



Axcient

BRC Protection 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 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.

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

Table of Contents

Introduction	4
Types of Devices Protected	4
Protection of Encrypted Files	4
Replication Method	5
Required Ports	6
Deduplication	6
Preparing Devices for Protection	7
Linux Machines	7
Running the Configuration Scripts	8
Windows Server 2008 SP1	8
Screen Sleep Timeout Option for Screen Shot Validation	9
Setting Up a New Service	10
Protect Devices with an Existing Service	14
Configure the Service Settings	17
Service Settings	17
Network	18
Network Utilities	19
Active Directory	19
Service-Wide Alerts & Thresholds	21
Service-Wide Protection Policy	23
Quality of Service	24
Bandwidth Check	24
SNMP Remote Management	26
Software Update	26
Cloud Replication Schedule	27
Business Hours	27
Time	28
Rebooting the Appliance	29
Configure the Site Settings	31
Notification Configuration	31
PSA Tool	33
Custom Alert Threshold Configuration	34
Device Custom Alert Configuration	34
Job Custom Alert Configuration	36
Exclude Files from a Job	38

PSA Tool Integration	41
Recommended Practices	41
Autotask Integration with the Axcient Web Application	42
Autotask Integration in the UMC	44
Autotask Appendix	46
ConnectWise Integration in the Axcient Web Application	51
ConnectWise Integration in the UMC	54
ConnectWise Appendix	56
Configure PSA Alerting	63

Introduction

This guide describes how to protect devices using an Axcient appliance-based service, and how to configure and reconfigure various protection settings.

The Axcient protection solution should be configured to suit your business protection needs before being implemented. Once these configurations have been made, you can quickly protect multiple devices while ensuring the devices meet the business data protection standards.

The Axcient appliance sits behind the business firewall in order to protect devices without disrupting business operations. You can protect devices by configuring the appliance to query the Active Directory for devices, or by manually entering the network information for a specific device.

Local and Cloud replication jobs can only occur while the Axcient appliance and target device are powered on with a functioning outbound Internet connection.

Types of Devices Protected

Axcient protects the following devices:

- Windows-based devices—such as laptops, desktops, and servers—are fully protected and can leverage full image and file replication jobs.
- Linux-based devices can only leverage Granular File Restore tools.

Protection of Encrypted Files

The Axcient protection solution supports protection and recovery of encrypted Windows files using the **BitLocker** encryption feature. Users will be able to successfully replicate and recover all data using this encryption feature.

Axcient does not support file encryption using another encryption tool, feature, or agent. You will not be able to replicate or recover data encrypted with anything other than BitLocker.

Foreign Characters Support

In AxOS version **6.4.9 and later**, the Axcient protection solution supports protection and recovery of foreign characters that are UTF-8 encoded.

Unsupported Files

If a Windows image replication job encounters an *unsupported file*, the file will be automatically excluded from the replication process, and a warning will be printed to the event log. Despite the warning, the replication job will still complete with a status of SUCCESS.

Please note that unsupported files will not be protected using the Axcient disaster recovery and business continuity features. You must make sure that all critical data is in a supported file format in order to be recoverable.

An unsupported file is one of the following:

- A file that has been encrypted using Encrypting File System (EFS)
- A file that has a name that is not supported by Windows, such as ending with a blank or a period

In some instances, a Windows device running a Unix application might rely on posix device files (`/dev`). While replication jobs will complete successfully, failovers and Bare Metal Restores (BMR) will not.

To resolve this, you must exclude the `/dev` file from the replication job by following the steps in the [File Exclusion](#) section.

Replication Method

To protect devices, the Axcient protection solution will first perform a seed replication job to capture the entire system image of the protected device. Once the initial seed replication job is performed, Axcient leverages Reverse Incremental methods for subsequent replication jobs to achieve rapid replication and rapid recovery, while ensuring that all new data changes are captured and preserved.

This means that after the initial seed replication completes, each successive incremental replication applies the changes to the full replication that was initially performed. This creates a new full restore point each time an incremental replication job completes successfully.

This recovery process is more efficient because each restore point is independent. No incrementals need to be applied to a restore point during a recovery. This ensures that there is never any chain-breaking because each restore point is always available due to each restore point being an independent system image.

Required Ports

You will need to have the following outgoing ports open in order to access the Axcient appliance and protected devices, as well as for replication jobs to complete successfully. These are standard ports, but you should confirm the following ports are open:

- TCP Port 7 - ICMP (Ping)
- TCP Port 22 - SSH (Inbound)
- UDP Port 53 - DNS (Outbound)
- TCP Port 80 - HTTP (Appliance UI)
- TCP/UDP Port 123 - NTP (Outbound)
- TCP Port 443 - SSL (HTTPS)
- (TCP/UDP) Ports 4015 - 4040 - Namespace (Outbound)

It is very important that Ports 4015 - 4040 be open. These are ports Axcient will use to replicate data to the Axcient Cloud. If these ports are not open, cloud replication jobs will not be able to complete successfully.

Deduplication

Axcient does not support deduplication for Windows 2012.

Preparing Devices for Protection

Some preparation work is required in order to ensure that image snapshots and file replication jobs are completed successfully. This section only applies to devices protected by an appliance-based service.

Axcient offers three configuration scripts:

- The *VSS Configuration Script* creates or confirms the shadow storage of the device drive. Also confirms VSS functionality on the device.
- The *Windows Configuration Script* confirms firewall sharing settings, and the Group Policy Object (GPO) settings will not affect permissions when protecting the device. This script also confirms that all necessary permissions are enabled to give the Axcient appliance full access to protect the device.
- The *Exchange Server Configuration Script* confirms that all firewall sharing settings and permission settings are enabled to give the Axcient appliance full access to protect the device. Axcient offers three different Exchange Server Configuration Scripts depending on the version of the Exchange Server:
 - Exchange 2003
 - Exchange 2007
 - Exchange 2010

These scripts must be downloaded as a **.vbs** file and run directly on the target device. All devices should run the VSS Configuration Script and the Windows Configuration Script before being protected. All three configuration scripts should be run when protecting an Exchange Server. In this case, choose the Exchange Server Configuration Script that is closest to your version.

These scripts must be run using *Microsoft Windows Based Script Host* while in an Administrator role on the device; otherwise many of the automated commands will not be able to run due to lack of permissions.

Linux Machines

When protecting Linux-based machine, you must **enable Samba Sharing**. It is very important for you to have an understanding of Linux-based operating systems or have a team member on hand able to assist.

If you do not enable Samba Sharing on the Linux device before attempting to protect the device, the Axcient Service will be unable to detect the device or protect it. The process to enable Samba Sharing is unique to the kind of Linux operating system and version.

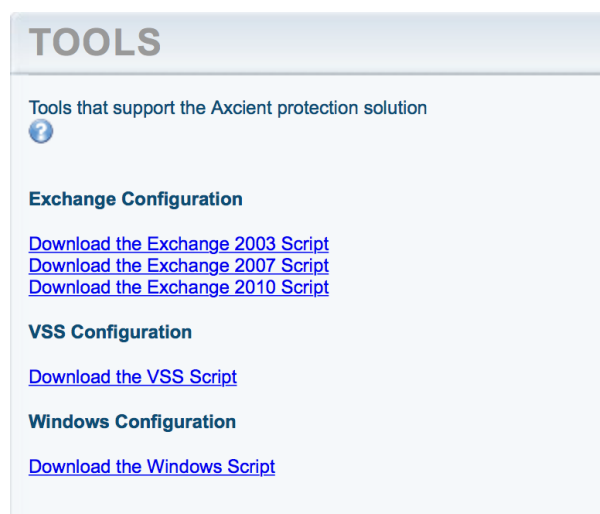
Currently, *only file replication and protection* is available for Linux operating systems. This means that the Granular File Restore tool can be leveraged for these machines, but not the BMR and Failover VM tools.

Running the Configuration Scripts

To install and run the configuration scripts:

1. Log in to the Axcient Unified Management Console (UMC) of an Axcient appliance.
2. On the UMC top navigation menu, click the **System** tab.
3. On the left-hand System navigation menu, click the **Tools** tab.
4. Right click the required scripts, select **Save Link As...** and save the file with the **.vbs** extension. Make sure that this file is saved on to the target device.
5. Navigate to the script, right click the file, select **Open With**, and then select **Microsoft Windows Based Script Host**. This is often the default script host for Windows machines.
6. Confirmation prompts will display for each step taken during the configuration script. If necessary, take any corrective action when indicated and then click **OK**. If no corrective action needs to be taken, simply click **OK**.

Figure 1 - Configuration Scripts Located in the UMC



Windows Server 2008 SP1

These additional steps only apply when recovering a Windows Server 2008 SP1 device with more than 4 drives that have been replicated by an **Axcient appliance running AxOS 6.5.1**.

When protecting a device with the Windows Server 2008 SP1 operating system, you must confirm that **the 955430 package has been installed on the target device** before performing the recovery. Please refer to the [Microsoft KB955430](#) article for more information and to download the package.

Without the 955430 package, WS2008 will be unable to install GPLPV drivers due to Windows not trusting the certificates used to sign drivers. This will mean that you will not be able to deploy a cloud failover VM for the device if it has more than 4 drives.

Screen Sleep Timeout Option for Screen Shot Validation

Screen shot validations are automatically performed after successful replication jobs to ensure that replicated devices can be successfully virtualized in the event of a disaster situation.

In order to ensure that screen shot validations can be successfully performed, please make sure the screen sleep timeout **option is set to 30 minutes or longer**.

This is because a Test VM is deployed in order to take the validation screen shot. This Test VM is deployed with minimal resources so the majority of the resources can be used by other processes on the appliance, which may result in a longer deployment process. If the Test VM goes to sleep during the deployment and the screen shot taken during the validation, it will be of a black screen and result in a failed validation.

Be advised that the longer deployment process **does not** reflect the actual deployment time for a Production Failover VM.

Setting Up a New Service

Below are the steps for how to begin protecting devices using a newly provisioned Axcient service.

STEP 1

On the Axcient Web Application Dashboard, Click on **Start Protecting** in either of the *New Service* event notifications.

The screenshot shows the Axcient Web Application Dashboard for a client named 'Yon Client' (status: Troubled). A blue banner at the top states 'New service Virtual Appliance is active!' with the message 'The wait is over! New service Yon Xiao Vapp is online and ready to begin protecting devices.' and buttons for 'START PROTECTING' and 'VIEW SERVICE'. Below this, the 'Activity of Interest for Yon Client' section shows a 'New Service' event titled 'Ready to be set up'. A table lists the service details:

NAME	TYPE	REGISTERED	
Yon Xiao Vapp	Virtual Appliance	3 days ago	Start Protecting

At the bottom, a red banner indicates '1 device requires attention'.

STEP 2

Read through the Axcient *End User Agreement*. Once you have read and understands the terms of the agreement, click **I Agree** to continue.

The screenshot shows the 'WUAF - YON XIAO VAPP SETUP' screen. It features a 'Welcome to Axcient' message with the text 'Just a little paperwork before we get started.' Below this is the 'End User Agreement' section, which includes the following text:

IMPORTANT - THIS IS A LEGAL AGREEMENT. YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

Please read this entire agreement carefully before using the Axcient service; you are accepting and agreeing to be bound by the terms of this Agreement.

1. Provision of Service.

1.1 Axcient hereby agrees to provide to you during the term of this Agreement the Axcient Service, consisting of off-site and/or on-site automated data protection, backup, and recovery services if applicable. A Data Protection Device, Virtual Data Protection Device (Virtual Appliance), or Direct-to-Cloud Agent embedded with proprietary software of Axcient (the "Axcient Software") is required to utilize the Axcient Service. The Axcient Service will

At the bottom, there are two buttons: 'I AGREE' (green) and 'I DON'T AGREE' (grey).

