button.



Figure 156 - Change Admin Password Window



## Exchange and SQL Server Database Backup

Axcient intelligently backs up Microsoft Exchange and SQL Server databases. In an image backup job or when you specify **Use Open File Manager** in a file backup job, Axcient does the following steps when backing up an Exchange or SQL Server database:

1. Alerts the application to quiesce the database gracefully to a safe state.
2. Takes a snapshot of the database.
3. Alerts the application that the database snapshot is complete.

For this process to work properly, it is essential that all pertinent files be included:

- In an image job, select all disks that contain Exchange or SQL Server database and transaction log files.
- In a file job, select all folders on every disk that contain Exchange or SQL Server database and transaction log files.

See the Exchange or SQL Server documentation for information about the database and transaction log files that must be backed up.

In the case of SQL in full recovery mode, the transaction logs need to be handled by SQL. Please refer to the following Microsoft SQL documentation on transactional logs for more information:

- [How to Back up a Transaction Log](#)
- [Working with Transaction Logs](#)

## Virtual Network Computing (VNC) Usage

A failover or test VM running on the Axcient appliance can be accessed in the following ways:

- If remote desktop (RDP) is enabled on the device, you can access the VM by opening a Remote Desktop Connection (**Start > All Programs > Accessories > Remote Desktop Connection**). See the Windows documentation for information about using remote desktop.
- If the **VNC Remote Desktop Support** box is checked when the VM is started, you can access the VM by opening a VNC client viewer.

The IP address (or host name) to use when accessing the VM differs for Windows remote desktop and VNC. Use the server IP address for Windows remote desktop.

Use the Axcient appliance IP address for VNC. When running multiple VMs, include the port number in the IP address. The first VM uses the default VNC port number, which is 5900. Subsequent VMs increment the port number by one (5901, 5902, and so on). For example, if an Axcient appliance with an IP address of 192.168.77.26 is running two VMs, enter 192.168.77.26:5900 for the first VM and 192.168.77.26:5901 for the second VM.

Virtual Network Computing (VNC) is a remote control application that allows you to view and interact with one computer through a client “viewer” application on another computer anywhere on the Internet. VNC is operating system independent,

so the target and client computers can be of different types (for example, the VNC viewer on a Windows system accessing a Linux system). VNC is freely and publicly available.

A variety of VNC clients are available for download including RealVNC, TightVNC, and UltraVNC. See the documentation for your VNC viewer. When starting any VNC viewer to access the VM, consider the following:

- **Keyboard/Mouse Activation** - When the VM starts, it must initially adjust device drivers, including mouse and keyboard drivers. This can take up to five minutes. This normally is obvious when first connecting to the VM through a VNC client, as it might not respond to mouse or keyboard activity during this period.
- **Ctrl-Alt-Del Key Sequence** - It is necessary to issue this keyboard sequence to login to the VM. Most VNC clients have a helper menu that is accessed through a function key (such as F8 on RealVNC). Access the helper menu to generate the **Ctrl-Alt-Del** sequence if you are not able to do so from your keyboard.

## Hyper-V Virtual Machine Guidelines

There are several factors to consider when working with Hyper-V virtual machines.

### MR Hyper-V VM Procedure

To complete a successful bare metal restore (BMR) from an image backup of a Hyper-V VM:

1. Turn on hardware-assisted virtualization for the target device. (The target device must support hardware-assisted virtualization.)
2. If the BIOS was edited to turn on hardware-assisted virtualization, power off the device and then power it on again. (It is not sufficient to simply reset the device.)
3. Perform the BMR (see [Restore Device Using BMR Recovery Disk](#) section).
4. Reboot the device.

### Hyper-V Backup Notes

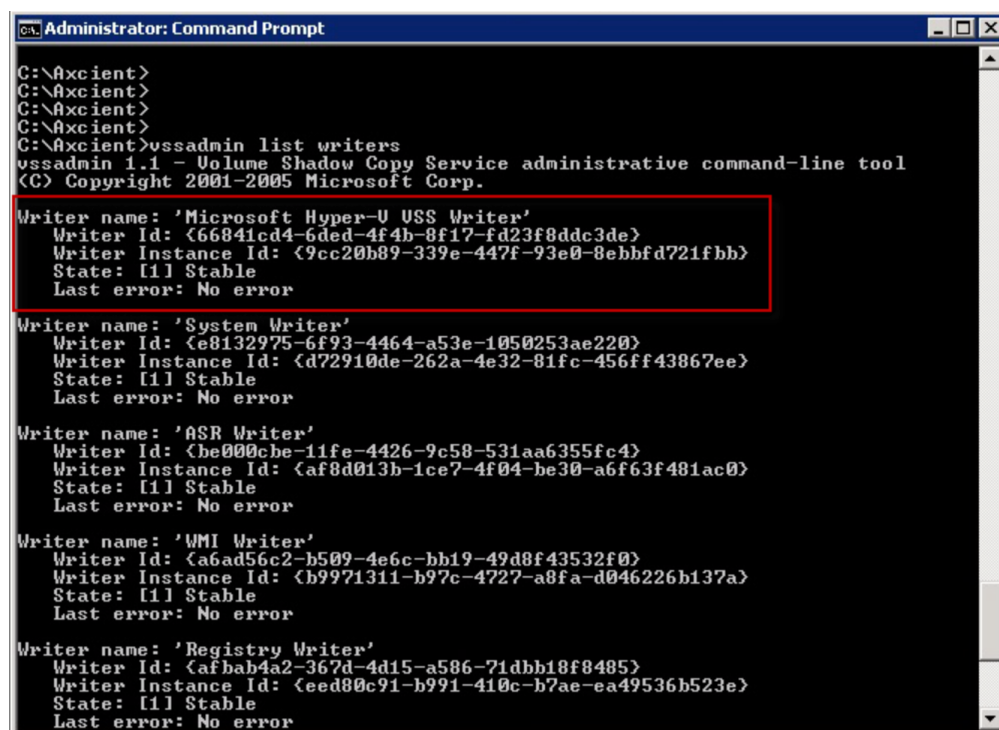
Consider the following when backing up Hyper-V virtual machines:

- An image backup can be created for each individual VM. All the usual backup protections (test or failover VM, BMR, and selected files restore) apply to each VM.
- A single image backup of the Hyper-V server can also be created. (The backup will include all *vhd* files if the partitions hosting these VMs are included.) However, while you can run a failover (or test) VM of the server, the individual VMs will not run in that server VM. A separate image backup is required for an individual VM to provide failover protection for that VM.

The Hyper-V VSS writer must be installed and enabled. To check the list of VSS writers, enter the command:

```
vssadmin list writers
```

Figure 157 - vssadmin Command Output



```

C:\Axcient>
C:\Axcient>
C:\Axcient>
C:\Axcient>
C:\Axcient>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Writer name: 'Microsoft Hyper-U USS Writer'
  Writer Id: {66841cd4-6ded-4f4b-8f17-fd23f8ddc3de}
  Writer Instance Id: {9cc20b89-339e-447f-93e0-8ebbf721fbb}
  State: [1] Stable
  Last error: No error

Writer name: 'System Writer'
  Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
  Writer Instance Id: {d72910de-262a-4e32-81fc-456ff43867ee}
  State: [1] Stable
  Last error: No error

Writer name: 'ASR Writer'
  Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
  Writer Instance Id: {af8d013b-1ce7-4f04-be30-a6f63f481ac0}
  State: [1] Stable
  Last error: No error

Writer name: 'VMI Writer'
  Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
  Writer Instance Id: {b9971311-b97c-4727-a8fa-d046226b137a}
  State: [1] Stable
  Last error: No error

Writer name: 'Registry Writer'
  Writer Id: {afb4a2-367d-4d15-a586-71dbb18f8485}
  Writer Instance Id: {eed80c91-b991-410c-b7ae-ea49536b523e}
  State: [1] Stable
  Last error: No error

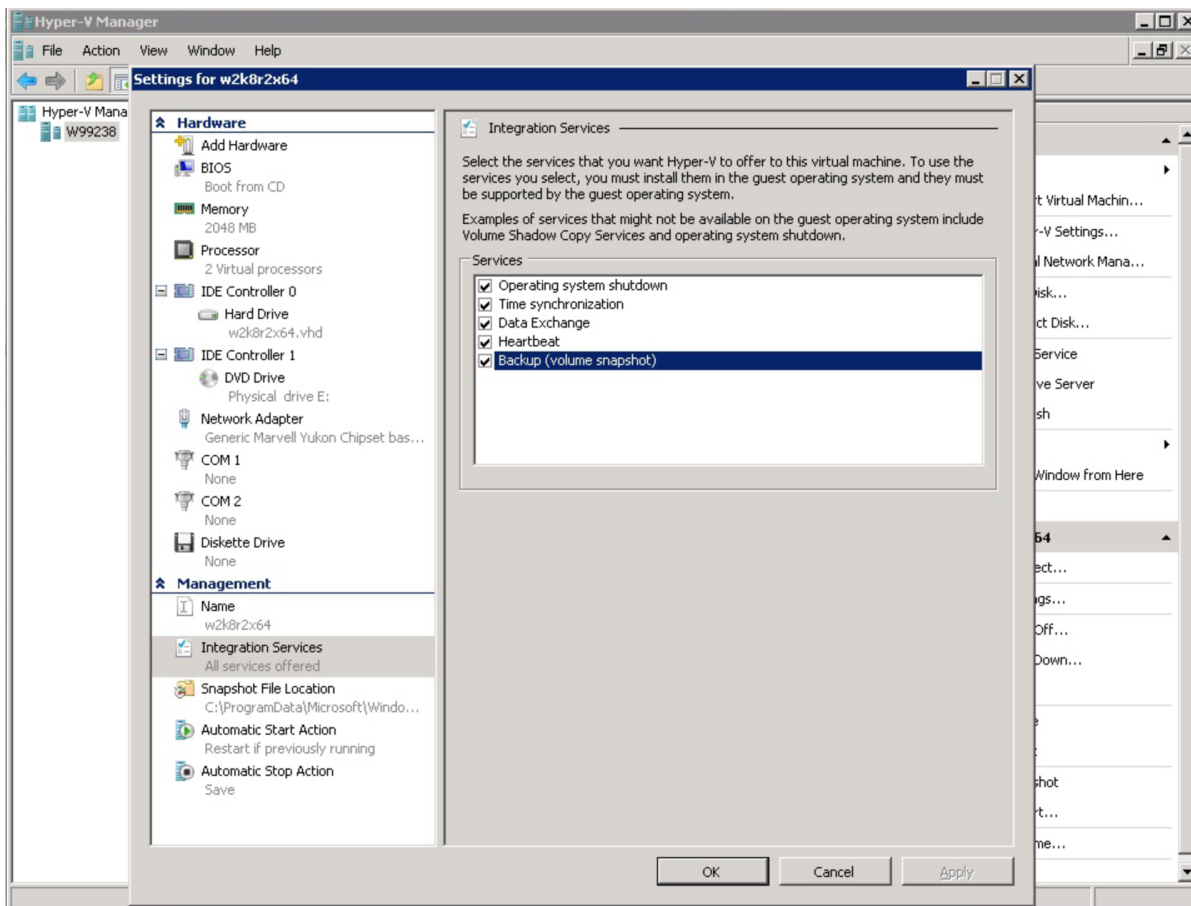
```

Hyper-V uses one of two mechanisms to backup each VM under Hyper-V:

- If the VM is configured to **saved state**, the VM is suspended while the snapshot is being taken. This means no one can access the VM until the snapshot is complete.
- If the VM is configured to **Child VM snapshot**, the VM remains active (most of the time) while the snapshot is being taken.

