Axcient

Fusion Protection Guide

axcient.com

NOTICE

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

Axcient assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. This document contains information that is 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

Replication Method Deduplication	5 5
Introduction	6
Types of Devices Protected Preparing a VM For Protection Install Latest VMware Tools Enable Change Block Tracking (CBT) Enable RDP Connection	- 6 - 6 . 8 . 9 . 11
Setting Up a New Service	12
How to Deploy the AVM Agent	17 . 17
Custom AVM Configurations	23
Configure Service Settings	25
Service Settings Service-Wide Alerts & Thresholds Protection Policy Defaults Bandwidth/QoS (Quality of Service) Business Hours Time Zone Notification Configuration	25 27 28 30 30 30 32 33
Configure Site Settings	34
Notification Configuration	34 35
Stop Replication Jobs	36
Unpark a Device	. 37
Delete an AVM	38
Unprotect a Device	39
Re-protect a Device	. 40
PSA Tool Integration	42
Recommended Practices . Autotask Integration with the Axcient Web Application . Autotask Appendix .	. 42 . 43 . 45

ConnectWise Integration in the Axcient Web Application	51
ConnectWise Appendix	54
Configure PSA Alerting	61

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.

Axcient does not support deduplication for Windows 2012.

Deduplication

Axcient does not support deduplication for Windows 2012.

Introduction

This guide describes how to protect devices using the Fusion service, as well as 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 these business data protection standards.

The Fusion service is an appliance-less, cloud solution. You will deploy one or more Axcient Virtual Managers (AVMs) on the ESX host where the target virtual machines(VMs) are located. The AVM will act as an intermediary, relaying replicated data from the protected devices to the Axcient Cloud.

Cloud replication jobs can only occur while the AVM and target devices are powered on with a functioning outbound Internet connection.

Types of Devices Protected

Fusion service protects the following devices:

• Full image and file replication and protection of Windows-based and Linux-based devices.

Foreign Characters Support

The Axcient protection solution supports protection and recovery of foreign characters that are UTF-8 encoded.

Unsupported Files

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

This means that unsupported files will not be protected using 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 a file with a name that is not supported by Windows, such as ending with a blank or a period.

Preparing a VM For Protection

You must prepare all VMs before deploying the AVM on the ESX host. Preparation steps include:

- Install the latest version of required VMware tools on target VMs.
- Enable VMware Change Block Tracking (CBT) on target VMs.
- Enable Windows Remote Desktop Protocol (RDP) on target VMs.

These steps are **required** in order to avoid any issues with protecting VMs. Failure to prepare or confirm the preparedness of VMs may result in the following:

- Failure to successfully complete replication jobs.
- Unable to directly access the VM desktop in the Virtual Office.

Install Latest VMware Tools

All VMs to be protected must have the latest VMware tools version installed.

To install the latest VMware tools:

	🛃 192.168.99.20 - vSphere Client				
	File Edit View Inventory Administration Plug-ins Help				
STEP 1	🖸 🔝 🏠 Home 🕨 🖓 Inventory 🕨 🗊 Inventory				
Right-click the appropriate VM, point to Guest , and select Install/Upgrade VMware Tools .	Image: Second State Summary Resource Allocation Performance Events Console Virtue Mage: State Open Console Install/Upgrade VMware Tools Guest Operating System. Performance Per				
STEP 2	Install/Upgrade Tools – □ × C Interactive Tools Upgrade Use this option to change the installed VMware tools component.				
In the <i>Install/Upgrade Tools</i> pop-up window, select the Automatic Tools Upgrade radio button. Click the OK button to save your settings.	 Automatic Tools Upgrade vCenter will upgrade VMware tools without interacting with the guest OS. The virtual machine will automatically reboot after the upgrade, if needed. 				
	Advanced Options: Upgrade behaviour can be adjusted using advanced options. Consult the vCenter documentation about using these options.				
	Help OK Cancel				

Enable Change Block Tracking (CBT)

Change Block Tracking (CBT) is automatically enabled on the target VMs after the AVM is deployed on the ESX host and the initial seed replication job begins.

In the event you would like to confirm that CBT is enabled on the VMs, follow the steps listed below. Before you can enable CBT, the target VM must be powered off. You can confirm CBT settings when the VM is online or offline.

To enable or confirm that CBT is enabled on a vSphere web client (5.5 or higher):

STEP 1 Right-click the powered-off VM and select the Edit Settings option.	Datacenter 1 EnterCluster	Guest OS Snapshots Open Remote Console Migrate Clone Fault Tolerance VM Policies Template Compatibility Edit Settings
STEP 2	Edit Settings	15
Click the Options tab and select General in the <i>Settings</i> list. In the <i>Configuration Parameters</i> section, click the Edit Configuration button to continue. Confirm the following settings:	Swap file location	Default Use the settings of the cluster or host containing Virtual machine directory Store the swap files in the same directory as the Datastore specified by host Store the swap files in the datastore specified by for swap files. If not possible, store the swap file directory as the virtual machine. Using a datasto to both hosts during vMotion might affect the vf for the affected virtual machines.
 ctkEnabled - Confirm that the value is true. To change the value, double click the field and enter the correct value. scsi#:#.ctkEnabled - Confirm that the value is true 	Configuration Parameters Latency Sensitivity	EDIT CONFIGURATION

for all drives in the VM. To change the value, double click the field and enter the correct value.

Click the **OK** button to save your settings.

Enable RDP Connection

You must enable the Allow users to connect remotely to your computer option in order to use a Remote Desktop Protocol (RDP) agent to access devices in the Virtual Office recovery tool. Using an RDP agent is the only way you can directly access the desktop of a virtualized device in the Virtual Office. Because of this, if this option is not enabled on the original device when a replication job occurs, and you select a restore point in the Virtual Office without this option enabled, you will not be able to RDP into the virtualized device in the Virtual Office.

System

To enable Remote Desktop on a device:

STEP 1

On the device, launch Control Panel, navigate to System and Security, and select System.

In the System window, click Remote Settings.

\leftarrow	- 🚽 🗸 🛧 🏓 🔿 Control Pane	el > System and Security > System		
	Control Panel Home	View basic information about your compute		
🗣 Device Manager		Windows edition		
P	Remote settings	Windows 10 Pro		
System protection		© 2018 Microsoft Corporation. All rights reserved.		
•	Advanced system settings			
		System		

STEP 2

In the Remote Desktop section, check the Allow remote connections to this computer checkbox.

Please note that the specific steps may differ from Microsoft OS to OS. However, the Allow remote connection option will still be located in the Remote section of the System Properties screen.

System Properties					
Computer Name Hardware Advanced System Protection Remote					
Remote Assistance					
\fbox Allow Remote Assistance connections to this computer					
What happens when I enable Remote Assistance?					
Advanced					
Remote Desktop					
Choose an option, and then specify who can connect.					
O Don't allow remote connections to this computer					
Allow remote connections to this computer					
✓ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)					
Help me choose Select Users					
OK Cancel Apply					

Setting Up a New Service

After you complete each preparation step, you can begin to set up a new Fusion service.

To set up a new Service:

STEP 1

Navigate to the Axcient Web Application *Dashboard* and expand the *Activities of Interest* section.

Click to expand the *New Service* activity and then click the **Start Protecting** link.



AXCIENT FOR ENTERPRISE SERVICE SETUP

STEP 2

In the *Setup* pop-up window, click the **Let's Do It** button to begin the configuration process.

Welcome! Let's set up your new service.

In the next few screens, we'll be configuring and reviewing your Axcient Virtual Manager (AVM) service. 😯

At the end of the setup, you'll be able to download and install your AVM on an ESX Host to protect VM devices.



You will be presented with the End User License Agreement.

After you review the agreement, click the **I Agree** button.

Let's get things officially started. Please read and accept the following EULA to continue. Axcient, Inc. End User Agreement IMFORTANT - 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

DECLINE AC

STEP 4

In the *Settings Review* screen, configure the *Service Alias* and *Bandwidth Limitation* settings.

The default QoS settings are 10 Mbps during business hours and Unlimited during non-business hours.

To edit settings, click the **Edit** link in the appropriate field.