STEP 3

Verify the network settings for the appliance. The fields listed here will be auto-populated as part of the installation process.

Once the network settings have been verified, click **Connect to Network**.

ZUAF - YON XIAO VAPP SETUP

Verify network settings

We've detected the following settings, but please check their accuracy to ensure a configuration that works with your environment. All fields are required.

IP ADDRESS:	192.168.99.19
SUBNET MASK:	255.255.255.0
DEFAULT GATEWAY:	192.168.99.1
DOMAIN:	axcient.inc
WORKGROUP:	WORKGROUP
DNS SERVER:	192.168.44.22
HOSTNAME:	axcient
SERIAL NUMBER:	VA0615A0011600007

CONNECT TO NETWORK Skip this step

STEP 4

Enter the Active Directory credentials. This step must be completely in order for the appliance to be able to query for devices to protect.

Please note that if the Active Directory credentials are not entered correctly, the appliance will not be able to find devices to protect.

ZUAF - YON XIAO VAPP SETUP

Enter Active Directory credentials

We'll use Microsoft Active Directory to retrieve a list of computers in your network. If you don't use AD, you can skip this step.

ACTIVE DIRECTORY SERVER	192.168.66.232
WINDOWS DOMAIN	sales
DNS DOMAIN	sales.mycompany.com
ADMINISTRATOR LOGIN	Administrator
ADMINISTRATOR USER PRINCIPAL NAME	ynaveh@axcient.com ⓘ
PASSWORD	• • • • •

START DISCOVERY Skip this step

STEP 5

Select the devices to protect by checking the checkbox for the device under the *Select* column.

Click **Protect Selected** to continue once the devices have been selected.

To avoid any issues, make sure that all devices are online during the protection process. Only devices that are online can be protected.

PROTECT DEVICES ON NANCY APP2

Looks like there are 8 unprotected devices for service Nancy App2

UNPROTECTED				PROTECTED	
SELECT	HEALTH	DEVICE NAME ▲	DEVICE TYPE	SERVICE	DISCOVERED
<input checked="" type="checkbox"/>	●	ADSERVER	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>	●	ENGINEERING	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>	●	FILES	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>	●	FINANCE	Server	Nancy App2	A minute ago
<input checked="" type="checkbox"/>	●	HR	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>	●	MAIL	Server	Nancy App2	A minute ago
<input checked="" type="checkbox"/>	●	MARKETING	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>	●	OPERATIONS	Server	Nancy App2	A Minute ago

8 selected

PROTECT SELECTED

Enter device details manually

STEP 6

The Protection Policy Summary screen will appear.

Click **Edit Policy Options** to begin configuring the Default Protection Policy for the service.

This Protection Policy will be applied to all devices protected under the service and can be reconfigured at any time.

PROTECT MULTIPLE DEVICES

Excellent.

The following protection summary will be applied to the 8 selected devices.

INTERVAL

Daily

RETENTION

1 month

Note that due to differences in OS and device type, all types of recovery may not be possible for every device.

Edit Policy Options

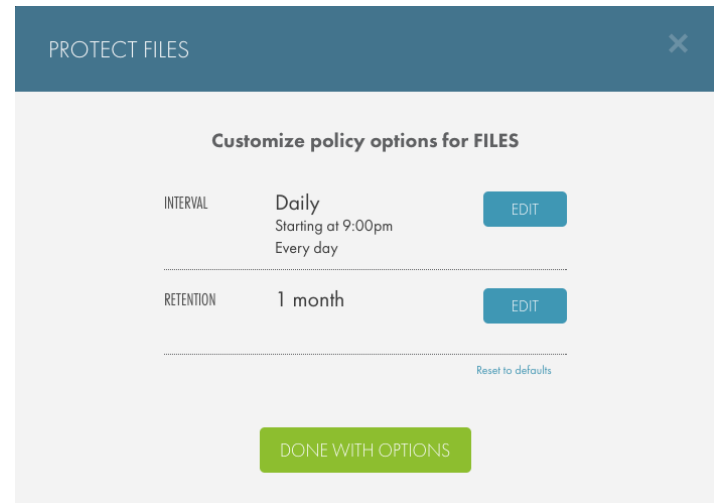
FINISH

STEP 7

You can configure the replication job interval schedule and the data retention policy for the service. Click the **Edit** button to edit either of these settings.

Click **Done With Options** to finish configuring the Default Protection Policy.

You will be returned to the *Protection Policy Summary* screen. Click the **Finish** button to finish protecting the devices.

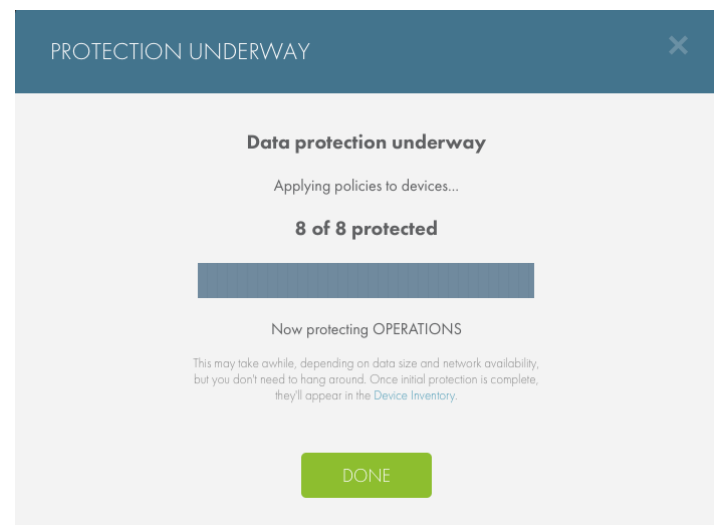


STEP 8

The selected devices are now being protected.

You are not required to stay at the *Protection Underway* screen. Click **Done** to move on to other work while the devices are being protected.

Please note that **all devices must be online** in order to be protected. You will receive an error message indicating which devices have failed to be protected and why.



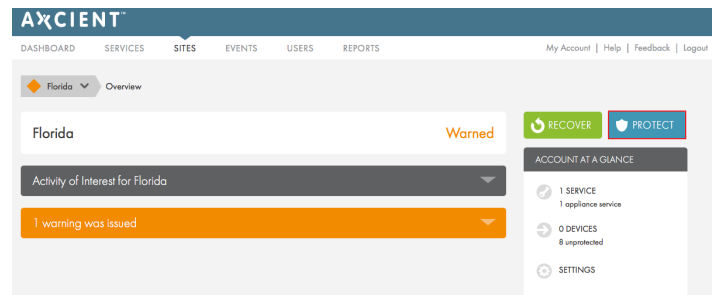
Protect Devices with an Existing Service

Please note that the service can only query devices from the Active Directory configured in the [Service Settings](#).

To protect devices using an existing service:

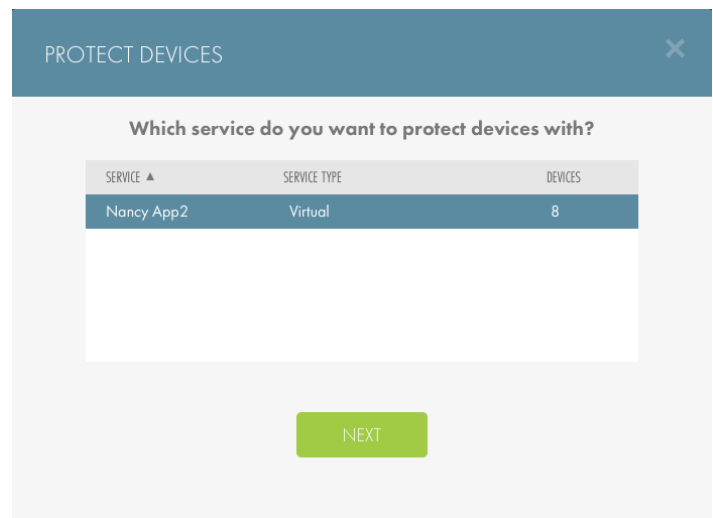
STEP 1

In either the *Service Details* page or the *Site Details* page, click the **Protect** button.



STEP 2

Select the service with which to protect the devices and click **Next**.



STEP 3

Select the device(s) you would like to protect and click **Protect Selected**.

Click **Enter device details manually** to manually enter the target device network information.

PROTECT DEVICES ON NANCY APP2

Looks like there are 8 unprotected devices for service Nancy App2

UNPROTECTED				PROTECTED	
SELECT	HEALTH	DEVICE NAME ▲	DEVICE TYPE	SERVICE	DISCOVERED
<input checked="" type="checkbox"/>		ADSERVER	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>		ENGINEERING	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>		FILES	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>		FINANCE	Server	Nancy App2	A minute ago
<input checked="" type="checkbox"/>		HR	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>		MAIL	Server	Nancy App2	A minute ago
<input checked="" type="checkbox"/>		MARKETING	Server	Nancy App2	A Minute ago
<input checked="" type="checkbox"/>		OPERATIONS	Server	Nancy App2	A Minute ago

8 selected Select all | Deselect all

PROTECT SELECTED

[Enter device details manually](#)

STEP 4

Confirm the Protection Policy that will be inherited from the service. If you do not want to configure a custom Protection Policy for the device(s) click **Finish**.

If you would like to configure a custom Protection Policy, click **Edit Policy Options**.

PROTECT MULTIPLE DEVICES

Excellent.

The following protection summary will be applied to the 8 selected devices.

INTERVAL

Daily

RETENTION

1 month

Note that due to differences in OS and device type, all types of recovery may not be possible for every device. ⓘ

[Edit Policy Options](#)

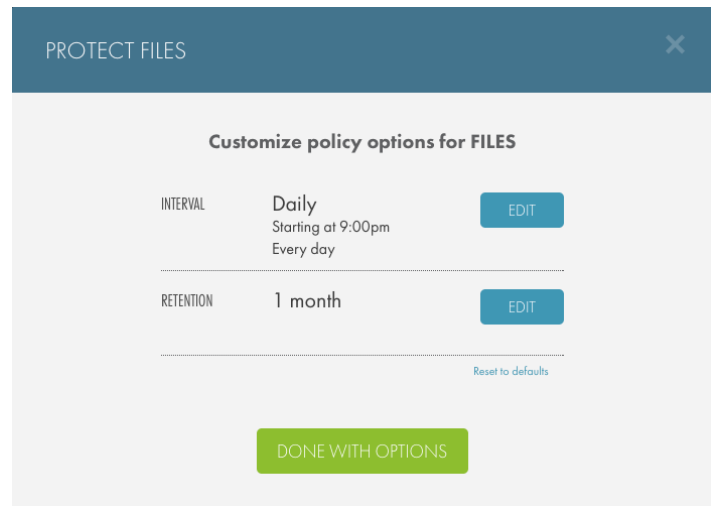
FINISH

STEP 4a

The Protection Policy configuration screen will appear if you click the **Edit Policy Options** link.

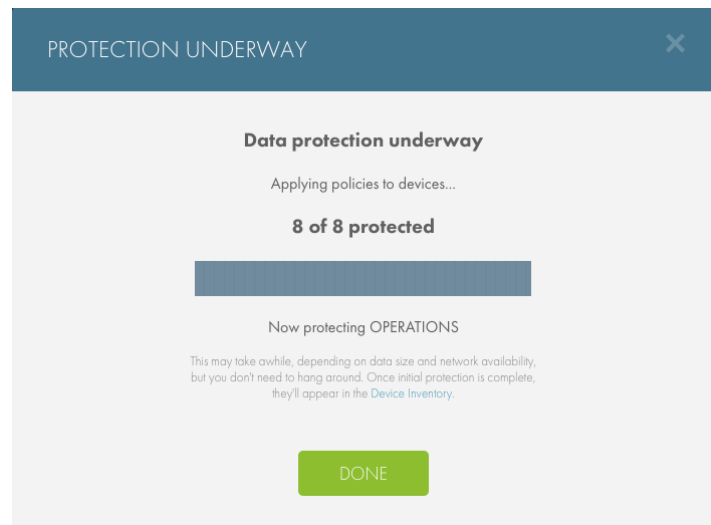
You will be able to edit the replication job interval and data retention settings for the device(s). Click the **Edit** button to edit the specific sections.

