

The background of the entire page is composed of several large, overlapping, abstract shapes in various shades of orange and red. These shapes are geometric in nature, featuring rounded corners and sharp edges, creating a dynamic and modern visual effect. The colors range from a deep, dark red to a bright, vibrant orange.

Axcient

UMC Best Practices 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

Setup Summary	5
Installation Guidelines	6
Device Guidelines	8
Replication Job Guidelines	11
Image Job Considerations	11
File Job Considerations	13
Additional Job Considerations	14
Initial Backup Strategy	19
Laptop Replication Strategy	21
Appliance Configuration Guidelines	22
System Settings	22
Monitoring Guidelines	29
User Dashboards	29
Reports	32
Event Log and Alerts	35
Troubleshooting	37
Backup Problems	38
Replication Fails Because of VSS Problem	38
Replication Fails Because of Permission Problem	42
Replication Fails Because of Windows Redirection	44
Replication Fails Because of Mount Problem	51
Replication Fails Using Samba	51
Replication Fails Due to Symbolic Links (Windows 7)	51
Replication Hangs After Lost Connection	51
Open Files Not Replicated	52
Files Missing When Creating Replication (XP)	53
Cannot Replicate Windows Encrypted Files	53
Cannot Set On Demand Job Retention Period	53
Not All Active Replication Jobs Running	55
Cloud Replications Are Slow	55
Restore Problems	59
Restoring UNIX Files on Windows Device Fails	59
Restore Fails Using Samba on Mac OS X	59
Cannot Restore to Target Location	59

Cannot Restore Files (Tree View Does Not Expand)	60
Virtual Machine and BMR Problems	61
BMR Fails at Final Boot (Windows 2003)	61
BMR Fails at Final Boot (Active Directory Server)	61
Failover VM Pause Shuts Down Server	61
Exchange not Working in VM	63
Cannot Access Running VM	63
Cannot Log Into Test VM	63
Restored Device Cannot Join Domain (Password Problem)	65
System Problems	66
Cannot Connect to the Web Application	66
System Performance Slows	67
System Time Incorrect	67
Cannot Register Appliance	68
Cloud Progress Bars Do Not Update	71
Appliance Running out of Space	71
Device Problems	73
Cannot Access Device	73
Cannot Add Device	73

Setup Summary

As part of the setup process, you need to complete the following steps, ensuring that you properly configure and maintain your Axcient protection solution:

1. **Analyze protection needs** - You will need to determine how much storage space is required for the locally replicated data, and what protection services are needed. Consider the following:
 - *Number and size of devices to protect* - Determine the number and size (disk space) of devices to protect. This number will dictate data storage needs of the Axcient appliance. It is common to underestimate the amount of data storage space required. While the Axcient protection solution is designed to grow as your needs grow, making a better estimates up front reduces the need and hassle of upgrading in the future.
 - *Type of protection* - Axcient can provide basic replication and protection for nearly any type of device, but it can also provide business continuity for most Windows-based devices and an application-aware mailbox replication option for Exchange servers. The number, scope, and type of replication jobs all affect the capacity and performance requirements needed from the Axcient appliance.
 - *Cloud replication requirements* - Replicating everything to the Axcient Cloud ensures complete disaster and Cloud virtual office protection, but it also means transferring significant amounts of data to the Axcient Cloud on a regular basis. Part of analyzing the protection needs is determining your Cloud requirements.
2. **Install the appliance** - The first task is to install the Axcient appliance at the designated site. Please refer to the [Installation Guidelines](#) section for an overview of steps to ensure a smooth installation process.
3. **Add devices** - The target devices address and credentials must be entered so the appliance can log into, and backup, those devices. Please refer to the [Device Guidelines](#) for more information on ensuring device connections work properly.
4. **Add replication jobs** - It is important to define one or more replication jobs for each protected devices. This will determine when, and what, data is replicated. Please refer to the [Replication Job Guidelines](#) section for more information on factors to consider when creating replication jobs.
5. **Configure appliance** - The appliance can run using all default settings, but it is likely you will want to customize some aspects of the appliance. Please refer to the [Appliance Configuration Guidelines](#) for more information on configuration options.
6. **Monitor progress** - When the Axcient protection solution is configured and running, monitoring operations is an ongoing need. Please refer to the [Monitoring Guidelines](#) for more information on the options available to simplify the monitoring process.

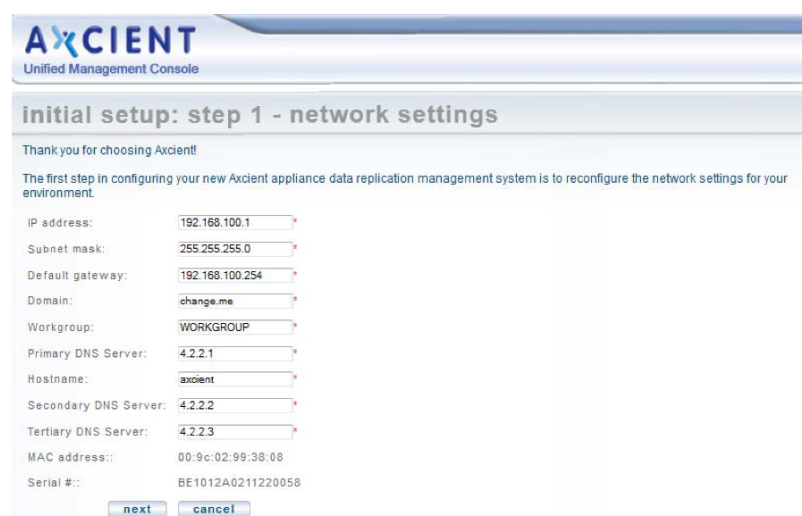
Installation Guidelines

Installing an Axcient appliance is typically a simple task if the network is set up properly. For full instructions, please refer to the [Axcient Installation Guide](#).

Consider the following before installing the appliance:

1. The Axcient appliances comes with predetermined network settings, some of which must be updated for your environment. Before you arrive at the installation network screen, be sure to have the correct values for the IP address, subnet mask, gateway, domain, workgroup, DNS server and hostname. If any of the values entered in this screen are incorrect, the appliance will not work properly.

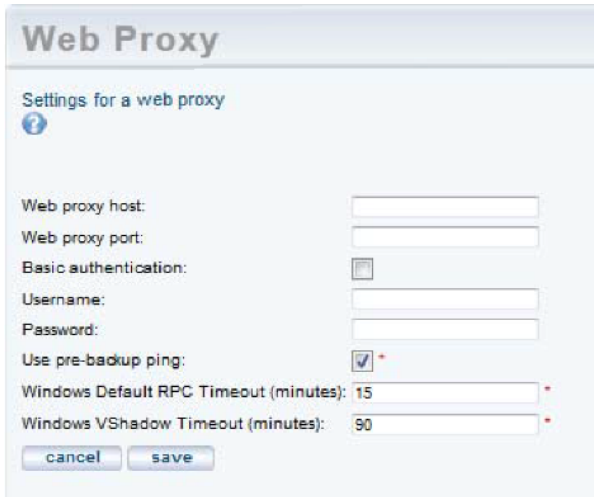
Figure 1 - Initial Setup: Network Settings



The screenshot shows the 'Initial setup: step 1 - network settings' screen of the Axcient Unified Management Console. The interface includes a header with the Axcient logo and a sub-header for the current step. Below the header, there is a message thanking the user for choosing Axcient and explaining that the first step is to reconfigure network settings. A list of network configuration fields follows, each with a text input box and a small red 'x' icon to its right. The fields and their values are: 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), and Serial # (BE1012A0211220058). At the bottom of the form, there are two buttons: 'next' and 'cancel'.

Field	Value
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

2. The Axcient appliance requires access through an internal network to the target devices, and Internet access to an Axcient data center, in order to provide protection. Check the firewall setting to make sure the Axcient appliance has such access. When using a web proxy, configure the Axcient appliance for that proxy server.

Figure 2 - Web Proxy Configuration Screen


Web Proxy

Settings for a web proxy

Web proxy host:

Web proxy port:

Basic authentication: ☐

Username:

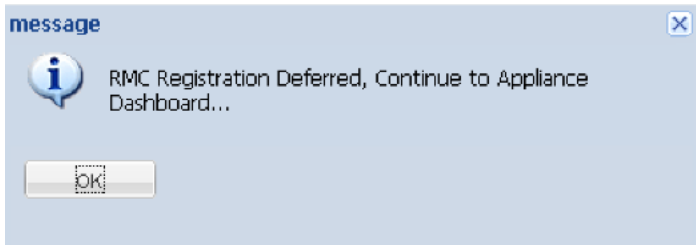
Password:

Use pre-backup ping: ☒

Windows Default RPC Timeout (minutes):

Windows VShadow Timeout (minutes):

3. 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.
4. In order to complete registration, the Axcient appliance must be able to access the Axcient Web Application, which runs in the Axcient data center. If you receive a registration deferred message during installation, see the [Cannot Register Appliance](#) section for possible causes and corrective actions.

Figure 3 - Deferred Registration Message

5. The Integrated Lights Out (ILO) feature can be configured at any time, but we recommend configuring the ILO as part of the initial installation, as enabling ILO requires physical access to the appliance. Please see the [Axcient Integrated Lights Out Guide](#) for full instructions on how to configure the ILO. For additional information, please reference the [iDRAC User Guide](#).

Note: Hard disks on this appliance are encrypted using Cloud Key Management (CKMS). For security reasons, the decryption key is not stored locally. The appliance will attempt to acquire the key during the boot process. Therefore, the appliance must be connected to the Internet when it is powered on. In the event that Internet access is not available, please contact Axcient Support and request a temporary key to unlock the appliance.

Device Guidelines

The Axcient appliance must have proper access to a device in order to protect it. Note the following guidelines when preparing, adding, or updating a device.

- **Enter device credentials** - When adding or updating a device, consider the following:
 - *Hostname or IP* - When using DHCP, it is best to enter a host name rather than an IP address. This will help you avoid needing to edit this field when the IP address changes on the device. Additionally, you must enter a fully qualified host name if the device is not on the same domain as the appliance. Otherwise, just the host name is sufficient.

Fully Qualified Host Name 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 creating a replication job. See the [Laptop Replication Strategy](#) 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`

For example, enter `axcient\admin` instead of just `admin`. In addition, the domain name must be in the Windows domain format (`axcient`), not the DNS format (`axcient.com`)

- *Administrative password* - Administrative passwords are updated periodically; you must remember to update the password in this field or the Axcient appliance will no longer be able to access the device.

Figure 4 - Add Device Screen



The screenshot shows a web-based form titled "add a device". The form 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".
- 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 of the form are two buttons: "cancel" and "save".

- *Enable file sharing* - The file sharing service must be enabled on a device before the Axcient appliance can replicate data. To turn on file sharing, see the appropriate section for the target operating system in the [Cannot Add a Device](#) section.

- *Configure Windows devices* - Because Axcient uses special features on 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. These scripts can be downloaded from the UMC tools page.

Figure 5 - Windows Configuration Scripts

The screenshot shows the 'TOOLS' section of the Axcient UMC interface. It contains a heading 'Tools that support the Axcient protection solution' with a help icon. Below this are three sections: 'Exchange Configuration' with links to download scripts for Exchange 2003, 2007, and 2010; 'VSS Configuration' with a link to download the VSS script; and 'Windows Configuration' with a link to download the Windows script. These three sections are enclosed in a red rectangular box. Below these sections are settings for 'Auto Prune Detection' (checkbox), 'Restore Points Minimum Number' (input field with value 30), 'Backup exceeded time threshold (in hours)' (input field with value 24), and a checkbox for 'Backup will be automatically cancelled if it exceeds the time threshold'. At the bottom are 'cancel' and 'save' buttons.

- *Verify connectivity* - After a device is added, it is a good practice to verify the connection. In the UMC, select the target device and then select the **test access** option. Connectivity access, data access, and control access tests are automatically performed. Device connectivity can be verified at any time.

Figure 6 - Device Test Access

The screenshot shows the 'devices' sidebar on the left with icons for file backup, mailbox backup, image backup, edit device, remove device, and test access. The main panel displays '192.168.99.221 - backup jobs' and 'Test Access Results for device: Large File Testing'. The results show: Connectivity Access: OK, Data Access: OK, and Control Access*: OK. A note at the bottom states: 'Note*: Control Access test is executed for Windows OS only.'

Replication Job Guidelines

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 replication jobs are only compatible with Windows-based devices.

Figure 7 - Image Replication Job Configuration

The screenshot shows the configuration for a backup job titled "172.18.8.14 - image backup". The configuration includes the following settings:

- Schedule name:** TestImage
- 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:, E:, and F: are all selected with checkboxes.
- Backup schedule type:** Daily
- Backup Offsite:** ☐
- Refresh interval:** No Refresh
- Start time:** 19:00 (7:00 PM)
- On these days:** Monday, Tuesday, Wednesday, Thursday, and Friday are selected.
- 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)
- MSSQL DB Password:** (Empty field)
- Allow Axcient to override VSS storage size limit for the duration of backup:** ☒
- Backup scan mode:** Block level scan (fast delta)

A reminder note states: "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)

Image Job Considerations

Image-based replication jobs are utilized by all of Axcient's business continuity and disaster recovery tools and are the primary method of replicating target device data. Consider the following:

- **Schedule type** - Dictates when and how often the replication job runs. The default is an hourly type that runs twice a day, at 8am and 6pm. Weigh the business protection requirements when deciding on the replication job schedule. Running more replication jobs increases storage and performance overhead, while running less does the opposite.
- **Image refresh** - Configure whether to enable the refresh mechanism, which is turned off by default. This creates a current backup image that is updated regularly without the overhead of saving each version (the current version is simply overwritten at each refresh). Enabling refresh is a good strategy for keeping an up-to-date version during business hours.

Retention method - Defines how long to keep old

- versions. Because image jobs replicate everything on a device, retention is usually kept short. The default is one week. Files jobs are often added for data that should be saved for longer periods. If storage space is not an issue, you can save image jobs for longer periods of time. Relatedly, you should also consider whether you want to configure a fixed retention period of use gradual retention. Please refer to the [Additional Job Considerations](#) section for more information.
- **Pre-backup log flushing** - This feature is turned on by default and *should be enabled for SQL databases*. For all other devices, having this feature enabled will not impact replication jobs in any way.

- **Allow Axcient to override VSS storage size limit for the duration of backup** - This feature is turned on by default. When this feature is enabled, Axcient will reset the VSS storage size for the duration of the backup to *unlimited* to avoid space constraints when creating the snapshot.

File Job Considerations

File jobs have the same schedule, retention and pre-backup log flushing considerations as image jobs. In most cases, an image job is the preferred method of replication as it will allow you to utilize all the business continuity and disaster recovery features available.

You can only protect Linux based operating systems using a file replication job. File replication jobs can be used for both Windows based and Linux based operating systems.

Additional considerations available for file jobs include:

- **Open file manager** - All image jobs use VSS, but file jobs for Windows devices use it only if the **Open File Manager** box is checked. Always select this box if it is presented as an option.
- **Preserve ACLs** - Preserving ACLs is normally a good practice and should be selected. It does take significantly more space to save, but preserving ACLs is usually worth the storage.
- **Preserve System State** - In contrast to preserving ACLs, saving system state is questionable because it requires substantially more time and space to save. In most cases, the value is not worth the storage and performance cost.