AXCIENT FOR ENTERPRISE SERVICE SETUF

×

Review the global default settings

This settings can later be changed or overridden for individual AVM/devices to change the behavior.

SERVICE DETAILS	
service alias IT Host	EDIT
BANDWIDTH LIMITATION © 100 Mbps O Unlimited Using default business hours	EDIT
■ BACK NEXT	

STEP 4a - Alias Configuration

In the *Service Alias* field, enter the preferred **Service** alias.

The *Entitlement* field cannot be edited because it is a paid-for-feature. To increase or otherwise change entitlements, please contact an Axcient sales representative.

These changes will be applied automatically. When you are finished, click the **Save** link.

AXCIENT FOR ENTERPRISE SERVICE SETUP

Review the global default settings

This settings can later be changed or overridden for individual AVM/devices to change the behavior.

SERVICE DETAILS	
service alias IT Host	CANCEL SAVE
BANDWIDTH LIMITATION 100 Mbps O Unlimited Using default business hours	EDIT

STEP 4b - Bandwidth Configuration

Configure WAN bandwidth usage for replication jobs during business and non-business hours.

For business hours, Axcient recommends setting a bandwidth that will not interfere with day-to-day business operations.

For non-business hours, Axcient recommends setting the limit to **No Limit** so replication jobs complete quickly. When you are ready, click the **Save** button to save all changes and return to the previous screen.

AXCIENT FOR ENTERPRISE SERVICE SETUI





Configure when the initial seed replication job and replication will occur.

In the *Initial Seed* section, select when initial seeding will take place. Please note that initial seeding may take a long time to complete for large devices, and can impact day-to-day operations.

You can select from the following options:

- Start Seeding Immediately The initial seed replication job will begin as soon as a device is protected.
- Delay Seeding Until Later Delay the initial seeding job to the set day and time.

In the *Run Replication Every* section, select when replication will occur. You can select from the following options:

- **Time Period** The time between each replication job.
- At All Times Always follow the same replication schedule.
- On specific days and times Follow the replication schedule on specific days and times.

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

RVICE SETUP		×
Set when	n initial seeding should happen.	
INITIAL SEED	Start seeding immediately	
	Delay seeding to a later time	
RUN REPLICATION EVERY	1 Hour	
	at all times	
	 on specific days and times 	
_		
	BACK NEXT	

Configure the alert thresholds that determine when an Axcient Virtual Manager (AVM) and a device fall out of the protection threshold.

- AVM Network Connectivity Loss Configure how long an AVM can lose connectivity before entering a Warned health status state.
- Most Recent Device Cloud Restore Point Configure the length of time between two successful device restore points before the device enters a Troubled health status state.

When you are ready, click the Next button.

AXCIENT FOR ENTERPRISE SERVICE SETU

Verify health threshold settings for this service.

These settings will be applied to all devices protected by this service, but you can always set custom thresholds per device or AVM.

AVM will become warned if it loses network connectivity for more than:

/UK					24 1100105
		BAC			

STEP 7

When you have finished the setup process, you will be presented with a link to download the Axcient Virtual Manager (AVM).

The AVM must be deployed on the ESX on which all the target VM devices are located.

Copy the link to download the AVM agent, and proceed to the <u>How to Deploy the AVM Agent</u> section for more information.

AXCIENT FOR ENTERPRISE SERVICE SETUP You're All Set! Time to install your Axcient Virtual Manager. https://fw-one1.axuptiva.net/d2c_agent/ey!: COPY LINK Download the AVM and deploy it on the ESX host to start protecting devices. Copy and share the link to deploy on other hosts. Learn more about best practices to protect your devices. View Service DOWNLOAD

How to Deploy the AVM Agent

The Axcient Virtual Machine (AVM) is a VM that is deployed on the same ESX host as the target devices. A single AVM can only protect a single ESX host and the VMs located on it. If you need to protect multiple ESX hosts, deploy an AVM on each separate host.

The AVM is generated as an OVA file from the Axcient Web Application. When the OVA is generated, you must create a VM on the target host using the OVA file. Once deployed, the AVM will automatically detect all VMs present on the ESX host and begin the protection process. The AVM relays the replicated data of the protected devices to the Axcient Cloud.

Please note that if the AVM is offline, or otherwise nonoperational, replicated data will not be transmitted to the Axcient Cloud and replication jobs will fail.

The AVM agent is not a local appliance; replicated data is not stored locally on the AVM.

AVM Sizing Considerations

The AVM sizing consideration matrix is designed to help you successfully plan the technical resources required to meet business recovery point objectives and requirements. These sizing considerations are for the AVM virtual machine that is created in order to replicate date of protected the ESX host and the target devices to the Axcient Cloud.

The matrix below is a guideline for how to allocate resources for the AVM virtual machine given a number of target guest VMs and your RPO needs.

Be aware that these are guidelines and other factors might affect the total RPO time such as network bandwidth and hardware limitations.

Number of Devices	1 Hour RPO	2 Hour RPO	4 Hour RPO
4 Guest VMs	4 vCPUs, 8GB RAM	4 vCPUs, 4GB RAM	4 vCPUs, 2GB RAM
5 Guest VMs	4 vCPUs, 10GB RAM	4 vCPUs, 5GB RAM	4 vCPUs, 3GB RAM
10 Guest VMs	4 vCPUs, 10GB RAM	4 vCPUs, 5GB RAM	4 vCPUs, 3GB RAM
15 Guest VMs	4 vCPUs, 10GB RAM	4 vCPUs, 5GB RAM	4 vCPUs, 3GB RAM

To deploy the AVM agent:

Note: These instructions will vary depending on your version of vSphere.

You will first need to capture the AVM Agent Installation link in one of the following locations:

- At the completion of the <u>initial service deployment</u> <u>process</u>.
- On the *Service Details* page, located in the *Service at a Glance* section.

Click the **Click to Highlight** button to copy the link.

٦L	OAD AGENT	
	Agent Installation Link	
	UNIQUE AGENT LINK FOR (Q5) https://fw- two1.axuptiva.net/d2c_agent/eyJzZXJpYWwiOiJjcTVqIn0	
	Click the link to download the agent installer. Copy and share the link with anyone who will be installing the agent to eligible devices. Press Command-C when the link is selected to copy it.	

STEP 2

Paste the AVM Agent Installation link in your preferred Internet browser to download the AVM agent OVA file.

The AVM agent OVA file will be downloaded to the local device. Be sure that the device has access to the ESX host through vSphere.

Make note of where the AVM agent OVA file is downloaded.



Log in to the vSphere Client (either Web or Windows). To begin deploying the AVM agent, click the File menu and select **Deploy OVF Template**.

Ø	
File Edit View Inventory Adm	ninistration Plug-ins Help
New	ntory 🕨 🗊 Inventory
Deploy OVF Template	
Export	+
Report	localhost.localdomain VMware ESXi, 5.1.0, 1065491
Browse VA Marketplace	Getting Started Summary Virtual Machines Resource Allo
Print Maps	
Exit	what is a Host?
	as ESX or ESXi, to run virtual machines. Hosts pro CPU and memory resources that virtual machines give virtual machines access to storage and netwo connectivity.
	You can add a virtual machine to a host by creating one or by deploying a virtual appliance.
	The easiest way to add a virtual machine is to dep virtual appliance. A virtual appliance is a pre-built machine with an operating system and software al installed. A new virtual machine will need an opera system installed on it, such as Windows or Linux.
Ø	Deploy OVF Template -
Source Select the source location.	

On the Source page, click the Browse button to navigate and select the downloaded AVM agent OVA file. Click Next to continue.

Source OVF Template Details Name and Location Disk Format Ready to Complete	Deploy from a file or URL C: Users\Administrator\Downloads\AxcientVirtualManager.ov Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
9	Deploy OVF Template
OVF Template Details	

Verify OVF template details.

STEP 5

On the OVF Template Details page, review the specific OVF template details.

Click Next to continue.