Click **Done with Options** button to finish protecting the device(s).



STEP 5

The device(s) will now be protected. Click **Done** to finish.



Configure the Service Settings

Configuring service settings is necessary for establishing replication job parameters. This includes the network settings of the service, the bandwidth thresholds, cloud replication schedule, business hours of the business, and time zone where the service is located.

To update service settings:

1. On the Axcient Web Application *Dashboard*, click **Services**.
2. On the *Services* pages, click the desired service.
3. On the *Service Details* page, click the **Configure Service** button.

Service Settings

The service settings for the Axcient appliance list general descriptive information about the Axcient appliance. This includes:

- **Service Alias** - The name of the service that appears throughout the Web Application. This field can be edited at any time.
- **Service Type** - The type of service. This field cannot be changed.
- **Service ID** - The ID for the service, which is automatically generated. This field cannot be changed.

Figure 2 - Service Settings Screen

Service Settings

ALIAS	<input type="text" value="NancyVAPP"/> ?
SERVICE TYPE	Gen2 Appliance
SERVICE ID	I4cs

SAVE Cancel

Service type and Service ID are not configurable. Please [contact support](#) to discuss changes in service.

Network

The network settings for the Axcient appliance are configured in the *Network* section of the *Configure Services* page.

As part of the installation process, the Network settings can be established either through DHCP or by manually configuring the appliance. The Network settings will already be populated when the Axcient appliance is successfully registered.

In the event that the network configurations of the Axcient appliance need to be changed, you can reconfigure them here. Otherwise, Axcient does not recommend changing the settings in this location, as this will interfere with the data protection process.

Figure 3 - Network Configuration Screen

Network

IP ADDRESS	192.168.99.192	?
NETMASK	255.255.255.0	?
GATEWAY	192.168.99.1	?
DOMAIN	pmlab.com	?
WORKGROUP	WORKGROUP	?
HOSTNAME	NancyVAPP	?
PRIMARY DNS	192.168.99.185	?
SECONDARY DNS	4.2.2.2	?
TERTIARY DNS	4.2.2.3	?

SAVE

Cancel

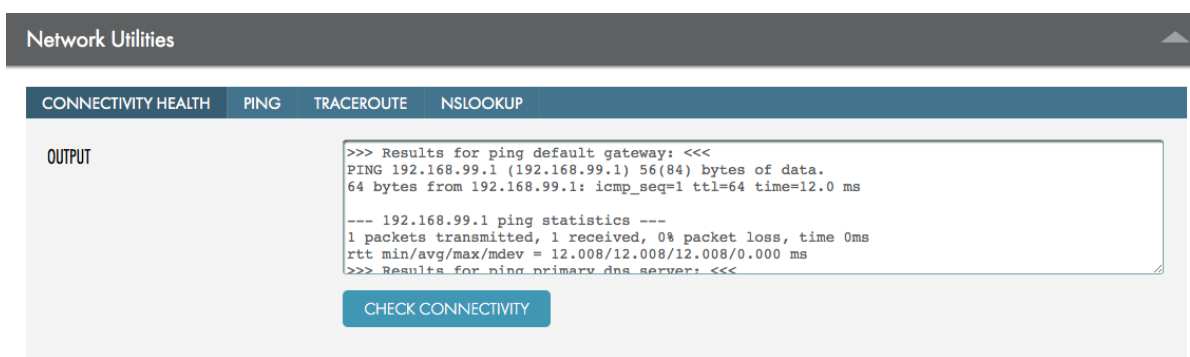
Network settings include your appliance IP address, netmask, gateway, DNS and other domain settings. This area also includes tools to test those addresses. Tools help troubleshoot addresses by pinging, running a traceroute and running an nslookup. This area also allows editing of the appliance alias. A unique alias allows easy identification in this management console.

Network Utilities

The Network Utilities tool is a collection of diagnostic tools that allow you to test the connectivity of the Axcient appliance. The diagnostic tools offered are:

- **Connectivity Health** - This tool attempts to ping the network Gateway. If the appliance cannot successfully ping the Gateway, local replication jobs will run, but cloud replication jobs will not. The Axcient appliance requires communication with Axcient's data center in order to stay registered and active. If the Axcient appliance is offline for more than **60 days** then the appliance deactivates and is no longer operational.
- **Ping** - This tool allows you to specify an IP address for the Axcient appliance to ping. This will confirm whether or not the appliance is able to communicate with the specified IP.
- **Traceroute** - This tool displays the route to a specific IP address from the Axcient appliance and measures transit delays of packets across the network.
- **NSlookup** - This tool, which is also referred to as the Name Server Lookup tool, will query the Domain Name System (DNS) to obtain the domain name of the specific IP address.

Figure 4 - Network Utilities Screen



Active Directory

Configuring Active Directory will allow you to query the business's Active Directory for devices to protect. If Active Directory is not configured, the Axcient appliance **will not be able to query devices to protect**.

When the Active Directory is configured, you can click the **Scan AD** button or the **Protect** button at the *Service Details* page or *Site Details* page. This feature will then discover devices to protect.

Figure 5 - Active Directory Configuration Screen

Active Directory

AD SERVER NAME	<input type="text" value="192.168.99.185"/>	?
WINDOWS DOMAIN	<input type="text" value="pmlab"/>	?
DNS DOMAIN	<input type="text" value="pmlab.com"/>	?
ADMIN LOGIN	<input type="text" value="administrator"/>	?
ADMIN USERNAME	<input type="text" value="yoav1"/>	?
PASSWORD	<input type="password" value="....."/>	?

Scan Active Directory
Start an Active Directory scan
for new devices

SCAN AD

SAVE

Cancel

Active Directory settings allow modification to the AD server, domain and include the login credentials. You can run an AD device scan from this area also.

The SCAN AD button runs a scan across Active Directory and searches for new devices. Results from the scan appear next to the button and links to the device inventory page where actions can be taken for the new devices.

Service-Wide Alerts & Thresholds

This section allows you to define the protection threshold under a specific Axcient Service. You can configure:

- The *Appliance connectivity loss alert* slider allows you to configure how long a device can lose connectivity before receiving an alert.
- The *Device's most recent local recovery point alert* slider allows you to configure an alert for when a device's most recent local recovery point is older than the specified period time.
- The *Device's most recent cloud recovery point alert* slider allows you to configure an alert for when a device's most recent cloud recovery point is older than the specified period of time.

The following alerts are not configurable, but will alert you when there may be important issues to investigate:

- A device's best local recovery point completed with warnings
- A device's best cloud recovery point completed with warnings
- The most recent cloud recovery point is outside the Protection Policy threshold, but there is a job currently **running an integrity check**. Integrity checks are used to verify that no data has been corrupted. These typically take longer than a standard cloud job and will enter a *Warned* state if the check takes longer than the configured device threshold.

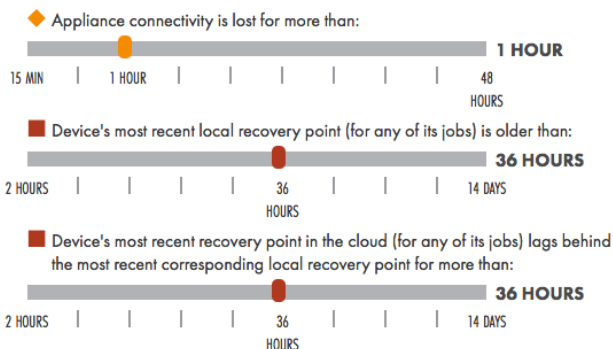
Additionally, a device's health status can be configured by navigating to the device's *Device Details* page, and then clicking the **Alerting** option. These settings will override the service-wide health status configuration.

Figure 6 - Service-Wide Alerts & Thresholds Configuration Screen

Service-Wide Alerts & Thresholds

Configurable thresholds:

Set custom alert thresholds for individual devices on their respective pages. Those settings override these unless you select otherwise during reset. [Reset these to defaults.](#)



These alerts are not configurable, but you can choose whether to be notified about them in [Site Settings](#).

- ◆ Device's best local recovery point within threshold **completed with warnings**.
- ◆ Device's best cloud recovery point within threshold **completed with warnings**.
- ◆ Device's best cloud recovery point is outside the threshold but there is a job currently **running an integrity check** (which may take longer than usual).*

**Note that this alert will not apply to appliances whose AxOS versions are older than 6.5.*

SAVE

Cancel

HOW THRESHOLDS WORK

Thresholds are service-wide and will be used to determine when a device's or client's health status changes.

Base them on your overall standard of protection and recovery point objective (RPO).

OVERRIDE BY DEVICE

Alerts can also be configured individually on device pages (if a particular device is of higher priority for instance, you may wish it to turn red sooner than the rest of your inventory).

THRESHOLD-BASED NOTIFICATIONS

Outgoing notifications are configured in [Site Settings](#) and are sent out based on the configured threshold settings.

RESET TO DEFAULTS

Service-Wide Protection Policy

You can configure the default protection policy for the Axcient Service. The policy defaults configured here will pre-populate the protection policy for new devices. Devices already protected by a protection policy will not be affected if these defaults are changed. Any changes to the Protection Policy default settings will only affect devices that are protected after the changes have been saved.

While a default protection policy is in place when you first begin using the Axcient service, Axcient recommends creating a protection policy that meets your specific business needs.

You will be able to configure:

- The interval on which the replication jobs occur (hourly, daily, or weekly)
- The time frame and days when the replication jobs will occur
- The frequency of the replication jobs
- The retention time of the replication jobs (how long replicated data will be stored)

You can also configure a unique Protection Policy for one or more new devices being protected during the protection process. You will be able to override the Service-Wide Protection Policy Defaults and protect devices using a custom policy.

Figure 7 - Service-Wide Protection Policy Defaults Configuration Screen

Service-Wide Protection Policy

Appliance-Based Services

INTERVAL Daily ▼

STARTING AT 9:00 ▼ PM ▼

FREQUENCY
☒ Every Day
☐ On Select Days

RETENTION 1 month ▼

SAVE

Cancel

Configure how frequent you want your jobs to run, when you'd like them to start. You could also set up how long you want your data to be stored.

Please note that these changes will **NOT** be applied to running jobs and will only apply from next job onward.

RESET TO DEFAULTS

Quality of Service

You can configure the Quality of Service (QoS) to optimize bandwidth usage and limit network loads for both business and non-business hours for local (LAN) and cloud (WAN) replication jobs. The lowest bandwidth usage that can be configured is **125kbps** and the highest that can be configured is **unlimited**. Unlimited means that the replication job will take up as much of the bandwidth pipe that is available at the time of the replication job. The higher the bandwidth usage, the quicker the replication jobs will complete.

For bandwidth usage during business hours, Axcient recommends consulting with your Network Administrator to determine what bandwidth throttling is best as to not impede on business operations. Weigh this decision based on the interval and frequency that the replication jobs will occur.

For bandwidth usage during non-business hours, Axcient recommends allowing as much bandwidth for the replication jobs as possible.

Figure 8 - Quality of Service Configuration Screen



Quality of Service allows you to optimize when backups run so they do not disrupt your daily business.

Settings allow throttling of WAN and LAN bandwidth during business and non-business hours.