Because there is less down time, it is recommend that the VM be configured to **Child VM snapshot**. To do this, the Hyper-V Integration Services must be installed, and the **Backup (volume snapshot)** box should be checked.

Figure 158 - Hyper-V Integration Service Page



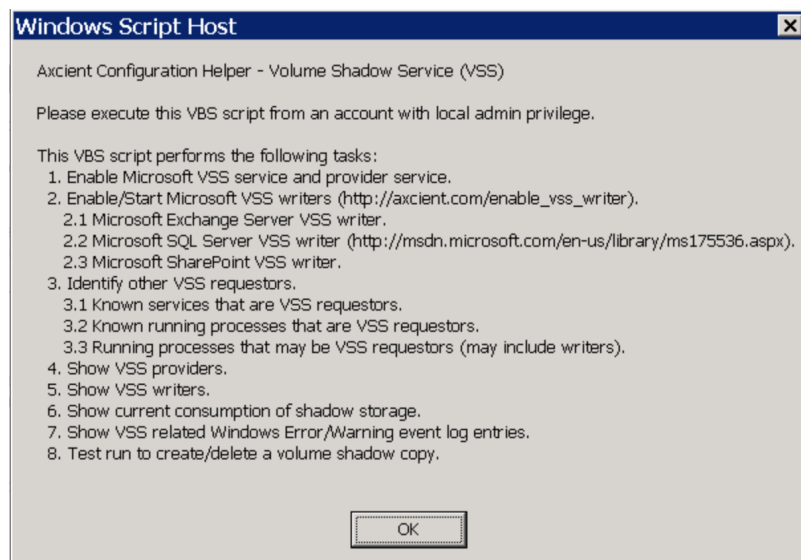
## VSS Configuration

For Windows-based devices, the Axcient appliance uses the Microsoft Volume Shadow Service (VSS) for image backup jobs (always) and file backup jobs (when *Open File Manager* is set). This requires that VSS is enabled and configured correctly. Axcient supplies an interactive script to help configure VSS. This appendix describes how to use the VSS configuration script.

To configure VSS through the Axcient script:

1. Log in as the local administrator on the target device.
2. Log in to the UMC of the appliance.
3. Click the **system** button at the top of the UMC page and then select the **tools** option in the left navigation menu.
4. The *Tools* page appears. Right-click on the **VSS Script** link and select **Save Link As** (or the corresponding option for your browser) to download the script file. The file name is *VSSConfig.vbs*. Download the file to the target device. (The location on the device does not matter.)
5. Open a command window (**Start > Run** and enter *cmd*), go to wherever you downloaded the script, and enter the following:  
`.\VSSConfig.vbs`
6. The VSS script introduction window appears. This window describes all the steps in the script. Read the text and then click the **OK** button. Additionally, An OK button will appear on all message boxes. Read the message and then click the **OK** button for each message box that appears in the script. In most cases, there is nothing else for you to do. However, some messages indicate conditions that might require additional action on your part, as noted in these instructions.

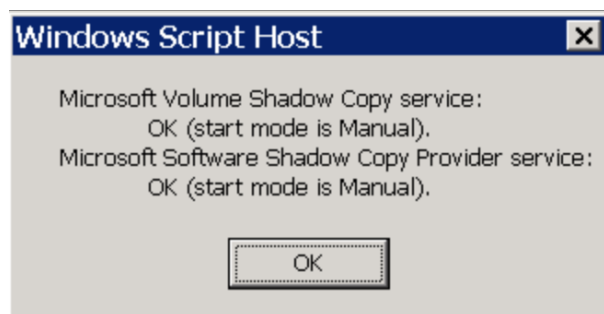
**Figure 159** - VSS Script - Introduction



7. The *Enable VSS service and provider service* box appears. In this step the script verifies or enables VSS, and it displays status messages. These messages are informational and can be ignored unless a WARNING message appears.

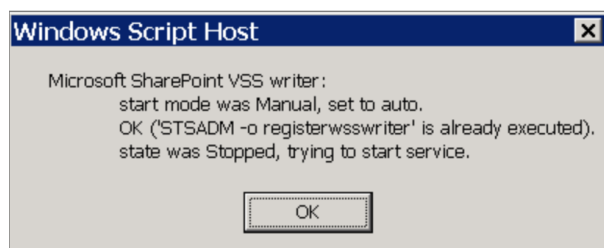
**CAUTION!** A message that starts with the word WARNING indicates a problem condition that might require attention. If you see a WARNING message in this or any subsequent step, record the message and contact Axcient customer support to debug the problem.

**Figure 146:** VSS Script - Progress



8. The *Enable/Start Microsoft VSS writers* box appears. In this step the script verifies or enables the VSS writers for the following applications:
- MS Exchange Server
  - MS SQL Server
  - MS SharePoint.
9. A status box appears for each application. Again, these messages are informational and can be ignored (unless a WARNING message appears). The figure below is a sample result for MS SharePoint. In this example the script found that the SharePoint VSS writer was stopped and is being restarted.

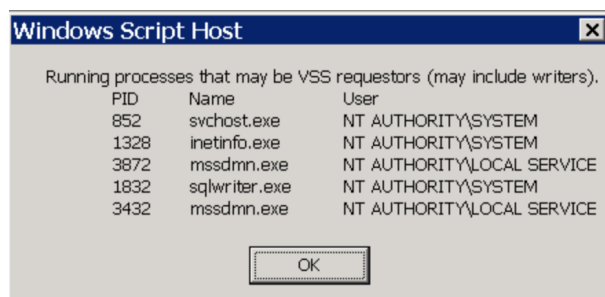
**Figure 160 -** MS SharePoint VSS Writer Example



10. The *Identify other VSS requestors* box appears. In this step the script searches for other applications that use VSS infrastructure. The purpose of this step is to identify other products that might conflict with the Axcient solution. It looks for the following:
- Known services that are VSS requestors.
  - Known running processes that are VSS requestors.

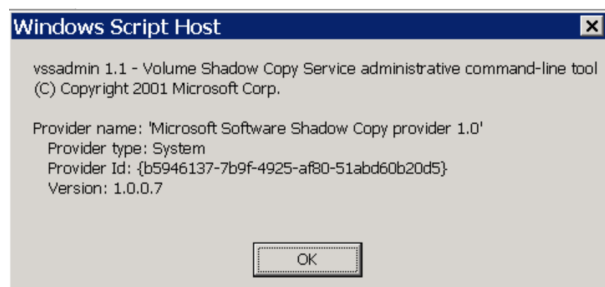
- Running processes that may be VSS requestors (may include writers).
11. The figure below illustrates the result from finding running processes that might be VSS requestors. Check to see if any of the listed services or processes are related to another backup product, because other backup products could potentially conflict with the Axcient solution.

**Figure 161** - Other VSS Requester Example



12. The *Show VSS providers* message box appears. In this step the script searches for providers of the VSS service. In most cases the search will return just the Microsoft Shadow Copy provider. However, some products provide their own VSS mechanism. If an additional provider appears, note that provider as it could be a potential issue for the Axcient solution.

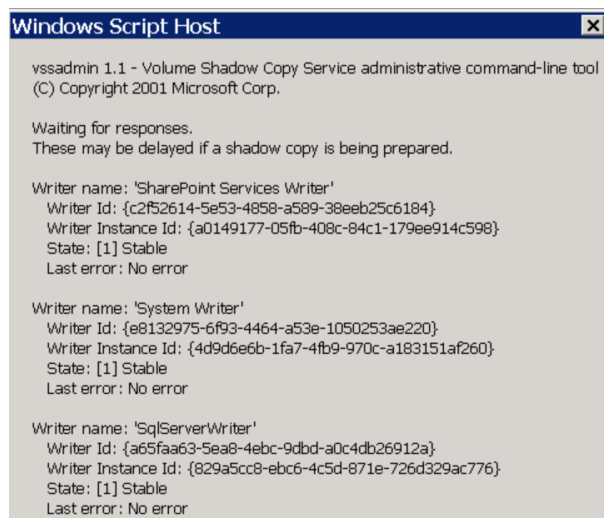
**Figure 162** - VSS Providers Example



13. The *Show VSS writers* message box appears, which lists the available writers. For each writer check the following fields:
- **State** - The value should be either *Stable* or *Wait for completion*.
  - **Last error** - The value should be *No error*.
14. Any other value in either field indicates a problem. In such a case note the writer and value and contact Axcient customer support to debug the problem.



Figure 163 - VSS Writers Example



```

Windows Script Host

vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

Waiting for responses.
These may be delayed if a shadow copy is being prepared.

Writer name: 'SharePoint Services Writer'
  Writer Id: {c2f52614-5e53-4858-a589-38eeb25c6184}
  Writer Instance Id: {a0149177-05fb-408c-84c1-179ee914c598}
  State: [1] Stable
  Last error: No error

Writer name: 'System Writer'
  Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
  Writer Instance Id: {4d9d6e6b-1fa7-4fb9-970c-a183151af260}
  State: [1] Stable
  Last error: No error

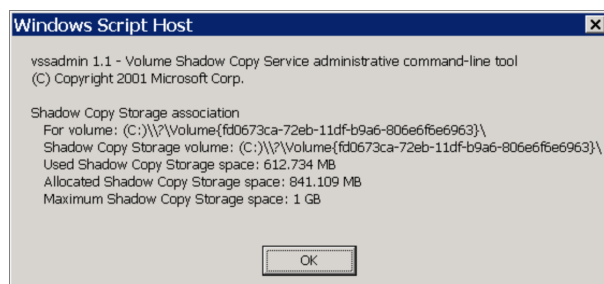
Writer name: 'SqlServerWriter'
  Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
  Writer Instance Id: {829a5cc8-ebc6-4c5d-871e-726d329ac776}
  State: [1] Stable
  Last error: No error

```

15. The *Show current consumption of shadow storage* message box appears. In this step the shadow size parameters are displayed. Check for the following:

- If the *Used Shadow Copy Storage space* value is nearly as large as the *Maximum Shadow Copy Storage space* value, consider increasing the maximum value.
- Even if the used space value is significantly less than the maximum space value, you might need to increase the maximum if many files on the volume are modified frequently.
- It is recommended that each storage volume have its own shadow copy storage volume. For example, if you have C: and D: volumes, you should see separate entries for each in this display. If not, create a shadow storage volume for the missing volume.