Source **OVF Template Details** Product: AxcientVirtualManager Name and Location Disk Format Version: Network Mapping Ready to Complete Vendor: Publisher: No certificate present Download size: 1.2 GB 2.7 GB (thin provisioned) Size on disk: 20.0 GB (thick provisioned) Description:

On the *Name and Location* page, type a descriptive name for the AVM.

Click Next to continue.

2

Disk Format

Deploy OVF Templat

Name and Location

Specify a name and location for the deployed template

:
entVirtualManager
ame can contain up to 80 characters and it

Deploy OVF Template

STEP 7

On the *Disk Format* page, select the preferred provision type.

Axcient recommends selecting **Thick Provision Eager Zeroed**.

Thin Provision might also work, but it is not recommended from an AVM resource utilization.

 Source OVF Template Details Name and Location Disk Format Ready to Complete
 Datastore:
 Roger_DS1

 Available space (GB):
 3532.4

 C
 Thick Provision Lazy Zeroed

 ©
 Thick Provision Eager Zeroed

 ©
 Thin Provision

In which format do you want to store the virtual disks?

Click Next to continue.

STEP 8

On the *Network Mapping* page, select the appropriate **VM network**.

The AVM must be on the same network as the target VMs that will be protected.

Click Next to continue.

Deploy OVF	Femplate	
d the deployed template use?		
Map the networks used in this OVF te	mplate to networks in your inventory	
Source Networks	Destination Networks	
VM Network	VM Network	
Description:		
The VM Network network		
	Deploy OVF 1 Id the deployed template use? Map the networks used in this OVF te Source Networks VM Network Description: The VM Network network	Deploy OVF Template Id the deployed template use? Map the networks used in this OVF template to networks in your inventory Source Networks Destination Networks VM Network VM Network Description: The VM Network network

On the *Ready to Complete* page, review the OVF details. When you have confirmed the OVF details, click the **Finish** button.

Power on the AVM.

STEP 10

When the AVM agent VM has been powered on, navigate to the Axcient Web Application *Dashboard*.

Expand the *Activities of Interest* section to view the New AVMs alert.

Hover your mouse over the right-hand side of the alert to expose the **Enter Credentials** link, and then click the link.

STEP 11

Enter the ESX host credentials where the AVM agent is located:

- ESX Hostname/IP Address Enter the host name or IP address of the ESX host where the AVM agent and the target devices are located.
- ESX Host Username Enter the ESX host username.
- ESX Host Password Enter the ESX host password.

If the ESX host belongs to a vCenter, click the **My Host Belongs to a vCenter** checkbox and enter the following:

- vCenter Hostname/IP Address Enter the hostname or IP of the vCenter where the target ESX host is located.
- vCenter Username Enter the username for the vCenter where the target ESX host is located.

Are these the options y	ou want to use?	
Source OVF Template Details Name and Location	When you click Finish, the dep	loyment task will be started.
Disk Format Network Mapping Ready to Complete	Ovp file: Download size: Size on disk: Name: Host/Cluster: Datastore: Disk provisioning: Network Mapping:	C:\Users\Administrato\Downloads\AxcientVitualManage 1.2 GB AxcientVirtualManage Iocalhost. datastore3 Thin Provision "VM Network" to "VM Network"

OVERVIEW	SERVICES	EVENTS	USERS	REPORTS	
•					
Mountain	View Vove	arview			
Mountai	n View				Unprotected
_	_	_	_	_	
Activity of	Interest for Mc	ountain View			A
					the second state of the second
🛣 Ne	W AVM	1	AVM registe	red. Enter credentia	is to start protecting devices. Less
AVM		SERVICE			
AVM 192.16	3.99.10	SERVICE	ervice		Enter Credentials
AVM 192.16	3.99.10	SERVICE Test Se	ervice		Enter Credentials

ENTER CREDENTIALS FOR 192.168.99.203

MΥ

Please	enter your	host credentials	below.

ESXI HOSTNAME/IP ADDRESS	192.168.99.203
ESXI HOST USERNAME	root
ESXI HOST PASSWORD	• • • • • • • •
HOST BELONGS TO A VCENTER	
ring vCenter credentials once will automatica my host on which AVMs will be deployed in	ally discover devices belonging to the current ESX host, and the future.
VCENTER HOSTNAME/IP ADDRESS	
VCENTER USERNAME	
VCENTER PASSWORD	
CLOSE	SAVE

• vCenter Password - Enter the password for the vCenter where the target ESX host is located.

Custom AVM Configurations

You can configure custom AVM settings that override settings configured in the *Service Configurations* page. You can configure the following custom settings for each AVM:

- Enable Custom Bandwidth Limits
- Enable Custom Replication Settings

To configure custom AVM settings:



In the *Custom AVM Settings* pop-up window, set custom settings for the AVM, which will override settings configured in Service Configurations.

- Click the **Enable Custom Bandwidth Limits** checkbox to define bandwidth limits for both business hours and non-business hours.
- Click the Enable Custom Replication Settings checkbox to define custom replication settings. You can optionally configure custom replication settings for specific days and times.

Click the **Save Custom Limits** button to save your changes.

CUSTOM AVM SETTINGS

Set custom bandwidth limits for PROD_AVM_FusionTest_do_not_delete

Custom setting for this AVM will **override** the setting configured in Service Configurations.

🗘 Durin	g busir	l ₪ Ness hou	Enable Jrs	Custom	Bandv	vidth Lii	mits		
1 MBPS		I	I	50 MBPS	I	I	I	I	No limit NO LIMIT
Durin	g non-	busines	s hours						_
1 MBPS	I	I	I	I	I.	I	I	I	No limit NO LIMIT
			Enable	Custom	Replic	ation S	ettings		
		F	lun rep	lication	every	12 H	ours	~	
		(at o	all times	5				
		(0 on	specific	a days	and tir	nes	_	
			su	N MON	I TUE	WED	THU F	RISAT	
			10	0:00 PN	1 ~	, to	05:00	MA (~
			You sche	may nee edule.	d to adj	ust your	Alert Th	reshold	s to accommodate th
		SA	VE CU	stom	LIMITS	5	Cance	el	

Configure Service Settings

You can configure Service Settings of an Axcient Service, giving you granular control over your Protection Policy. This includes configuring when backup jobs occur, what it means for a device to fall out of protection threshold, and what kinds of alerts are sent to which recipients.

Axcient lets you quickly protect many VMs on an ESX host using a pre-configured Service Protection Policy that is automatically applied to the target VMs.

The ability to configure the Protection Policy powers Axcient's Manage by Exception philosophy by allowing you to define a protection threshold. Once configured, notifications will appear on the Web App *Dashboard* and *Service Details* page of the appropriate Service, as well as in emails to dedicated team employees, if configured.

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

To access the *Service Configuration* page:

STEP 1

On the Axcient Web Application, click the **Services** tab in the top navigation menu.

On the *Services* page, find the service to be configured, click the drop-down menu, and select **View Service**.

STEP 2

On the *Service Details* page, click the **Configure Service** button. You can then update the following settings:

- Service Settings
- Service-Wide Alerts and Thresholds
- Service-Wide Protection Policy
- Bandwidth and QoS (Quality of Service)
- Business Hours
- Time Zone
- Notification Configuration

Service Settings

The Service Settings section of the *Configure Service* page allows you to configure a few key settings, including:



				CONFIGURE SERVICE
_tusion_test	t		Axcient Fusion	
	SERVICE ID	55qc	RECOVER	ENTITLEMENTS AT A GLANCE
	DEVICES	100 %		0.0000
	STORAGE	89 %	PROTECT	200 GB entitled
	SERVICE KEY	50ae-uqj6-cj1x-410y View AVM Download Link		178 GB used
				1 year

- Alias Configure the name of the Service as it appears in the Axcient Web Application.
- Auto-Protect Devices that are protected under this service will automatically inherit the Protection Policy Defaults configured under the service.



Figure 1 - Service Settings Configuration Section

Service-Wide Alerts & Thresholds

The Service-Wide Alerts and Thresholds section of the *Configure Service* page allows you to define a device protection threshold under a specific Axcient Service. You can configure:

- AVM Network Connectivity Loss Configure how long an AVM can lose connectivity for before falling in to a Warned health status.
- **Device Most Recent Cloud Replication Point** Configure how old the most recent cloud restore point can be before the device falls in to a **Troubled** health status.

