

The background of the page is a solid orange color. Overlaid on this are several large, abstract, rounded geometric shapes in various shades of orange and red. These shapes are arranged in a way that they appear to be layered or overlapping, creating a dynamic and modern visual effect. The shapes include a large 'X'-like form, a curved shape on the right, and a large shape at the bottom right.

# Axcient

## Fusion 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

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

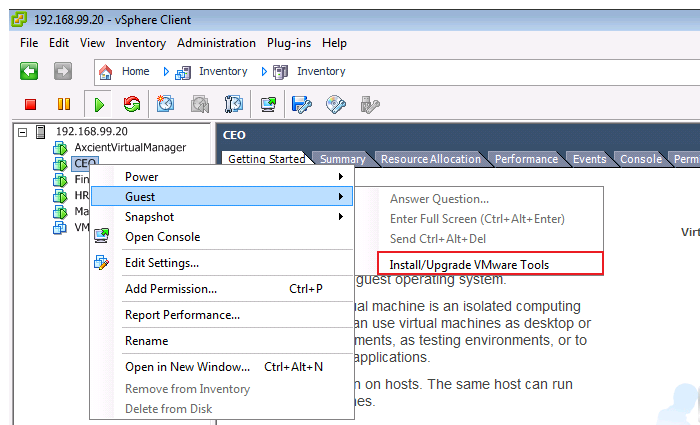
# Install Latest VMware Tools

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

To install the latest VMware tools:

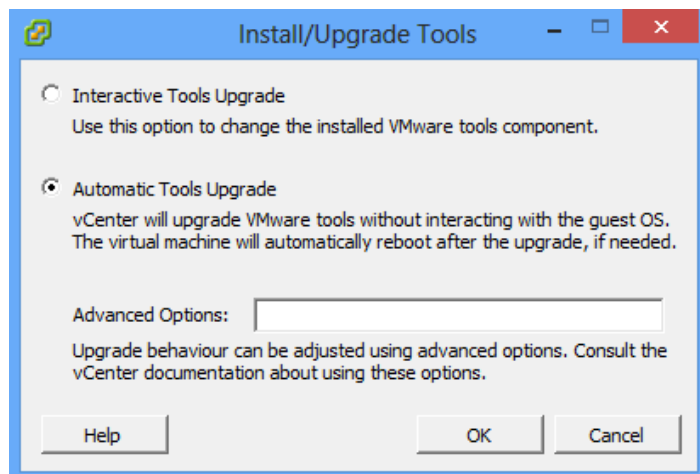
## STEP 1

Right-click the appropriate VM, point to **Guest**, and select **Install/Upgrade VMware Tools**.



## STEP 2

In the *Install/Upgrade Tools* pop-up window, select the **Automatic Tools Upgrade** radio button.  
Click the **OK** button to save your settings.





## Enable Change Block Tracking (CBT)

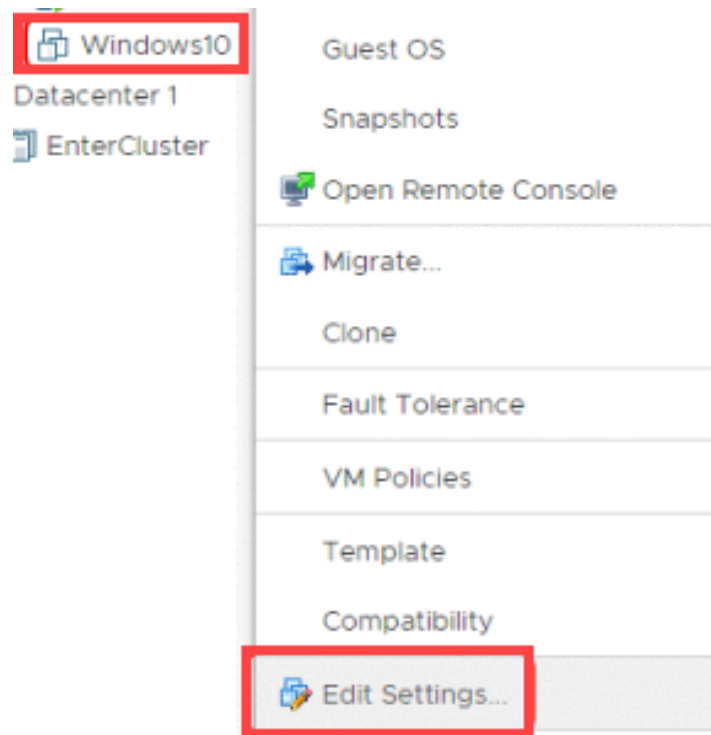
Change Block Tracking (CBT) is automatically enabled on the target VMs after the AVM is deployed on the ESX host and the initial seed replication job begins.