Figure 164 - Shadow Storage Example



```

Windows Script Host

vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

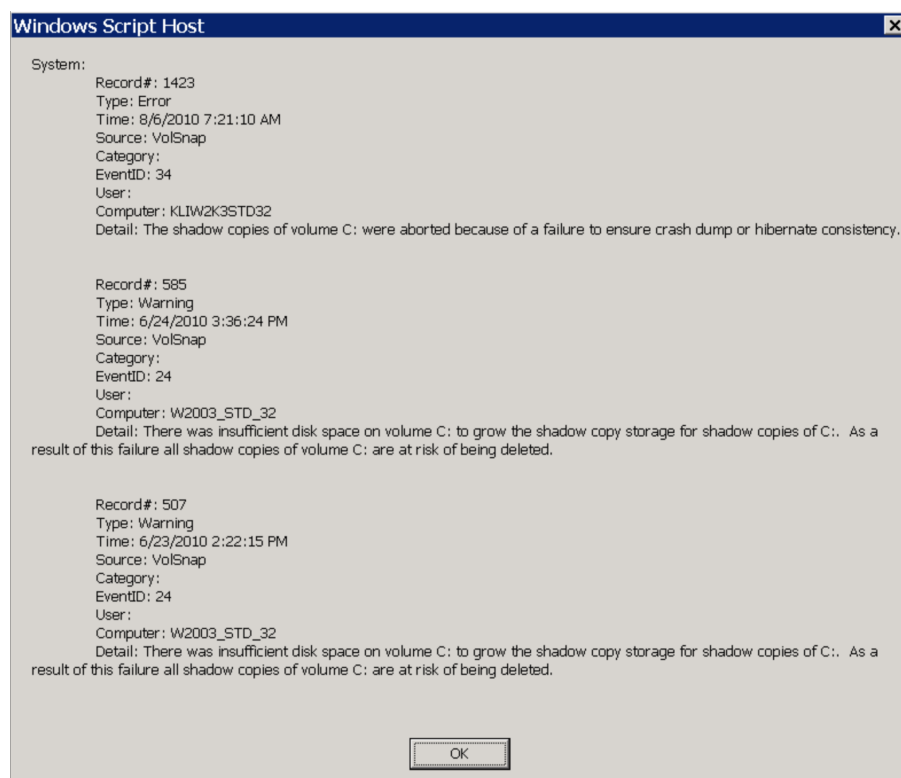
Shadow Copy Storage association
For volume: (C:)\?\Volume{fd0673ca-72eb-11df-b9a6-806e6f6e6963}\
Shadow Copy Storage volume: (C:)\?\Volume{fd0673ca-72eb-11df-b9a6-806e6f6e6963}\
Used Shadow Copy Storage space: 612.734 MB
Allocated Shadow Copy Storage space: 841.109 MB
Maximum Shadow Copy Storage space: 1 GB

OK

```

16. The *Show VSS related Windows Error/Warning event log entries* message box appears. In this step VSS-related error and warning messages from the (1) application, (2) security, and (3) system logs are displayed. Review the log entries for possible problems. The figure below illustrates results from a system error log. In this example the shadow copy for volume C: is failing because of insufficient space, which means disk space must be freed up before continuing.

Figure 165 - System Error Log Example



17. The *Test run to create /delete a volume shadow copy* message box appears. In this step the script attempts to create a shadow copy and then reports the results. You should see the following messages:

*OK shadow\_name created successfully*

*OK shadow\_name deleted successfully*

These messages mean that a VSS copy has successfully been created and deleted. This is an indication that VSS will work for the Axcient solution. However, this test does not use any VSS writers, so it does not ensure that VSS is fully configured for Axcient. If you do not get a success message, contact Axcient customer support to debug the problem.

18. The *Done* message box indicates the script has completed.

## Windows Configuration

In order to protect a device, the Axcient appliance requires an appropriate login account and certain enabled services. Axcient supplies an interactive configuration script to help set up a Windows-based device properly. This appendix describes how to use the Windows configuration script.

The login account used by the Axcient appliance needs to have administrative privilege and also be part of the Backup Operators group. For additional information about this please see:

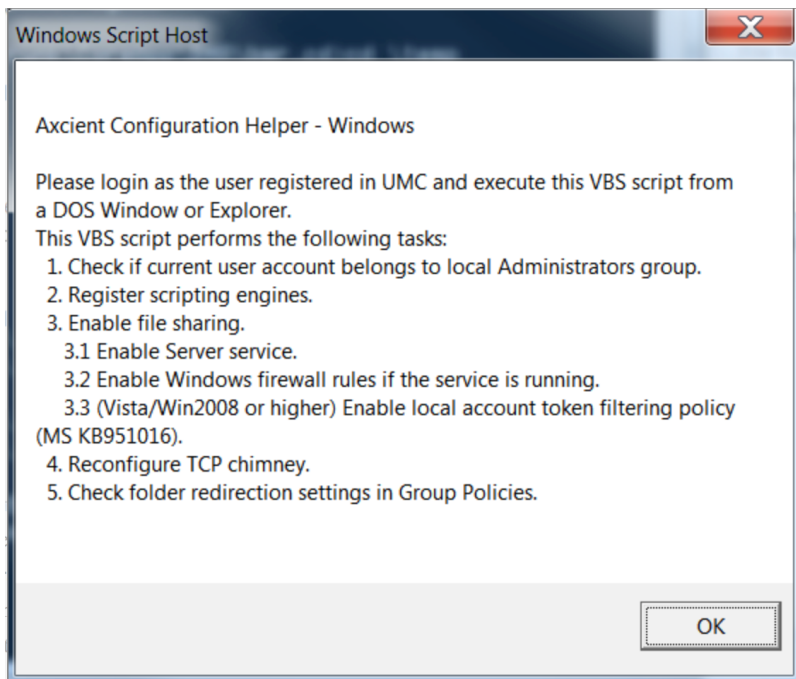
[http://technet.microsoft.com/en-us/library/cc785098\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc785098(v=ws.10).aspx)

<http://technet.microsoft.com/en-us/library/dd277404.aspx>

To configure a Windows device through the Axcient script:

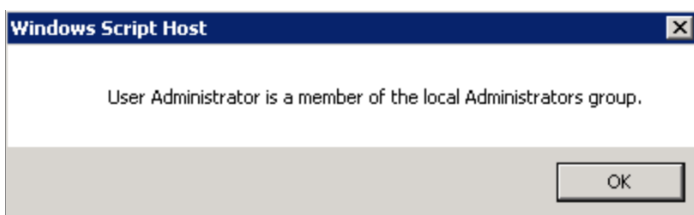
1. Log in as the local administrator on the target device using the same credentials you specified when you added the device to the Axcient appliance.
2. Log in to the UMC of the appliance.
3. Click the **system** button at the top of the UMC page and then select the **tools** option in the left navigation menu.
4. The *Tools* page appears. Right-click on the **Windows Script** link and select **Save Link As** (or the corresponding option for your browser) to download the script file. The file name is *WindowsConfig.vbs*. Download the file to the target device. (The location on the device does not matter.)
5. Open a command window (**Start > Run** and enter *cmd*), go to wherever you downloaded the script, and enter the following:  
`.\WindowsConfig.vbs`
6. The Windows script introduction window appears. This window describes all the steps in the script. Read the text and then click the **OK** button. Additionally, An OK button will appear on all message boxes. Read the message and then click the **OK** button for each message box that appears in the script. In most cases, there is nothing else for you to do. However, some messages indicate conditions that might require additional action on your part, as noted in these instructions.

Figure 166 - Windows Script - Introduction



7. The *Check if the current user account ...* box appears. This step checks whether the current user belongs to the local Administrator group. One of the following responses appears:
- User <name> is a member of the local Administrators group.
  - User <name> is not a member of the local Administrators group.

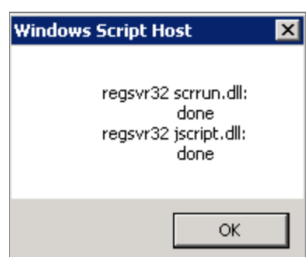
Figure 167 - Windows Script - Check User Account



8. The *Register scripting engines* box appears. This step checks for two scripting engines that the Axcient appliance requires, *scrrun.dll* and *jscrip.dll*. The response for each will be done (meaning properly registered) or a WARNING message. If a WARNING message appears (for example, because a file is missing), read the message and try to correct the problem.

**Caution!** A message that starts with the word WARNING indicates a problem condition that might require attention. If you see a WARNING message in this or any subsequent step, record the message and contact Axcient customer support to debug the problem.

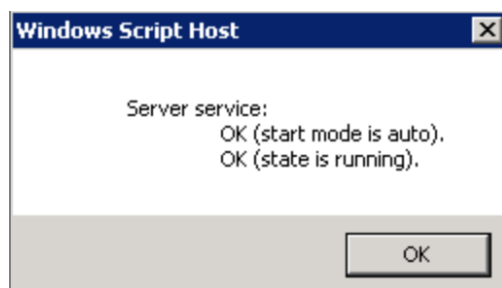
Figure 168 - Windows Script - Scripting Engine Check



9. The *Enable file sharing* box appears. This step does the following:

- a. Checks whether the file sharing is enabled (an Axcient requirement) and attempts to enable file sharing if it is disabled.
  - An OK status for both mode and state appears if file sharing is properly enabled.
  - If it is not in auto mode or running, the message indicates the script is attempting to set the mode to auto or start the service.

Figure 169 - Windows Script - Enable File Sharing

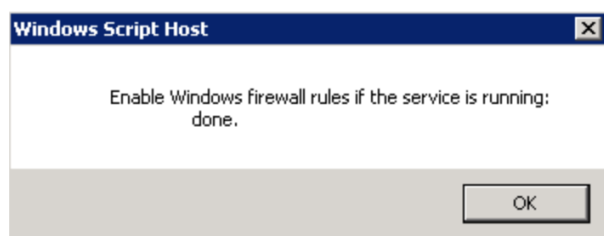


10. Checks whether Windows firewall rules are enabled. The response is either *done* (meaning enabled) or the following WARNING message:

*WARNING: Windows Firewall service is not running or does not exist. No rules to enable.*

In most cases this WARNING message appears because you are using another firewall product. If so, allow the Axcient appliance access through the firewall of that product. If you are using a web proxy, configure the Axcient appliance for that web proxy (see [Configure Web Proxy](#) section).

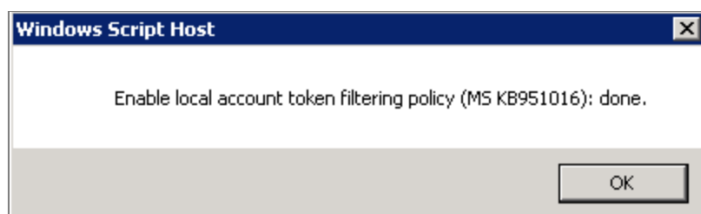
Figure 170 - Windows Script - Enable Firewall Rules



11. Checks whether a local account token filtering policy is enabled). The response is either done (meaning enabled) or the following error message:  
*failed, err = error\_code*

There are several possible causes for the error, and the *error\_code* provides guidance in troubleshooting the problem.

**Figure 171** - Windows Script - Enable Token Filtering Policy



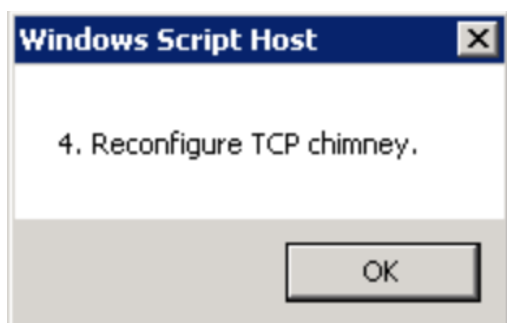
12. Alerts you to install the *File and Printer sharing for Microsoft networks* service. This is informational only; the script takes no action. Follow the instructions in the message to install this service (or verify it is already installed).

**Figure 172** - Windows Script - Start Connection Service



13. The *Reconfigure TCP Chimney* box appears. This step reconfigures certain default parameters to work properly in this situation. When the reconfiguration is complete, a *Done* box appears, which means this step (not the script) is finished.

**Figure 173** - ndows Script - Reconfigure TCP Chimney



14. The *Check folder redirection settings in Group Policies* box appears. If folder redirection is used, the default permissions prevent Axcient from backing up the redirected folders. This step checks the permissions of redirected

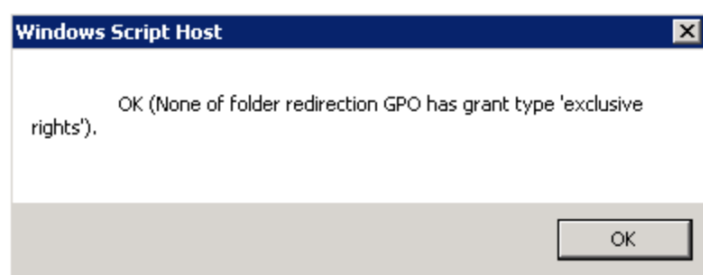
folders and returns one of the following messages:

- OK (None of folder redirection GPO has grant type 'exclusive rights').
- Found at least one folder redirection GPO with grant type 'exclusive rights.' A BACKUP JOB WILL NOT BE ABLE TO COPY FILES FROM THESE DIRECTORIES.