Additionally, a non-configurable alert will effect the health status of a device:

• Device Recent Restore Point Warning - A device will fall in to a Troubled health status state when the most recent restore point completed successfully with warnings.

Figure 2 - Service-Wide Alerts & Thresholds Configuration Section



Protection Policy Defaults

The Protection Policy Defaults section of the Configure Service page allows you to manage policy settings.

Axcient uses the Graduated Retention method of retaining data in the Axcient Cloud. You can configure the cloud retention in order to determine how long data should be stored in the Axcient Cloud. The retention options are based on the entitlements purchased. In order to increase the amount of time data can be retained in the Axcient Cloud, you must contact their Axcient account manager or contact Axcient Support.

You can also configure when the initial seeding job will begin. You have the following options:

- **Start Seeding Immediately** This will begin the initial seed replication job as soon as the AVM has been deployed and the target VMs have been detected.
- Delay Seeding to a Later Time You can configure a specific day and time for the initial seed replication job to begin. The seeding job will begin as soon the configured date and time is reached, based on the Time Zone specified in the Time Zone configuration section.
- **Run Protection Every** You can specify protection frequency, choosing to run the same protection schedule at all times or on specific days and times.
- **AVM Replication Setting** You can configure the AVM replication schedule. By default, the AVM will attempt to perform an application-consistent snapshot of protect devices. Alternatively, you can configure crash-consistent snapshots.
 - An application-consistent snapshot process involves using VSS writers, which the application(s) will respond to by flushing all memory content and I/O operations so the application is consistent. This means that buffers are flushed, operations are completed, files closed, etc. This results in no data in the memory or any operations being lost in the snapshot process. Once the snapshot is complete, the VSS writers will then tell the application to resume normal operations.

An application-consistent snapshot takes the most up-to-date snapshot of the device to include, rather than ignore, any in-process operations in the replication. This is most suited for database applications.

• Crash-consistent snapshot means that the snapshot is not application consistent and data would be preserved but any transaction in memory and not committed to the disk will be lost. The crash-consistent shapshot will replicate the device data as-is, and when recovered, will restore the data in the same system state as when the snapshot was taken. No pending operations, open files, or unfinished business will be replicated or restored. If there is data in the memory or if there are I/O operations in process or pending, the crashconsistent snapshot will ignore them.



Figure 3 - Protection Policy Default Configuration Screen

Bandwidth/QoS (Quality of Service)

The Bandwidth and QoS section of the *Configure Service* page allows you to configure the bandwidth usage settings for cloud replication jobs during business and non-business hours.

- **During business hour** Set how much bandwidth usage the cloud replication job can use during business hours. Axcient recommends configuring a lower bandwidth threshold so the replication jobs do not interfere with the device and network connectivity that may effect day-to-day operations.
- **During non-business hours** Set how much bandwidth usage the cloud replication job can use during non-business hours. Axcient recommends configuring a higher bandwidth threshold so that the replication jobs can complete quickly.

WAN									Quality of Service allows you to optimize when replicatic run so they do not disrupt your daily business.
QoS vo limits w	ilues selec ill not be c	ted below affected	will apply	to every AVN	1 protecte	ed by this se	ervice. AVA	As with custom bandwidth	Settings allow throttling of WAN bandwidth during busin and non-business hours
🙃 Du	ring busin	iess hours							RESET TO DEFAULTS
MBPS	1	I		50 MBPS	I	I	I	No limit NO LIMIT	
MBPS	 uring non-l	 business ho	 DUITS	50 MBPS	I	I	I	No limit No limit	

Figure 4 - Bandwidth/QoS (Quality of Service) Configuration Screen

Business Hours

The Business Hours section of the *Configure Service* page allows you to configure the business hours for the service. The business hours configuration works in tandem with the <u>Time Zone</u> and <u>Protection Policy Default</u> settings to automatically begin replication jobs on schedule.

The business hours configuration should reflect the accepted business hours of the Site where the target devices are being protected.

Figure 5 - Business Hours Configuration Screen

Business Hours

SUNDAY	Closed	V	AM	~	to	Closed	×	AM	V
MONDAY	9:00	V	AM	V	to	5:00	V	PM	\checkmark
TUESDAY	9:00	V	AM	V	to	5:00	V	PM	~
WEDNESDAY	9:00	V	AM	V	to	5:00	V	PM	~
THURSDAY	9:00	V	AM	V	to	5:00	V	PM	~
FRIDAY	9:00	V	AM	V	to	5:00	V	PM	~
SATURDAY	Closed	V	AM	V	to	Closed	V	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 Zone

The Time Zone section of the *Configure Service* page allows you to configure the time zone where target devices protected by the service are located. The time zone configuration works in tandem with the <u>Business Hours</u> and <u>Protection Policy</u> <u>Defaults</u> settings to automatically begin replication jobs on schedule.

In the *Service Time Zone* drop-down menu, you can configure the time zone which will be applied to all devices protected by the service. All replication jobs, and other time-dependent configurations will operate based on the time zone configured here.

	Figure 6 - Time Zone Configura	tion Screen
Time Zone		
SERVICE TIME ZONE	(GMT-08:00) Pacific Time (US & Canada) 🛛 🗸 🚱	All application data is shown using the global time zon
RESULTING LOCAL TIME	10 Jun, 2019 12:35 PM	However, because your service may be deployed in mul
UTC	10 Jun, 2019 7:35 PM	locations, you can choose to have QoS and Business Ho honor the local device's time zone instead.
SAVE	ancel	Note that changing the time zone restarts the replication service. Do not change the time zone while any replication are in progress.
		RESET TO DEFAULTS

Notification Configuration

The Notification Configuration section of the *Configure Service* page allows you to configure notifications so that you stay informed of significant changes in the status of a device. These triggers are based on Alert Configurations.

The following notifications are generated:

- Warned Action may need to be taken to prevent replications from becoming troubled.
- **Troubled** The most recent recovery point is older than threshold defined for the service.

You can enter one or more email addresses where notifications will be delivered.

Health digest notifications configuration	Notifications are outgoing messages intended to keep
Get a health overview of your devices and services every day	informed of significant changes in the status of a sit devices. Their triggers are based on threshold an
	connectivity settings defined on the Service Configure
EMAIL	WARNED Action may need to be taken to preve
	replications from becoming troubled
	+ Add Another TROUBLED The most recent recovery point is older threshold defined for the service
	RESET TO DEFAULTS

Configure Site Settings

You can configure the Sites Settings that will apply to all protected services and devices registered under the Site.

To access the *Site Settings* page:

STEP 1

On the Axcient Web Application, click the **Sites** tab in the top navigation menu.

On the *Sites* page, click the **Details** button for the target Site.

STEP 2

On the *Site Details* page, click the **Settings** button under the *Account at a Glance* section.

You will be able to configure the following settings:

- Notification Configuration
- PSA Tool

Notification Configuration

In the Notification Configuration section of the *Site Settings* page, you can configure notifications for one or more users. These notifications include devices, cloud replication jobs, and connectivity.

Emails can be configured to receive only specific kinds of alerts. This ensure that the appropriate team members receive the alert notifications and can take appropriate steps to resolve them.

+ ADD SITE	Showing 67 of 8,729 Sites	
FILTER SITES	Fusion_test_site DETAILS	IRE_fusion_test_site
test Site	AVINS 1	AVMS 5
HEALTH	DEVICES 3 troubled of 5 total	DEVICES 4 troubled of 5 total
Troubled	SERVICES 1 total	SERVICES 2 total



	Figure 7	- Notificatior	n Configuratio	n Sectio	on
Notification Configuration					
Outgoing notifications will be sent by t	utgoing notifications will be sent by these methods: informed of significant changes in the sta		Notifications are outgoing messages intended to keep you informed of significant changes in the status of a site's devices		
INFO Email	LOCAL/D2C JOBS	CLOUD JOBS	CONNECTIVITY		without having to be logged in to the application. Their triggers are based on Alert Configurations set above, and the settings are site-wide.
admin@partner.com			I	\otimes	RESET TO DEFAULTS
support@partner.com	a	1	2	\otimes	
+ Add another					
Configure your chosen PSA tool in the section	below.				
SAVE Cancel					

PSA Tool

In the PSA Tool section of the *Site Settings* page, you can integrate the Autotask and ConnectWise Professional Services Automation (PSA) tools with the Axcient protection solution. 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.