Figure 8 - File Job Additional Considerations

Note

Because files can be restored from an image replication job, file replication jobs are not needed for devices protected by an image job. However, the retention period for image jobs are typically shortened, so add a file job for data that needs to be saved for long periods of time.

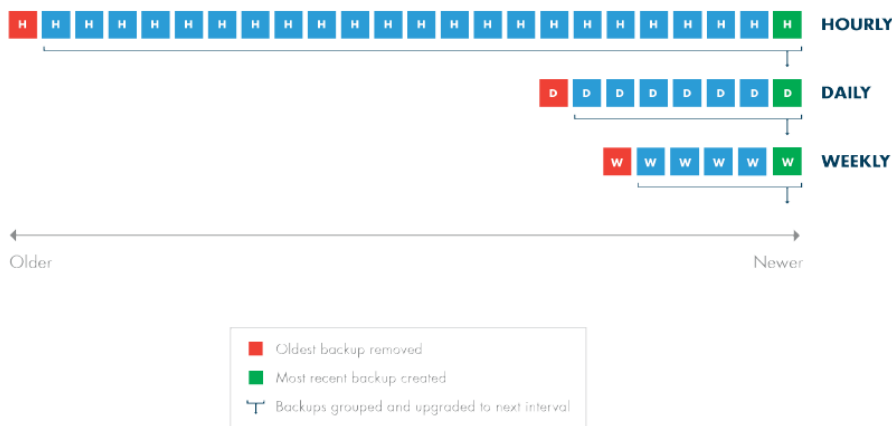
Additional Job Considerations

You should also consider the following job configurations:

- **Fixed retention vs. graduated retention** - An important consideration for image and file jobs is whether to retain backup versions for a set period of time or use graduated retention to retain backup versions for longer periods of time. Fixed retention is sufficient for short to medium durations, but consider graduated retention in order to keep data for longer durations.

A backup version is retained for a period of time; it is then 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 grow as they are promoted to higher types. Note that the job size will continue to grow until each applicable type is filled. You can use fixed retention for some jobs and graduated retention for other jobs, depending on your needs.

Figure 9 - Graduated Retention Timeline



- **Data exclusion** - You might want to exclude some data from an image or file job if the data is not needed. This can substantially reduce the size and time of the replication job.
 - **Exclude disk** - You might exclude a disk that is dedicated to temporary or log files that do not need to be replicated. You might also decide to exclude external USB drives; 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 (BMR) feature reserves X and Z drive labels, so the BMR will not work with X or Z drives. X and Z drives should be renamed or excluded if BMR protection is needed.

Figure 10 - Drive Exclusion/Inclusion Section of Image Job Config

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:

- **Exclude files** - Exclude certain folders or directories with a drive as needed. This will decrease the total size and time of the replication job.

Figure 11 - Exclude Files

192.168.77.233 - backup from folders

select files to backup

☐ - Ignore
☒ - Onsite only
☐ - Onsite and Offsite

Bold italics indicate that the directory has mixed backup content

File tree view showing C: drive contents:

- Boot
- Bootmgr
- Bootmgr.bak
- BOOTNXT
- cygwin
- Documents and Settings
- inetpub
- null
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Users
- Windows

E: drive is also visible at the bottom of the tree.

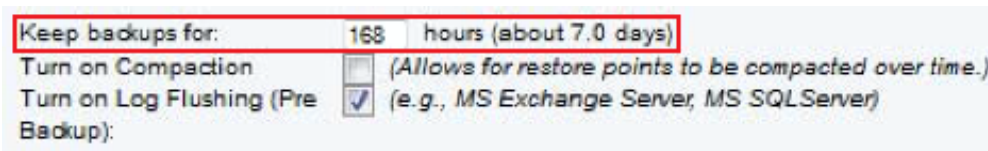
- **Analyze job profile** - When a replication job has been running for some time and the size seems too large (or too small), you can analyze the job in question in more detail. You can run a profile report that displays detailed information about each version of the job that allows you to analyze whether any files should be excluded to reclaim space.

Figure 12 - Drive Exclusion/Inclusion Section of Image Job Config



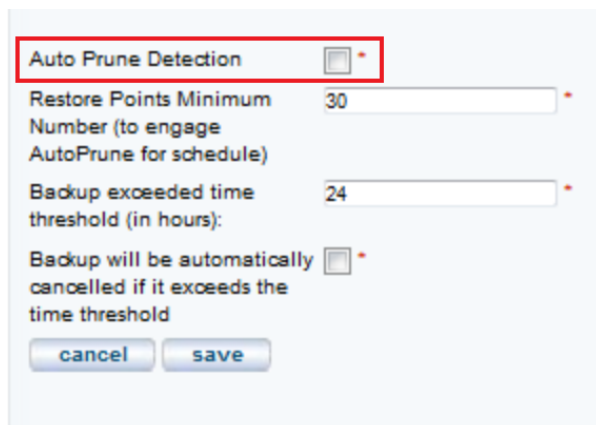
- **Reduce retention** - If it becomes necessary to reclaim space on the appliance, there are several ways to reduce replication job size. As described above, you can proactively exclude data from the job, or run a job profile to identify suspect files that can be excluded. In addition to these two methods, you can also reduce the retention period. You can reduce retention in various ways:
 - *Manually reduce retention* - Manually reduce the retention period for one or more jobs. For example, you can change the **Keep backups for** value from 30 to 15 days to remove half the retained version forward.

Figure 13 - Drive Exclusion/Inclusion Section of Image Job Config



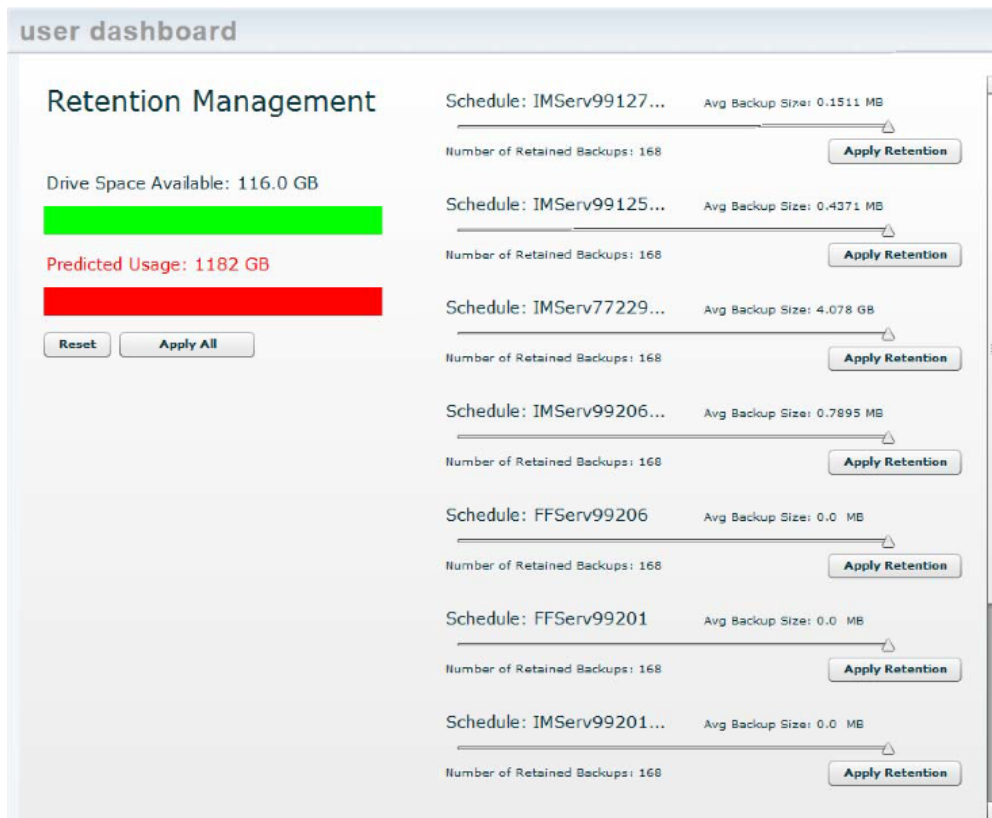
- *Auto prune retention* - Enable pruning, which checks for free space and automatically deletes the oldest backups if space is inadequate.

Figure 14 - Drive Exclusion/Inclusion Section of Image Job Config



- *Set retention management* - The UMC dashboard includes a retention management link that allows you to quickly change the retention setting for the largest job.

Figure 15 - Drive Exclusion/Inclusion Section of Image Job Config



Initial Backup Strategy

The time it takes to run a replication job is directly related to the available network bandwidth. If unchecked, the Axcient appliance will use all available bandwidth when running a 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.

The initial run for each backup job can be lengthy, as all data must be copied. When adding a device, it is common to create an image job and/or a large file job. The initial device backup could take days depending on the amount of data to replicate and the speed of the network.

Consider the following in the initial backup planning:

1. **Onsite Backups (internal network)** - Bandwidth throttling is enabled continuously and set at 1 Gbit/second for both the internal upload and download rates by default.
 - a. When creating 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.
 - b. If there is no image job and there is concern 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 do not apply, consider restricting the bandwidth to something less than 1Gbit/second during the week, such as 100 Mbit/second.
 - c. Turn off bandwidth throttling during the first weekend (or non-business days) and set the replication job to start that Friday evening so the initial replication can run without throttling from Friday night through Monday morning. Additionally, 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 jobs that do not impact normal business hours.
2. **Offsite Backups (Internet)** - Offsite backups (or Cloud replication) is limited by the Internet connection. Bandwidth throttling is on continuously and set at 1 Mbps 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 during business hours.
 - b. All Cloud replication jobs can be run in two different methods:
 1. The default method of all Cloud replication jobs placed in a queue and run sequentially at a set time each day. Set the start time to minimize the impact on other business traffic through the Internet. This typically means setting the start time to a time after the close of regular business.
 2. *Unbundled Offsites* is an opt-in feature that begins a Cloud replication job as soon as a the corresponding local replication job completes.
 - c. Determine the slow hours for the business and consider turning off external throttling during those hours. Typically, the start of this period would coincide with the Cloud job start time described above.

- d. Determine the amount of data to be replicated in the Cloud. If the amount of data to transfer will take more than 14 days to transfer through the Internet connection, call Axcient Technical Support and request a direct attached storage (DAS) transfer. A DAS device is connected directly to the Axcient appliance, the data is copied to the DAS device, and the DAS device is shipped to the Axcient data center.

Cloud upload time can be calculated as follows:

1. Determine the actual upload speed of the Internet connection in Mbps. There are a variety of tools available for free on the Internet.
2. Determine the amount of data in GBs to be replicated to the Cloud. For an initial replication, where all jobs are to be replicated in the Cloud, this is the total amount of data on the appliance.
3. Calculate the upload time as follows:

$$\text{Time} = ((\text{Data} * 1024 * 8) / \text{Speed}) / 86400$$

Time is in days, Data is in GBs, and Speed is the upload speed in Mbps.

Laptop Replication Strategy

Axcient requires that a device be connected to the network in order to replicate its data. However, laptop computers are often not connected to the network. To replicate a laptop that is seldom connected to the network, consider using one of the following backup strategies:

- **Set "Backup On Connect" Feature** - When creating a backup job for a laptop device, select 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.

On a Windows laptop, a pop-up window appears when the job begins to notify you that a job is in progress, and cautioning you not to disconnect until the job is complete.

- To implement a pop-up window message for Linux or Mac OS X laptops, use 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 replicate their respective laptops. You can then create an on-demand replication job that they can execute whenever they log in to the UMC. This gives them control to replicate their data whenever is it convenient for them. This is recommend only if other automatic options are not feasible, because it requires that you train users on how to create a replication job and leave the responsibilities to these users. When using this strategy, write a procedure that describes precisely what actions to take. To implement this strategy, do the following:
 - a. Add a laptop owner as a new user with the following permissions: *Create a Backup, Restore from a Backup, UMC User*. You can also grant additional permissions as needed.
 - b. Add a laptop as a device and set the *Additional user assigned* field to the new user.

Appliance Configuration Guidelines

The Axcient appliance can be configured in a number of ways. This section describes some of those options.

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 can be configured through the UMC **systems** tab.

Quality of Service

The Quality of Service (QoS) settings determine when and how much bandwidth throttle to enforce. If QoS is turned off completely - that is a value of zero in the field - the Axcient appliance will use all available bandwidth as needs. This is usually a good strategy during non-business hours, which is why the default values disable throttling during non-business hours.

If throttling during business hours is needed to reduce contention, remember that image backup jobs are processing intensive so do not reduce the internal upload or download rate below the 1000 Mbps default value for image jobs. Without image jobs, reducing these values might not adversely affect performance, but monitor replication job speed after adjusting the value to assess 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 Cloud jobs during those hours, so monitor whether Cloud replication speed is acceptable after reducing this value. By default, external bandwidth is set to 1 Mbps.

Figure 16 - Quality of Service Configuration Screen

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: :

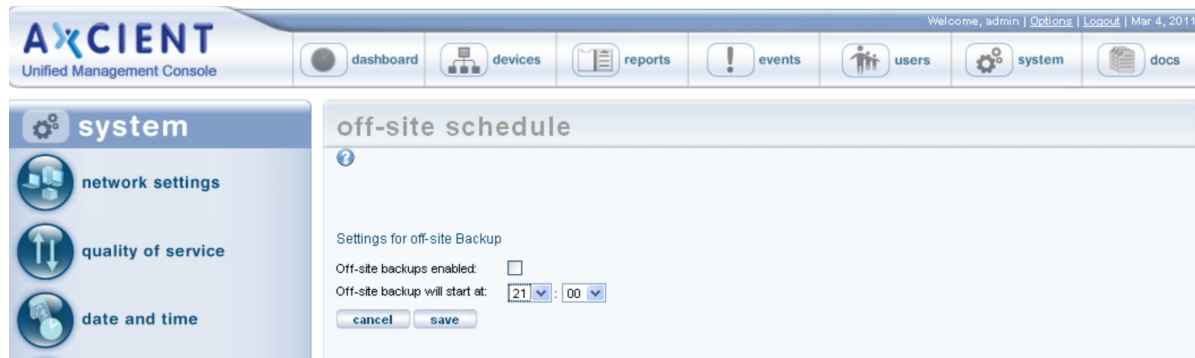
Sat Start: : Stop: :

Cloud Replication

When creating a replication job, specify what data should be saved in the Cloud as well as locally. You can specify one of two ways by which data is replicated to the Axcient Cloud:

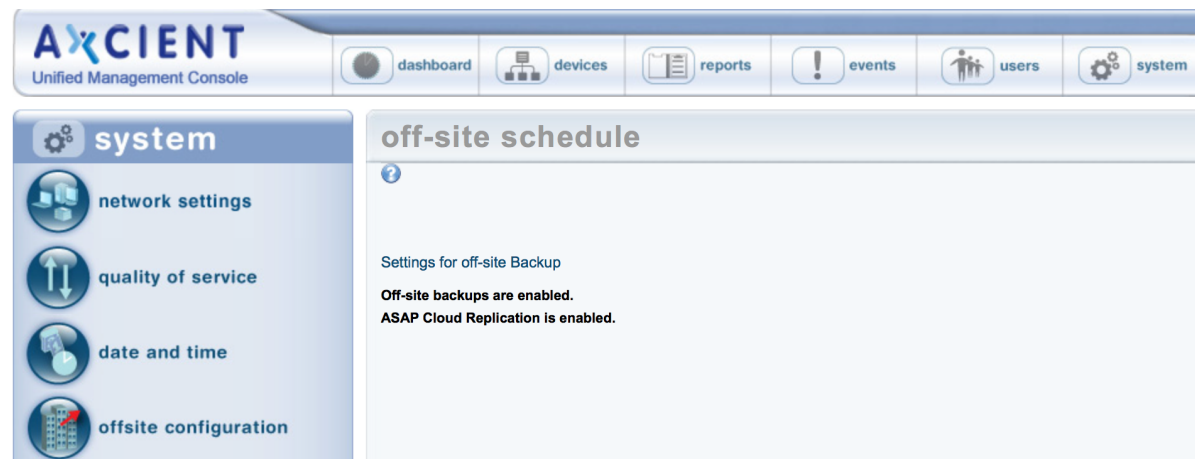
1. The default method of all Cloud replication jobs placed in a queue and run sequentially at a set time each day. Set the start time to minimize the impact on other business traffic through the Internet. This typically means setting the start to a time after the close of regular business.