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.



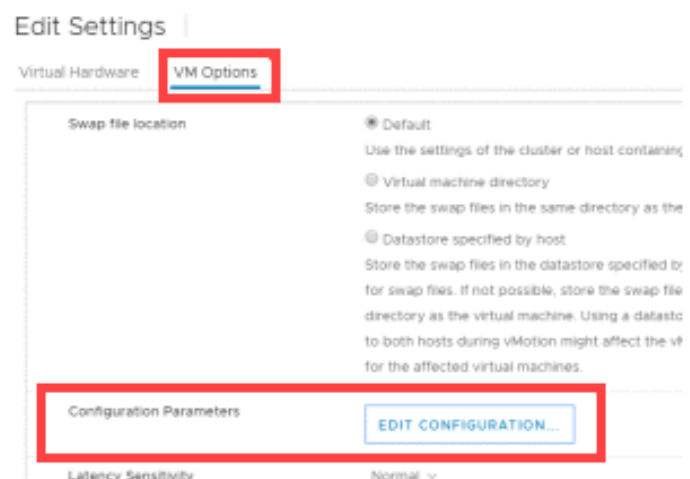
### STEP 2

Click the **Options** tab and select **General** in the *Settings* list.

In the *Configuration Parameters* section, click the **Edit Configuration** button to continue.

Confirm the following settings:

- **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**



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

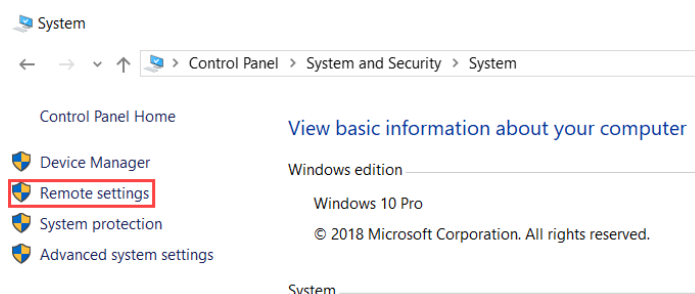
You must enable the *Allow users to connect remotely to your computer* option in order to use a Remote Desktop Protocol (RDP) agent to access devices in the Virtual Office recovery tool. Using an RDP agent is the only way you can directly access the desktop of a virtualized device in the Virtual Office. 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.

To enable Remote Desktop on a device:

## STEP 1

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

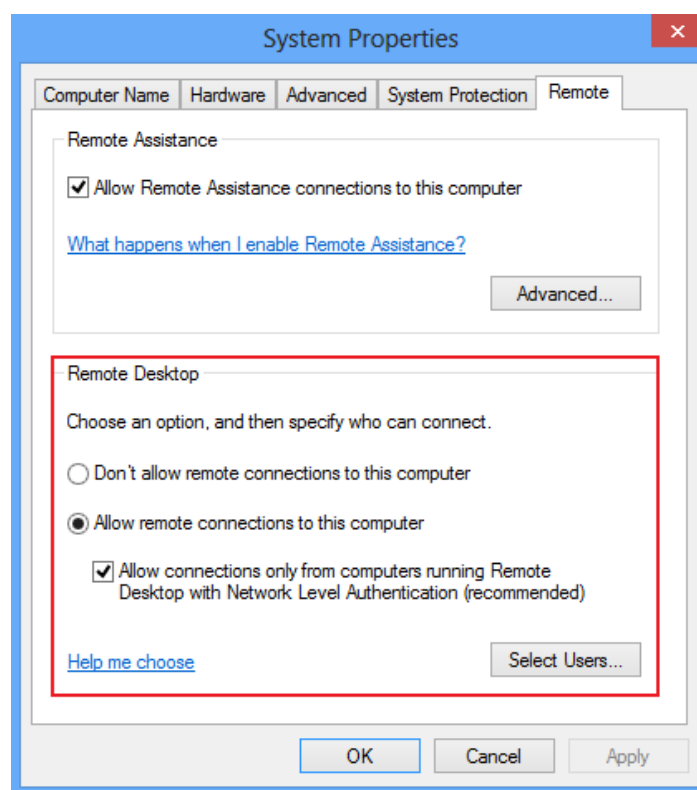
In the *System* window, click **Remote Settings**.