15. The OK message indicates there is no problem (either redirection is not used or the redirected folders have permissions that allow Axcient to back up the folders.) However, if the second message appears, you must change the redirected folder GPO to allow Axcient to back up the redirected folders. The second message includes a link to an Axcient knowledge base (KB) article that describes how to change the redirected folder GPO. Click here to see that article. (A login page may appear because the KB library resides in the password-protected Axcient support portal.)

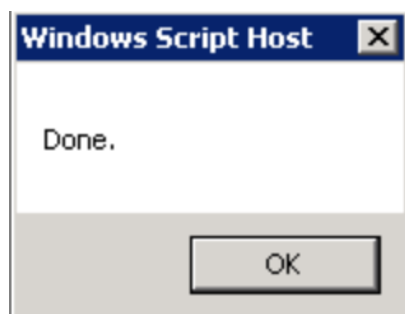
Found at least one folder redirection GPO with grant type 'exclusive rights.' A BACKUP JOB WILL NOT BE ABLE TO COPY FILES FROM THESE DIRECTORIES.

**Figure 174** - Windows Script - Check Folder Redirection Settings



16. A final *Done* box appears. This indicates the script has completed.

**Figure 175** - Windows Script - Enable Firewall Rules



## Autotask Integration

You can optionally integrate with the Autotask PSA tool, which will allow you to configure specific events to publish to the PSA.

Because the UMC is appliance-specific, you will need to log into each appliance to configure settings separately. Alternatively, you can inherit PSA settings already configured through the Axcient Web Application (RMC) . For more information, please reference the [Axcient Business Recovery Cloud Protection Guide](#).

If Autotask has already been integrated successfully, please continue to the [How to Configure Alerting](#) section for more information on how to configure specific events to publish to the PSA tool.


To integrate Autotask on the UMC:

1. On the UMC, click the **System** tab on the top navigation menu.
2. On the left navigation menu, click the **PSA** option. The *PSA* page displays.
3. Optionally, on the *PSA* page, click the **Inherit PSA Configuration Info from RMC** checkbox to inherit PSA settings already configured through the Axcient Web Application (RMC) . For more information, please reference the [Axcient Business Recovery Cloud Protection Guide](#).
4. Alternatively, on the *PSA* page, select **Autotask** from the drop-down menu and click the **Configure PSA Tool** button.
5. Enter the following information:
  - In the *Username* field, enter the **username** used to log in to the administrating Autotask account.
  - In the *Password* field, enter the **password** used to log in to the administrating Autotask account.
  - In the *Confirm Password* field, confirm the **password** entered in the *Password* field.
  - In the *Account ID* field, enter the **Account ID** of the target Client site. This is automatically generated when creating an Account in autotask. For instructions on how to obtain the Account ID, please refer to the [How to Obtain the Account ID](#) section below.
  - In the *Queue ID* field, enter the **Queue ID** for the appropriate Service Desk Queue. This will bundle similar tickets to help the person monitoring quickly respond and resolve issues. For instructions on how to obtain the Queue ID, please refer to the [How to Obtain Queue ID](#) section below.
  - In the *Priority* field, enter the **ticket priority** assigned for tickets automatically published to Autotask. Leave this field empty to automatically set the priority to that of default settings in Autotask.
6. Click the **Save** button when you are finished.



Figure 176 - Autotask Configuration Page

**PSA**

 **Autotask Configuration**

Username

Password

Confirm Password

Account ID

Queue ID

Priority

## How to Obtain the Account ID

The Account ID is found in the *Account Details* page of the desired Account. To obtain the Account ID:

1. On the top navigational menu, hover the mouse over the **My...** tab and click **Accounts** under the *CRM* section.
2. Look for the desired Account using the Search field.
3. Click on the desired Account or right-click and select **View Account**.
4. The *Account ID* is located in the left-hand section.

Figure 177 - Autotask Account ID Page

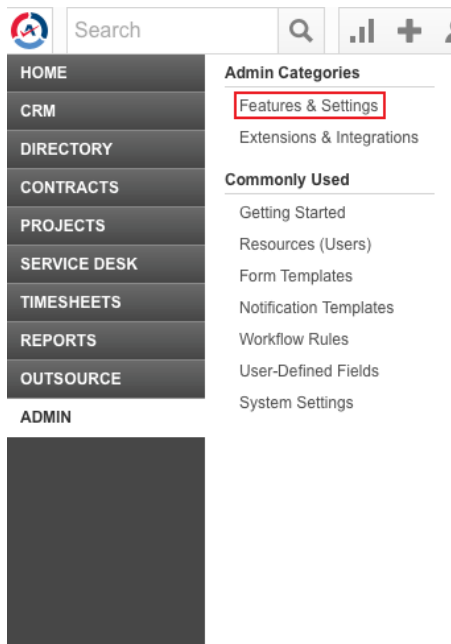
The screenshot displays the Autotask CRM interface. On the left, the 'MY ACCOUNTS' sidebar shows a search field and a list of accounts. A red box highlights the 'Accounts (164)' link in the 'CRM' section. A right-click context menu is open over the 'Anchor Network Solutions' account, with 'View Account' highlighted. The main area shows the 'ACCOUNT - Anchor Network Solutions (ID: 30243651) | Active Customer' page. The 'Account ID' is displayed as 30243651. The page also shows account details such as 'Account Manager: Steve Perry', 'Territory Name: asia', and 'Status: Active'.

## How to Obtain the Queue ID

The Queue ID is found in the *Queue Details* page of the desired Service Desk Queue, located in the *Features & Settings* section. To obtain the Queue ID:

1. On any page, hover the mouse over the Autotask 'A' logo to bring up the drop-down menu. Hover the mouse over the **Admin** option and then click the **Features & Settings** option.

**Figure 178** - Autotask Features & Settings Option



2. Expand the *Service Desk (Tickets)* section and click the **Queues** option.

Figure 179 - Autotask Service Desk Queues Option

Features & Settings

Extensions & Integrations

Expand All

Collapse All

+ APPLICATION-WIDE (SHARED) FEATURES

+ YOUR ORGANIZATION

+ RESOURCES/USERS (HR)

+ ACCOUNTS & CONTACTS

- SERVICE DESK (TICKETS)

**Queues**  
Set up the folders that will contain tickets with similar characteristics, and assign resources to monitor them.

**Sources**  
Set up a list of ways a ticket can enter Autotask, which can be used in workflow rules and reports.

**Task & Ticket Statuses**  
Manage this list of statuses that can be assigned to a ticket.

**Priorities**  
Define the levels of urgency associated with tickets.

**Issue & Sub-Issue Types**  
Set up the issue and sub-issue types that will categorize your tickets for routing, workflow, searching and reporting purposes.

**Service Level Management**  
Create and manage Service Level Agreements.

**Support Email Address**  
Set up a default email address to use as the sender for notification emails from Autotask.

**Ticket Resolution Metrics**  
Configure the section on the Service Desk Dashboard that shows a series of horizontal bar graphs that measure the actual performance of the support team against self-determined goals.

**Summaries**  
Activate/de-activate and re-order the summary metrics that display on the Service Desk Dashboard.

- Right-click the desired Service Desk Queue and click the **Edit Queue Details** option.

**Figure 180** - Click the Edit Queue Details Option

←

SERVICE DESK QUEUES

Set up the folders that will contain tickets with similar characteristics, and assign resources to monitor them.

+ New

Save

Cancel

	Name ^	Description
	Administrative	Administrative
	Anchor HD	Tier 1 Helpdesk Requests
	AutoQueue	
	Autotask Consulting	Autotask Consulting
	CLEP	
	Client Portal	Service Desk
	CSD	CSD
	Helpdesk	Escalated Helpdesk Requests

Edit Queue

Edit Queue Details

Inactivate Queue

Delete Queue

- The Queue ID is located in the *Queue Summary* page that appears.

**Figure 181** - Autotask Queue ID Location

<https://ww2.autotask.net/autotask/popups/administration/QueueDetails.aspx?objectId=29878555&type=queue>

QUEUE SUMMARY

Save & Close

Cancel

Summary

Resources

Queue Name\*

Anchor HD

☒ Active

Queue Location\*

British Columbia

+

Queue Number

29878555

Queue Description

Tier 1 Helpdesk Requests

☒ Appears in Client Portal

When this is not checked, tickets in this queue will not display in the Client Portal

Queue Location

British Columbia

## ConnectWise Integration

You can optionally integrate with the ConnectWise PSA tool, which will allow you to configure specific events to publish to the PSA.

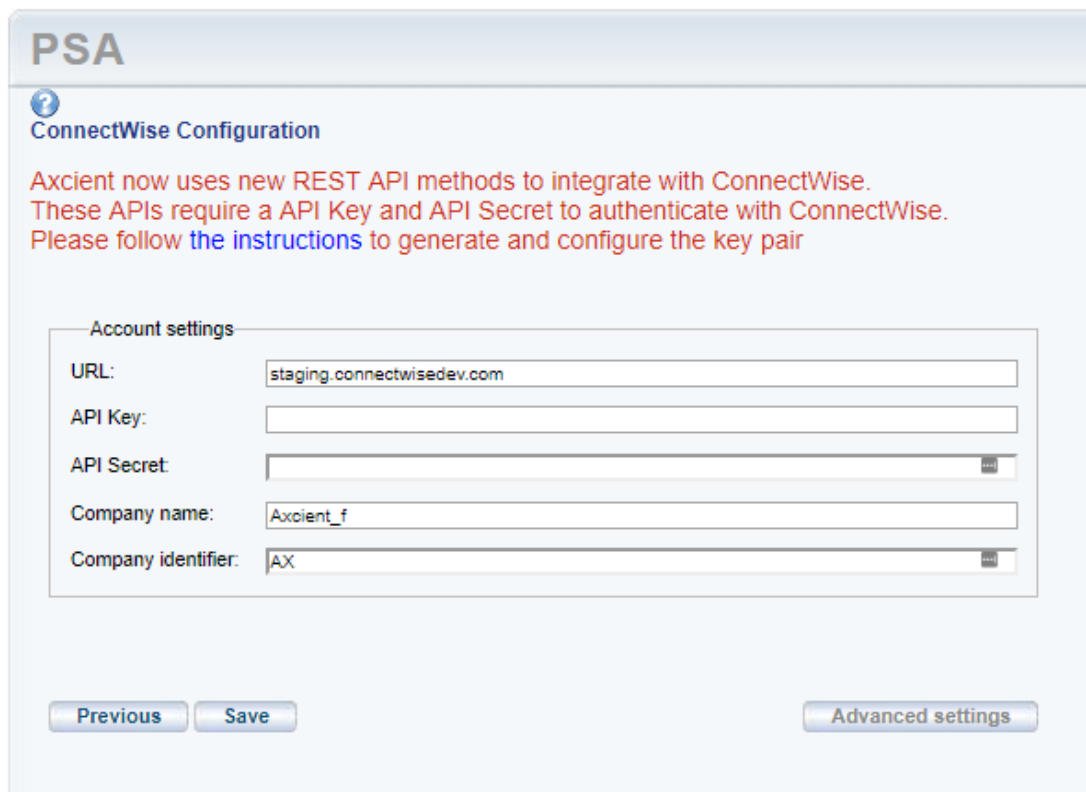
Because the UMC is appliance-specific, you will need to log into each appliance to configure settings separately. Alternatively, you can inherit PSA settings already configured through the Axcient Web Application (RMC). For more information, please reference the [Axcient Business Recovery Cloud Protection Guide](#).