Figure 17 - Default Cloud Replication Method



2. *Unbundled Offsites* is an opt-in feature which begins a Cloud replication job as soon as a the corresponding local replication job completes.


Figure 18 - Unbundled Offsites Replication Method



Graduated Retention

When using graduated retention for some or all jobs, review the settings. The settings determine the time intervals before replication versions are either discarded or promoted to the enet type. The default values are as depicted in the figure below. If any of these default values are not desirable, change the value as desired.

Figure 19 - Graduated Retention Configuration Screen



The image shows a web-based configuration window titled "Graduated Retention Defaults". Below the title is a help icon and the text "Default Settings for the rules used for graduated retention." There are four input fields with labels: "Default Hourly" (value 48), "Default Daily" (value 14), "Default Weekly" (value 5), and "Default Monthly" (value 12). Each field has a small red asterisk to its right. At the bottom left are "cancel" and "save" buttons.

Setting	Value
Default Hourly	48
Default Daily	14
Default Weekly	5
Default Monthly	12

Ports

As noted in the [Installation Guidelines](#) section, the Axcient appliance uses several ports which must be open. The installation guidelines list common ports that are used but is not a complete list. See the [Appliance Specifications](#) section for a complete description of port use.

Third Party Support

Axcient provides feature to support some third party tools:

- **SNMP** - Axcient supports SNMP and provides a custom Axcient MIB. To use SNMP, enter the appropriate information by navigating to **system > SNMP**. SNMP is turned off by default.

Figure 20 - SNMP Configuration Screen

SNMP Settings

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

Read community: public

Trap sink: 172.18.5.49

Trap sink community: public

Use inform notifications (trap is default): ☐

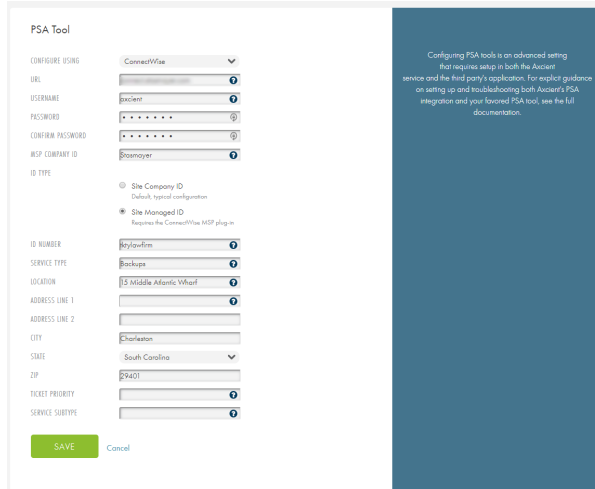
Use V1 traps (V2 is default): ☐

Enable SNMP: ☒

Schedule Name	Index
OffSite Backup	1
Alert Digest	2
Usage History	3
TestImage	4
TestImageMbr2016	6
FF	7
2016gptimg	9
TestMbr	10

- **PSA Tool** - Axcient supports the ConnectWise and Autotask PSA tool integration. This will allow you to integrate the tool with the Axcient alert mechanism to generate tickets directly in the PSA tool. Axcient provides a custom configuration screen for each supported PSA tool.

Figure 21 - SNMP Configuration Screen



The image shows a web-based configuration screen for a PSA Tool. The screen is divided into two main sections: a form on the left and a blue informational panel on the right.

PSA Tool Configuration Form:

- CONFIGURE USING:** A dropdown menu with "ConnectWise" selected.
- URL:** A text input field with "https://example.com" and a help icon.
- USERNAME:** A text input field with "axcient" and a help icon.
- PASSWORD:** A password input field with masked characters and a help icon.
- CONFIRM PASSWORD:** A password input field with masked characters and a help icon.
- WSP COMPANY ID:** A text input field with "00000000" and a help icon.
- ID TYPE:** Two radio button options:
 - ☐ Site Company ID (Default, typical configuration)
 - ☒ Site Managed ID (Requires the ConnectWise WSP plugin)
- ID NUMBER:** A text input field with "00000000" and a help icon.
- SERVICE TYPE:** A text input field with "Backups" and a help icon.
- LOCATION:** A text input field with "15 Middle Atlantic Wharf" and a help icon.
- ADDRESS LINE 1:** A text input field with " " and a help icon.
- ADDRESS LINE 2:** A text input field with " " and a help icon.
- CITY:** A text input field with "Charleston" and a help icon.
- STATE:** A dropdown menu with "South Carolina" selected.
- ZIP:** A text input field with "29401" and a help icon.
- TICKET PRIORITY:** A text input field with " " and a help icon.
- SERVICE SUBTYPE:** A text input field with " " and a help icon.
- Buttons:** A green "SAVE" button and a blue "Cancel" button.

Blue Panel Text:

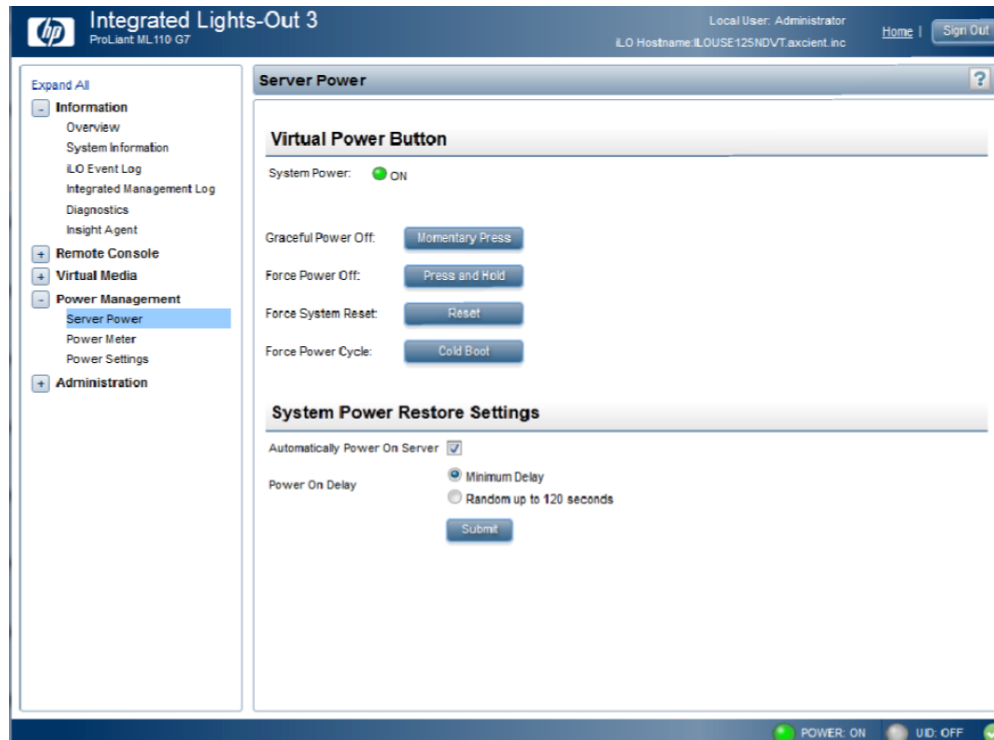
Configuring PSA tools is an advanced setting that requires setup in both the Axcient service and the third party's application. For explicit guidance on setting up and troubleshooting both Axcient's PSA integration and your favored PSA tool, see the full documentation.

Remote Hardware Maintenance

An Integrated Lights Out (ILO) feature is built in to the Axcient hardware appliance which 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, but is it not feasible to physically check the appliance if there is a hardware problem.

Please refer to the [ILO Configuration Guide](#) for information on how to configure the ILO. For additional information, please reference the [iDRAC User Guide](#).

Figure 22 - ILO Configuration Example



Monitoring Guidelines

Axcient provides a number of ways to monitor the protection solution.

User Dashboards

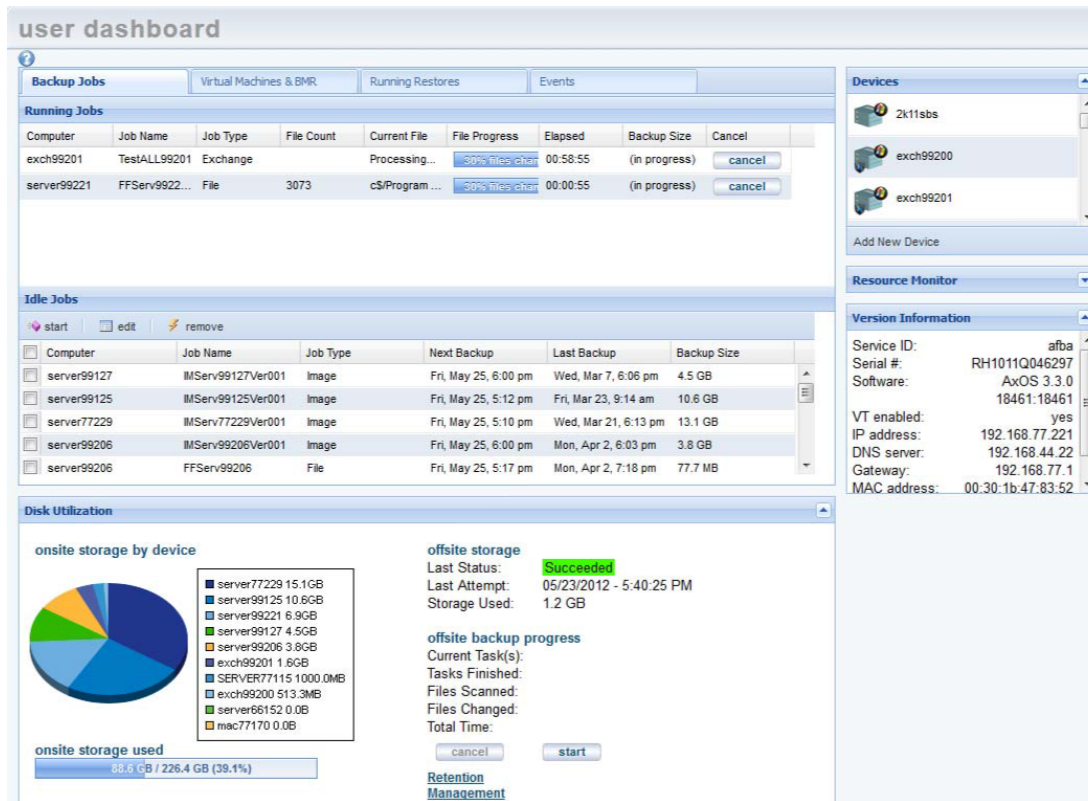
Both the UMC and the Axcient Web Application include dashboards that appear as the first screen when you first log in.

UMC Dashboard

The UMC dashboard includes multiple sections that allow you to monitor the protection solution. Be aware that all information displayed in the UMC is only for a specific appliance and the devices it protects.

- **Devices Section** - Located in upper-right hand corner, this section allows you to quickly see and access devices protected by the appliance.
- **Backup Jobs Tab** - Located in the center of the dashboard, this tab contains two sections:
 - *Running Jobs Section* - Shows what jobs are currently running and provides progress information for each job.
 - *Idle Jobs Section* - Shows the remaining jobs and allows you to quickly start or edit any of the jobs listed.
- **Virtual Machines & BMR Tab** - Displays information about running virtual machines (VM) or Bare Metal Restores (BMR). The *Control* button allows you to quickly start, stop, or otherwise manage VMs and BMRs for each image replication job.
- **Offsite Progress Section** - Displays the status information about running Cloud replication jobs. In this example, no information is displayed, which means a Cloud replication job is not currently running.

Figure 23 - UMC Dashboard



Web Application Dashboard

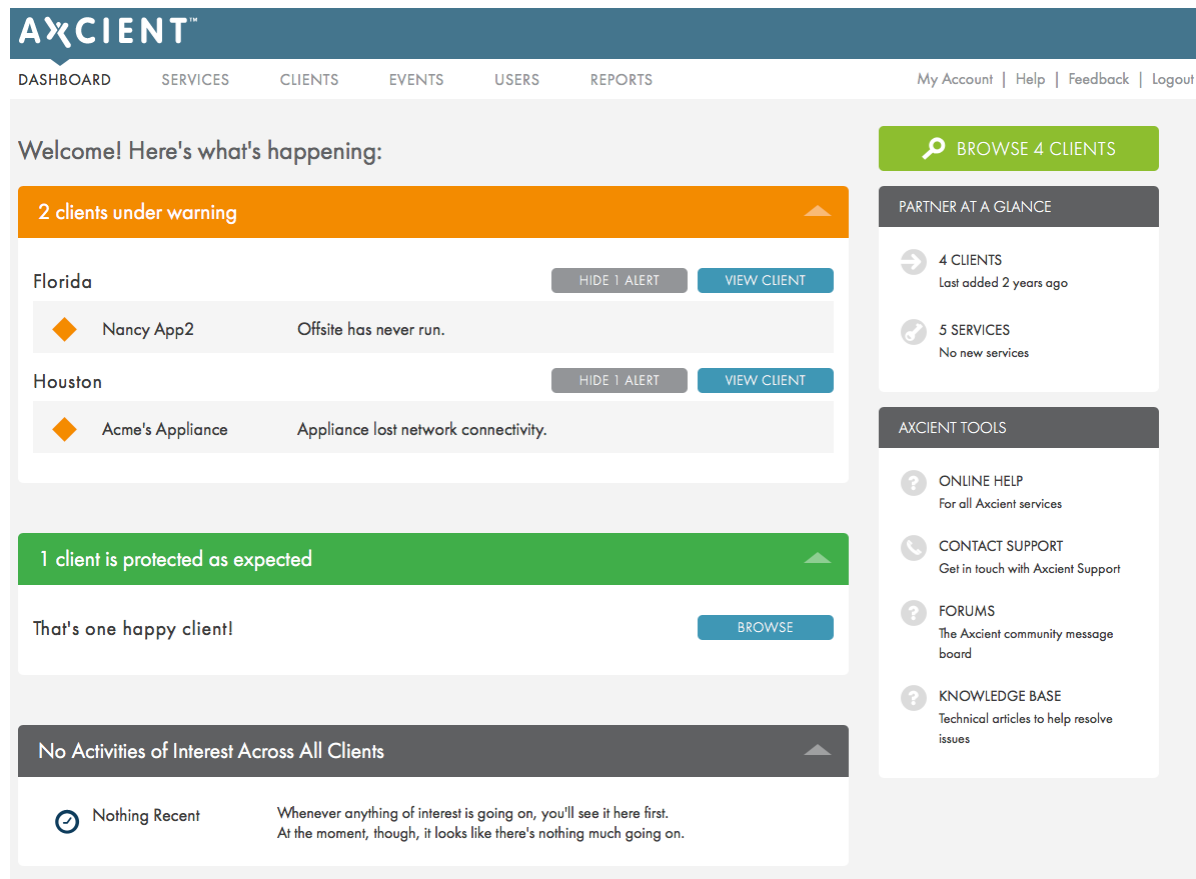
The Web Application Dashboard provides summary health status information for all Clients, Services, and their protected device on a single interface. The Web Application dashboard includes information about appliance and device connectivity, and health status alerts based on the Health Status Policy configuration, which must be set in the Web Application.