For complete instructions, please reference the **PSA Tool Integration** section of this guide.

Figure 8 - PSA Configuration Section

PSA Tool			
CONFIGURE USING	Select a PSA Tool	~	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.

Stop Replication Jobs

You can park a device to stop a replication job.

When you park a device while a replication job is running, the job will stop and the device will assume a parked system state. The replication job completion will still be listed in the *Event* page, even if the device is parked while the replication job is running.

Parking a device does not remove the device from the Web Application. Instead, it changes the system status to *Parked*. This does the following:

- Scheduled replication jobs will no longer occur as scheduled once a device is parked.
- Preserves all existing restore points for the device before the device was parked.

To park a device:

IRE_fusion_test_site 🗸 Overvier STEP 1 👌 RECOVER 🛛 👘 PROTE IRE_fusion_test_site Troubled On the Site Details page, click the Devices link under the Account at a Glance section. ubuntu 12-10 Device is outside of the protection threshold win2k8r2 ٠ win2k8r2 STEP 2 🔶 Warne 10.2.165.4, 172.30.165.4 10.2.170.172 Windows Server 2008 R2 On the *Devices* page, click to expand the desired device. Click the **Park** button to park the device.

Unpark a Device

You can unpark a parked device at any time. Unparking a device will continue the replication jobs as configured in the Protection Policy.

To unpark a device:

STEP 1

On the *Site Details* page, click the **Devices** link under the *Account at a Glance* section.

STEP 2

On the *Devices* page, click to expand the desired device. Click the **Unpark** button to unpark the device.

IRE_fusion_test_site V Overview			
IRE_fusion_test_site		Troubled	
			ACCOUNT AT A GLANCE
Activity of Interest for IRE_fusion_	test_site	▼	2 SERVICES
4 devices require attention		•	2 Fusion services 5 DEVICES All protected
ubuntu 12-10	Device is outside of the protection threshold.		SETTINGS
win2k8r2	Device is outside of the protection threshold.		
win2k8r2	55qc - IRE_fusion_test	AVM_PROD_nesx 2.8-109	Never
win2k8r2			
Parked			
	RUNNING ON 10.2.165.4, 172.30.165.4	LATEST CLOUD RP Never	RECOVER
	DEVICE IP 10.2.170.172	05 Windows	Server 2008 R2 UNPARK
	win2k8r2 is parked, so it's no longer being actively b	acked up but is available for recov	VIEW DEVICE

Delete an AVM

There may be some situations where the AVM must be deleted from the ESX host. In the event that you need to delete an AVM from the ESX host, do not delete the AVM while a replication job is in progress. It is possible that one of the client machine's disks may still be attached and this associated disk can be lost. A disk lost in this manner is **not recoverable**.

In order to avoid causing damage to the VMs on the ESX host, you will need to park all devices protected by the AVM. Parking a device will stop all future replication jobs from beginning. Be aware that if a device is parked while a replication job is running, the replication job will run until completion but no more replication jobs will begin thereafter. It is recommended that once all devices are parked, that you wait some time to ensure that the replication jobs have completed.

You will see the following ESX error if the AVM has been deleted while a replication job is in progress. If you see this error, then unrecoverable damage has been caused to one or more of the VMs on the ESX host:

Figure 9 - AVM Deletion Error

	File /vm	fs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk was not found	
\odot	See the	error stack for details on the cause of this problem.	
	Time:	4/5/2016 12:14:58 PM	
	Target:	Wind2k8R2-two	
	ESXi:	172.20.13.10	
🖃 Erroi	r Stack		
- 14 A			
Failed Canno The sy VMwa Modul Canno Canno The sy VMwa	to start the ot open the stem cann rre ESX can le Disk pov ot open the stem cann rre ESX can	virtual machine. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two-000004.vmdk' or one of the snapshot disks it depends on. ot find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two.vmdk". Verify the path is valid and try again. er on failed. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1-000004.vmdk' or one of the snapshot disks it depends on. of find the file specified not find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk' or one of the snapshot disks it depends on. of find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two/Wind2k8R2-two_1.vmdk'. Verify the path is valid and try again.	
Failed Canno The sy /Mwa Modul Canno The sy /Mwa	to start thi ot open the stem cann re ESX can le Disk pov ot open the stem cann re ESX can	virtual machine. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two-000004.vmdk' or one of the snapshot disks it depends on. ot find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two.vmdk". Verify the path is valid and try again. er on failed. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1-000004.vmdk' or one of the snapshot disks it depends on. ot find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk' or one of the snapshot disks it depends on. ot find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two/Wind2k8R2-two_1.vmdk". Verify the path is valid and try again.	
Failed Canno The sy VMwa Modul Canno The sy VMwa	to start thi open the vstem cann re ESX can le Disk pov to open the vstem cann re ESX can	virtual machine. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two-000004.vmdk' or one of the snapshot disks it depends on. ot find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two.vmdk". Verify the path is valid and try again. <i>er</i> on failed. disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1-000004.vmdk' or one of the snapshot disks it depends on. ot find the file specified not find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk'. Verify the path is valid and try again. <i>f</i> find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two/Wind2k8R2-two_1.vmdk". Verify the path is valid and try again. <i>f</i> find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk". Verify the path is valid and try again.	4

Unprotect a Device

If necessary, you can unprotect and delete a device from the Web Application.

Warning!

Clicking the **Unprotect** button will delete the device and all replicated data from the Axcient Cloud and Web Application. This will result in total data loss for the device. You will be unable to recover any data from the unprotected device.

To unprotect a device and delete a device from the Axcient Web Application:

STEP 1

On the *Site Details* page, click the **Devices** link under the *Account at a Glance* section.

STEP 2

On the *Devices* page, click to select the device.

In the *Device Details* page, click the **Unprotect** button to stop protecting the device.

You will be prompted to confirm your selection.

IRE_fusion_test_site V Overview			
IRE_fusion_test_site		Troubled	
Activity of Interest for IRE_fusion_test_site		-	ACCOUNT AT A GLANCE
4 devices require attention		^	5 DEVICES All protected
ubuntu 12-10 Device	is outside of the protect	ion threshold.	SETTINGS
win2k8r2 Device	is outside of the protect	ion threshold.	
IRE_fusion_test_site V Device	s 🗸 ubuntu 14	1-10	
ubuntu 14-10			Troubled
	RUNNING ON	172.20.17.5	PAPK
	05	Ubuntu Linux (64-bit)	
	SERVICE	55qc - IRE_fusion_test	UNPROTECT
	DEVICE IP	172.20.17.215	
	AVM	PROD_AVM_IRE_fusion_test_DC	D_NO

Re-protect a Device

You can re-protect a device on a host which has been previously unprotected. Reprotecting a device will not repopulate any recovery points from the time before the target device was unprotected.

To re-protect a device:

	IRE_fusion_lest_site V Overview	
STEP 1	IRE_fusion_test_site Troubled	
On the <i>Site Details</i> page, click the Protect button.	Activity of Interest for IRE_fusion_test_site Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going an, you'll see it have first. Image: Nothing Recent Whenever anything of interest is going and you'll see it have first. Image: Nothing Recent Whenever anything of interest is going and you'll see it have first. Image: Nothing Recent Whenever anything of interest is going and you'll see it have first. Image: Nothing Recent Merge: Nothing Recent Im	COUNT AT A GLANCE 2 SERVICES 2 Factor services 3 SEVICES Al protected 3 SETTINGS
STEP 2	PROTECT DEVICES	×
	Which service do you want to protect devices wi	ith?
On the <i>Protect</i> screen, select the appropriate Fusion	SERVICE A SERVICE TYPE DEVI	ICES
service if prompted and then click the Next button.	IRE_fusion_test Fusion 5	
	IRE_new_fusion_service Fusion 0	
	NEXT	

On the Protect Devices screen, click the Unprotected tab and select the devices to protect.