## 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.



# Setting Up a New Service

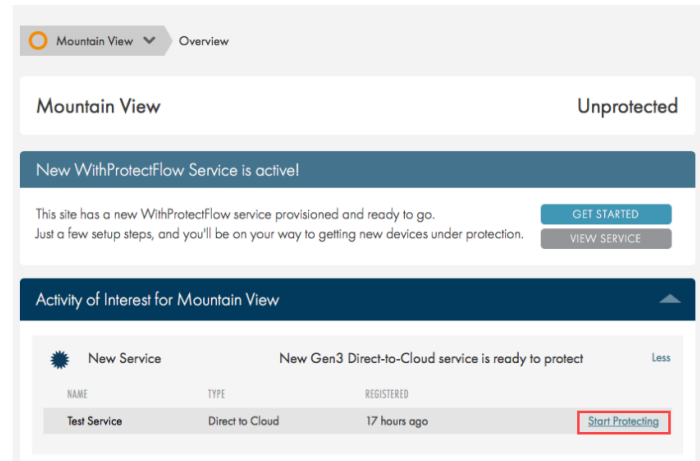
After you complete each preparation step, you can begin to set up a new Fusion service.

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.



## STEP 2

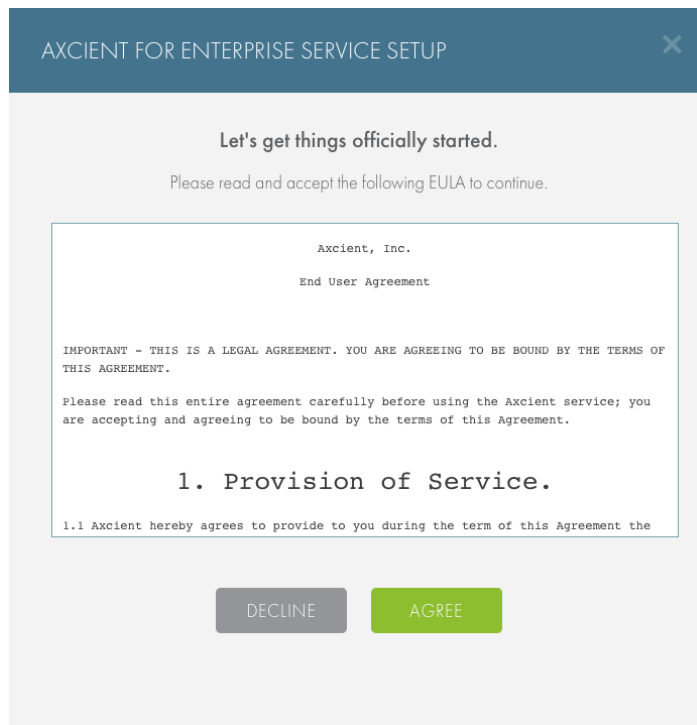
In the *Setup* pop-up window, click the **Let's Do It** button to begin the configuration process.



## STEP 3

You will be presented with the End User License Agreement.

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



AXCIENT FOR ENTERPRISE SERVICE SETUP

Let's get things officially started.

Please read and accept the following EULA to continue.