Use the Bandwidth Check and Connectivity Health to diagnose your connection to see how bandwidth is effected by sending different packet sizes.

RESET TO DEFAULTS

Bandwidth Check

Axcient includes a diagnostic tool that allows users to test the Axcient appliance bandwidth usage. This is handy for detecting if traffic shaping or other issues are impeding the optimal flow of traffic between the appliance and Axcient data center.

Choose to send 2MB, 8MB, or 32MB of data using the existing QoS configuration. Uncheck the checkbox to use unlimited bandwidth for the test.

Figure 9 - Bandwidth Check Screen

Bandwidth Check

AMOUNT OF DATA TO SEND

☐ 2MB ☐ 8MB ☐ 32MB

BANDWIDTH RESTRICTION

☒ Run check using Data Center and current QoS
Uncheck to test Internet speed using maximum available bandwidth.

RUN

Cancel

```
>>> Results for Offsite Bandwidth Check: <<<
Uploading to Data Center with current QoS restrictions applied.
Checking Off-Site bandwidth with current QoS
Warning: Permanently added '[162.245.72.82]:4024' (RSA) to the list of known hosts.

Authorized users only. All activity may be monitored and reported.
```

SNMP Remote Management

Configure the Simple Network Management Protocol (SNMP) and trap settings to integrate the Axcient protection solution in to already existing network management environments.

Figure 10 - SNMP Remote Management Configuration Screen



The screenshot shows the 'SNMP Remote Management' configuration screen. It includes fields for 'READ COMMUNITY' (set to 'public'), 'TRAP SINK' (set to '192.168.100.1[:162][,...]'), and 'TRAP SINK COMMUNITY' (set to 'public'). There are checkboxes for 'USE INFORM NOTIFICATIONS' and 'USE V1 TRAPS', both of which are currently unchecked. At the bottom, there are 'SAVE' and 'Cancel' buttons. To the right of the form is a blue informational box with the text: 'SNMP settings let you change access and trap settings.'

Software Update

The current appliance software version is displayed here. Users have the ability to toggle automatic updates with the option of updating the Axcient appliance as soon as the update becomes available or during a designated time.

Figure 11 - Software Update Configuration Screen

Software Update

This appliance is running AxOS version 6.0.3.

UPDATE AUTOMATICALLY

ENABLED

SCHEDULE AUTO UPDATES

- ☒ **Run as soon as an update becomes available**
Allow updates whenever the appliance is free to be rebooted.
- ☐ **Run at a target time**
Allow update and reboot to only occur at a given time during the week.

SAVE

Cancel

Software Update displays the appliances current version and allows toggling of automatic updates.

Cloud Replication Schedule

Configure when the cloud replication jobs will occur for devices. You have two options:

- **Run immediately after local job** - The cloud replication job will occur automatically and immediately after a device completes its local job. This is useful if you want cloud jobs to run more frequently rather than once a day. This may help relieve WAN traffic for cloud replication jobs.
- **Follow existing schedule** - The cloud replication job will run as per the schedule specified in the Unified Management Console (UMC). Configured jobs will replicate to the Axcient Cloud every 24 hours as a single cloud job.

You can reconfigure the Cloud Replication Schedule settings at any time.

Figure 12 - Cloud Replication Schedule Configuration Screen

Cloud Replication Schedule

RUN CLOUD REPLICATION

☒ **Run immediately after local job**

Cloud replication will begin as soon as local replication completes successfully.

☐ **Follow existing schedule**

Cloud replication will run as specified on the appliance (UMC).

SAVE

Cancel

Cloud replication (also known as "offsites") offer better protection and recovery options if they run frequently. Because each job will be incremental and therefore smaller, increased frequency should not present a significant performance issue.

To change the previously-defined cloud replication schedule, login to the UMC.

RESET TO DEFAULT

Business Hours

Designate the business hours for your business. The Business Hours configuration works in tandem with QoS to control bandwidth usage for replication jobs.

Figure 13 - Business Hours Configuration Screen

Business Hours

SUNDAY	Closed	AM	to	Closed	AM
MONDAY	9:00	AM	to	5:00	PM
TUESDAY	9:00	AM	to	5:00	PM
WEDNESDAY	9:00	AM	to	5:00	PM
THURSDAY	9:00	AM	to	5:00	PM
FRIDAY	9:00	AM	to	5:00	PM
SATURDAY	Closed	AM	to	Closed	AM

SAVE

Cancel

Time settings allow you to change your business' hours of operation.

Business hours are used in tandem with QoS to give you control over bandwidth usage. You can change each day of the week's hours of operation with an option to be 'Closed'.

RESET TO DEFAULTS

Time

Specify the time zone of the Axcient appliance in order to ensure that Business Hours and QoS operate in line with your business's actual operating hours.

Figure 14 - Time Configuration Screen

Time

SERVICE TIME ZONE	(GMT-08:00) Pacific Time (US & Canada) ⓘ
RESULTING LOCAL TIME	28 Jan, 2015 3:36 PM
GMT	28 Jan, 2015 11:36 PM

SAVE

Cancel

Time zone settings allow you to change the time zone your appliance's data is displayed in.

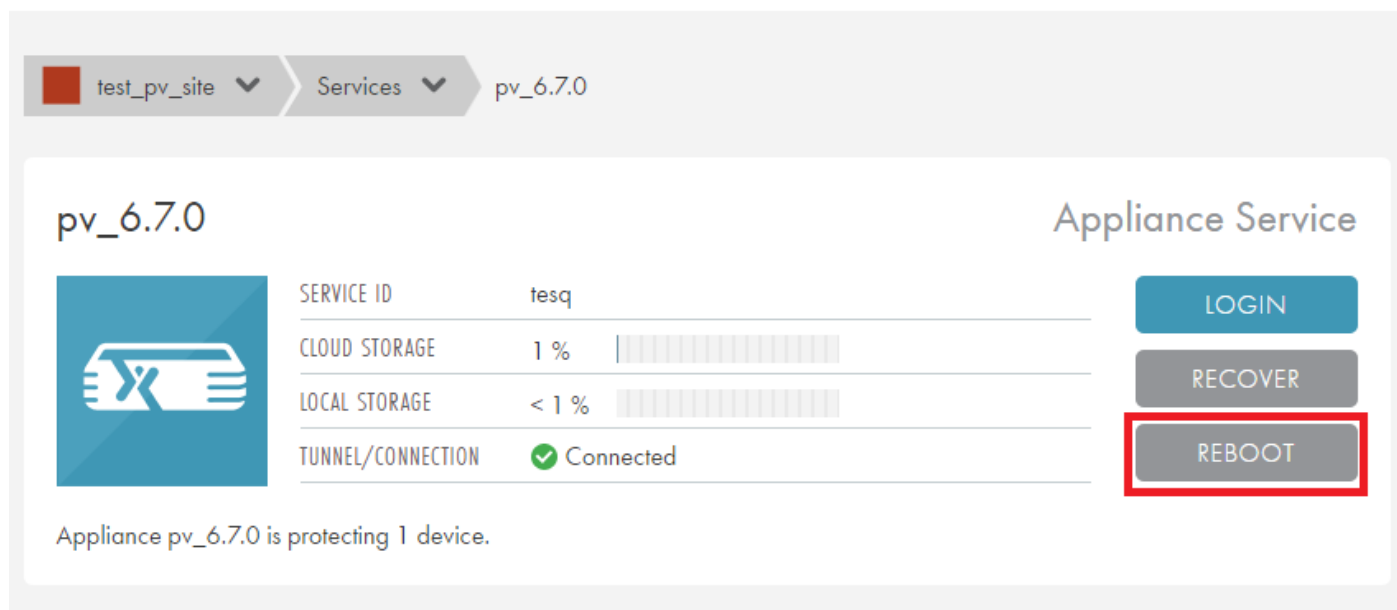
RESET TO DEFAULTS

Rebooting the Appliance

If the appliance requires a reboot, you can initiate the reboot process from the *Service Details* page.

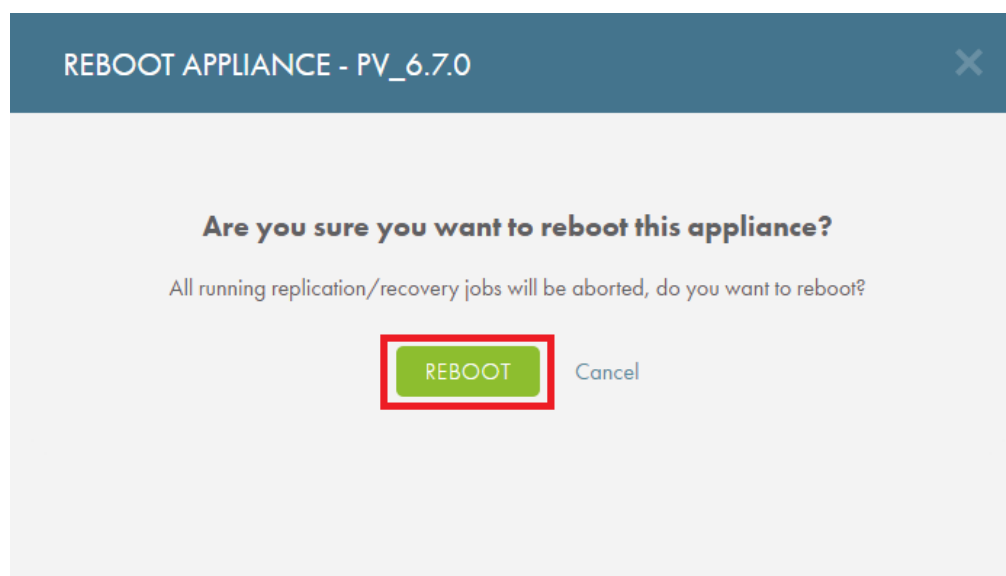
1. On the Axcient Web Application, navigate to the *Service Details* page.
2. On the *Service Details* page, click the **Reboot** button located in the *Appliance Service* section.

Figure 15 - Service Details Page



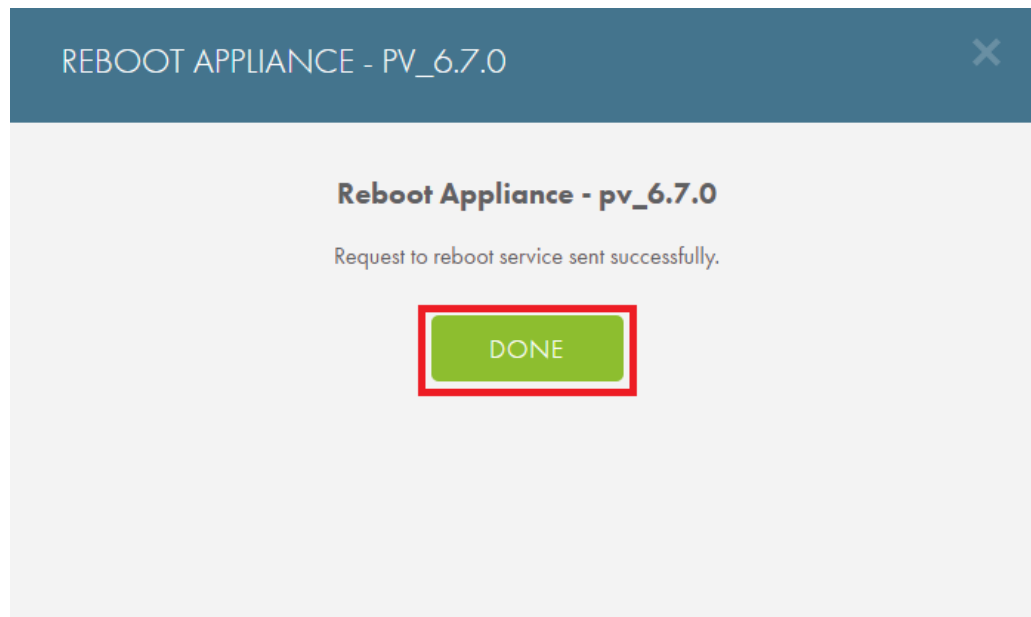
3. In the *Reboot Appliance* dialog box, click the **Reboot** button. The reboot process will initiate.