Click the Next button to continue.

PROTECT DEVICES ON IRE_FUSION_TEST

1 device is not protected yet. Select devices you want to start protecting

	U١	NPROTECTED		PROTECTED
SELECT	HEALTH	DEVICE NAME 🔺	AVM	DISCOVERED
	0	win2k8r2	AVM_PROD_	_nesx2_D A month ago
1 select	ed			Select all Deselect all
			NEXT	

In the Protect Settings screen, review the Protection Policy details.

Click the **Next** button to continue.

PROTECTION SETTINGS FOR SELECTED DEVICE

Selected devices will be protected using the below service-wide settings. These settings can be changed from IRE_fusion_test page.

THRESHOLD ALERTING	Cloud RP - 24 hours Connectivity - 60 minutes	
RETENTION	1 Year	
BANDWIDTH/QOS	50 Mbps500 Mbps	
SEEDING START TIME	Start seeding immediately	
BACK	NEXT	

PROTECTION UNDERWAY

STEP 5

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

Here we go!
Now protecting win2k8r2.
\odot
Nothing much left to see here!
DONE

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:

	iRE V Overview	
STEP 1	IRE	Troubled RECOVER PROTECT
In the Site Details page, click the Settings link.	Activity of Interest for IRE_fusion_test_site	ACCOUNT AT A GLANCE
	4 devices require attention	5 DEVICES
	ubuntu 12-10 Device is outside of the protection threshold.	SETTINGS
	 win3kRr9 Davies is nutride of the nonderline threshold 	
STEP 2 In the <i>PSA Tool</i> section, click the Edit button.	PSA Tool No PSA is configured. Using a PSA tool con help you stay informed of system events and outmore support Rickeling. Art Mis time, Ascient Imagesters with: • Antotax Test PSA Connection Verify the site can connect to your PSA tool	EDIT Configure a Professional Services Automation Tool to further (regrote the Aucent service with your evablished office routines.
STEP 3 In the <i>Configure Using</i> drop-down menu, select Autotask and update the following fields:	PSA Tool COMINGRE USING Aurotask USERNAME Bettry/Brackethportheerdemo com @ PASSWORD •••••••• COMINAN PASSWORD •••••••• Aurotask © COMINAN PASSWORD •••••••• ACCOUNT ID © ACCOUNT ID © OHERE IP ©	Configuring PSA tools is on odvanced setting from requires setup in both the Avcient service and the hild party application. For explicit particate on setting up and houb/entry both Avcient's PSA integration and your favored PSA hool, see the full documentation.

- 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 <u>How to Obtain Queue</u> ID section below.

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

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.

How to Enable the API Role in Autotask

The administering Autotask resource account, used to integrate with your Axcient product, must be configured as an API user. You can either create a new resource account or update an existing resource account. In this example, we will create a new resource account.

To configure a new resource account:

- 1. Hover your mouse on the Autotask icon to activate the main navigation menu.
- 2. Point to the Admin tab and select Resources (Users).
- 3. Click the **New** button to create a new resource user.
- 4. Click the General tab and enter basic account information.
 - In the First Name field, enter a first name of the resource.
 - In the Last Name field, enter a last name of the resource.
- 5. Click the **Security** tab and create **login credentials**.
 - In the Security Level field, select API User (System).
 - In the API Tracking Identifier field, select the Integration Vendor option and then select Axcient from the dropdown menu.
- 6. Using the main navigation menu, point to Admin and select Features & Settings.
- 7. Click to expand the Resources/Users accordion menu and select the Protected Data Permissions link.
- 8. Find the resource account and ensure the **View Protected Data** checkbox is selected.
- 9. Click the **Save** button when you are finished.

Figure 10 - Autotask Security Screen

Save & Close Save Save & Copy Cancel Tabs with * contain	required fields
eneral* Security* HR* Approvers* Associations* Skills	Attachments
EDENTIALS	TWO-FACTOR AUTHENTICATION
Username *	Require Two-Factor Authentication for this Resource
Active Password *	Option 1 - AuthAnvil AuthAnvil offers a strong authentication platform to cover multiple assets (including Windows network, production devices and web-based software) with a single solution, allowing you to consolidate security management and token use. It also provides a source of
Confirm Password *	new revenue by allowing you to manage strong authentication for client assets on the same platform. To learn more about AuthAnvil Two-Factor Authentication or sign up, Click here
Security Level * API User (system)	Option 2 - CRYPTOCard Tokens
Allow Resource to access links to Datto pages from within Autotask (Datto Integration must be enabled)	Option 3 - TOTP (Google Authenticator, etc.) Time-based one-time password
Allow Resource To Edit Skills	
Allow Resource to Create, Edit, and Delete Knowledgebase Articles	
Allow Resource to send bulk emails By checking this box you agree to the Contact Group Terms and Conditions	API TRACKING IDENTIFIER
Resource is not required to Submit Timesheets	API version 1.6 & later require the use of an API tracking identifier. Once assigned, this cannot be changed.
TOTO	○ None
	 Integration Vendor \$
	Custom (Internal Integration)
	Generate

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 11 - Autotask Account Details Screen