The Web Application uses a *Manage by Exception* philosophy, escalating and notifying you whenever the health status of services or devices change. These notifications include:

- **Activities of Interest** - Displays important events occurring across all Clients and Services. All individual activities include direct links to the corresponding activity. These include any VMs, BMRs and exposed UNC mount points.
- **Required Attention (Troubled)** - Highest positioned health status alert. Also referred to as Troubled, these are devices that have fallen out of protection threshold as configured in the Protection Policy. Devices that have failed the Cloud replication will be reported here as well. The expanded list includes individual entries with direct links to help resolve the issue.
- **Warning** - Signifies an appliance or device that has lost connectivity for an extended period of time as configured in the Protection Policy. This section also lists local or Cloud replication jobs that completed with warnings. The expanded list includes individual entries with direct links to help resolve the issue.
- **Protected as Expected** - Devices that are healthy and do not need attention at this time. Expand the section and click the **Browse** button to view all protected Clients.

Additionally, you can quickly navigate to the specific Clients or Services by clicking the corresponding **Clients** or **Services** link in the top-navigation menu, or by clicking the appropriate links in the *Partner at a Glance* section.

Figure 24 - Web Application Dashboard



Reports

Both the UMC and Web Application include a set of predefined reports that can be run.

UMC Reports

The UMC provides the following reports:

- **Backup History** - Displays a graph of total and incremental storage use.
- **Job Profile** - Displays job profile data and is accessed from a link in the **Backup History** report.
- **Scheduled Backups** - Displays summaries of the defined jobs.
- **Backup Times** - Displays a history of job runs.
- **Current Disk Usage** - Displays a pie graph of storage space used per job.

Figure 25 - UMC Reports



Web Application Reports

The Web Application allows you to generate the following reports based on customizable fields:

- **Appliance Summary** - Summarizes general usage across Axcient Clients and Services.
- **Primary Job** - Summarizing local jobs run across Axcient Clients or Services.
- **Offsite Job** - Summarizes all Cloud replication jobs run across Axcient Clients or Services.
- **Cloud Statistics** - Summarizes VM failovers in the Cloud. This is an easy way to keep track of usage of the Cloud VM business continuity feature.
- **Appliance Details** - Detailed PDF report about a specific Axcient appliance.
- **Auditor** - Report summarizing activities. This report is configurable based on action taken, time, entity, and user.
- **Definitions** - List of predefined report configurations or parameters.

All reports can be downloaded as CSV files.

Figure 26 - Web App Reports

Axcient

DASHBOARD SERVICES SITES EVENTS USERS **REPORTS** My Account | Help | Feedback | Logout

AxOS & D2C reports Fusion Reports Definitions **Auditor** Notifications

SEARCH ▼

ACTION

TIME RANGE

-- Show All --

ENTITY

USER

RUN REPORT

Show 10 records

First Previous Next Last

RECORD #	DATE	USER	ACTION	ENTITY	DESCRIPTION	ACTIONS
No data available in table						

Showing 0 to 0 of 0 entries

First Previous Next Last

Event Log and Alerts

The UMC event log provides information about each action on the Axcient appliance. To access the Event log, click the **Events** tab in the top navigational menu. Here you can view across all devices protected by the Appliance.

Figure 27 - UMC Events Page

The screenshot shows the UMC Events page with a filtering sidebar on the left and a table of events on the right. The sidebar includes filters for Onsite Backup Events, Type, and Schedule. The table displays 4,036 results with columns for Type, Date, Action, User, and Details.

Type	Date	Action	User	Details
USER_LOGIN	01/25/2016 - 2:25:26 PM	User: admin logged in	admin	View
USER_LOGIN	01/25/2016 - 2:25:26 PM	User: admin logged in	admin	View
USER_LOGIN	01/25/2016 - 2:25:26 PM	User: admin logged in	admin	View
SYSTEM_SHUTDOWN	01/25/2016 - 11:31:33 AM	The system is shutting down. All running jobs and other processes will be stopped.	system	View
SERVER_ALIVE_BACKUP_SUCCEEDED	01/24/2016 - 9:13:14 PM	Backup Daily for hr Policy on hr completed Successfully (Included drives - C:)	RMC_USER-yoav1	View
BACKUP_DATA_CHANGE	01/24/2016 - 9:13:14 PM	Backup size for hr Policy on machine HR has changed by 37.8 KB	UBS	View
SERVER_ALIVE_BACKUP_STARTED	01/24/2016 - 9:00:59 PM	Backup Standard Started for hr Policy on hr	RMC_USER-yoav1	View
SERVER_ALIVE_BACKUP_SUCCEEDED	01/23/2016 - 9:14:53 PM	Backup Daily for hr Policy on hr completed Successfully (Included drives - C:)	RMC_USER-yoav1	View
BACKUP_DATA_CHANGE	01/23/2016 - 9:14:53 PM	Backup size for hr Policy on machine HR has changed by 3.3 KB	UBS	View
SERVER_ALIVE_BACKUP_STARTED	01/23/2016 - 9:00:07 PM	Backup Standard Started for hr Policy on hr	RMC_USER-yoav1	View
SERVER_ALIVE_BACKUP_SUCCEEDED	01/22/2016 - 9:15:46 PM	Backup Daily for hr Policy on hr completed Successfully (Included drives - C:)	RMC_USER-yoav1	View
BACKUP_DATA_CHANGE	01/22/2016 - 9:15:46 PM	Backup size for hr Policy on machine HR has changed by 35.3 KB	UBS	View
SERVER_ALIVE_BACKUP_STARTED	01/22/2016 - 9:00:16 PM	Backup Standard Started for hr Policy on hr	RMC_USER-yoav1	View
SERVER_ALIVE_BACKUP_SUCCEEDED	01/21/2016 - 9:12:22 PM	Backup Daily for hr Policy on hr completed Successfully (Included drives - C:)	RMC_USER-yoav1	View
BACKUP_DATA_CHANGE	01/21/2016 - 9:12:22 PM	Backup size for hr Policy on machine HR has changed by 101.8 KB	UBS	View
SERVER_ALIVE_BACKUP_STARTED	01/21/2016 - 9:00:25 PM	Backup Standard Started for hr Policy on hr	RMC_USER-yoav1	View
SERVER_ALIVE_BACKUP_SUCCEEDED	01/20/2016 - 9:08:34 PM	Backup Daily for hr Policy on hr completed Successfully (Included drives - C:)	RMC_USER-yoav1	View
BACKUP_DATA_CHANGE	01/20/2016 - 9:08:34 PM	Backup size for hr Policy on machine HR has changed by 35.3 KB	UBS	View
SERVER_ALIVE_BACKUP_STARTED	01/20/2016 - 9:00:33 PM	Backup Standard Started for hr Policy on hr	RMC_USER-yoav1	View

Export options: [CSV](#) | [Excel](#) | [XML](#)

Additionally, you can configure automatic alerting to a specific user configured in the UMC, or to an integrated PSA tool. To configure automatic alerting, click the **configure alerting** option in the left-hand menu.

At a minimum, we recommend that you configure alerts when *FAILED* messages are logged. These alerts can be sent to a user or published to a PSA tool. Additionally, you may also want to consider setting automatic alerting for warning messages, especially those for key actions, such as events related to local and Cloud replication.

Review the log entries periodically to determine which messages are most important.

Figure 28 - UMC Alerting Configuration Example

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

Device Events

visible in log ☒ publish to psa tool ☐

notify someone

Exchange Mailbox Backup Events

visible in log ☒ publish to psa tool ☐

notify someone

Troubleshooting

In addition to this chapter, Axcient provides several resources to assist you when encountering a problem:

- **Event Log** - Contains details about problems and other events that occur in the Axcient appliance. The event will contain specific information about what exactly happened, which will help you and/or the Axcient Customer Support representative isolate and resolve the issue.
- [Error Messages Manual](#) - Search for specific error messages that appear in the Event Log, their causes, and solutions. This document is regularly updated.
- **Knowledge Base Library** - Axcient has a knowledge base library resolving common issues Axcient customers encounter. To access the Knowledge Base, log in to the [Axcient User Portal](#) using the credentials provided by Axcient. If credentials were not distributed, please contact [Axcient Support](#).
- [Axcient Technical Support](#) - Contact Axcient Technical Support if you are unable to resolve any issues with Axcient protection solution.

Backup Problems

Replication Fails Because of VSS Problem

On Windows-based devices, the Axcient appliances uses Microsoft Volume Shadow Service (VSS) for image replication jobs (always) and file replication jobs (when *Open File Manager* is set).

Problem	Solution
Another protection solution is preventing the Axcient appliance from properly using VSS.	If another protection solution is installed on the protected device, adjust the backup schedule appropriately so that the Axcient replication job schedule and the other third party replication schedule do not overlap.
Windows shadow copies, configured on the protected device, are interfering with Axcient backups.	Disable Windows shadow copies entirely or adjust the schedule appropriately so that the Axcient backup job and windows shadow copies do not overlap.
The VSS writer for a target application is not registered.	If an error message refers to a disabled VSS writer, register the writer as described in the following procedure.
VSS is not enabled for this device.	Axcient provides a VSS configuration script that is run on the target device. This script enables VSS, registers application writers and identifies potential issues.
Backup might fail if insufficient shadow copy space is allocated.	Allocated adequate space as described in the procedure at the end of this section.

Before executing a job, the Axcient appliance checks whether the VSS writer is enabled for certain applications on the protected device. If one of those application is present and the VSS writer is not register correctly, the image job aborts and a failure message appears in the event log. The following applications are checked:

- Microsoft Exchange
- Microsoft SQL
- Microsoft Share Point
- Microsoft Active Domain (NTDS)

In most supported system configurations, the VSS writers are *enabled* by default. In Windows BS 2003, they are *disabled* by default. If the device is running Windows BS 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:

- a. Change to the directly `%COMMONPROGRAMFILES%\Microsoft shared\web server extensions\<#>\bin`

Where <#> is 12, 14 or other higher number.

- b. Enter the following command:

```
STSADM -o registervsswriter
```

Active Domain (NTDS) VSS Writer

The VSS writer is a built-in function in Windows 2003 and later versions. When configuring backups in the UMC, you have the option to exclude VSS writers from being backed up. This feature is useful when VSS writers are interfering with the backup process.

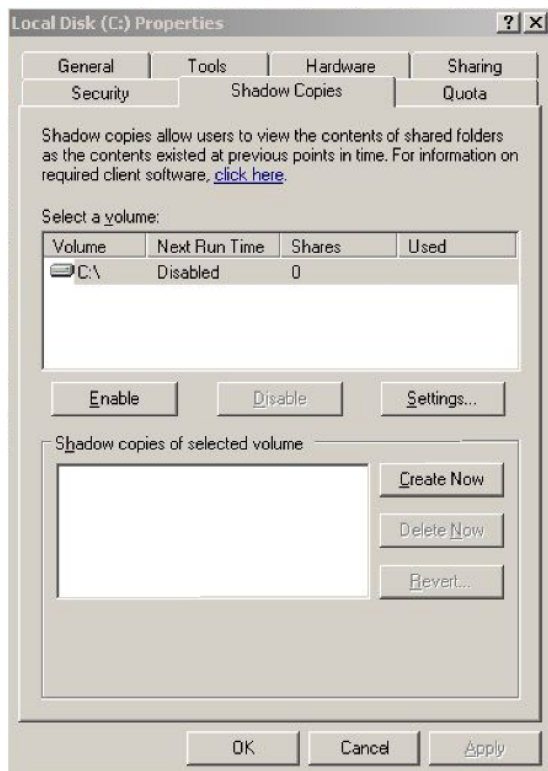
Allocate Shadow Copy Space Procedure

To allocate additional shadow copy space, do the following:

1. Open a Windows Explorer window, select the target drive, and right-click to select the **Properties** option from the menu.
2. Select the **Shadow Copies** (Windows 2003) or **Configure Shadow Copies** (Windows 2008 Server), select the target value, and click the **Settings** button.

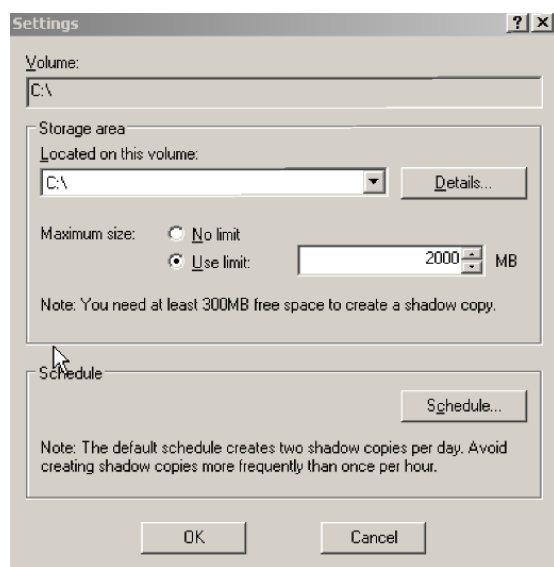
Figure 29 -

Figure 30 - Shadow Copies Tab



3. In the *Maximum Size* field, do one of the following and then click **OK** to close the window:
 - a. Click **No Limit** (recommend).
 - b. Click **Use Limit** and enter the size. As a best practice, we recommend setting this at 25% of the size of the disk.
4. In the *Properties* window, click **OK** to save and close.

Figure 31 - Shadow Copies Tab



Replication Fails Because of Permission Problem

A permission problem can cause a job to fail.

Figure 32 - Permission Error Example

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	View

Problem	Solution
The replication job does not have permission to replicate some or all of the target files because either the user credentials or file permissions do not allow the job 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 job. Consider setting proper permissions at the highest level possible and then working down to the sub-directories to ensure they inherit the correct permissions.

Problem	Solution
Windows file redirection is enabled, and the replication job does not have permission to replicate the redirected files.	The default permission for Windows folder redirection is the <i>grant user exclusive rights</i> , which means an administrator does not have read access to the redirect folders to replicate them. Please refer to the Replication Fails Because of Windows Redirection section below.