Figure 16 - Reboot Appliance Dialog Box



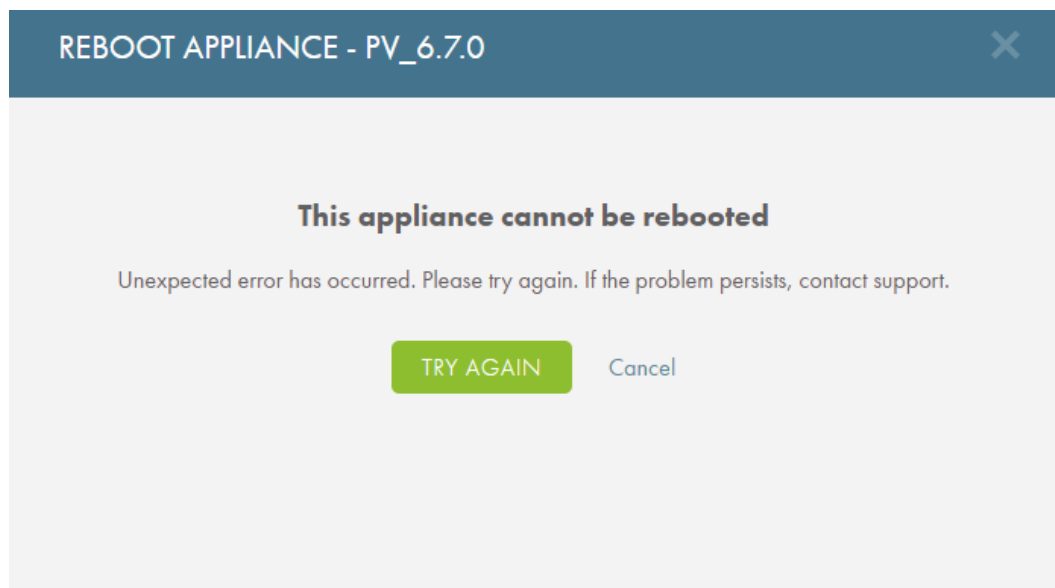
4. If the reboot process initiates successfully, you will be prompted to click the **Done** button to close the dialog box.

Figure 17 - Completed Reboot Confirmation



5. If the process does *not* initiate successfully, you will be prompted to retry the operation. This message might display if you are experiencing network problems, or if the appliance is offline. Click the **Try Again** button to retry the process. Alternatively, click the **Cancel** button to cancel the process and close the dialog box.

Figure 18 - Error Message



Configure the Site Settings

You have the ability to configure the Site Settings of an Axcient Site. From here, you can configure the alerting rules across all Services registered under the Site.

The Axcient Service can be integrated with third-party Professional Services Automation (PSA) tools, including Autotask and ConnectWise. This will allow users to maintain automation with existing tools. You can configure the PSA tool from the *Site Settings* page. Only one PSA tool may be configured at a time per Site.

Configurations are not permanent and can be changed at any time to accommodate a dynamic environment.

To launch the Site Settings configuration page:

1. On the *Axcient Web Application*, click **Sites**.
2. On the *Sites* page, click the **Details** button for the desired Site.
3. On the *Sites Details* page, click the **Settings** button under the *Account at a Glance* section.

Notification Configuration

You can select which email addresses receive alert emails. These users will be alerted when significant errors have occurred in the health status of the client's devices. These triggers are based on the Site-Wide Alerts & Threshold configuration settings.

These alerts can be configured based on:

- Local/D2C, Cloud and Connectivity issues
- Health Status (Warning and Troubled)

When a PSA tool is configured, you can assign notifications to be sent to the PSA tool.



















For more information, please refer to the [How to Configure Alerting](#) section.

Figure 19 - Notification Configuration Screen

Notification Configuration

Per-event notifications configuration

Messages will be sent informing you of significant changes in health or connectivity

NOTIFICATION TYPE	APPLIANCE			INFO
EMAIL	LOCAL REPLICATIONS	CLOUD REPLICATIONS	APP CONNECTIVITY	INFO
ascott@axcient.com	 	 		
PSA	 	 		
ConnectWise	 	 		

Health digest notifications configuration

Get a health overview of your devices and services every day

NOTIFICATION TYPE
EMAIL
--

EDIT

Notifications are outgoing messages intended to keep you informed of significant changes in the status of a site's devices. Their triggers are based on Alert Configurations set above, and the settings are service-wide.

PSA Tool

Third-party Professional Services Automation (PSA) tools can be integrated with the Axcient protection services to allow you to maintain existing automation, rather than introduce new ones. Currently, Axcient supports:

- [Autotask](#)
- [ConnectWise](#)

There are two important steps to ensure the PSA tool successfully captures and transmits events:

1. On the *PSA Tool Selector* page, select your preferred PSA tool . All required information must be entered correctly for the Axcient appliance to establish a connection.
2. On the *Notification Configuration* page, configure events that will automatically open PSA tickets.

When these steps are completed, the Axcient appliance will publish tickets directly to the PSA tools. For more information on how to configure triggering events, please refer to the [How to Configure Alerting](#) section.

Figure 20 - PSA Tool Configuration Screen

PSA Tool

CONFIGURE USING

SAVE

Car

Select a PSA Tool

Select a PSA Tool

AutoTask

ConnectWise

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.

Custom Alert Threshold Configuration

You can configure alert thresholds at both the device and job level. These options give you granular control over alerting options so that you can customize and prioritize notifications.

Performing a custom configuration will override the device thresholds defined in the [Site Settings](#) page.

Device Custom Alert Configuration

To configure custom alerting for a device:

1. On the Axcient Web Application, navigate to the appropriate *Device Details* page.
2. On the *Device Details* page, click the **Alerting** link located in the *Protection at a Glance* section. The *Custom Alert Configuration* dialog box displays.
3. In the *Custom Alert Configuration* dialog box, click the **Enable Custom Device Thresholds** checkbox. The dialog box expands to display customization options:
 - *Local Backup Threshold* is a custom alert for when the device's most recent local recovery point for any job is older than the configured threshold.
 - *Cloud Backup Lag Threshold* is a custom alert for when a device's most recent cloud recovery point for any job is older than the most recent local recovery point by more than the configured threshold.
4. Optionally, click the **Disable all cloud replication alerts for this device** checkbox found below each custom alert to turn off alerts for the device.
5. Optionally, uncheck the **Enable Custom Device Thresholds** checkbox to revert back to settings defined in the *Service Settings* page and any custom setting at the device level.
6. Click the **Save Threshold Settings** button to save your settings.

Figure 21 - Device Custom Alert Configuration Screen

[illegible]

Job Custom Alert Configuration

To configure custom alerting for a job:

1. On the Axcient Web Application, navigate to the appropriate *Job Details* page.
2. On the *Job Details* page, click the **Job Thresholds** link located in the *Job Settings* section. The *Custom Alert Configuration* dialog box displays.
3. In the *Custom Alert Configuration* dialog box, click the **Enable Custom Job Thresholds** checkbox. The dialog box expands to display customization options:
 - *Local Replication Threshold* is a custom alert for when the job's most recent local recovery point is older than the configured threshold.
 - *Cloud Replication Lag Threshold* is a custom alert for when a job's most recent cloud recovery point is older than the most recent local recovery point by more than the configured threshold.
4. Optionally, click the **Disable all cloud replication alerts for this job** checkbox found below each custom alert to turn off alerts for the job.
5. Optionally, uncheck the **Enable Custom Job Thresholds** checkbox to revert back to settings defined in the *Service Settings* page and any other custom setting at the device level.
6. Click the **Save Threshold Settings** button to save your settings.

Figure 22 - Job Customer Job Alert Configuration Screen

CUSTOM ALERT CONFIGURATION

Set custom alerting threshold for SQL Job

These custom job thresholds will override both the global thresholds defined in [Service Settings](#) and any custom setting at the protected device level.

☒ Enable Custom Job Thresholds

LOCAL REPLICATION THRESHOLD

Trigger a troubled alert when this job's most recent **local** recovery point is older than:

2 HOURS

3 DAYS

1 MONTH

1 YEAR

36 hours

☐ Disable all local replication alerts for this job

CLOUD REPLICATION LAG THRESHOLD

Trigger a troubled alert when this job's most recent recovery point in the **cloud** lags behind the most recent local recovery point by more than:

2 HOURS

3 DAYS

1 MONTH

1 YEAR

36 hours

☐ Disable all cloud replication alerts for this job

SAVE THRESHOLD SETTINGS

Cancel

© 2019 Axcient, Inc. All Rights Reserved.

37

Exclude Files from a Job

This feature is only available on AxOS version 6.5.1 or later.

You can exclude drives, folders, and files from replication jobs by clicking the **Exclusions** button in the *Job Details* page.

To include or exclude a drive, folder, or file:

1. On the *Job Details* page, click the **Exclusions** link found in the *Job at a Glance* panel. The *Exclusions* dialog box displays.

NOTE: By default, the *Exclusions* dialog box will use the \$ symbol instead of the : symbol. These symbols are interchangeable and either can be used when creating exclusion and inclusion rules. The : symbol is used in this document.

2. In the *Exclusions* field, configure items to be excluded:

- To exclude an entire drive, enter the drive letter in the following format:

`<Drive Letter>:/`

Example: `E:/`

- To exclude a folder from a drive that is being backed up, enter the drive letter and target folder in the following format:

`<Drive Letter>:/<Folder Name>`

Example: `C:/Documents`

- To only exclude a specific file from a drive and folder being backed up, enter the drive letter, along with the target folder and the specific file in the following format:

`<Drive Letter>:/<Folder Name>/<File Name>`

Example: `C:/Desktop/Old_Image.png`

3. In the *Inclusions* field, configure items to be included:

- To include a drive, no additional step is necessary. All drives are included in the replication job as long as no Exclusion rule is set in the *Exclusions* field.
- To include a folder from an excluded drive, enter the drive letter along with the target folder in the following format:

`<Drive Letter>:/<Folder Name>`

Example: `E:/Music`

- To include a specific file from an excluded folder, enter the drive letter along with the target folder and the specific file in the following format:

`<Drive Letter>:/<Folder Name>/<File Name>`

Example: `C:/Documents/Test_File.docx`

4. When all of the exclusion and inclusion rules are configured, click the **Save Exclusions** button.

Figure 23 - Exclusions Screen

EXCLUSIONS

Enter a complete path to exclude or include a file or folder

Your changes will apply to future jobs, and only if the path exists in this device's file structure. Enter one path per line.

Remove drive path from **both** exclusions and inclusions to no longer track it.

EXCLUSIONS3 total

E:
C:/Documents
C:/Desktop/Old_Image.png

INCLUSIONS3 total

C:
E:/Music
C:/Documents/Test_File.docx

SAVE EXCLUSIONS

Cancel

© 2019 Axcient, Inc. All Rights Reserved.

39

Additional Exclusion and Inclusion Notes

- When a device is added, all detected drives will populate the *Inclusions* section of *Exclusions* dialog box.
- Axcient recommends that you **do not** delete a drive from the *Inclusions* field in order to exclude it from the replication job.

If a drive is removed from the *Inclusions* field but not added to the *Exclusions* field, it will be implicitly included in the replication job. A drive must be explicitly listed in the *Exclusions* field in order to be excluded from the replication job.