WrxCOUNTS WrxCOUNTS WrxCOUNTS Tread Reparts NACCU Treadersh (i) Wrandersh (in) Treadersh (ii) Wrandersh (iii) Treadersh (iii) Wrandersh (iiii) Treadersh (iiii) Wrandersh (iiii) Treadersh (iiii) Wrandersh (iiii) Treadersh (iiiii) Wrandersh (iiii) Treadersh (iiiii) Wrandersh (iiiii) Beness (iiiiiiii) Wrandersh (iiiii) Beness (iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	admin 🔍 🔒 🕇	≗ ≅ ★ 🖮	STEVE PERRY LOGOUT	S
Image: Stand Stands () Image: Stand Stand Stands () Image: Stand Stands () Image: Stand Stand Stand Stand Stands ()		MY		
NAACI Tais A totas: (1) Name: Nume: Nume: Nume: None: None:		Service Desk Waiting My Approval		
Activity Benesk Report Bill Desk Report Bill Desk Report Bill Desk Report Bill Desk Report Bill Corr Desk Report Bill Corr Desk Report Bill Corr Desk Report Bill Desk Report Bill Desk Report Bill Corr Desk Report Bill Cord	- SEARCH	Tasks & Tickets (13) Timesheets (0) Workspace & Queues Time Off Requests (4)		1
Oucles (2) Image: Control Image: Co	Account Name or Number Phone Country City State Zip Code	Open Tickets (12) Expense Reports (0) Overdue Tickets (12) Macclaneous Submitter Tickets (524762) Projects (0) Cosed Tickets Calendar Cosed Tickets (10) From Templates Service Calls (10) Protile Cisma Protile Optimulities (3) Optimulities (3)	Account Manager Petry, Stave Pe	
I how Account is a log of a columner of		Quotes (2) Notes (0) To-Dos (40)	Account - Anchor Network Solutions - Google Chrome	•]-
Account • 1:14:13: API PRTEST 1:214:13: API PRTEST Accient Rogar Accient Rogar Ancheck Clawa Ancheck Roger Phan Ancient Roger Phan Bids Garge edited Company A Company A Company A Dickenson House of the Clawa Company A Dickenson pic Dickenson pic Dickenson pic Dickenson pic Dickenson pic	New Account	Terrabute >	https://ww2.autotask.net/autotask35/crm/account/account/detail.aspx?accountId=30243651	
12-16-13-AP/PRTEST Activation Activation Activation Ancheck Clawa Ancher Network Solutions Ancher Noper ham Set Computation Beds Grage edited Beds Grage edited Obco Beds Grage edited Obco Company A Chusie Mansons House of the Cream Company A Dickenson pic Derver Metro Brona Dickenson pic Derver Metro Brona Dickenson pic	😇 Account 🔺	Timesneets	Pa 🔤 ACCOUNT - Anchor Network Solutions (ID: 30243651) Active Customer 🖈 🚱	
ABC123 Ancheck Clawa Ancheck SanDepp Ancheck SanDeps Ancheck SanDeps Ancheck Namo Ancheck SanDeps Ancheck SanDeps Ancheck Namo Ancheck Namo Ancheck Namo Ancheck SanDeps Ancheck Namo Ancheck SanDeps Ancheck Namo BasennyCig Basen	12-18-13 - API PRTEST	Time Of Requests (0)	Fill Reveal France France	ome
Ancheck Clawa Expense Reports Bels Carger Run Expense Reports Bels Carger Run Expense Reports Bels Carger Run Expense Reports <td< td=""><td>ABC123</td><td>Time Cir Requests (0)</td><td>Edit • New V Tools V Report LiveLinks V</td><td>ome</td></td<>	ABC123	Time Cir Requests (0)	Edit • New V Tools V Report LiveLinks V	ome
Anchole Kap Diago Expension Regions Anchole Kap Diago Inchor Network Solutions Anchor Network Solutions Inchor Network Solutions Autotask Zere Account - AA COM See Configuration Autotask Zere Account See Configuration Accient Roger Pham Account Note Boes Account Note Account Note See Gospan data and Nuck See Configuration Bese mic New Account Note See Configuration Active Opp. See Configuration Active Opp. See Configuration See Configuration See Configuration Active Opp. See Configuration Active Opp. See Configuration See Configuration See Configuration Active Opp. See Configuration See Configuration See Configuration Active Opp. See Configuration See Configuration See Configuration See Configurati	Amcheck Ottawa	Fine Summary	Activity for Anchor Network Solutions	pme
Anerican Pride Coop Anerican Pride Coop Antobar Network Solutions Balarmine Solosoni Heating and Plumbing Chromon Lubrink Annore Notae Cortae Solosoni Heating and Pl	Amcheck San Diego	Expense Reports	Anchor Network Solutions	ome
Anchor Network Solutions Anchor Network Solutions <td>American Pride Co-op</td> <td></td> <td>map</td> <td>ome</td>	American Pride Co-op		map	ome
Aubtask Zera Account: - AA/COM Aubtask Zera Account: - AA/COM See Configuration See Conf	Anchor Network Solutions		(P) 000-000-0000	ome
Autorats1 auto	Autotask Zero Account - QA.COM		Site Configuration	ome
Accient RAC Test Account Accient Roger Phan Accient Roger Phan Accient Roger Phan base myOrg Account Manager Sleve Peny Beds cange effed Account Note Beds cange effed New Account Beds cange effed New Account Note Beds cange effed New Tickt Lat Echt Note Solo Account Note New Tickt Lat Echt Note Solo Company A New Tickt Dickters on pic New Tickt Dickters on pic New Tickt Dickters on pic New Tickt Dickters on pic<	Autotask1		wall Note V Add	ome
 Accient Roger Pham Accient Roger Steve Perry Acc	Axcient RMC Test Account		Tax Exempt No To Doc R Notes Construction	bme
● Actient Roger Pham ▲ Count Manager Steve Penry > base myCrg ● Ent Account Biderme ● New Account Note Bobs Garage edited ● Sci Classification > New Account Note ■ Account Yourd Braconier Heating and Plumbing ● Sci Classification Braconier Heating and Plumbing ■ Cancel Account Witard Bytes and Junk ■ Reassign Lead Witard © Concerty A ● Cancel Account Witard © Daritist ■ New Ticket LinkLinks >> © Deriver Helter Borna >> © Deriver Helter Borna >> Dickenson pic >> Dickenson pic >> Dickenson pic Last Activity 032/32/21/4	 Axcient Roger Pham 		Tickets Contracts Projects	er
base.myCrig Edit Account Bidemic Wew Account Bidemic New Account Bobs Gaage etited New Account Note Dooo Set Classification Close Opontunity Wizard Cole Opontunity Wizard Chuctle Mansons House of Lee Cream Cancel Account Note Denver Metro Bona Congrany A Denver Metro Bona New Textel Denver Metro Bona New Textel Denver Metro Bona VaR Street Dickenson pic VaR Street Diskenson pic Last Activity Diskenson pic Last Activity Diskenson pic	 Axcient Roger Pham 		Account Manager Steve Perry	er
Bidemic Construction Bidemic New Account Note Bobs Garage edited Set Classification Bobs Garage edited Set Classification Bracenier Heating and Plumbing Close Goptminity Wizard Bracenier Heating and Plumbing Close Goptminity Wizard Chuckle Mansons House of for Came Cancel Account Wizard Chuckle Mansons House of for Came Cancel Account Wizard Congray A New Tricket Darthst LiveLinks Delver Metro Boma Delver Account Dickenson plic VAR Street Drixts Last Activity Drixts Last Activity Dicksons plic	base.myOrg	Edit Account	Creer by Date (new to old) •	pme
Bobs Garage edited Set Classification Set Classification Active Opp. So On Active Opp. So On Booso Close Opontunity Wizard Active Opp. So On Active Opp. So On Braconier Heating and Plumbing Losd Opontunity Wizard Defe defe defe. So On Active Opp. So On Braconier Heating and Plumbing Losd Opontunity Wizard Defe defe. Defe. Active Opp. So On Chuckle Khansons House of Ice Cream Concard, Account Wizard Defe. Defe. Managed 398bad/2-4799- Workplace Site 4 Managed 398bad/2-4799- Workplace Site 4 <td>Bidermic</td> <td></td> <td>There are no items to display from the last 6 months</td> <td>ome</td>	Bidermic		There are no items to display from the last 6 months	ome
bood Color Opportunity Ward Amount Bracenier Heating and Plumbing Lost Opportunity Ward Color Opportunity Ward Brytes and Junix Reassing Ladd Ward D Orbustle Mansons House of Ice Cream Cancel Account Ward D Company A Cancel Account Ward D D Influst LiveLinks So 0.00 Company A Cancel Account Ward D Deriver Metro Boma VarBate Account VarBate Account Ward Dickenson pic VarBate Account Market 71985 Dickenson pic Last Activity 03/29/2014 X	Bobs Garage edited	Ret Classification	D: Active Opp. \$0.00 To view activity older than 6 months, use the menu in the top-left corner and select "Notes", or click here	ome
Braconier Heating and Plumbing Lobid Oppriumity Waard Closed Opp. \$0.00 Byles and Junk Reassign Load Witard Dubid Dubid Chuckie Masons House of Ice Cream Image 3908 dat02-e796-witard Gold Coppriumity Waard Chuckie Masons House of Ice Cream Image 3908 dat02-e796-witard Gold Coppriumity Waard Chuckie Masons House of Ice Cream Image 3908 dat02-e796-witard Gold Coppriumity Waard O Dartist LiveLinis Image 3908 dat02-e796-witard Derver Metro Boma Managed 3908 dat02-e796-witard Dickenson Jice VAR Street 71885 Dickenson Jice Lab Tokity 03292014	booo	Close Opportunity Wizard	Amount	ome
Bytes and Junk Reassign Lead Wizard Amount Chuckle Khanson House of Ice Cream Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A Image: Company A	Braconier Heating and Plumbing	Lost Opportunity Wzard	Closed Opp. \$0.00	ome
Chuckle Mansons House of Ice Cream © Cancel Account Wizard EabTechID 600 Company A In New Tickst Managed 3988482-9799- Workplace stell 4179-3030- Unick 1000 4179-3030- Unick 1000 <td< td=""><td>Bytes and Junk</td><td>Reassign Lead Wizard</td><td>DP Amount</td><td>ome</td></td<>	Bytes and Junk	Reassign Lead Wizard	DP Amount	ome
Company A Managed 3008402-679-1 O Darthost LineLinis >> Deriver Metro Boma College Account Delete Account VARStrett 751965 Dickenson pic Last Activity 03292014	Chuckie Mansons House of Ice Cream	Cancel Account Wizard	Lablechild bulk bulk and	
Darthst LiveLinks GUID c0088ea76527 Derver Metro Boma X Delete Account VAR Street 751965 Dickmon pic Last Activity 03/29/2014	Company A	New Ticket	manageo subsato_erys- Workplace Site 419-b306-	
Deriver Metro Boma ¥ Delete Account VAR Street Account ID 751985 Account ID Dickenson pic Last Activity 03/29/2014 .	1 Dartfust	LiveLinks >>	GUID c0088be76527	ome
Dickenson pic Account ID DKS Sports Last Activity 03/29/2014 ,	Denver Metro Boma	X Delete Account	VARStreet 751985	ome
DKS Sports Last Activity 03292014	Dickenson plc		Account ID	
	DKS Sports		Last Activity 03/29/2014 -	ome
Dr. Tongues 3-D House of Pancakes	Dr. Tongues 3-D House of Pancakes			omer