Replication Fails Because of Windows Redirection

If employing a Windows redirection, the redirected files might not be replicated. 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, do the following:

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 below)

Everyone - Read and Execute

Administrators - Full Control

System - Full Control

- c. NTFS Permissions (when general note #1 applies)

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)

CREATE OWNER - Full Control (Subfolders and Files Only)

System - Full Control (This Folder, Subfolder and Files)

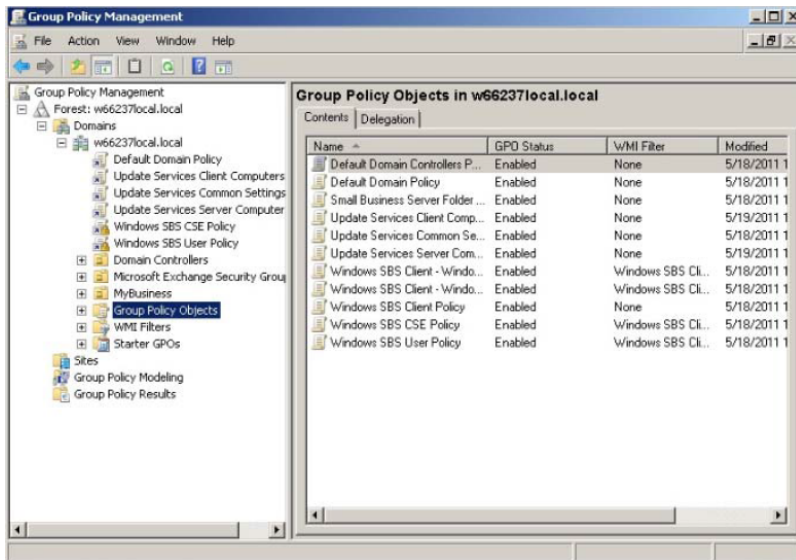
Domain Admins - Full Control (This Folder, Subfolders and Files)

2. Start the Group Policy Manager (**Start > Control Panel > Administrative Tools > Group Policy Manager**).

3. Create a new Group Policy Object (GPO) called Axcient Folder Redirection:

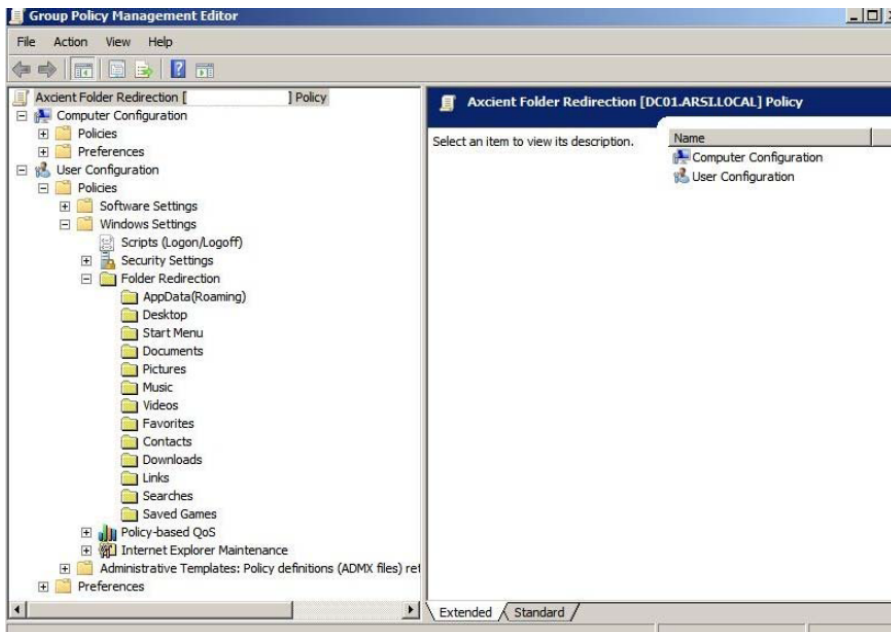
- a. Open the tree to the target domain.
- b. Right-click *Group Policy Objects* and select **New**.
- c. Enter the name **Axcient Folder Redirection** and click **OK**.

Figure 33 - Folder Redirection: Group Policy Manager



4. Expand the *Group Policy Objects* folder, right-click on the newly created *Axcient Folder Redirection* entry, and click **Edit**.
5. The *Group 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 34 - Folder Redirection: Group Policy Management Editor

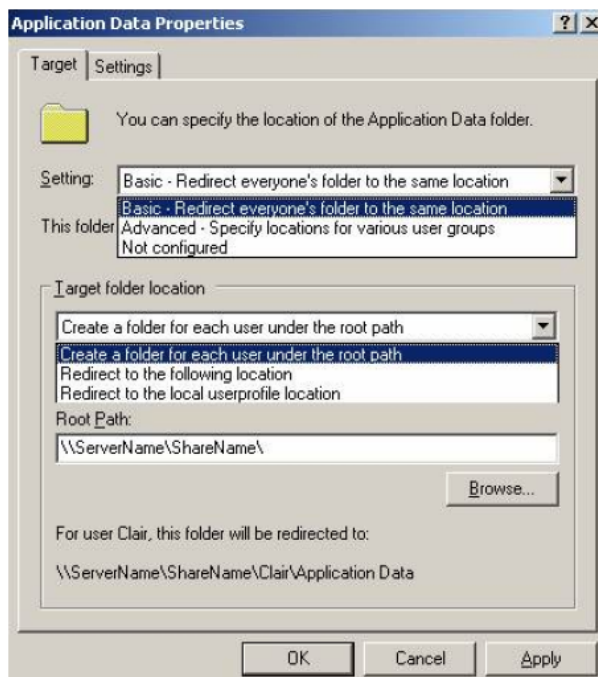


6. Enable folder redirection for a desired target (such as **Desktop** or **Documents**):
 - a. Select the target, right-click, and select **Properties** to display the properties window for that target.
 - b. Click the **Target** tab. In the *Setting* field, select **Basic - Redirect everyone's folder to the same location**.
 - c. In the Root Path field, enter:

\\ServerName\ShareName\

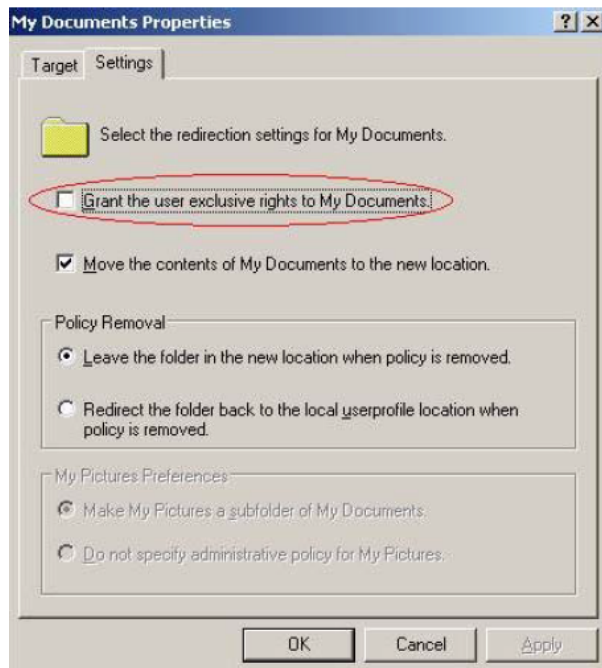
Where *ServerName* is the name of the server and *ShareName* is the name of the share folder created above.

Figure 35 - Folder Redirection: Properties Target Tab



- d. Click the **Settings** tab. Uncheck the **Grant the user exclusive rights to My Documents** checkbox.
- e. When both the *Target* and *Settings* tab fields are correct, click the **OK** button.

Figure 36 - Folder Redirection: Properties Target Tab



7. Repeat Step 6 for each desired target (Desktop, Documents, Pictures and so on).
8. When all settings are configured, select 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 displays, prompting you to select the newly created Folder Redirection GPO.
 - d. Click the **OK** button when you are finished.
9. To test that the configuration is correct, reboot the client machine and then log in as a user. If the folder redirection is successful, the following event appears in the application log:

Event ID: 401

Source: Folder Redirection

Description: Successfully redirected my Documents. The folder was redirected from <original_path> to \\ServerName\ShareName\UserName\My Documents.

General Notes

- Use the step1-c NTFS permission when group policy is configured to redirect to a location where the GPO will automatically create the destination folder (user's individual Application Data, Desktop, or My Documents folder).
- User configuration settings in GroupPolicy take effect at the first login after the policy is saved and replicated to the user's login service.
- Computer configuration settings in Group Policy take effect when the machine reboots and logs on to Active Directory. Therefore, the user must reboot a terminal server before new computer configuration settings are applied.
- The following error message indicated the user still has exclusive rights. If the following message appears, please repeat Steps 6- 6d:

```
Event ID: 101
User: <name>
Computer: <name>
Description:
Failed to perform redirection of folder <name>.
The new directors for the redirected folder could not be created.
The folder is configured to be redirected to <path>.
The following error occurred: Access is denied.
```


SBS 2008 and 2011 Notes

This section applies to devices running Windows Small Business Server (SBS) 2008 or 2011. The Console for SBS 2008 and 2011 does not expose the capability to turn off the *exclusive* bit in the folder redirection GPO, and may overwrite an existing folder redirection GPO named *Small Business Server Folder Redirection Policy*. Therefore, we recommended the following:

1. 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 to retain the original exclusive ACL, which prevents Axcient from replicating them. To fix this, do the following:
 - 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 a local system, grant the proper ACL at the root of the redirected folder recursively to BUILTIN\Administrators:

```
icacls C:\users\FolderRedirection \t \c \grant "BUILTIN\Administrators":  
(OI) (CI) (F)
```

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, do the following:

1. Log into a client device as administrator, and run the following command:

```
gpupdate /force
```

2. Reboot the device.
3. Log in as a regular user and navigate to a redirected folder.
4. Enter the following command:

```
gpresult /scope user /v
```

5. Check the section under *Folder Redirection*. The first time folder redirection takes effect, a system event ID 501 source *Folder redirection* should appear.
6. Repeat procedure for each client device.

Replication Fails Because of Mount Problem

A mount problem can cause a job run to fail. The table below lists potential mount problems.

Figure 37 - Mount Error Message Example

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	View
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	View

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 has changed, log in to the UMC and update the password for that device.

Replication Fails Using Samba

On a Linux (or other UNIX) system running an older (pre-3.3.1) version of Samba, replications might fail if some of the replicated 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.

Replication Fails Due to Symbolic Links (Windows 7)

On a Windows 7 system, attempting to replicate a directory with symbolic links will cause the replication to fail. To work around this problem, remove symbolic links (or the folders that include them) from the replication job. 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.

Replication Hangs After Lost Connection

When a network outage occurs that breaks the connection between a protected device and the Axcient appliance while a replication job is in progress, the replication job can hang indefinitely. To resolve this problem, simply cancel and restart the replication 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 replication 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 replication 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 Replicated

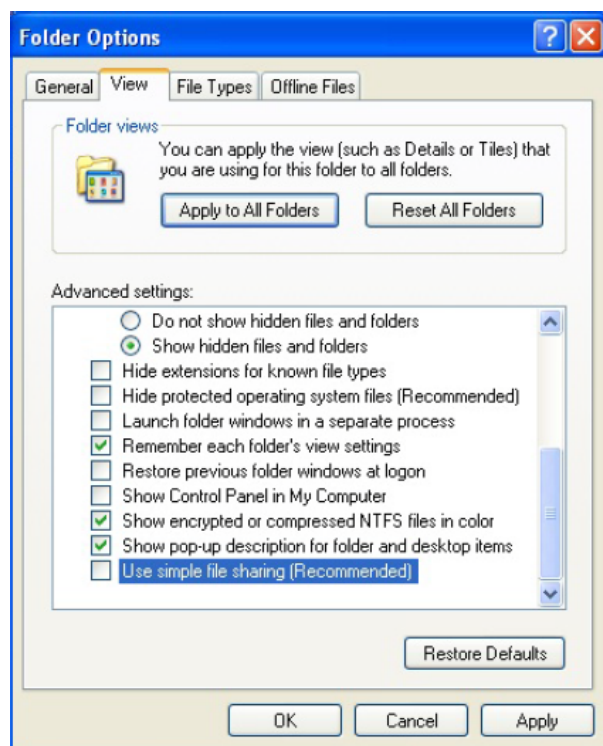
In a file replication job, some files might not be replicated because they were being used (open and locked) at the time the backup job ran. If this is a Windows device, check the **Use Open File Manager** box in the job definition, which invokes VSS so the Axcient appliance can back up any files regardless 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 Replication (XP)

If Simple File Sharing is enabled when creating a replication 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* screen appears. Select the **View** tab and deselect (disable) the *Use simple file sharing [Recommended]* box.

Figure 38 - Folder Options Screen



Cannot Replicate Windows Encrypted Files

The Axcient protection solution supports protection and recovery of Windows files encrypted using the **BitLocker** encryption feature native to Windows devices.

The Axcient appliance cannot access files encrypted by another encryption method. As a result it cannot replicate or restore any data encrypted by another tool.

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 version of an image on demand job are saved indefinitely and can be selected for use in a VM or BMR.

Not All Active Replication Jobs Running

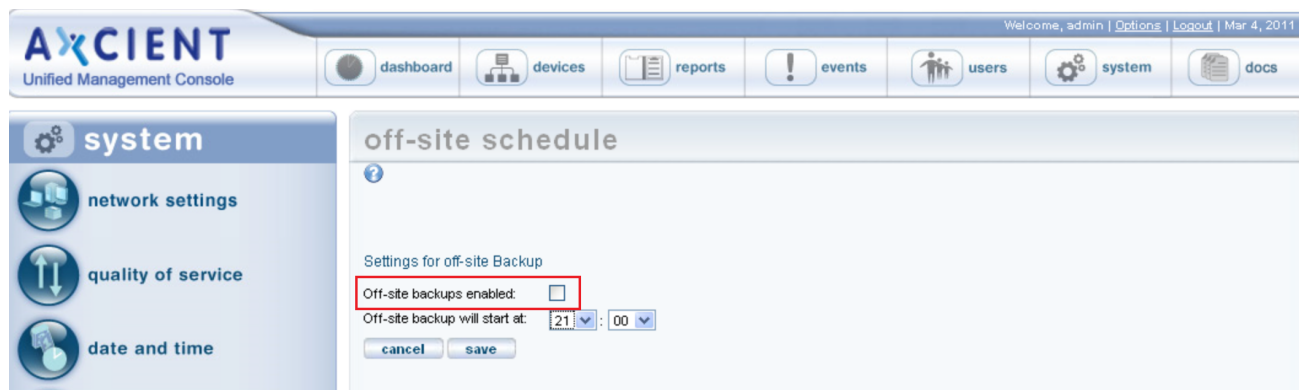
You can schedule any number of replication jobs to run at any time, but the Axcient appliance runs a maximum of five replication jobs simultaneously. If more than five are scheduled concurrently, the sixth and subsequent jobs are put in a queue. When a job completes, the next job in the queue starts 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.