Example: In the figure below, the `E: /` drive is not listed in the *Inclusions* field. Instead, the `E: /Personal` folder is listed. In this case, there is no need to explicitly list a folder in the *Inclusions* field because the `E: /` drive is not explicitly listed in the *Exclusions* field. Because it is not listed in the *Exclusions* field, the entire `E: /` drive will be replicated during regularly scheduled replication jobs.

You need to list folders and files in the *Inclusions* field only when the containing drive and folder are listed in the *Exclusions* field.

Figure 24 - Exclusion Example

PSA Tool Integration

This section describes how to integrate the Autotask and ConnectWise Professional Services Automation (PSA) tools with the Axcient protection solution. The instructions listed here assume that you have already configured the PSA tool as needed.

An Axcient Client can only be configured with a single Autotask account or a single ConnectWise account. You will not be able to configure an Axcient Service with multiple Autotask or ConnectWise accounts.

Additionally, you cannot have both Autotask and ConnectWise PSA tools operating at the same time on a single Site. You will need to select a single PSA tool to integrate with each Site.

Recommended Practices

Before integrating the PSA tool, Axcient recommends the following:

- When integrating with Autotask, create a unique *Client Account* for the desired Client site(s), whether these are customers or remote offices. If necessary, create a *Service Desk Queue* for the Client site(s). This is a way to categorize similar tickets and designates resources to monitor and respond to tickets in the queue.
- When integrating with ConnectWise, create a unique *Integrator Login* for the desired Client site(s) and Company Account, whether these are customers or remote offices. For instructions on how to create an Integrator Login or any other ConnectWise-specific questions, please refer to [online ConnectWise support](#).

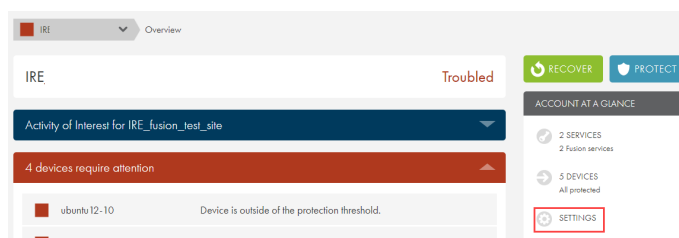
Autotask Integration with the Axcient Web Application

You can configure Autotask integration settings from the *Site Settings* page.

To integrate with the Autotask PSA Tool:

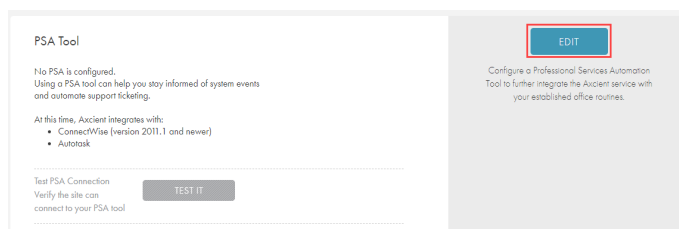
STEP 1

In the *Site Details* page, click the **Settings** link.



STEP 2

In the *PSA Tool* section, click the **Edit** button.



STEP 3

In the *Configure Using* drop-down menu, select **Autotask** and update the following fields:

- In the *Username* field, enter the **username** used to log in to the administrating Autotask account.
- In the *Password* field, enter the **password** used to log in to the administrating Autotask account.
- In the *Confirm Password* field, confirm the **password** entered in the *Password* field.
- In the *Account ID* field, enter the **Account ID** of the target Client site. This is automatically generated when creating an account in Autotask. For instructions on how to obtain the Account ID, please refer to the [How to Obtain the Account ID](#) section below.

 This screenshot shows the 'PSA Tool' configuration form. The 'CONFIGURE USING' dropdown is set to 'Autotask'. The form includes fields for 'USERNAME' (lhperry@axcientpartnerdemo.com), 'PASSWORD' (masked with dots), 'CONFIRM PASSWORD' (masked with dots), 'ACCOUNT ID' (80243651), and 'QUEUE ID' (29878555). There are 'SAVE' and 'Cancel' buttons at the bottom.

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.

- In the *Queue ID* field, enter the **Queue ID** for the appropriate Service Desk Queue. This will bundle similar tickets so that you can quickly respond and resolve issues. For instructions on how to obtain the Queue ID, please refer to the [How to Obtain Queue ID](#) section below.

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

Autotask Integration in the UMC

You can integrate the Autotask PSA tool in the UMC in addition to the Web Application (RMC). This will allow you to configure specific events to publish to the PSA tool.

Because the UMC is appliance-specific, you will *need to log in to each appliance* to integrate with Autotask. When you log in to the UMC, you can optionally inherit configuration settings from the Web App.

If Autotask has already been integrated, please continue to the [How to Configure Alerting](#) section for more information on how to configure specific events to publish to the PSA tool.

To integrate Autotask in the UMC:

1. On the UMC, click the **System** tab in the top navigation menu.
2. On the left navigation menu, click the **PSA** option. The *PSA* page displays.
3. Optionally, on the *PSA* page, click the **Inherit PSA Configuration Info from RMC** checkbox to inherit PSA settings already configured through the Axcient Web Application (RMC) .
4. Alternatively, on the *PSA* page, select **Autotask** from the drop-down menu and click the **Configure PSA Tool** button.
5. Enter the following information:
 - In the *Username* field, enter the **username** used to log in to the administrating Autotask account.
 - In the *Password* field, enter the **password** used to log in to the administrating Autotask account.
 - In the *Confirm Password* field, confirm the **password** entered in the *Password* field.
 - In the *Account ID* field, enter the **Account ID** of the target Client site. This is automatically generated when creating an account in Autotask. For instructions on how to obtain the Account ID, please refer to the [How to Obtain the Account ID](#) section below.
 - In the *Queue ID* field, enter the **Queue ID** for the appropriate Service Desk Queue. This will bundle similar tickets so that you can quickly respond and resolve issues. For instructions on how to obtain the Queue ID, please refer to the [How to Obtain Queue ID](#) section below.
 - In the *Priority* field, assign a **priority number** to determine the ticket order assigned for tickets automatically published to Autotask. Leave this field empty to automatically set the priority to that of the default setting in Autotask.
6. Click the **Save** button.

Figure 25 - Autotask Configuration Screen in the UMC

PSA

AutoTask Configuration

Username

Password

Confirm Password

Account ID

Queue ID

Priority

Autotask Appendix

As part of the Autotask integration process, you will need to complete a set of basic configuration tasks within the Autotask platform.

This section of the guide outlines basic configuration tasks that take place within the Autotask platform. As a best practice, however, we recommend referencing Autotask documentation for complete configuration steps.

Obtain the Account ID

The Account ID is found in the *Account Details* page of the appropriate account. To obtain the Account ID:

1. On the top navigational menu, point to the **My...** tab and click **Accounts** under the *CRM* section.
2. Use the *Search* field to find the account.
3. Click the **account** or right-click the account and select **View Account**.
4. The *Account ID* is located in the left-hand section.

Figure 26 - Autotask Account Details Screen

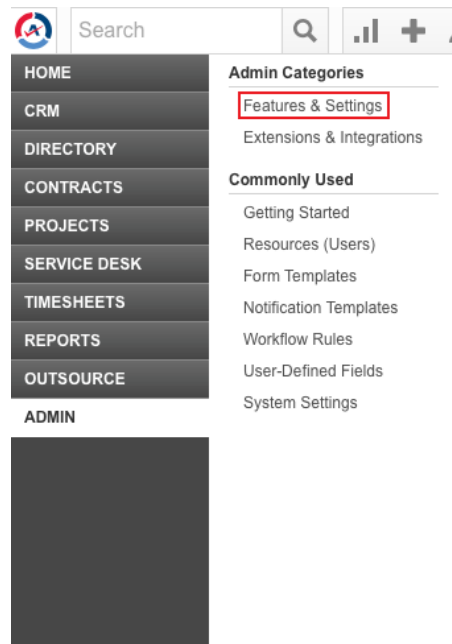
The screenshot displays the Autotask CRM interface. On the left, the 'MY ACCOUNTS' sidebar shows a search field and a list of accounts. A red box highlights the 'Accounts (164)' link in the 'CRM' section. A right-click context menu is open over the 'Anchor Network Solutions' account, with 'View Account' highlighted. The main area shows the 'Account Details' for 'Anchor Network Solutions (ID: 30243651) | Active Customer'. The 'Account ID' is displayed as 30243651. The 'Account Manager' is Steve Perry. The 'Territory Name' is Asia. The 'Region Name' is CO. The 'Market Segment' is not specified. The 'Competitor' is not specified. The 'Total Opportunity Amount' is not specified. The 'Status' is not specified. The 'Activity for Anchor Network Solutions' section shows a list of activities, with a note indicating that there are no items to display from the last 6 months.

Obtain the Queue ID

The Queue ID is found in the *Queue Details* page of the appropriate Service Desk Queue, located in the *Features & Settings* section. To obtain the Queue ID:

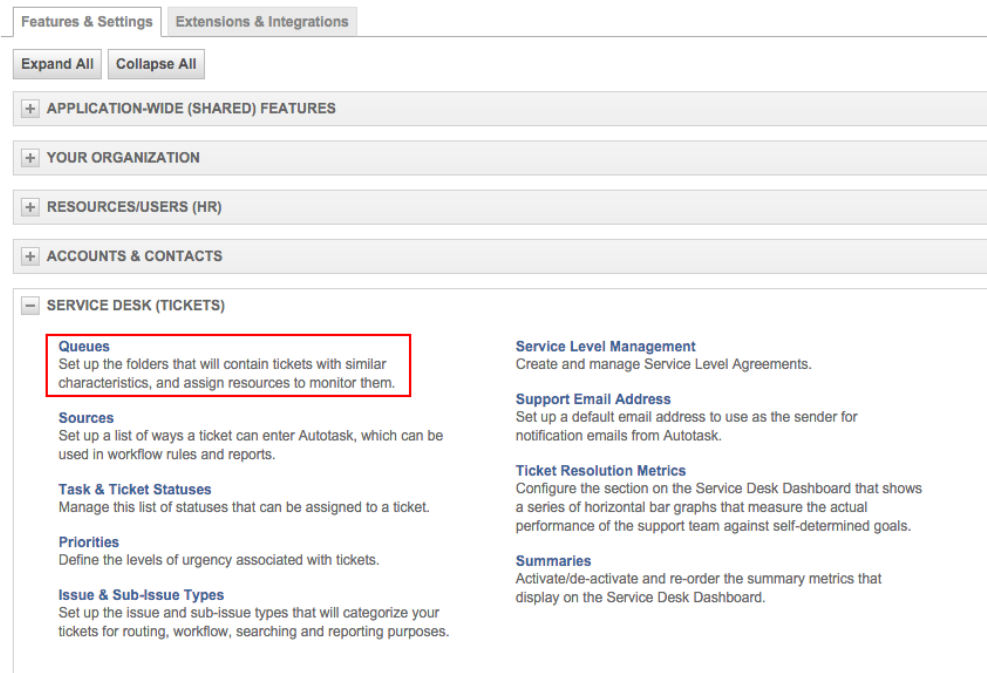
1. On any screen, point to the Autotask 'A' logo to access the drop-down menu. Point to the *Admin* option and then click the **Features & Settings** option.

Figure 27 - Autotask Features & Settings Option



2. Expand the *Service Desk (Tickets)* section and click the **Queues** option.

Figure 28 - Queues Option in the Service Desk Section



- Right-click the desired *Service Desk Queue* and select the **Edit Queue Details** option.