Axcient, Inc.  
End User Agreement

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

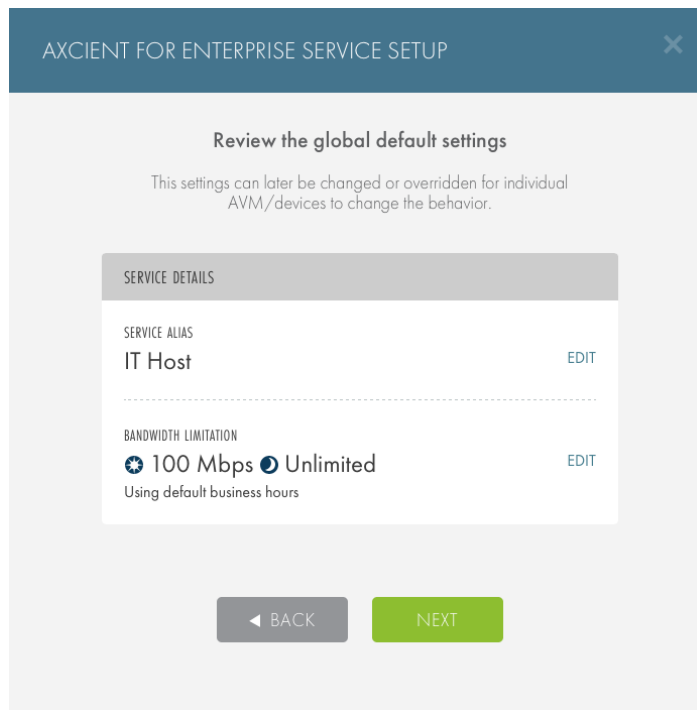
DECLINE AGREE

## 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 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 EDIT

BANDWIDTH LIMITATION  
☒ 100 Mbps 
 ☐ Unlimited EDIT  
 Using default business hours

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 Unlimited EDIT

Using default business hours

BACK NEXT

## 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 SETUP

Set WAN bandwidth allowance for service atd - raa4.

Customize bandwidth for an individual device on the device's detail page.

During business hours

1 MBPS 50 MBPS 100 Mbps NO LIMIT

During non-business hours

1 MBPS 50 MBPS NO limit

BACK SAVE

## STEP 5

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.

The screenshot shows a 'SERVICE SETUP' window with a close button (X) in the top right corner. The main heading is 'Set when initial seeding should happen.' Below this, there are two sections: 'INITIAL SEED' and 'RUN REPLICATION EVERY'. The 'INITIAL SEED' section has two radio button options: 'Start seeding immediately' (which is selected) and 'Delay seeding to a later time'. The 'RUN REPLICATION EVERY' section has a dropdown menu currently set to '1 Hour', and two radio button options below it: 'at all times' (which is selected) and 'on specific days and times'. At the bottom of the form are two buttons: 'BACK' with a left arrow and 'NEXT'.

## STEP 6

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 SETUP

**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:

1 HOUR | | | | | | | | 24 HOURS

■ Device's most recent recovery point is older than:

1 HOUR | | | | | | | | 24 HOURS

◀ BACK NEXT

## 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 [How to Deploy the AVM Agent](#) 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/eyl:](https://fw-one1.axuptiva.net/d2c_agent/eyl:) [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 data 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:

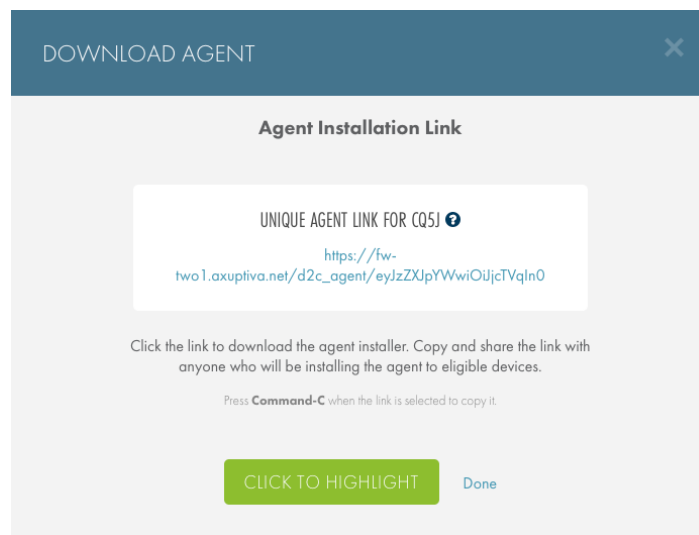
**Note:** These instructions will vary depending on your version of vSphere.