Cloud Replications Are Slow

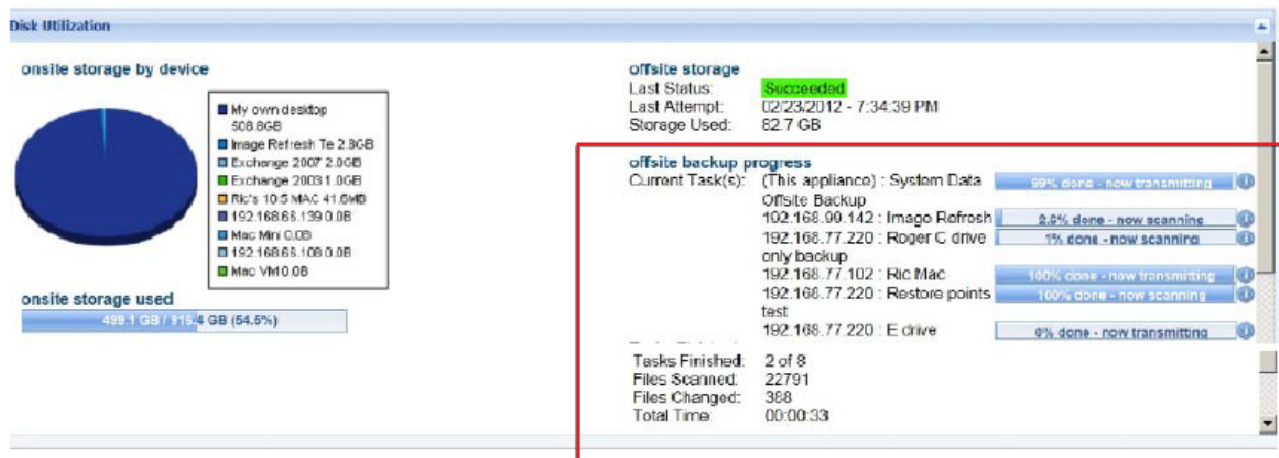
Cloud replication performance can be affected by a number of factors. First, if on demand Cloud replication jobs are not running, make sure the **off-site backups enabled** box is checked in the *Offsite Configuration* page under the UMC system tab. This is not enabled by default, so you must check the box before any offsite backups will run.

Figure 39 - Offsite Backup Enabled Box



When a Cloud replication job is running, check the status in the *Disk Utilization* section of the UMC dashboard. This provides dynamic information about offsite backup progress.

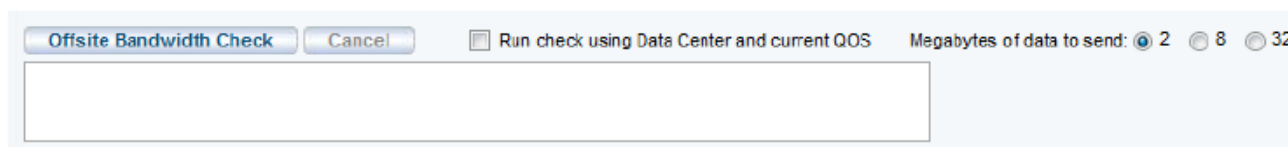
Figure 40 - Cloud Replication Example



If the progress seems too slow, check the transmission speed:

1. Determine the actual upload speed of the Internet connection and the time it should take to upload the data.
2. Click the **system** tab in the top navigational menu and then select the **network utilities** option from the left-hand menu.
3. Locate the **offsite bandwidth check** tool. This tool sends 2, 8 or 32MB file from the appliance to the Axcient data center, which tests both raw throughput across the Internet and processing time within the data center for small and large files.

Figure 41 - Offsite Bandwidth Check Tool



There are several possible reasons why offsite performance might be slow. The table below lists potential offsite performance problems.

Problem	Solution
Bandwidth throttling is on too high.	Review the QoS settings and assess whether they should be changed.
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"> • If the throughput is comparable for small and large files, then there is no traffic shaping. • If the small file throughput is greater than the large file, then traffic shaping is likely impeding the Cloud replication. <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.	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.
Offsite mailbox and image jobs use 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 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 <i>Job Profile</i> report on that job to determine if there are problem files. 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.

Restore Problems

This section covers issues when attempting to restore data from a replication job.

Restoring UNIX Files on Windows Device Fails

If a device has been replicated running Linux or another UNIX-based operating system and attempts 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.

Windows rejects file names with any of the following characters: \ / : * ? " < > |

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, do the following:

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 illegal characters), and then move to the target Windows system.

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

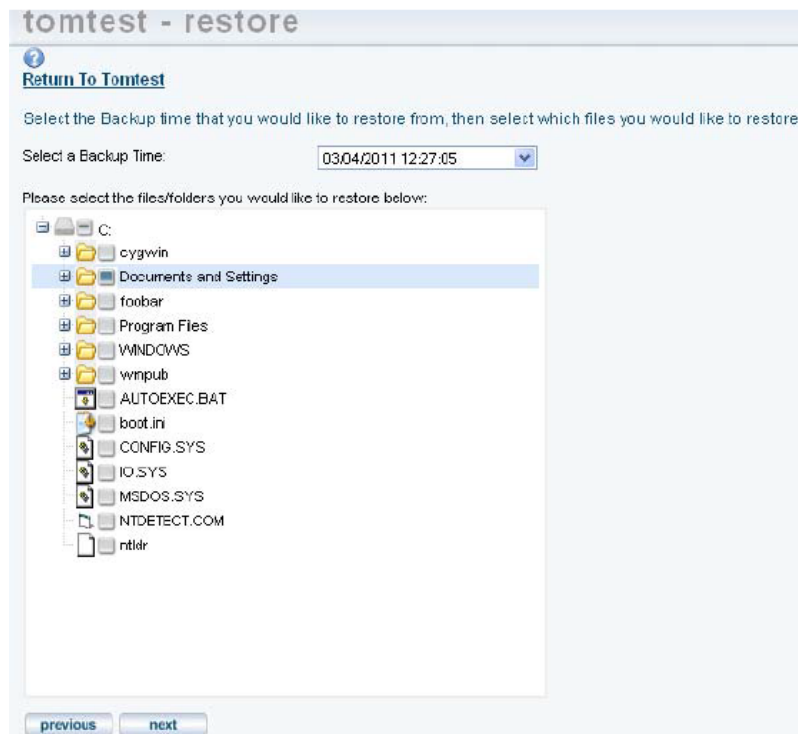
It is possible to choose a target directory to restore files for which you do not have write permission. In this case, even though you were allowed to select the target directory, the Axcient appliance could not write to that directory, so the restore failed. To avoid this problem, make sure you have write permission before attempting the restore operation or choose an alternative target location to which you 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:

- When using Internet Explorer (IE), the browser hangs when trying to display the content tree. This can usually be solved by either switching to a different browser or running IE in compatibility mode.
- There is a permission problem that prevents the browser from displaying the tree. Check that proper (read) permissions for content on that device.

Figure 42 - File Restore Tree View



Virtual Machine and BMR Problems

This section covers issues when trying to run a VM or execute a BMR.

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 screen (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:

1. Boot the device using the original Windows Server 2003 CD, and run the Windows Setup.
2. *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 the computer, or contact the computer manufacturer for more information.

BMR Fails at Final Boot (Active Directory Server)

When performing a BMR of a system with Active Directory installed, the device might fail to boot and instead display a blue screen (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 up to navigate to the *Advanced Boot Options* screen.
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 in to normal mode.

You should now be able to log in using domain user credentials.

Failover VM Pause Shuts 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, do the following:

1. Submit a second pause command to pause the VM.
2. Select from the following options:
 - If the original device is not viable, leave it shut down and continue working with the VM as needed.
 - If the original device is viable, stop the VM and restart the original device.

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. Navigate 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 not, right-click 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 Into Test VM

When a test VM is first started, Active Directory credentials cannot be used to log in to 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 in to the domain. This can be performed either before or after the test VM has been started. Follow the steps for the appropriate version (Windows 2003 or 2008):
 - Windows 2003
 - a. Right-click **My Computer** and select the **Change...** button.
 - b. Under the *Member of* checkbox, select the **workgroup** radio-button option. Enter a name for the workgroup to join and click **OK**. Enter the domain account credentials with authority to remove a host from a domain.
 - c. A *welcome to the group* message displays. Click **OK** to continue.
 - d. A message to reboot displays. Click **OK** but do not reboot.
 - e. Select the **Change...** button.
 - f. Under the *Member of* section, select the **Domain** radio-button option, enter the name of the domain and click **OK**. You might be asked to authenticate in order to proceed. Enter the domain account credentials with authority to add a host to a domain.

- g. A *welcome to the domain* message displays. Click **OK**.
- h. A message to reboot displays. Click **OK** and reboot.

- Windows 2008
 - a. Right-click **Computer** and under the *Computer name, domain and workgroup settings* section, click **Change Settings**.
 - b. The *System Properties* window displays. Under the *Computer Name* tab, click **Change...**
 - c. Under the *Member of* section, select the **Workgroup** radio-button.
 - d. Enter a name for the workgroup to join and then click **OK**.
 - e. A message displays, indicating that the administrator password is required to log in. Ensure that you have access to the local (non-domain) credentials; then click **OK**.
 - f. A *welcome to the workgroup* message displays. Click **OK**.
 - g. A message displays, alerting you that you need to restart the computer to apply the changes. Click **OK**.
 - h. Click the **Close** button on the *System Properties* window.
 - i. A message displays, alerting you that you need to restart the computer to apply the changes. 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 displays. 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**).
- 3. Domain credentials can now be used to log in to 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. When restoring (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.

System Problems

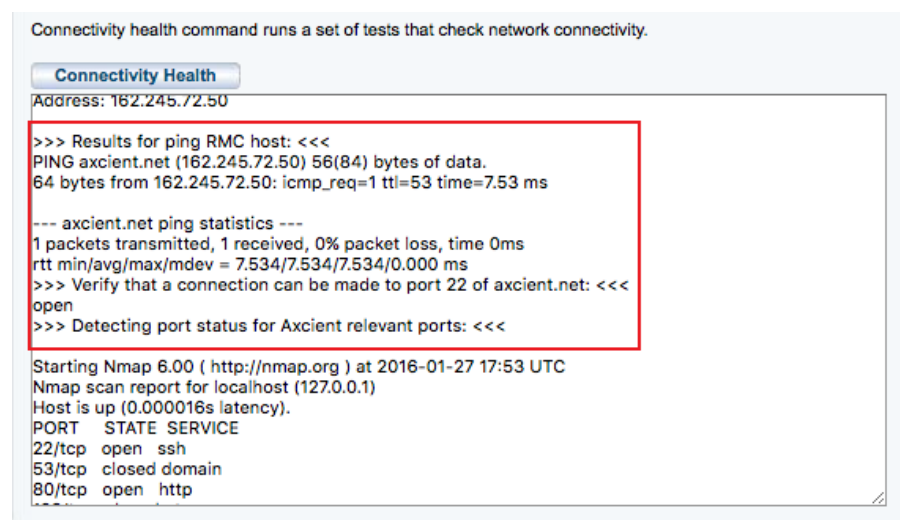
This sections covers issues related to the Axcient appliance or the Web Application.

Cannot Connect to the Web Application

A number of conditions can prevent access to the Web Application. To check connectivity between the Axcient appliance and the Web Application:

1. In the UMC, click the **system** tab in the top navigation menu.
2. Click the **network utilities** option in the left-hand menu.
3. Click the **Connectivity Health** button, which automatically tests access to the Web Application (and gateway, DNS lookup, and port 22).

Figure 43 - Connectivity Health Check



Problem	Solution
One or more appliance network settings are not correct.	Click the UMC system tab and then the network settings option to verify that the IP address, gateway, domain, workgroup, and DNS server are all correct, or update them as needed.

Problem	Solution
A needed port is not open.	The appliance communicates with the Web App 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.	<p>Configure the Axcient appliance for the proxy server. If running the Microsoft ISA firewall and configuring the proxy server does not fix the problem, turn off the web proxy as follows:</p> <ul style="list-style-type: none"> • In the <i>ISA Server Management</i> console, click on the Firewall Policy node. • In the <i>Toolbox</i> tab, click Protocols. • Expand <i>All Protocols</i>, right-click HTTP, and then click Properties. • Click Apply to update the firewall.
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 the network if the problem persists.
Appliance has not been registered.	Register the appliance using the Register Now 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.

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 Web Application can fail for a variety of reasons. The table below describes possible reasons (and corrective actions) for registration failing.

Problem	Solution
Registration failed because it is blocked by a web proxy server.	Configure the Axcient appliance for the proxy server.
Registration failed because the RMC did not find the appliance at the specified IP address.	If the Axcient appliance has been up since the IP was changed 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"> Register using a different browser other than Internet Explorer. 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.
Registration failed because either the specified DNS name is not correct or the DNS server is not forwarding/answering.	Change the DNS Server 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, do the following:

1. In the UMC, click the **system** tab in the top navigation menu.
2. Click the **network utilities** option in the left-hand menu.
3. In the *Network Utilities* screen, click the **Connectivity Health** button. This option tests access to the gateway, DNS lookup, Web Application and port 22 (checks whether it is open). The results appear in the box below the button.

Please note that hard disks on this appliance are encrypted using Cloud Key Management (CKMS). For security

reasons, the decryption key is not stored locally. Instead, the appliance will attempt to acquire the key during the boot-up process. For this reason, you must connect the appliance to the Internet before it is powered on. In the event that the Internet is not accessible, you must contact Axcient Support to acquire a temporary key to unlock the appliance.

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
```

Cloud Progress Bars Do Not Update

Browsers cache pages to improve performance by re-displaying 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 Cloud replication jobs. If the offsite backup progress bars on the dashboard do not update regularly, 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*

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 it is no longer necessary to refresh the page every time it is loaded, repeat this procedure and set the default value back to 3.

- **Internet Explorer:** *Reset Refresh Rate*

1. Start Internet Explorer and navigate to **Tools > Internet Options**.
2. In the *General* tab, click the **Settings** button in the *Browsing History* section.
3. A *Temporary Internet Files and History Settings* window displays. Under *Check for new versions of stored pages*, click the **Every time I visit the webpage** button (the default is **Automatically**). This Sets IE to refresh every time it is loaded.
4. Click the **OK** button.
5. When it is no longer necessary to refresh the pages every time they are loaded, repeat this procedure and reset 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. These messages indicate that the Axcient appliance is dangerously low on storage space, which could lead to failed backups and even data corruption. In this situation, analyze the storage requirements and do one of the following:

- Reduce the space currently used. This can only be done by one or more of the following:
 - a. Reducing the retention period of selected jobs.
 - b. Reducing the schedule frequency of selected jobs.
 - c. Deleting jobs.

- Use the Prune feature to prune backup data on an appliance and create additional free space.
- Contact [Axcient Technical Support](#) to get a larger capacity appliance that better fits your needs.

Device Problems

This section covers issues when trying to add or connect to a device.

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, do the following:

1. In the UMC, click the **devices** tab in the top navigation menu.
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 click the **Save** button.

Cannot Add Device

The following sections describe possible reasons why an Axcient appliance fails to add a device.

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.

Problem	Solution
Hostname or IP address not found.	<p>Consider the following:</p> <ul style="list-style-type: none"> When entering a host name, you can simply enter 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: hostname.subdomain.domain.com If the IP address was entered and DHCP is being used, 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 screen.

Problem	Solution
Administrative name not accepted.	<p>Consider the following:</p> <ul style="list-style-type: none"> You must have full administrative privilege on the device. For Exchange servers, and some other devices, the entered name must include the domain in the following form: <p>domain\name (Example: axcient\admin)</p> In addition, the domain name must be in the Windows domain format, not the DNS format. <ul style="list-style-type: none"> Correct: axcient\admin Incorrect: axcient.com\admin
Administrative password not accepted.	If the password was changed, the password must be updated in the device screen.

Figure 44 - Add Device Screen

add a device

Hostname or IP:

Operating system:

Device type:

Administrative username:
(Domain name required for Exchange Server. Format: domain\username)

Administrative password:

Device alias:

Additional user assigned:

Firewall Blocking Access (Windows/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, do the following:

1. Navigate to the *Windows Firewall* screen.
2. Select the **Exceptions** tab.
3. Click to select the **File and Printer Sharing** checkbox.
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. Navigate 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
```