If ConnectWise has already been integrated successfully, please continue to the [How to Configure Alerting](#) section for more information on how to configure specific events to publish to the PSA tool.

To integrate ConnectWise with the UMC:

1. On the UMC, click the **System** tab in the top navigation menu.
2. On the left navigation menu, click the **PSA** option. The *PSA* page displays.
3. Optionally, on the *PSA* page, click the **Inherit PSA Configuration Info from RMC** checkbox to inherit PSA settings already configured through the Axcient Web Application (RMC) .
4. Alternatively, on the *PSA* page, select **ConnectWise** from the drop-down menu and click the **Configure PSA Tool** button.
5. Enter the following information:
  - In the *URL* field, enter the **domain** portion of the address used to access ConnectWise. Enter the URL as illustrated in the following example:
    - **Correct** - *connectwise.com*
    - **Incorrect** - *www.connectwise.com*
    - **Incorrect** - *http://connectwise.com*
  - In the *API Key* field, enter the **public API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
  - In the *API Secret* field, enter the **private API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
  - In the *Company Name* field, specify your **company name**. For more information on how to obtain the company name, please refer to the [Obtain Login Information](#) section.
  - In the *Company Identifier* field, enter the appropriate **Client ID number**. For more information on how to obtain the ID, please refer to the [Obtain Client Information](#) section.
  - Optionally, to configure advanced settings, click the **Advanced Settings** button and update all appropriate fields.
6. Click the **Save** button.

Figure 182 - ConnectWise Configuration Screen in UMC



The image shows a web-based configuration screen for PSA (Professional Services Automation) integration with ConnectWise. The screen has a light blue header with the text "PSA". Below the header, there is a section titled "ConnectWise Configuration" with a question mark icon. A red text block explains that Axcient now uses new REST API methods for integration and provides instructions on where to find API keys and secrets. The main part of the screen is a form titled "Account settings" containing five input fields: "URL" (pre-filled with "staging.connectwisedev.com"), "API Key" (empty), "API Secret" (empty with a toggle for visibility), "Company name" (pre-filled with "Axcient\_f"), and "Company identifier" (pre-filled with "AX" and a toggle for visibility). At the bottom, there are three buttons: "Previous", "Save", and "Advanced settings".

**PSA**

**ConnectWise Configuration**

Axcient now uses new REST API methods to integrate with ConnectWise. These APIs require a API Key and API Secret to authenticate with ConnectWise. Please follow [the instructions](#) to generate and configure the key pair

**Account settings**

URL:

API Key:

API Secret:

Company name:

Company identifier:

## ConnectWise Appendix

As part of the ConnectWise integration process, you will need to complete a set of basic configuration tasks within the ConnectWise platform.

This section of the guide outlines basic configuration tasks that take place within the ConnectWise platform. As a best practice, however, we recommend referencing ConnectWise documentation for complete configuration steps.



## Obtain the API Key

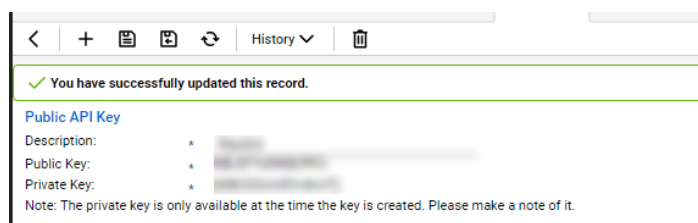
You can obtain API information within the ConnectWise service. For the purposes of integrating ConnectWise with the Axcient protection solution, you will need to create a new API key.

To create a new API key:

1. Log in to ConnectWise and open the *System* menu.
2. In the *System* menu, click the **Members** link.
3. In the *Members* page, click the **API Members** tab and then click the **plus icon** to create a new API Member.
  - In the *Member ID* field, enter **Axcient**.
  - In the *Role ID* field, make sure the role is configured with Add, Update, and Close tickets.
  - Click the **Save** button *but do not close the window*. After you click the **Save** button, you will be given access to the *API Keys* tab.
4. Click the **API Keys** tab and then click the **plus icon** to create a new API key.
  - In the *Description* field, type **Fusion**.
  - Click the **Save** button *but do not close the window*.
  - Record the *public key* and *private key* before you close the window. You will not be able to view the private key again after this window is closed.

The image below details the location of the *public key* and *private key fields* (API Secret).

**Figure 183** - ConnectWise API Key Screen



## Obtain Login Information

ConnectWise login information is created when first setting up the ConnectWise service. For the purposes of integrating ConnectWise with the Axcient protection solution, you will need to enter the login information used to connect to ConnectWise.

The image below details the location of the *URL*, *Username*, *Password*, and *MSP Company ID* field values.

**Figure 184** - ConnectWise Login Screen



The image shows the ConnectWise login interface. At the top left is the ConnectWise logo. Below it are four input fields: 'Site' with the value 'staging.connectwisedev.com', 'Company' with the value 'Axcient\_f', 'User Name' with the value 'admin1', and 'Password' with masked characters '\*\*\*\*\*'. Below the password field is a blue 'Login' button. To the right of the button are three links: 'Forgot your password?', 'Clear Cache', and 'About'.

## Obtain Client Information

To obtain the Client information required to finish integrating ConnectWise, you will first need to create a new Company Account for the target Client site. Please refer to [online ConnectWise support](#) for instructions on how to create a Company Account.

To obtain the required Client Company information:

1. Log in to ConnectWise.
2. On the left-hand navigation menu, expand the *Companies* tab and click the **Companies** option. The *Company Search* page displays.
3. In the *Company Name* field, enter the **name of the target company**.
4. Select the target **Company** that was entered in the *Search* field and note the following information:
  - Company address information, including *Address Line 1 and 2*, *City*, *State*, and *Zip*.
  - The *Territory* field, which corresponds to the *Location* field in the Axcient Web App.

- The *Company ID* field, which corresponds to the *Company ID* field in the Axcient Web Application.

**Figure 185** - ConnectWise Company Screen

ArtSpace

Company Notes Contacts Opportunities Tracks Activities Service Projects Agreements Documents Profile Surveys Sites Team Options Configuration

Company: ArtSpace

Company: \* ArtSpace Site: Main

Phone: 250 3rd Avenue North

Fax: Minneapolis, MN 55401

Web Site: http://www.artspaceusa.org

Company Details

Type: \* Customer Company ID: \* ArtSpace

Status: \* Active Market:

Territory: Clearwater Office Date Acquired: Wed 11/29/2006

Primary Contact

Name: Gary Email: will@artspaceprojects.org

Title:

Phone: (612) 333-9012 Type:

Relationship:

## Obtain Service Type and Subtype

The Service type and subtype are determined by the ConnectWise user account. This ConnectWise account is associated with a specific Service Board which must be configured as needed by the administrative user. For more information regarding Service Boards, please refer to [online ConnectWise support](#).

This section will guide you on how to find ConnectWise field values; however, it is your responsibility to determine which values to enter in the ConnectWise configuration screen in the Axcient Web App.

To obtain ConnectWise field information:

1. On the left-hand navigation menu, click **System** and then select **Setup Tables**.
2. In the *Table* column, enter **Service Board** in the *search* field and press the **Enter** key.
3. Click the **Service Board** option.
4. On the *Service Board List* screen, click the appropriate **Service Board**.
5. Click the **Types** tab to view a list of *Service Types* that can be used in the ConnectWise configuration screen.

**Figure 186** - ConnectWise Types List

Setup Tables > Service Board List > Type List			
Type List			
Board	Statuses	Types	Subtypes
Items	Auto Templates		
←	+	🔍	Search Clear
Service Type ▲	Default	Request For Change	Inactive ▼
Break-fix			
Proactive			
Reactive			
Roger Pham Type			
Server			
Warranty			

6. Click **Subtypes** tab to view a list of *Service Subtypes* that can be used in the ConnectWise configuration screen.

ConnectWise Subtypes List

Setup Tables > Service Board List > Subtype List

**Subtype List**

Board   Statuses   Types   Subtypes   Items

←   +   Search   Clear

Service Subtype ▲	Types	Inactive
		▼
<u>Roger Pham Subtype</u>	5	
<u>st1</u>	5	
<u>st2</u>	5	

## Obtain Priority

The Service priority is determined by ConnectWise user account. This ConnectWise account is associated with a specific Service Board which must be configured as needed by the administrative user. For more information regarding Service Boards, please refer to [online ConnectWise support](#).

This section will guide you on how to find ConnectWise field values; however, it is your responsibility to determine which values to enter in the ConnectWise configuration screen in the Axcient Web App. The priority entered in the ConnectWise configuration screen within the Web App will determine the priority setting for the automatically generated ticket.

To obtain these values:

1. On the left-hand navigation menu, click **System** and then select **Setup Tables**.
2. In the *Table* column, enter **SLA** in the *search* field and press the **Enter** key. Click the **SLA** option.
3. On the *SLA List* screen, select the appropriate **SLA option**.
4. Enter one of the listed values in the *Priority* field in the ConnectWise configuration screen.

**Figure 187** - ConnectWise SLA Screen

Setup Tables > SLA List > SLA

**SLA**

SLA Setup SLA by Priority ⚙️

← + 📄 📋 🗑️

*i* Updated: 6/24/2005 4:14:05 PM by user10

SLA Name:

Based on:

Calendar:

*i* Calendar options are defined in the [Calendar Setup Table](#)

Default? ☒ Use this SLA if no SLA exists for the customer / agreement

SLA Application Order:

**Default Response Matrix:**

	High Urgency	Medium Urgency	Low Urgency
High Impact	Priority 1 - Emergency Respoi	Priority 2 - Quick Response	Priority 3 - Normal Response
Medium Impact	Priority 2 - Quick Response	Priority 3 - Normal Response	Priority 3 - Normal Response
Low Impact	Priority 3 - Normal Response	Priority 3 - Normal Response	Priority 3 - Normal Response

**Default Response Goals:**

Respond within:	<input type="text" value="4.00"/> hours	Goal Percent:	<input type="text" value="80"/>
Plan within:	<input type="text" value="24.00"/> hours	Goal Percent:	<input type="text" value="80"/>
Resolved within:	<input type="text" value="48.00"/> hours	Goal Percent:	<input type="text" value="80"/>

## How to Configure Alerting

You can configure both entire event categories or individual events to publish tickets to a PSA tool through the UMC. This will give you more control over which events should be published to the PSA tool.

You will need to configure the events to publish to the PSA for each appliance.

Once a PSA tool has been configured:

1. On the UMC, click on the **Events** tab in the top navigation menu.
2. On the left navigation menu, click on the **Configure Alerting** option.
3. On the *Alerting* page, select the alerts types that should be publish to the PSA tool.

Events are sorted into specific event categories:

- 1** Configure all events under a specific category by checking the **Publish to PSA Tool** box next to the primary event category.
- 2** Configure specific events to publish to the PSA tool by expanding the event category, and checking the **Publish to PSA Tool** box for the specific event. Be aware that the *Publish to PSA Tool* box next to the primary event category will be checked even though only specific events have been selected. This is to help you quickly find where events have been configured to publish to the PSA tool.

You can come back and reconfigure which events are published to the PSA tool at any time.