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:

$\textcircled{\black}{\black}$	Search		+ اו. ۹							
ном	E	Admin	Admin Categories							
CRM		Featu	Features & Settings							
DIRE	CTORY	Exter	Extensions & Integrations							
CONT	TRACTS	Comm	Commonly Used							
PROJ	IECTS	Getti	Getting Started							
SEDV		Reso	Resources (Users)							
JERV	ICE DESK	Form Templates								
TIME	SHEETS	Notification Templates								
REPC	ORTS	Work	flow Ru	les						
OUTS	OURCE	User	User-Defined Fields							
ADMI	N	Syste	em Setti	ngs						

Figure 12 - Autotask Features & Settings Option

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





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

	Figure 14 - Edit Queue Details Option							
🗲 si	ERVICE DESK QUEUES							
Set up the	et up the folders that will contain tickets with similar characteristics, and assign resources to monitor them. New Save Cancel							
	Name 🔺		Description					
<i>⊘</i> ×	Administrative		Administrative					
0 ×	Anchor HD		Tier 1 Helpdesk Requests					
1 ×	AutoQueue	/ Edit Queue						
1 ×	Autotask Consulting	Redit Queue Details	Autotask Consulting					
ØΧ	CLEP	Inactivate Queue						
P	Client Portal	X Delete Queue	Service Desk					
ØΧ	CSD		CSD					
ØΧ	Helpdesk		Escalated Helpdesk Requests					

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

Fiaure	15 -	Oueue	Number	Location
		20000		

https://ww2.autotask.net/autotask/popups/administration/QueueDetails.aspx?objectId=29878555&type=queue	
QUEUE SUMMARY	8
Summary Resources	
Queue Name*	
Anchor HD I Active	
Queue Location* British Columbia	
Queue Number	
29878555	
Queue Description	
Tier 1 Helpdesk Requests	
Appears in Client Portal When this is not checked, tickets in this queue will not display in the Client Portal	
Queue Location	

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:

	IRI V Overview		
STEP 1	IRE.	Troubled	
			ACCOUNT AT A GIANCE
In the Site Details page, click the Settings link.	Activity of Interest for IRE_fusion_test_site	-	2 SERVICES
	4 devices require attention		5 DEVICES All protected
	ubuntu 12-10 Device is outside of the protection threshold.		SETTINGS
	win?kRr? Device is outside of the protection threshold		
	PSA Tool	C -1	EDIT
STEP 2	No PSA is configured. Using a PSA tool can help you stay informed of system events and automate support ficketing.	Tool t	o further integrate the Axcient services with vour established office routines.
In the PSA Tool section, click the Edit button.	At this fitme, Accient integrates with: ConnectVias (venion 2011.1 and newer) Autotask		
	Test PSA Connection Verify the site can connect to your PSA tool		

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 <u>Obtain Client Information</u> 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	itiging correctwisedex con	0
API KEY	Respict 86.001 (194	0
API SECRET	•••••	0
MSP COMPANY ID	Axcient_f	0
COMPANY ID	AX	
SERVICE TYPE	Warranty	0
LOCATION	Tampa Office	0
ADDRESS LINE 1	2106 SHADYHILL TER	0
ADDRESS LINE 2		
CITY	Harrells	
STATE	Florida	~
ZIP	34667	
TICKET PRIORITY	Priority 1 - Emergency Response	0
SERVICE SUBTYPE	stl	0

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 Appendix

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

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

Obtain the API Key

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

To create a new API key:

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

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

Figure 16 - 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.

Site:	staging.connectwisedev.com
Company:	Axcient_f
User Name:	admin1
Password:	*****

Figure 17 - ConnectWise Login Screen

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 <u>online ConnectWise support</u> 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.

ArtSpace															
Company	Notes	Contacts	Opportunities	Tracks	Activities	Service	Projects	Agreements	Documents	Profile	Surveys	Sites	Team	Options	Configuratio
+ +	88	c 🕤	🏦 More 🔻 Lir	iks 🔻 Histo	ory 🔻 🛛 🖀										
Company:	ArtSpace														
Company: *	ArtSpace							Site: Main							•
Phone:							<u> </u>	250 3rd Avenue	North						•
Fax:	1							Minneapolis, MN	55401						
Web Site:	http://ww	w.artspaceusa.	org				3								
Company	Details														
Type: *	Customer						•	Company ID: *	ArtSpace						
Status: *	Active						-	Market:							•
Territory:	Clearwate	rOffice					•	Date Acquired:	Wed 11/29/2006						•
Primary C	ontact														
	Name:	Gary						Email:	will@artspac	eprojects.or	1				
	Title:							Type:							
	Phone:	<u>(612) 333-901</u>	2					Relationsh	iip:						
iii 1															

Figure 18 - ConnectWise Company Screen

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 <u>online ConnectWise support</u>.

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.

Setup Tables > Service Boar	d List ≽ Type	List		
Type List				
Board Statuses	Types	Subtypes	Items	Auto Templates
🔶 🕂 🗋 Search	Clear			
Service Type 🔺	Default	Request For	Change	Inactive
1	_			•
Break-fix				
Proactive				
Reactive				
Roger Pham Type				
Server				
Warranty				

Figure 19 - ConnectWise Types List

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	s > Service Boa	ard List > Sub	type List	
Subtype Lis	st			
Board	Statuses	Types	Subtypes	Items
+ +	Search C	lear		
Service Su	btype 🔺	Types	Inact	tive
		_		-
Roger Phan	n Subtype	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 <u>online ConnectWise support</u>.

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.

A			
А			
SLA Setup SI	LA by Priority		
日十日間	â		
	-		
1 Updated: 6/24	4/2005 4:14:05 PM by user10		
SLA Name:	andard SLA		
Based on:	4y Company Calendar V		
Calandari			
Calendar:	~		
i Calendar opt	tions are defined in the <u>Calendar Setup Table</u>		
Default?	✔ Use this SLA if no SLA exists for the customer / agreement		
SLA Application O			
	Orden:		
Default Response	se Matrix:		
Default Respons	se Matrix: High Urgency Medium Urgency Low Urgency		
Default Respons	Order:		
Default Respons High Impact Medium Impact	Se Matrix: High Urgency Medium Urgency Low Urgency Priority 1 - Emergency Respoi Priority 2 - Quick Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 2 - Quick Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response		
Default Respons High Impact Medium Impact Low Impact	Se Matrix: High Urgency Medium Urgency Low Urgency Priority 1 - Emergency Respon v Priority 2 - Quick Response v Priority 3 - Normal Response v Priority 2 - Quick Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v		
Default Respons High Impact Medium Impact Low Impact Default Respons	See Matrix: High Urgency Medium Urgency Low Urgency Priority 1 - Emergency Respoi Priority 2 - Quick Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 2 - Quick Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response Re Goals: Priority 3 - Normal Response Priority 3 - Normal Response Priority 3 - Normal Response		
Default Respons High Impact Medium Impact Low Impact Default Respons Respond within:	Set Matrix: High Urgency Medium Urgency Low Urgency Priority 1 - Emergency Respon v Priority 2 - Quick Response v Priority 3 - Normal Response v Priority 2 - Quick Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v Priority 3 - Normal Response v set Goals: 4.00 hours Goal Percent: 80		
Default Respons High Impact Medium Impact Low Impact Default Respons Respond within: Plan within:	Order:		

Figure 20 - ConnectWise SLA Screen

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**.

Configure PSA Tool Alerting in the Web Application

To configure alerting and notifications in the Axcient Web Application:



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 appliancebased and D2C services. The options include Warning and Offline health statuses.

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