Figure 29 - Edit Queue Details Option

The screenshot shows the 'SERVICE DESK QUEUES' management interface. At the top, there's a header with a back arrow and the title. Below it, a sub-header explains the purpose: 'Set up the folders that will contain tickets with similar characteristics, and assign resources to monitor them.' There are three buttons: '+ New', 'Save', and 'Cancel'. Below these is a table with two columns: 'Name' and 'Description'. The table lists several queues: Administrative, Anchor HD, AutoQueue, Autotask Consulting, CLEP, Client Portal, CSD, and Helpdesk. A right-click context menu is open over the 'Autotask Consulting' queue, showing options: 'Edit Queue', 'Edit Queue Details' (highlighted with a red box), 'Inactivate Queue', and 'Delete Queue'.

Name	Description
Administrative	Administrative
Anchor HD	Tier 1 Helpdesk Requests
AutoQueue	
Autotask Consulting	Autotask Consulting
CLEP	
Client Portal	Service Desk
CSD	CSD
Helpdesk	Escalated Helpdesk Requests

- Note the Queue ID is located in the *Queue Summary* screen.

Figure 30 - Queue Number Location

The screenshot shows the 'QUEUE SUMMARY' screen for a specific queue. The browser address bar shows the URL: <https://ww2.autotask.net/autotask/popups/administration/QueueDetails.aspx?objectId=29878555&type=queue>, where the '29878555' is highlighted with a red box. The page has a header with a question mark icon. Below the header are 'Save & Close' and 'Cancel' buttons. There are two tabs: 'Summary' (selected) and 'Resources'. The 'Summary' tab contains several fields: 'Queue Name*' (Anchor HD), 'Queue Location*' (British Columbia), 'Queue Number' (29878555, highlighted with a red box), and 'Queue Description' (Tier 1 Helpdesk Requests). There is also a checkbox for 'Appears in Client Portal' which is checked. At the bottom, there is a section for 'Queue Location'.

ConnectWise Integration in the Axcient Web Application

You can configure ConnectWise integration settings from the *Site Settings* page.

To integrate with the ConnectWise PSA tool:

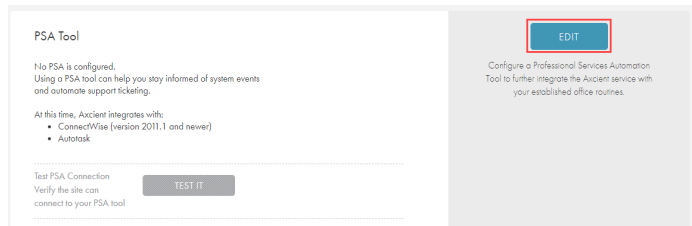
STEP 1

In the *Site Details* page, click the **Settings** link.



STEP 2

In the *PSA Tool* section, click the **Edit** button.



STEP 3

In the *Configure Using* drop-down menu, select **ConnectWise** and update the following fields:

- In the *URL* field, enter the **domain** portion of the address used to access ConnectWise. Enter the URL as illustrated in the following example:
 - **Correct** - *connectwise.com*
 - **Incorrect** - *www.connectwise.com*
 - **Incorrect** - *http://connectwise.com*
- In the *API Key* field, enter the **public API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
- In the *API Secret* field, enter the **private API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
- In the *MSP Company ID* field, specify the **company name**. For more information on how to obtain the ID, please refer to the [Obtain Login Information](#) section below.
- In the *Company ID* field, enter the appropriate **company ID**. For more information on how to obtain the ID, please refer to the [Obtain Client Information](#) section.
- In the *Service Type* field, specify the type of **service action** to take. The value entered here must match the value in the corresponding *Service Type* field in ConnectWise. For more information, please refer to the [Obtain Service Type and Subtype](#) section.
- In the *Location* field, specify the **client location**. The value must match the *Territory* field in ConnectWise. For more information, please refer to the [Obtain](#)

PSA Tool

CONFIGURE USING	ConnectWise
URL	<input type="text" value="https://connectwise.com"/>
API KEY	<input type="text" value="XXXXXXXXXXXX"/>
API SECRET	<input type="text" value="XXXXXXXXXXXXXXXXXXXX"/>
MSP COMPANY ID	<input type="text" value="Axcient_f"/>
COMPANY ID	<input type="text" value="AX"/>
SERVICE TYPE	<input type="text" value="Warranty"/>
LOCATION	<input type="text" value="Tampa Office"/>
ADDRESS LINE 1	<input type="text" value="2106 SHADYHILL TER"/>
ADDRESS LINE 2	<input type="text" value=""/>
CITY	<input type="text" value="Harrells"/>
STATE	<input type="text" value="Florida"/>
ZIP	<input type="text" value="34667"/>
TICKET PRIORITY	<input type="text" value="Priority 1 - Emergency Response"/>
SERVICE SUBTYPE	<input type="text" value="st1"/>

SAVE

Cancel

[Client Information](#) section.

- In the *Address Line 1* field, enter the **client company street address**. This is not a required field.
- In the *Address Line 2* field, enter the second line of the **client company street address**. This is not a required field.
- In the *City* field, enter the **client company city**. This is not a required field.
- In the *State* field, enter the **client company state**. This is not a required field.
- In the *Zip* field, enter the **client company ZIP code**. This is not a required field.
- In the *Ticket Priority* field, enter the **ticket priority number**, which must match a ticket priority set on the server. If left blank, the ticket priority set on the server will be used. For more information, please refer to the [Obtain Priority](#) section.
- In the *Service Subtype* field, enter the **service subtype**, which must match a subtype set on the server. If left blank, the service subtype defaults on the server will be use. For more information, please refer to the [Obtain Service Type and Subtype](#) section.

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

ConnectWise Integration in the UMC

You can integrate the ConnectWise PSA tool in the UMC in addition to the Web Application (RMC). This will allow you to configure specific events to publish to the PSA tool.

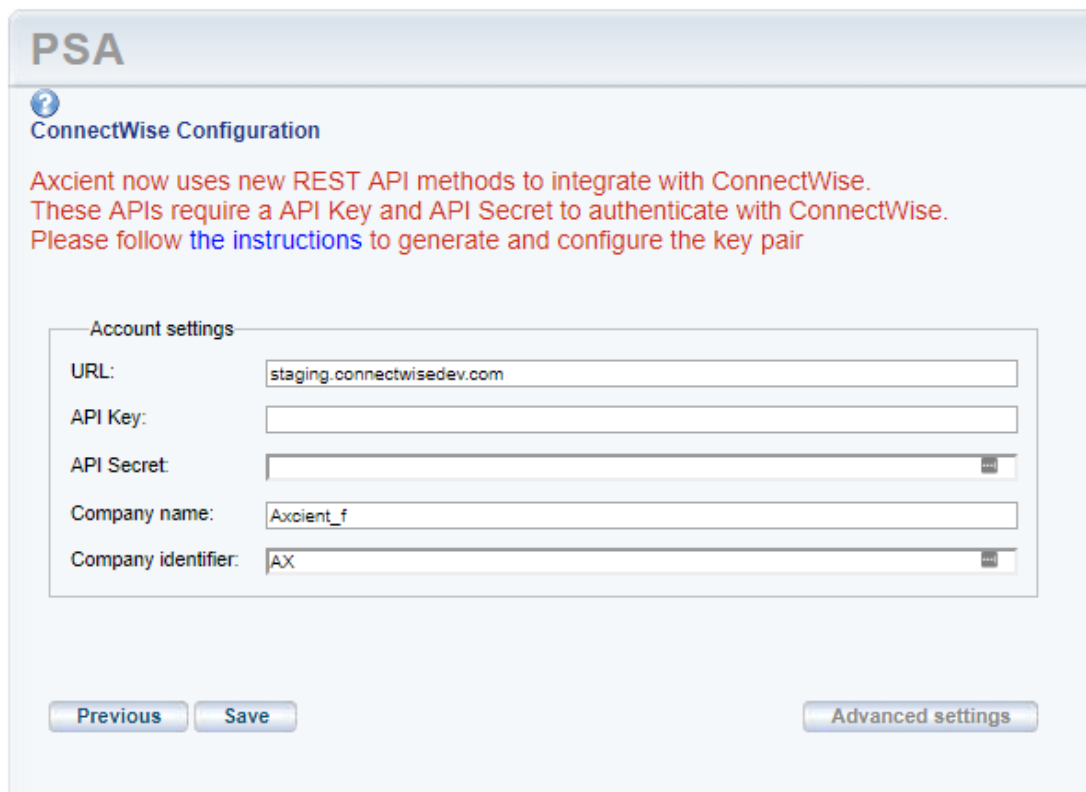
Because the UMC is appliance-specific, you will *need to log in to each appliance* to integrate with ConnectWise. When you log in to the UMC, you can optionally inherit configuration settings from the Web App.

If ConnectWise has already been integrated successfully, please continue to the [How to Configure Alerting](#) section for more information on how to configure specific events to publish to the PSA tool.

To integrate ConnectWise in the UMC:

1. On the UMC, click the **System** tab in the top navigation menu.
2. On the left navigation menu, click the **PSA** option. The *PSA* page displays.
3. Optionally, on the *PSA* page, click the **Inherit PSA Configuration Info from RMC** checkbox to inherit PSA settings already configured through the Axcient Web Application (RMC) .
4. Alternatively, on the *PSA* page, select **ConnectWise** from the drop-down menu and click the **Configure PSA Tool** button.
5. Enter the following information:
 - In the *URL* field, enter the **domain** portion of the address used to access ConnectWise. Enter the URL as illustrated in the following example:
 - **Correct** - *connectwise.com*
 - **Incorrect** - *www.connectwise.com*
 - **Incorrect** - *http://connectwise.com*
 - In the *API Key* field, enter the **public API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
 - In the *API Secret* field, enter the **private API key** generated in ConnectWise. For more information on the API, please refer to the [Obtain API Information](#) section.
 - In the *Company Name* field, specify your **company name**. For more information on how to obtain the company name, please refer to the [Obtain Login Information](#) section.
 - In the *Company Identifier* field, enter the appropriate **Client ID number**. For more information on how to obtain the ID, please refer to the [Obtain Client Information](#) section.
 - Optionally, to configure advanced settings, click the **Advanced Settings** button and update all appropriate fields.
6. Click the **Save** button.

Figure 31 - ConnectWise Configuration Screen in UMC



The image shows a web-based configuration screen titled "PSA" in the top left corner. Below the title is a section header "ConnectWise Configuration" preceded by a question mark icon. A red text block provides instructions: "Axcient now uses new REST API methods to integrate with ConnectWise. These APIs require a API Key and API Secret to authenticate with ConnectWise. Please follow [the instructions](#) to generate and configure the key pair". Below this is a form titled "Account settings" containing five input fields: "URL:" with the value "staging.connectwisedev.com", "API Key:" (empty), "API Secret:" (empty with a toggle icon), "Company name:" with the value "Axcient_f", and "Company identifier:" with the value "AX" (also with a toggle icon). At the bottom of the form are three buttons: "Previous", "Save", and "Advanced settings".

PSA

ConnectWise Configuration

Axcient now uses new REST API methods to integrate with ConnectWise.
These APIs require a API Key and API Secret to authenticate with ConnectWise.
Please follow [the instructions](#) to generate and configure the key pair

Account settings

URL:

API Key:

API Secret:

Company name:

Company identifier:

ConnectWise Appendix

As part of the ConnectWise integration process, you will need to complete a set of basic configuration tasks within the ConnectWise platform.

This section of the guide outlines basic configuration tasks that take place within the ConnectWise platform. As a best practice, however, we recommend referencing ConnectWise documentation for complete configuration steps.