**Figure 188 - Event Alerting Page**

# alerting

Bare Metal Restore Lock Events

visible in log

publish to psa tool

notify someone

BMR image-lock FAILED

visible in log

publish to psa tool

notify someone

BMR image-lock info

visible in log

publish to psa tool

notify someone

BMR image-lock started

visible in log

publish to psa tool

notify someone

BMR image-lock SUCCEEDED

visible in log

publish to psa tool

notify someone

BMR image-lock warning

visible in log

publish to psa tool

notify someone

Bare Metal Restore Unlock Events

visible in log

publish to psa tool

notify someone

BMR image-unlock FAILED

visible in log

publish to psa tool

notify someone

BMR image-unlock info

visible in log

publish to psa tool

notify someone

BMR image-unlock started

visible in log

publish to psa tool

notify someone

BMR image-unlock SUCCEEDED

visible in log

publish to psa tool

notify someone

BMR image-unlock warning

visible in log

publish to psa tool

notify someone

Device Events

visible in log

publish to psa tool

notify someone

Exchange Mailbox Backup Events

visible in log

publish to psa tool

notify someone

Exchange Mailbox Restore Events

visible in log

publish to psa tool

notify someone

Export Copy Events

visible in log

publish to psa tool

notify someone

Network Events

visible in log

publish to psa tool

notify someone

Offsite Backup Events

visible in log

publish to psa tool

notify someone

Offsite DAS Copy Events

visible in log

publish to psa tool

notify someone

Onsite Backup Events

visible in log

publish to psa tool

notify someone

Restore Events

visible in log

publish to psa tool

notify someone



## Access BMR Utilities

BMR utilities (except the memory test) are accessed from the BMR utilities page. To access this page, select the **Utils/Tools** option on the BMR boot login page. The utilities page includes the following menu options:

- **Manually partition disk**—Starts the Disk Partitioner utility that allows you to partition the target device before restoring that device (see [Disk Partitioning Utility](#) section).
- **Un-identified device explorer**—Starts the UDI utility that allows you to identify unknown components on the target devices (see [Unknown Device Identifier Utility](#) section).
- **DOS Window**—Provides a DOS window for command line access.
- **Return**—Returns to the BMR Recovery Disk CD login page.

Figure 189 - BMR Utilities Page



## Memory Test Utility

The Memtest 86 utility checks the physical memory in the device. If the message *Pass complete, no errors* appears at the bottom of the page after completing 100% of the tests, the device can be used for BMR. If any of the memory is not good, this device cannot be used for BMR.

Unlike the other utilities that you access from the BMR Utilities page, this utility must be selected from the initial BMR boot page:

- To start the test, select the **memtest86** option on the initial BMR boot page, and click the **Enter** key. The *Memtest 86* page appears and the test starts automatically.
- To return to the initial BMR Recovery Disk CD page, press the **Esc** key.

Figure 190 - Memtest86 Utility

```

Memtest-86 v3.5 : Pass 65% #####
Intel Core 2 1995 MHz : Test 35% #####
L1 Cache: 32K 32700 MB/s : Test #8 [Modulo 20, Random pattern]
L2 Cache: 2048K 14997 MB/s : Testing: 200K - 260M 260M Using CPU:0
L3 Cache: None : Pattern: 6af18c06-17
Memory : 260M 9778 MB/s :-----
Chipset : Intel i440BX

Time: 0:07:49 Cached: 260M Test_Sel: Std Pass: 1
MemMap: e820 Iter: 6 CPU_Sel: Single Errors: 0
Rsvd_Mem: 4K Act_CPUs: 1 ECC_Mem: off ECC Err: 0

Pass complete, no errors, press Esc to exit

```

## Disk Partitioning Utility

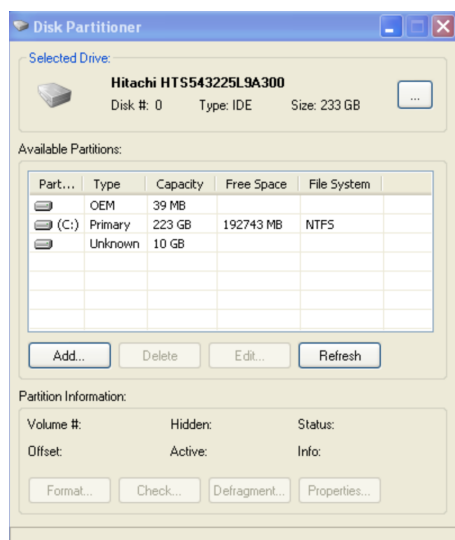
**IMPORTANT!** This utility is available for 32-bit systems only.

The Disk Partitioner utility can reconfigure the partition table on the target device. Use this utility if you want to change the target device partitions before performing a BMR restore on that device.

To change the partitions on the target device:

1. From the *BMR utilities* page (see [Access BMR Utilities](#) section), select the **Manually partition disk** option.
2. The *Disk Partitioner Utility* window appears. To select a drive to partition, click the **ellipsis (...)** button in the upper right.

Figure 191 - Disk Partitioner Utility



3. The *Select Hard Disk* window appears. Select a drive from the list and then click the **OK** button. (If any drives are missing from the displayed list, click the **Refresh** button.)

Figure 192 - Select Hard Disk Window



4. In the *Disk Partitioner Utility* window, select the drive and then click the **Add** button.
5. The Create Partition window appears. Do the following in the specified fields:
  - a. **Partition Size (MB)** - Enter the size (in MBs) of the partition.
  - b. **Partition Type** - Select the type of partition from the pull-down list. Select Primary for a bootable device or Secondary for a non-bootable device.

- c. **Assign Letter Drive** - Select the drive letter to assign from the pull-down list.
- d. Click the **OK** button to create this partition in the table.

**Figure 193** - Create Partition Window



6. Repeat *Step 4* and *Step 5* to create additional partitions. (Click the **Refresh** button to update the current list.)
7. To change existing partitions, do the following in the *Disk Partitioner* window and follow instructions on the page:
  - To delete a partition, select the drive, and click the **Delete** button.
  - To resize a partition, select the drive, and click the **Edit** button.

When you select a drive in the Disk Partitioner Utility window, four additional buttons become active at the bottom of the page: format, check, defragment, and properties. The utility will perform these actions, but they are irrelevant at this point because the disk will be reformatted as part of the BMR restore process.

## Unknown Device Identifier Utility

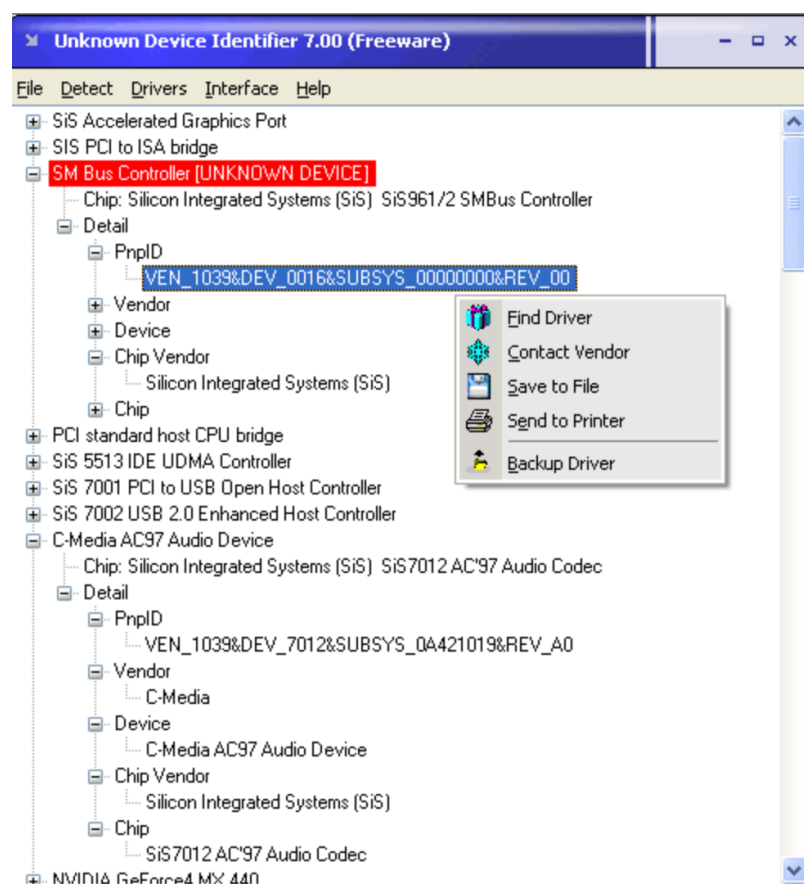
**IMPORTANT!** This utility is available for 32-bit systems only.

If the BMR Recovery Disk CD does not include all required device drivers, you must download the missing drivers. If you know the device make and model, you can search the web using that information to locate and download the required drivers. However, if there are unknown components, you can use the Unknown Device Identifier utility to determine the identity of those components. Use this utility if you get an error message such as “Cannot enable network interface. Please load appropriate driver” and you do not know what driver to download.

To identify unknown devices:

1. From the BMR utilities page (see [Access BMR Utilities](#) section), select the Un-identified device explorer option.
2. The *Unknown Device Identifier* window appears. Search through the tree view of devices, and record the name of the components in question.
3. Search the web for the appropriate drivers using the obtained component information, and download those drivers. (Although the utility includes a download option, it is unlikely to work in this instance.)

Figure 194 - UDI Utility

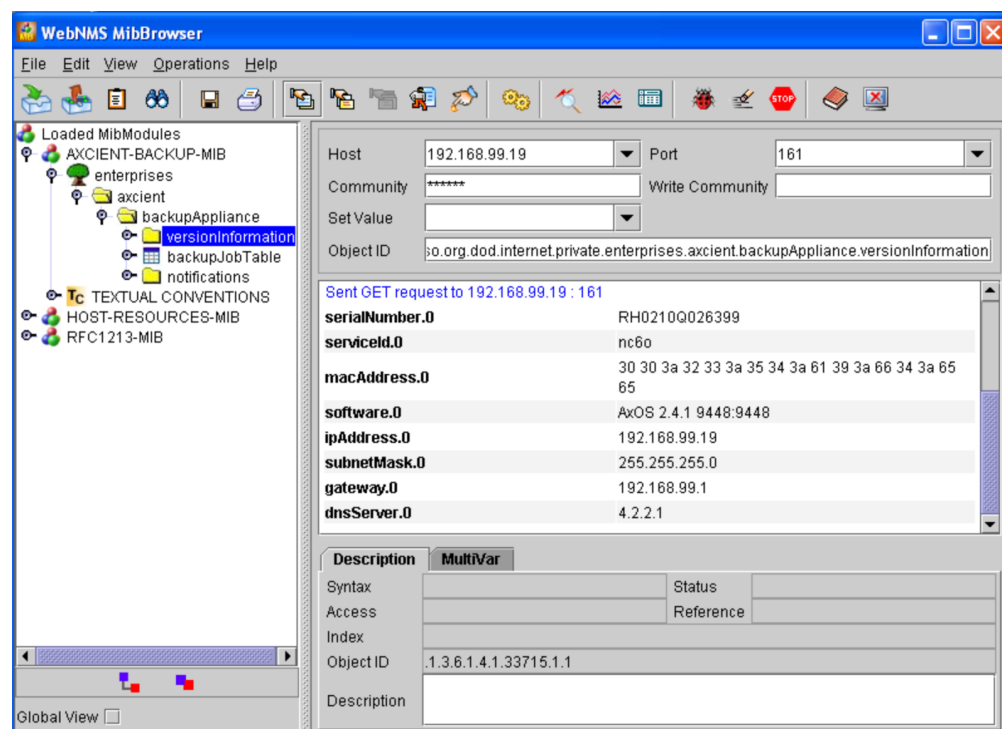


# SNMP View MIB Information

## Version Information

The Axcient MIB provides version information relevant to the Axcient appliance. This is the same version information that is displayed in the User Dashboard (see [Version Information Panel](#) section). The figure below displays the version information as seen through the WebNMS MibBrowser. The left side displays the selected section from the Axcient MIB (**enterprises > axcient > backupAppliance > versionInformation**), and the right side displays the results. The table below describes each of the version fields.