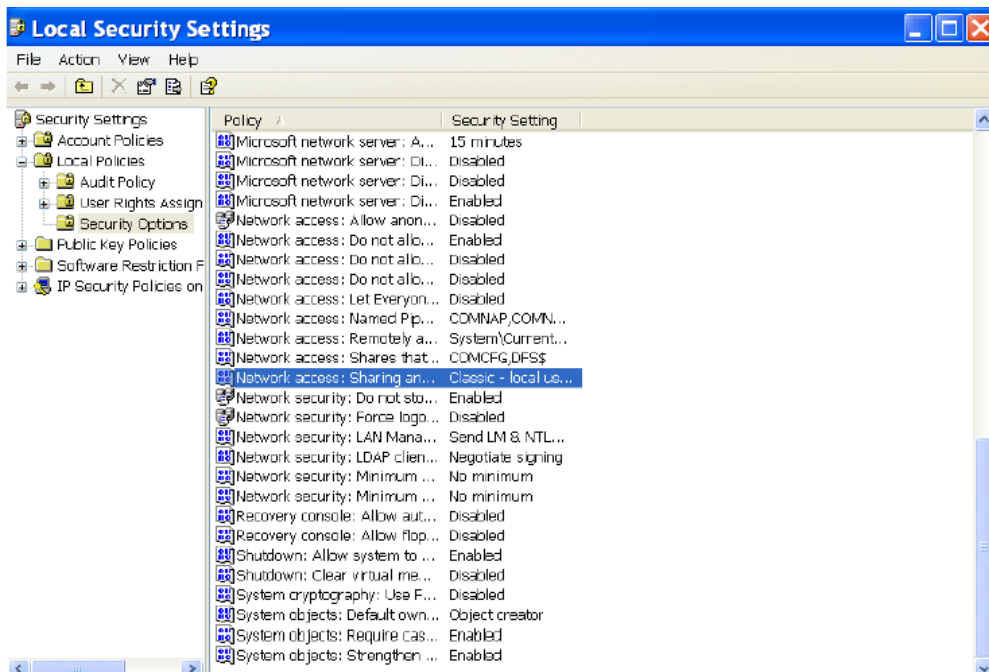
Local User Not authenticated (Windows XP)

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. Navigate to *Security Options*.
2. Double click to open the following policy:

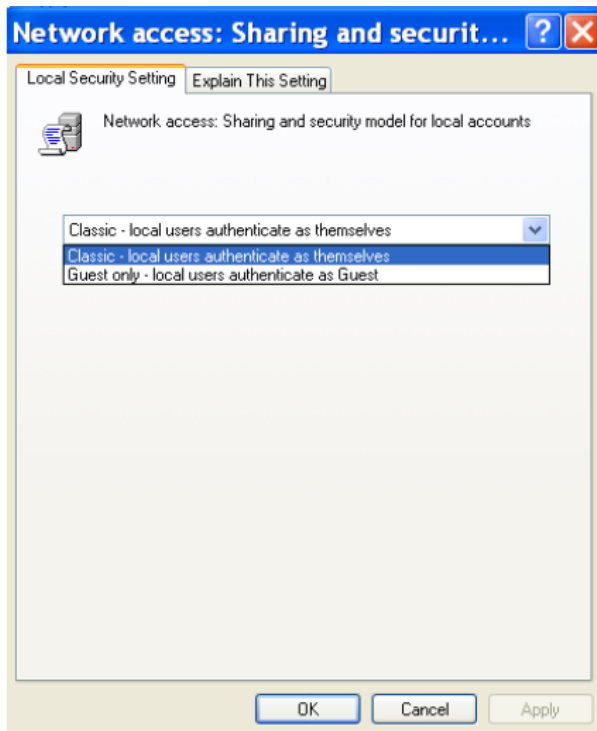
Network access: Sharing and security model for local accounts

Figure 45 - Local Security Setting Screen



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 46 - Local Security Settings Tab

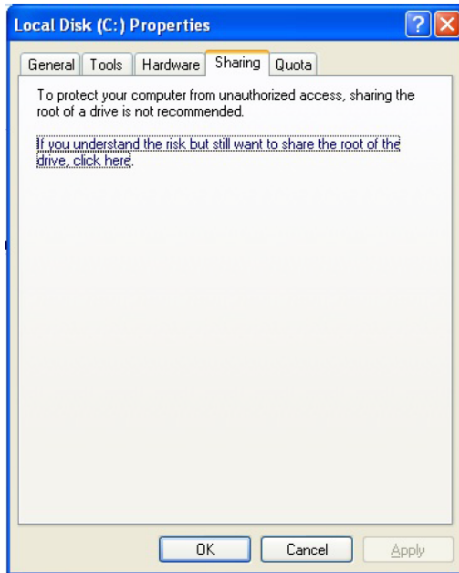


File Sharing Not Enabled (XP)

File sharing is not enabled by default. Activate it as follows:

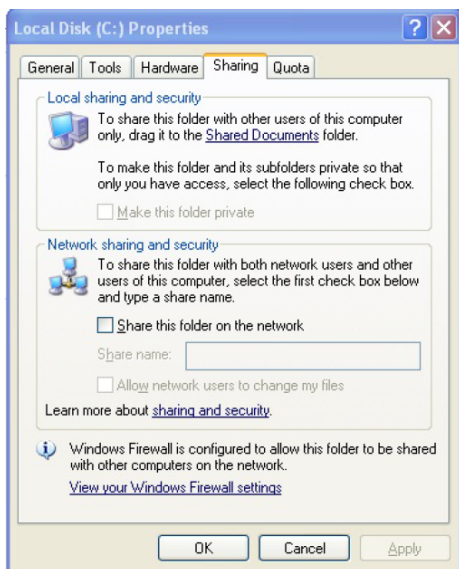
1. From *My Computer*, select the system disk (typically C:), right-click the drive, and select **Properties**.
2. In the *Properties* window, select the **Sharing** tab.
3. If file sharing is not enabled, the message *If you understand the risk but still want to share the root of the drive, click here* displays. Click this message.

Figure 47 - Properties Sharing Screen 1



4. The *Sharing* tab refreshes. Click the **OK** button (do not change any settings on the screen).

Figure 48 - Properties Sharing Screen 2

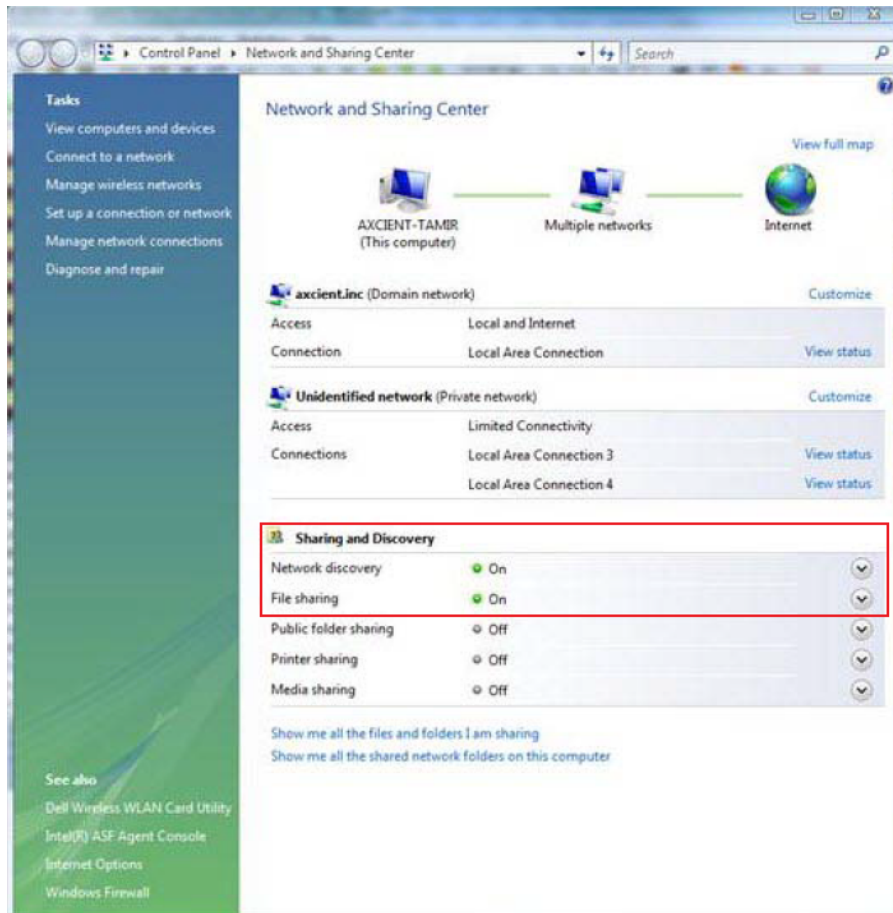


File Sharing Not Enabled (Vista)

Network discovery and file sharing are not enabled by default. Activate them as follows:

1. Launch the *Network and Sharing Center*.
2. In the *Sharing and Discovery* section, click the **On** button for *Network Discovery* and *File sharing*.

Figure 49 - Network and Sharing Center Screen



File Sharing Not Enabled (Mac OS X)

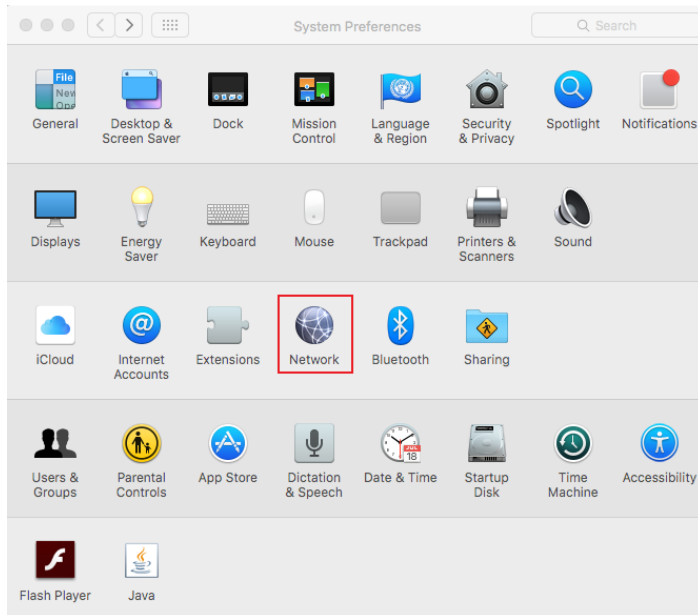
The Axcient appliance cannot access a device until file sharing is enabled. To enable file sharing when running Mac OS X,:

Warning!

This procedure applies to Mac OS X and later. The procedure for earlier versions of the Mac OS will vary.

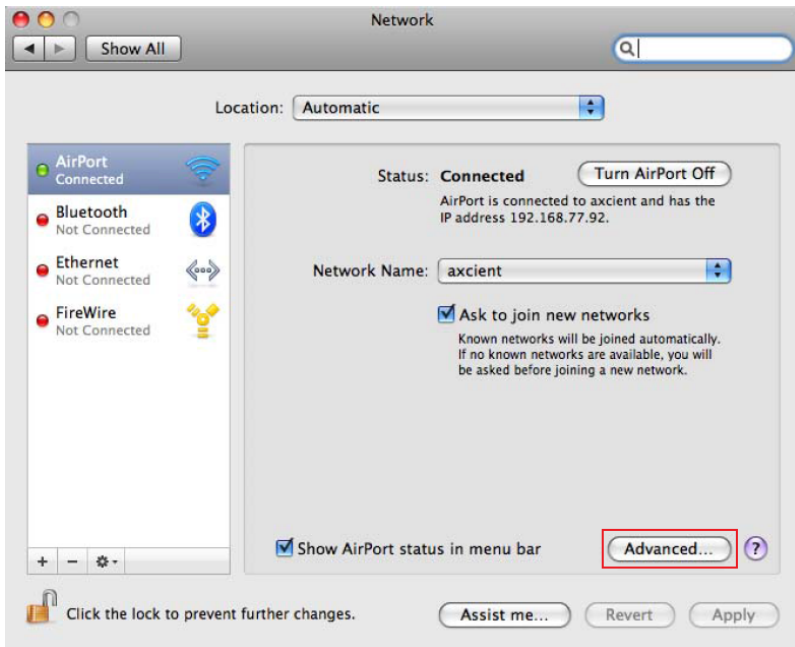
1. Navigate to *System Preferences* and select the **Network** icon under the *Internet & Network* section.

Figure 50 - Mac OS X System Preferences



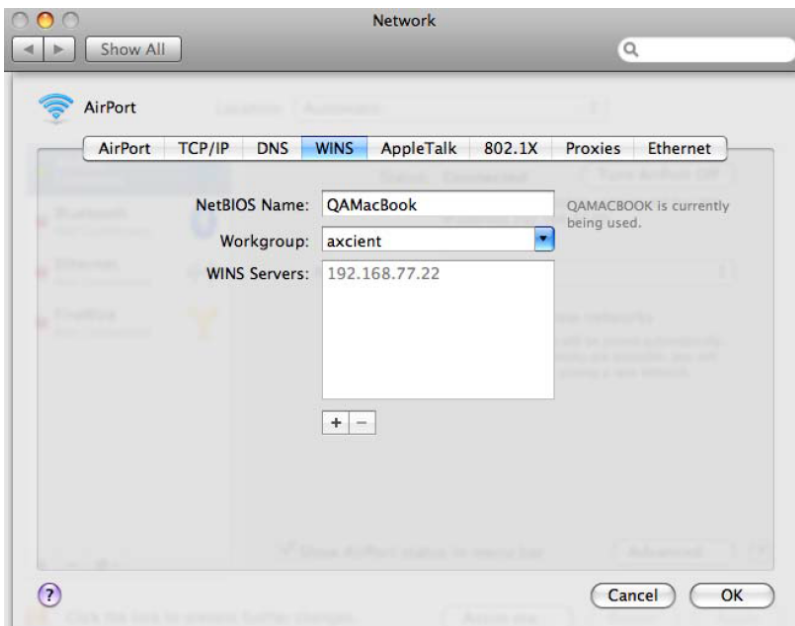
2. Select the network from the left-hand list and click the **Advanced** button.

Figure 51 - Mac OS X Network (Main)



3. Select **WINS** from the top menu. In the *WINS* display, enter the name (if the display name is not correct). Then, select a workgroup from the drop-down menu and click the **OK** button.