Obtain the API Key

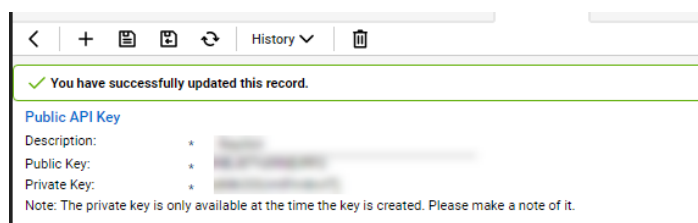
You can obtain API information within the ConnectWise service. For the purposes of integrating ConnectWise with the Axcient protection solution, you will need to create a new API key.

To create a new API key:

1. Log in to ConnectWise and open the *System* menu.
2. In the *System* menu, click the **Members** link.
3. In the *Members* page, click the **API Members** tab and then click the **plus icon** to create a new API Member.
 - In the *Member ID* field, enter **Axcient**.
 - In the *Role ID* field, make sure the role is configured with Add, Update, and Close tickets.
 - Click the **Save** button *but do not close the window*. After you click the **Save** button, you will be given access to the *API Keys* tab.
4. Click the **API Keys** tab and then click the **plus icon** to create a new API key.
 - In the *Description* field, type **BRC**.
 - Click the **Save** button *but do not close the window*.
 - Record the *public key* and *private key* before you close the window. You will not be able to view the private key again after this window is closed.

The image below details the location of the *public key* and *private key fields* (API Secret).

Figure 32 - ConnectWise API Key Screen



Obtain Login Information

ConnectWise login information is created when first setting up the ConnectWise service. For the purposes of integrating ConnectWise with the Axcient protection solution, you will need to enter the login information used to connect to ConnectWise.

The image below details the location of the *URL*, *Username*, *Password*, and *MSP Company ID* field values.

Figure 33 - ConnectWise Login Screen



ConnectWise®

Site:

Company:

User Name:

Password:

[Login](#) [Forgot your password?](#) [Clear Cache](#) [About](#)

Obtain Client Information

To obtain the Client information required to finish integrating ConnectWise, you will first need to create a new Company Account for the target Client site. Please refer to [online ConnectWise support](#) for instructions on how to create a Company Account.

To obtain the required Client Company information:

1. Log in to ConnectWise.
2. On the left-hand navigation menu, expand the *Companies* tab and click the **Companies** option. The *Company Search* page displays.
3. In the *Company Name* field, enter the **name of the target company**.
4. Select the target **Company** that was entered in the *Search* field and note the following information:
 - Company address information, including *Address Line 1 and 2*, *City*, *State*, and *Zip*.
 - The *Territory* field, which corresponds to the *Location* field in the Axcient Web App.

- The *Company ID* field, which corresponds to the *Company ID* field in the Axcient Web Application.

Figure 34 - ConnectWise Company Screen

ArtSpace

Company Notes Contacts Opportunities Tracks Activities Service Projects Agreements Documents Profile Surveys Sites Team Options Configuration

Company: ArtSpace

Company: * ArtSpace Site: Main

Phone: 250 3rd Avenue North

Fax: Minneapolis, MN 55401

Web Site: http://www.artspaceusa.org

Company Details

Type: * Customer Company ID: * ArtSpace

Status: * Active Market:

Territory: Clearwater Office Date Acquired: Wed 11/29/2006

Primary Contact

Name: Gary Email: will@artspaceprojects.org

Title:

Phone: (612) 333-9012 Type:

Relationship:

Obtain Service Type and Subtype

The Service type and subtype are determined by the ConnectWise user account. This ConnectWise account is associated with a specific Service Board which must be configured as needed by the administrative user. For more information regarding Service Boards, please refer to [online ConnectWise support](#).

This section will guide you on how to find ConnectWise field values; however, it is your responsibility to determine which values to enter in the ConnectWise configuration screen in the Axcient Web App.

To obtain ConnectWise field information:

1. On the left-hand navigation menu, click **System** and then select **Setup Tables**.
2. In the *Table* column, enter **Service Board** in the *search* field and press the **Enter** key.
3. Click the **Service Board** option.
4. On the *Service Board List* screen, click the appropriate **Service Board**.
5. Click the **Types** tab to view a list of *Service Types* that can be used in the ConnectWise configuration screen.

Figure 35 - ConnectWise Types List

Setup Tables > Service Board List > Type List			
Type List			
<div> <div>Board</div> <div>Statuses</div> <div>Types</div> <div>Subtypes</div> <div>Items</div> <div>Auto Templates</div> </div>			
<div> <div>←</div> <div>+</div> <div>🔍</div> <div>Search</div> <div>Clear</div> </div>			
Service Type ▲	Default	Request For Change	Inactive ▼
<u>Break-fix</u>			
<u>Proactive</u>			
<u>Reactive</u>			
<u>Roger Pham Type</u>			
<u>Server</u>			
<u>Warranty</u>			

6. Click **Subtypes** tab to view a list of *Service Subtypes* that can be used in the ConnectWise configuration screen.

ConnectWise Subtypes List

Setup Tables > Service Board List > Subtype List

Subtype List

Board Statuses Types Subtypes Items

← + Search Clear

Service Subtype ▲	Types	Inactive
		▼
<u>Roger Pham Subtype</u>	5	
<u>st1</u>	5	
<u>st2</u>	5	

Obtain Priority

The Service priority is determined by ConnectWise user account. This ConnectWise account is associated with a specific Service Board which must be configured as needed by the administrative user. For more information regarding Service Boards, please refer to [online ConnectWise support](#).

This section will guide you on how to find ConnectWise field values; however, it is your responsibility to determine which values to enter in the ConnectWise configuration screen in the Axcient Web App. The priority entered in the ConnectWise configuration screen within the Web App will determine the priority setting for the automatically generated ticket.

To obtain these values:

1. On the left-hand navigation menu, click **System** and then select **Setup Tables**.
2. In the *Table* column, enter **SLA** in the *search* field and press the **Enter** key. Click the **SLA** option.
3. On the *SLA List* screen, select the appropriate **SLA option**.
4. Enter one of the listed values in the *Priority* field in the ConnectWise configuration screen.

Figure 36 - ConnectWise SLA Screen

Setup Tables > SLA List > SLA

SLA

SLA Setup SLA by Priority ⚙️

← + 📄 📋 🗑️

i Updated: 6/24/2005 4:14:05 PM by user10

SLA Name:

Based on:

Calendar:

i Calendar options are defined in the [Calendar Setup Table](#)

Default? ☒ Use this SLA if no SLA exists for the customer / agreement

SLA Application Order:

Default Response Matrix:

	High Urgency	Medium Urgency	Low Urgency
High Impact	Priority 1 - Emergency Respoi	Priority 2 - Quick Response	Priority 3 - Normal Response
Medium Impact	Priority 2 - Quick Response	Priority 3 - Normal Response	Priority 3 - Normal Response
Low Impact	Priority 3 - Normal Response	Priority 3 - Normal Response	Priority 3 - Normal Response

Default Response Goals:

Respond within:	<input type="text" value="4.00"/> hours	Goal Percent:	<input type="text" value="80"/>
Plan within:	<input type="text" value="24.00"/> hours	Goal Percent:	<input type="text" value="80"/>
Resolved within:	<input type="text" value="48.00"/> hours	Goal Percent:	<input type="text" value="80"/>

Configure PSA Alerting

You must configure which alerts will be published to the PSA tool. If you successfully integrate a PSA tool but neglect to configure alerting, then **no alerts will be published to the PSA tool**.

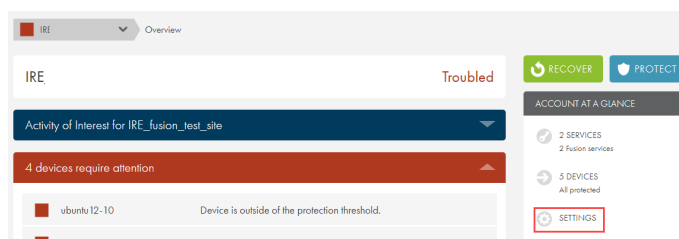
There are two ways you can configure the PSA tool once it has been successfully integrated with the Axcient protection solution: in the Web Application (RMC) or the UMC.

Configure PSA Tool Alerting in the Web Application

To configure alerting and notifications in the Axcient Web Application:

STEP 1

in the *Site Details* page, click the **Settings** link.



STEP 2

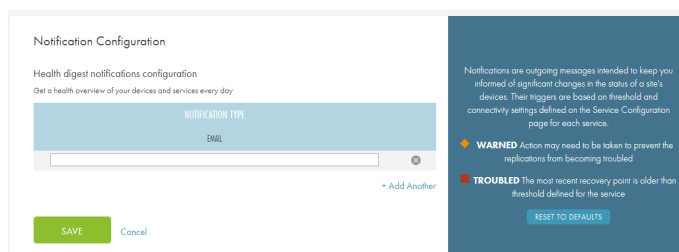
In the *Notifications* section, click the **Edit** button.



STEP 3

Configure alerting for the PSA tool as needed. Notifications are published based on the *Service-Wide Alerts & Thresholds* configuration settings. The following alerts can be configured for devices protected under the Site:

- *Local/D2C Jobs* allow you to configure notifications to be published when a device health status changes due to a local job, or for a D2C replication job to the cloud. The options include **Warning** and **Requires Attention**



health statuses.

- *Cloud Jobs* allow you to configure notifications to be published when a device health status changes due to a cloud job. This applies only to appliance-based services. The options include **Warning** and **Requires Attention** health statuses.
- *Connectivity* allows you to configure notifications to be published when devices health status changes due to loss of connectivity. This applies to both appliance-based and D2C services. The options include **Warning** and **Offline** health statuses.

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

Configure PSA Tool in the UMC

On the UMC, you can configure individual events that will trigger tickets in your PSA tool. You will need to configure events for each appliance.

After a PSA tool has been configured:

1. On the UMC, click the **Events** tab in the top navigation menu.
2. On the left-hand navigation menu, click the **Configure Alerting** option.
3. On the *Alerting* screen, select alerts to publish to the PSA tool.

Figure 37 - Alerting Configuration Screen in the UMC

The screenshot shows the 'alerting' configuration screen in the UMC. The screen is titled 'alerting' and has a search icon. It displays a list of event categories and their associated events. Each event has checkboxes for 'visible in log' and 'publish to psa tool', and a 'notify someone' button. A red box highlights the 'publish to psa tool' column for the 'Bare Metal Restore Lock Events' category, with a red circle and the number '1' next to it. An orange box highlights the 'publish to psa tool' column for the 'Bare Metal Restore Unlock Events' category, with an orange circle and the number '2' next to it.

Event Category	Event Name	visible in log	publish to psa tool	notify someone
Bare Metal Restore Lock Events	BMR image-lock FAILED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
	BMR image-lock info	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
	BMR image-lock started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
	BMR image-lock SUCCEEDED	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
	BMR image-lock warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
Bare Metal Restore Unlock Events	BMR image-unlock FAILED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	notify someone
	BMR image-unlock info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	notify someone
	BMR image-unlock started	<input checked="" type="checkbox"/>	<input type="checkbox"/>	notify someone
	BMR image-unlock SUCCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	notify someone
	BMR image-unlock warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	notify someone
Device Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Exchange Mailbox Backup Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Exchange Mailbox Restore Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Export Copy Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Network Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Offsite Backup Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Offsite DAS Copy Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Onsite Backup Events		<input type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone
Restore Events		<input checked="" type="checkbox"/> visible in log	<input type="checkbox"/> publish to psa tool	notify someone

Events are sorted by specific event categories:

- 1** Configure all events under a specific category by checking the **Publish to PSA Tool** checkbox next to the primary event category.
- 2** Configure specific events to publish to the PSA tool by expanding the event category and checking the **Publish to PSA Tool** checkbox for the specific event. Be aware that the *Publish to PSA Tool* option next to the primary event category will be checked even though only specific events have been selected. This is to help you quickly find where events have been configured.

You can reconfigure events at any time.