Figure 195 - MIB Browser - Version Information



## Axcient MIB Fields - Version Information

Name (OID)	Description
<i>serialNumber</i> (.1.3.6.1.4.1.33715.1.1.1.0)	Displays the unique serial number assigned to this Axcient appliance.
<i>serviceld</i> (.1.3.6.1.4.1.33715.1.1.2.0)	Displays the unique service identification number assigned by the RMC to this Axcient appliance.
<i>macAddress</i> (.1.3.6.1.4.1.33715.1.1.3.0)	Displays the Media Access Control (MAC) address for the network interface card (NIC).
<i>software</i> (.1.3.6.1.4.1.33715.1.1.4.0)	Displays the version of the software running on the Axcient appliance.
<i>ipAddress</i> (.1.3.6.1.4.1.33715.1.1.5.0)	Displays the IP address of the Axcient appliance.
<i>subnetMask</i> (.1.3.6.1.4.1.33715.1.1.6.0)	Displays the IP address of the Axcient appliance.
<i>gateway</i> (.1.3.6.1.4.1.33715.1.1.7.0)	Displays the IP address of the main gateway used by the Axcient appliance.
<i>dnsServer</i> (.1.3.6.1.4.1.33715.1.1.8.0)	Displays the IP address of the DNS server used by the Axcient appliance.

## SNMP Backup Jobs Information

The Axcient MIB provides information about (1) each defined backup job in the Axcient appliance and (2) the results from the last successful run of each job. (Unsuccessful backup job runs are not reported through the MIB.)

The figure below displays backup job information as seen through the WebNMS MibBrowser. In this example, the first three jobs—Offsite Backup, Alert Digest, and Usage History—are internally generated jobs for those functions. The remaining four jobs were created by a user. There are over 40 fields of information about the backup jobs, and this MIB viewer displays five at a time with a scroll bar to display the other fields. The table below describes the backup job fields available through the MIB. The fields are grouped into two sections:

- **Job Information** - The first 20+ fields provide information about the backup job.
- **Results Information** - The remaining fields provide results from the last successful run of the backup job.

Figure 196 - MIB Browser - Version Information

jobName	jobBackupType	jobsEnabled	jobScheduleSum...	jobStartHour
OffSite Backup	offsite(51)	true(1)	Daily at 2:16 PM on SuM...	14
Alert Digest	emailAlertDigest(77)	true(1)	Daily at 6:00 AM on SuM...	6
Usage History	history(61)	true(1)	Daily at 6:30 AM on SuM...	6
testsh	hourly(1)	true(1)	Hourly from 12:00 AM - 1...	0
Server Alive	hourly(1)	true(1)	Hourly from 3:00 AM - 7...	3
foreign, acl	hourly(1)	true(1)	Hourly from 12:00 AM - 1...	0
Exchange Mailboxes	daily(2)	true(1)	Daily at 7:00 PM on MoT...	19

### Axcient MIB Fields - Backup Job Information

Name (OID)	Description
<i>jobId</i> (.1.3.6.1.4.1.33715.1.2.1.1)	Displays the internal identifier assigned to the job.
<i>jobName</i> (.1.3.6.1.4.1.33715.1.2.1.2)	Displays the name of the job.
<i>jobBackupType</i> (.1.3.6.1.4.1.33715.1.2.1.3)	Displays the type of backup job. In most cases, this refers to the scheduled frequency for the job. The non-frequency types are as follows: <ul style="list-style-type: none"> <li>• <b>cdp</b> - reserved for future use</li> <li>• <b>onetime</b> - on-demand job</li> <li>• <b>offsite</b> - offsite job, which is an internal job type (see <a href="#">Schedule Cloud Backup Job</a> section)</li> <li>• <b>history</b> - usage history, which is an internal job type</li> </ul>

Name (OID)	Description
	<ul style="list-style-type: none"> <li><b>qos</b> - bandwidth throttling job, which is an internal job type (see <a href="#">Set Bandwidth Usage (Quality of Service)</a> section)</li> <li><b>emailAlertDigest</b> - job to e-mail a digest of alerts, which is an internal job type (see <a href="#">Configure Event Notification</a> section)</li> </ul>
<i>jobScheduleSummary</i> (.1.3.6.1.4.1.33715.1.2.1.5)	Displays when this job is scheduled to run in the following form: <ul style="list-style-type: none"> <li><b>frequency</b> - hourly, daily, weekly, monthly, yearly</li> <li><b>start</b> time - time such as 6:30 AM or 7:00 PM. For hourly jobs the interval ("every X hours") is also included.</li> <li><b>days</b> - The days the week, month, or year are listed. For example the standard five-day work week is listed as "MoTuWeThFr"</li> </ul>
<i>jobStartHour</i> (.1.3.6.1.4.1.33715.1.2.1.6)	Displays the hour the job is scheduled to start.
<i>jobStartMinute</i> ("1.3.6.1.4.1.33715.1.2.1.7)	Displays the minute (within the start hour) the job is scheduled to start.
<i>jobLastBackupResult</i> (.1.3.6.1.4.1.33715.1.2.1.8)	Displays whether the last job run succeeded. An "empty" value means the job has never been run.
<i>jobLastSucceedBackup</i> (.1.3.6.1.4.1.33715.1.2.1.10)	Displays the last time this job was run successfully.
<i>jobStatus</i> (.1.3.6.1.4.1.33715.1.2.1.11)	Displays the current status of the job (running, not running, or waiting-to-run). Waiting-to-run applies to offsite jobs only.
<i>jobEveryHours</i> (.1.3.6.1.4.1.33715.1.2.1.12)	Displays how frequently an hourly job is to run. Hourly jobs can be every hour (1), every other hour (2), every third hour (3), and so on.
<i>jobEndHour</i> (.1.3.6.1.4.1.33715.1.2.1.13)	Displays the hour in the day an hourly job is scheduled to stop using a 24-hour clock (0-23). For example, if an hourly job is scheduled to run from 8:00am to 5:00pm, the end hour value is 17 (5:00pm).
<i>jobEndMinute</i> (.1.3.6.1.4.1.33715.1.2.1.14)	Displays the end minute (within the final hour) for the last time a repetitively scheduled job will run.
<i>jobDayOfMonthOrYear</i> (.1.3.6.1.4.1.33715.1.2.1.15)	Displays the day of the month or year when the backup job is scheduled to run. Applies to monthly or yearly jobs only.
<i>jobsOffsite</i> (.1.3.6.1.4.1.33715.1.2.1.16)	Displays whether this is an offsite job.
<i>jobRetentionMethod</i> (.1.3.6.1.4.1.33715.1.2.1.17)	Displays the backup frequency interval (such as hourly or daily) specified for this job. This interval is used in determining the retention period.
<i>jobRetentionLength</i> (.1.3.6.1.4.1.33715.1.2.1.18)	Displays the amount of time the job will be retained. The value is in the units listed for jobRetentionMethod (previous field). For example, if the retention method value is week and the length value is 52, the retention period is a year (52 weeks).
<i>jobUserCreator</i> (.1.3.6.1.4.1.33715.1.2.1.19)	Displays the name of the UMC user who created this job (see <a href="#">Manage Users</a> section).
<i>jobDeviceUser</i> (.1.3.6.1.4.1.33715.1.2.1.20)	Displays the name of the administrative user for the target device (see <a href="#">Add a Device</a> section).
<i>jobDeviceAddress</i> (.1.3.6.1.4.1.33715.1.2.1.21)	Displays the IP address or host name of the device being backed up.
<i>jobDeviceOsType</i> (.1.3.6.1.4.1.33715.1.2.1.22)	Displays the type of operating system specified for the device (see <a href="#">Add a Device</a> section).

## Axcient MIB Fields - Backup Job Results Information

Name (OID)	Description
<i>jobRsItId</i> (.1.3.6.1.4.1.33715.1.2.1.24)	Displays the unique internal identifier of this job run.
<i>jobRsItStartTime</i> (.1.3.6.1.4.1.33715.1.2.1.25)	Displays the date and time the job run started.
<i>jobRsItEndTime</i> (.1.3.6.1.4.1.33715.1.2.1.26)	Displays the date and time the job run ended.
<i>jobRsItElapsedTime</i> (.1.3.6.1.4.1.33715.1.2.1.27)	Displays the duration (elapsed time) of the job run in hours, minutes, and seconds.
<i>jobRsItSourceFiles</i> (.1.3.6.1.4.1.33715.1.2.1.28)	Displays the number of source files found on the target device that need backing up.



Name (OID)	Description
jobRsltSourceFilesSize (.1.3.6.1.4.1.33715.1.2.1.29)	Displays the size of the source files (from the previous field).
jobRsltNewFiles (.1.3.6.1.4.1.33715.1.2.1.30)	Displays the number of files backed up. Source files that were previously backed up and had not changed are not included in this count.
jobRsltNewFilesSize (.1.3.6.1.4.1.33715.1.2.1.31)	Displays the size of the files backed up (from the previous field).
jobRsltDeletedFiles (.1.3.6.1.4.1.33715.1.2.1.32)	Displays the number of files that were deleted since the last backup run.
jobRsltChangedFiles (.1.3.6.1.4.1.33715.1.2.1.33)	Displays the number of files that were modified since the last backup run.
jobRsltChangedFilesSize (.1.3.6.1.4.1.33715.1.2.1.34)	Displays the size of the modified files (from the previous field).
jobRsltChangedMirrorSize (.1.3.6.1.4.1.33715.1.2.1.35)	Displays the size used to change the mirror copy.
jobRsltIncrementFiles (.1.3.6.1.4.1.33715.1.2.1.36)	Displays the total number of increment files (files created to track version changes).
jobRsltIncrementFilesSize (.1.3.6.1.4.1.33715.1.2.1.37)	Displays the size of the increment files (from the previous field).
jobRsltTotalDestinationSizeChange (.1.3.6.1.4.1.33715.1.2.1.38)	Displays the amount the complete backup changed in size from the previous backup run.  <b>Note:</b> In the case of a mailbox job, this value might not change (display a value of “0”) even when the data changes because a mailbox job is saved as a blob file that never decreases in size. Deleting data does not decrease the file size; it simply leaves “empty” (available) space in the blob file that new data can fill. The file will not increase in size until the empty space is filled.
jobRsltErrors (.1.3.6.1.4.1.33715.1.2.1.39)	Displays the number of errors detected during the backup job.
jobRsltIsValid (.1.3.6.1.4.1.33715.1.2.1.40)	Displays whether the backup job run was successful. Because only successful runs are reported, this value is always “true”.
jobRsltSentToDc (.1.3.6.1.4.1.33715.1.2.1.41)	Displays whether the backup job results were successfully reported to the Axcient data center.
jobRowStatus (.1.3.6.1.4.1.33715.1.2.1.42)	Displays the standard SNMP row status value. This value is always “active”.
jobHoursSinceLastBackup (.1.3.6.1.4.1.33715.1.2.1.43)	Displays the number of hours since the last run of this job (either successful or unsuccessful).
jobHoursSinceLastSucceedBackup (.1.3.6.1.4.1.33715.1.2.1.44)	Displays the number of hours since the last successful run of this job.
jobIsRefresh (.1.3.6.1.4.1.33715.1.2.1.45)	Displays whether the backup job run is for a refresh, which updates the “current” image. This applies to image jobs only (see <a href="#">Back Up System Images</a> section).