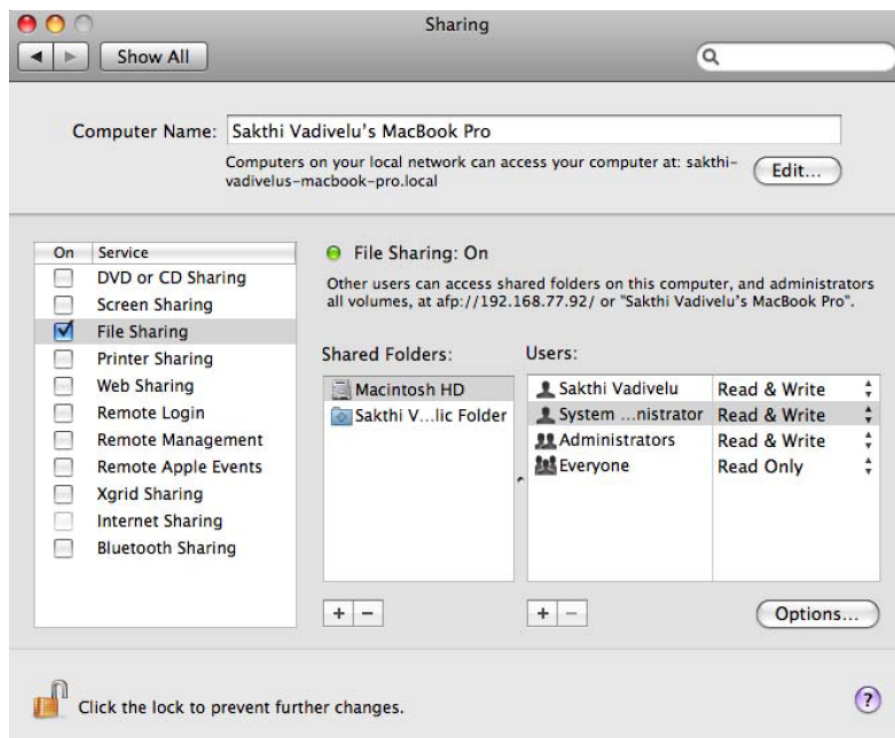
Figure 52 - MAC OS X Network Advanced)



4. The main network screen displays. Click **Apply** and then click the **back** arrow button.
5. In the *System Preferences* window, click **Sharing** under the *Internet & Network* section.

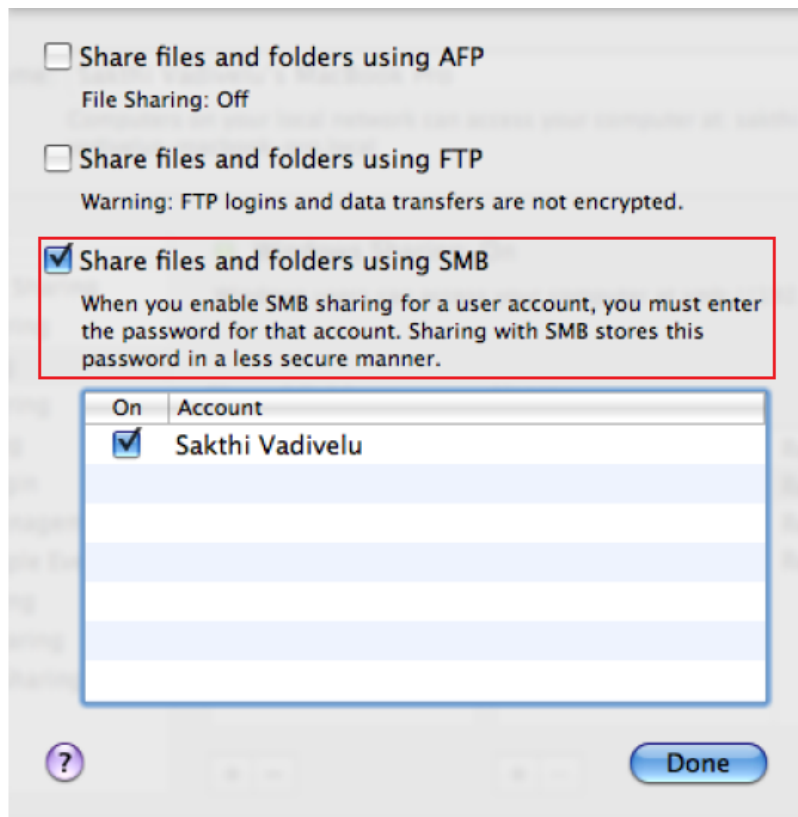
6. In the *Sharing* window, update the following:
 - a. Select the **File Sharing** box in the left pane.
 - b. Select the **folders to share** from the middle pane. Click **plus (+)** to open a window to select folders and files. After making the selection, click **Add**. The middle pane lists the selected files. Click the **minus (-)** button to remove files from the list.
 - c. Select **the user** from the right pane. Click the **(+)** button to open a window to select a **user** (or add a new user). After making the selection, click **Select**. The right pane lists the allowed users and their permissions. Click the **minus (-)** button to remove users from the list.

Figure 53 - Mac OS X Sharing (Main)



7. Click the **Options** button, and then click the **Share Files and folders using SMB** checkbox. Click **Done** when you are finished.

Figure 54 - Mac OS X



File Sharing Not Enabled (Samba)

The Axcient appliance cannot access a device until file sharing is enabled. To enable file sharing when running Samba in a UNIX-based operating system:

1. Verify the device is running the latest version of Samba as follows:

- a. Check for the latest version of installed applications (which includes Samba). To do this, enter the following command:

```
sudo apt-get install update
```

- b. Install the latest version of Samba. To do this, enter the following command:

```
sudo apt-get install samba
```

If the latest version is already installed, a message displays, indicating that is already installed. Otherwise, the installation will begin and a message will display when it has completed.

2. Navigate to the `/etc/samba` directory:

```
cd /etc/samba
```

3. Edit the `smb.conf` file. For example to use `vi` as the editor enter the following command:

```
vi smb.conf
```

4. The `smb.conf` file is the Samba configuration file. The file includes instructions on how to define a share area and allows you to configure a variety of options. The Axcient appliance requires that the following three share parameters be set for any area that will be protected:

- The `path` parameter is set to the starting point. Include the full path to the share location. For example, to be able to replicate 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
```

- Create as many share entries as necessary to allow the appropriate access. The following example configures a rootshare that sets the entire device (starting at root) as a shareable 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:

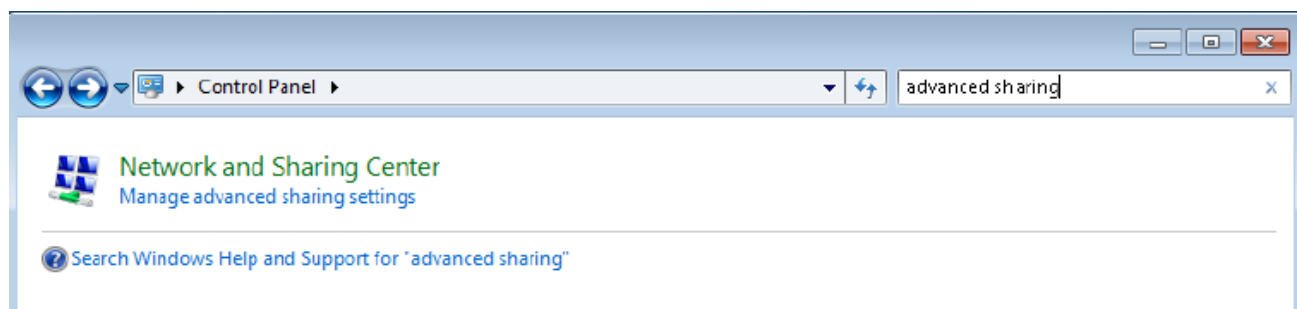
1. Enable file sharing.
2. Enable the built-in Administrator user.

Enable File Sharing

File sharing is disabled by default. To enable file sharing:

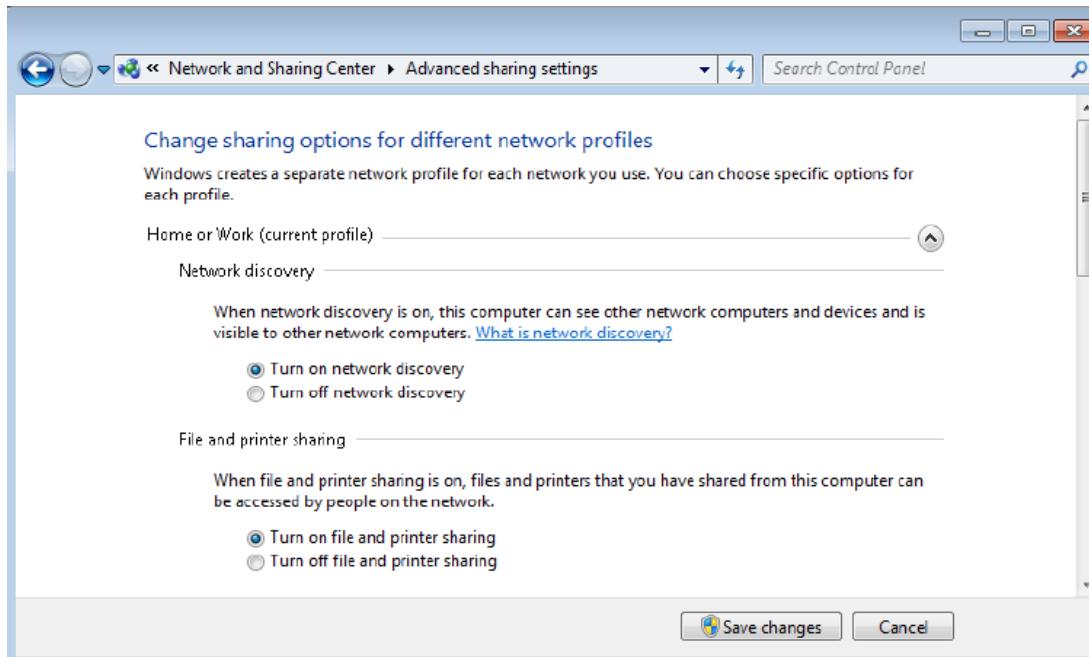
1. Select the **Start** menu and open the *Control Panel*.
2. Type *advanced sharing* in the upper-right hand search box and then click the **manage advanced sharing settings** option.

Figure 55 - Control Panel Search (advanced sharing)



3. A Change Sharing Options dialog box displays. Update the following:
 - a. Turn on network discovery by selecting the **Turn on network discovery** option under the *Network discovery* section.
 - b. Turn on file sharing by selecting the **Turn on file sharing and printing** option under the *File and printer sharing* section.
 - c. Click the **Save changes** button.

Figure 56 - Advanced Sharing Settings

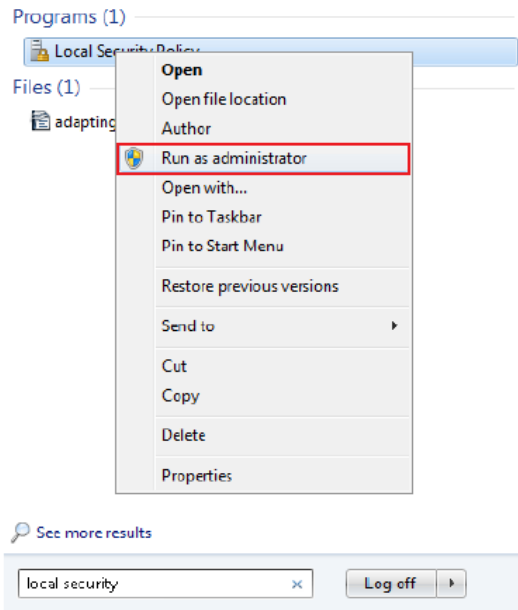


Enable Administrator

The built-in administrator user account is disabled by default. To enable the administrator:

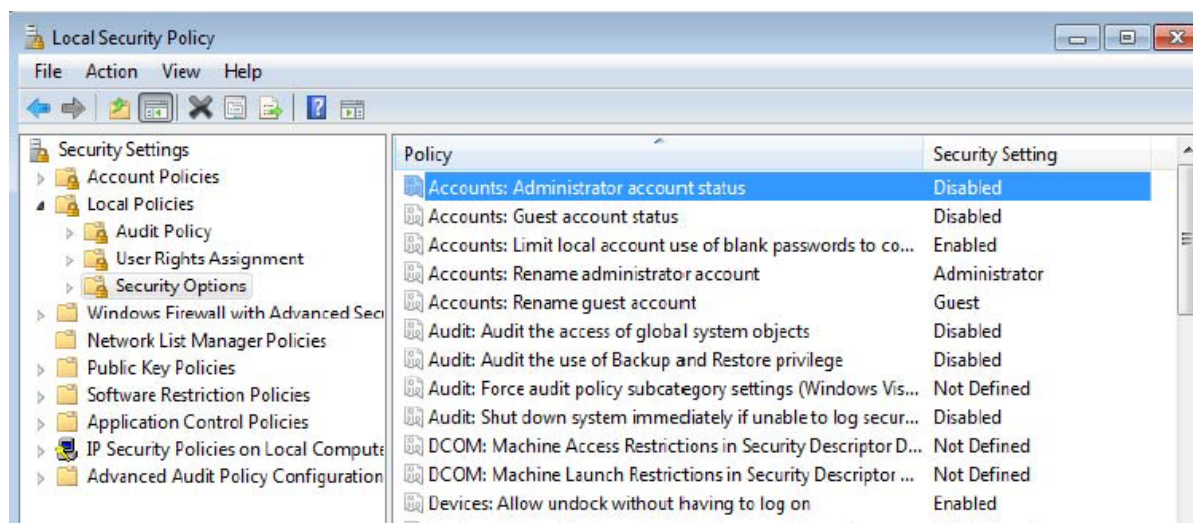
1. Select the **Start** menu and type *local security* in the search field.
2. Right-click the **Local Security Policy** option and select the **Run as administrator** option.

Figure 57 - Local Security Policy Menu



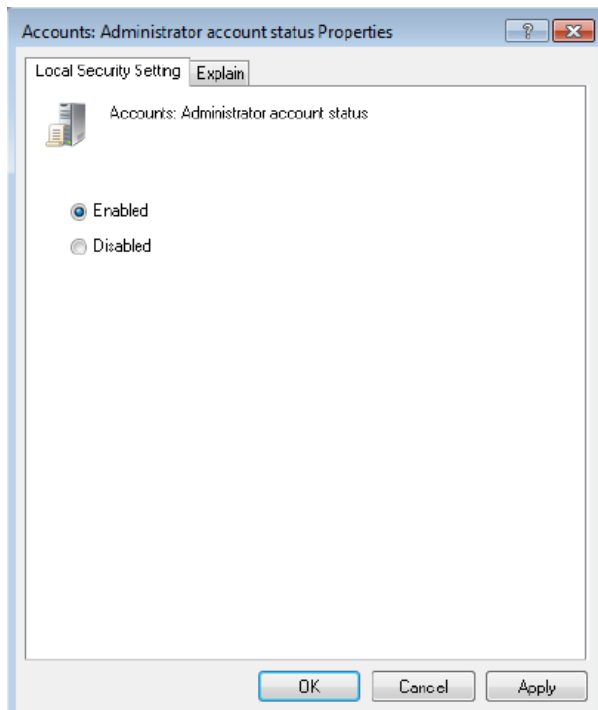
3. The *Local Security Policy* window displays. In the left-hand pane, select **Local Policies** and then select **Security Options**.
4. In the *Security Options* section, double-click to open **Accounts: Administrator account status**.

Figure 58 - Security Options: Administrator Account Status



5. The *Administrator account properties* window, select the **enabled** option and then click the **OK** button.

Figure 59 - Enable Administrator Window



6. Open the **Control Panel**.
7. Type *user* in the search box and then click **User Accounts**.

Figure 60 - Control Panel Search (Users)



8. Select **Manage another account** from the selection list.
9. Select **Administrator** from the list of accounts.
10. Select **Create password** from the list of actions.
11. Enter (and confirm) the new password. You can optionally enter a password hint as well.
12. When you are ready, click the **change password** button.

Figure 61 - Change Administrator Password Window