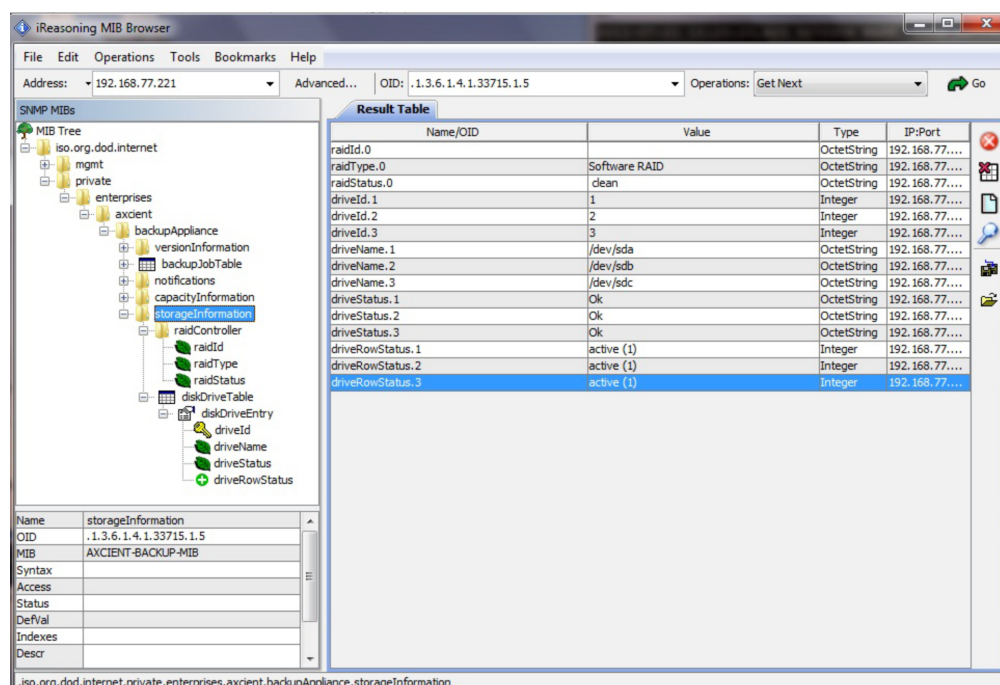
## Storage and Capacity Information

The Axcient MIB provides storage (RAID and drive status) and capacity (onsite and offsite free and used disk space) information. The tables below describes the storage and capacity fields available through the Axcient MIB.

The figure below displays the storage information as seen through the iReasoning MIB Browser. The left side displays the selected section from the Axcient MIB (**enterprises > axcient > backupAppliance > storageInformation**), and the right side displays the results. In this example the results include the RAID and disk information from three drives.

**NOTE-** These fields are available when running SNMP version 2 only (not version 1).

**Figure 197** - MIB Browser - Storage Information



### MIB Fields - Capacity Information

Name (OID)	Description
<i>onsiteStorageUsed</i> (.1.3.6.1.4.1.33715.1.4.1.0)	Displays total storage space used on the Axcient appliance.
<i>onsiteStorageFree</i> (.1.3.6.1.4.1.33715.1.4.2.0)	Displays total storage space available on the Axcient appliance.
<i>offsiteStorageUsed</i> (.1.3.6.1.4.1.33715.1.4.3.0)	Displays the space used in the Axcient data center (offsite) to store backup jobs from this Axcient appliance.
<i>runningVMs</i> (.1.3.6.1.4.1.33715.1.4.4.0)	Displays the number of VMs currently running on the appliance.

### MIB Fields - Storage Information

Name (OID)	Description
<i>raidId</i> (.1.3.6.1.4.1.33715.1.5.1.1.0)	Displays the RAID identification number. Axcient uses either RAID 1 or RAID 5 depending on the appliance model type.
<i>raidType</i> (.1.3.6.1.4.1.33715.1.5.1.2.0)	Displays whether this is a hardware or software RAID.

Name (OID)	Description
<i>raidStatus</i> (.1.3.6.1.4.1.33715.1.5.1.3.0)	Displays a RAID health status value. Status values are for either hardware or software RAID implementations as indicated in the previous field.
<i>driveID</i> (.1.3.6.1.4.1.33715.1.5.2.1.1)	Displays an internal drive ID number.
<i>driveName</i> (.1.3.6.1.4.1.33715.1.5.2.1.2)	Displays the drive path and file name.
<i>driveStatus</i> (.1.3.6.1.4.1.33715.1.5.2.1.3)	Displays the drive health status (either OK or failed).
<i>driveRowStatus</i> (.1.3.6.1.4.1.33715.1.5.2.1.4)	Displays the standard SNMP row status value. This value is always “active”.

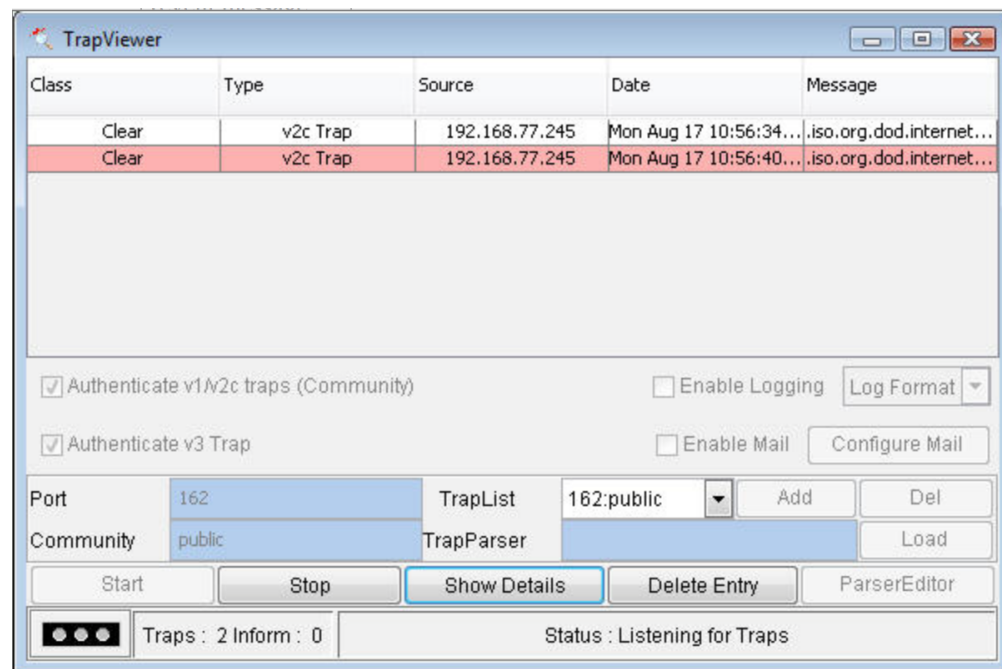
## Event (Trap) Information

The Axcient SNMP implementation supports a trap receiver. The trap events are the same events that appear in the event log (see [Event Logging](#) chapter). The table below describes the event information available through the Axcient MIB. Figures below displays the AdventNet MibBrowser trap viewer with two Axcient events listed. This is an informational event indicating that the admin user logged into the Axcient appliance. Note the severity is *INFO* and the event type is *USER\_LOGIN*. This corresponds to the Axcient event type *USER\_LOGIN*.

MIB Fields - Event (Trap) Information

Name (OID)	Description
BevSeverity (.1.3.6.1.4.1.33715.1.3.1.1.0)	Displays the event severity. This is a derived value from the event type, which often includes a word at the end that indicates severity. For example, the event types <i>BMR_RESTORE_LOCK_FAILED</i> and <i>BMR_RESTORE_LOCK_WARNING</i> have an implicit severity as the last word of the name. This information is parsed, and a severity value of <i>FAILED</i> or <i>WARNING</i> is entered (as appropriate) when one of these event types occurs.
BevEventType (.1.3.6.1.4.1.33715.1.3.1.2.0)	Displays the event type.
BevDate (.1.3.6.1.4.1.33715.1.3.1.3.0)	Displays the event date.
BevUser (.1.3.6.1.4.1.33715.1.3.1.5.0)	Displays the name of the user that generated the event.

Figure 198 - MIB Browser - Trap Viewer



**Figure 199** - MIB Browser - Trap Details

Trap Details	
TimeStamp	0 hours, 16 minutes, 21 seconds.
Enterprise	
Generic Type	
Specific Type	
Message	.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 0 hours, 16 minutes, 21 seconds.: .iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.33715.1.4.2: .iso.org.dod.internet.private.enterprises.axcient.backupAppliance.notifications.backupEventFields.bevSeverity.0: INFO: .iso.org.dod.internet.private.enterprises.axcient.backupAppliance.notifications.backupEventFields.bevEventName.0: USER_LOGIN: .iso.org.dod.internet.private.enterprises.axcient.backupAppliance.notifications.backupEventFields.bevDate.0: 2009-8-17, 10: 55: 47 .1,-8: 0: .iso.org.dod.internet.private.enterprises.axcient.backupAppliance.notifications.backupEventFields.bevMessage.0: login: .iso.org.dod.internet.private.enterprises.axcient.backupAppliance.notifications.backupEventFields.bevUser.0: admin:
Severity	Clear
Entity	192.168.77.245
RemotePort	58011
LocalPort	162
Community	public
Node	192.168.77.245
Source	192.168.77.245
TimeReceived	Mon Aug 17 10:56:40 PDT 2009
HelpURL	0-0.html

## Configuring MIB Browser

To view information about an Axcient appliance in a MIB browser:

1. Install the MIB browser on your computer.
2. Download *the AXCIENT-BACKUP-MIB.txt* file and other standard MIBs if needed (see [Configure SNMP](#) section) to the appropriate folder in the MIB browser. Check the MIB browser documentation for the correct location.
3. Open the MIB browser and connect it to the Axcient appliance by entering the appropriate IP address or host name.

## Required Firewall Ports

ICMP traffic should be allowed for the appliance in any direction.

	Source	Target	Target port	Description
<b>RMC Communication</b>	Appliance	axcient.net (162.245.72.50)	22 tcp	ssh
<b>RMC Communication</b>	Appliance	axcient.net (162.245.72.50)	4022 tcp	ssh aux
<b>Local Backups</b>	Appliance	Windows/Linux device	135 tcp	MS RPC
<b>Local Backups</b>	Appliance	Windows/Linux device	137-138 udp/tcp	SMB
<b>Local Backups</b>	Appliance	Windows/Linux device	139 tcp	SMB
<b>Local Backups</b>	Appliance	Windows/Linux device	445 tcp	CIFS
<b>Local Backups</b>	Windows device	Appliance	10600-10700 tcp	IR/FD replication
<b>Offsite Backups</b>	Appliance	198.73.17.10	22 tcp	Offsite USA
<b>Offsite Backups</b>	Appliance	198.73.17.10	443 tcp	Offsite USA
<b>Offsite Backups</b>	Appliance	198.73.17.10	4000-6000 tcp	Offsite USA
<b>Offsite Backups</b>	Appliance	198.73.23.20	22 tcp	Offsite Canada
<b>Offsite Backups</b>	Appliance	198.73.23.20	443 tcp	Offsite Canada
<b>Offsite Backups</b>	Appliance	198.73.23.20	4000-6000 tcp	Offsite Canada
<b>NTP</b>	Appliance	0.pool.ntp.org	123 udp	NTP
<b>NTP</b>	Appliance	1.pool.ntp.org	123 udp	NTP
<b>NTP</b>	Appliance	2.pool.ntp.org	123 udp	NTP
<b>NTP</b>	Appliance	ntp.ubuntu.com	123 udp	NTP