## STEP 1

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

- At the completion of the [initial service deployment process](#).
- On the *Service Details* page, located in the *Service at a Glance* section.

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

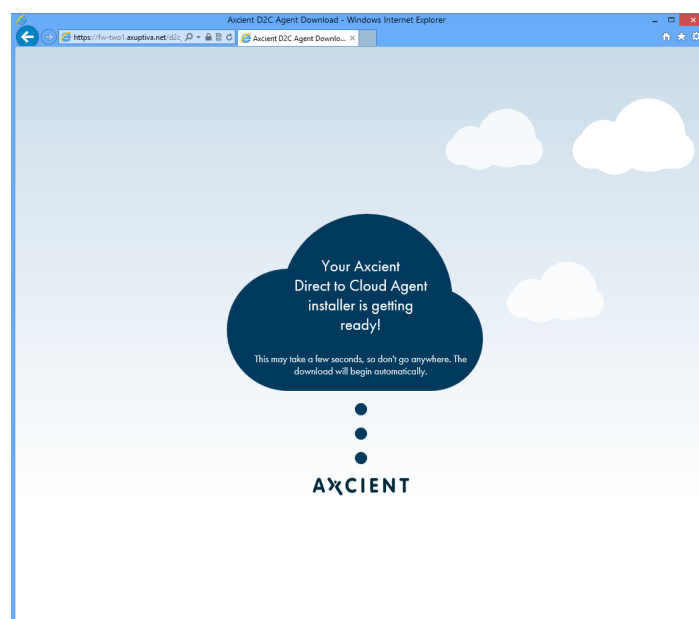


## STEP 2

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

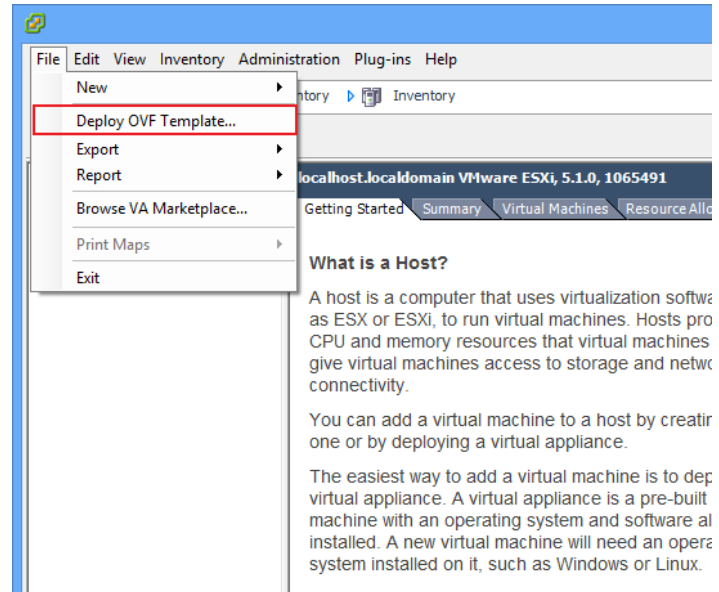
The AVM agent OVA file will be downloaded to the local device. Be sure that the device has access to the ESX host through vSphere.

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



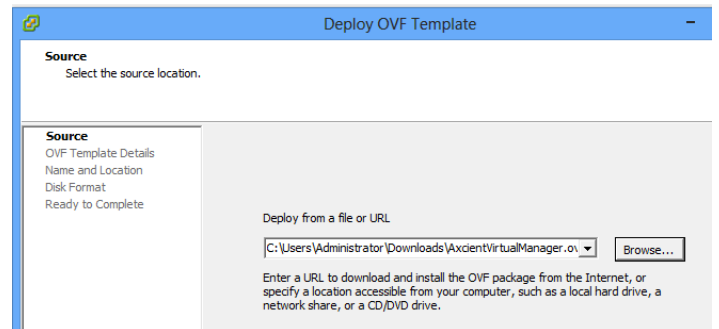
### STEP 3

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**.



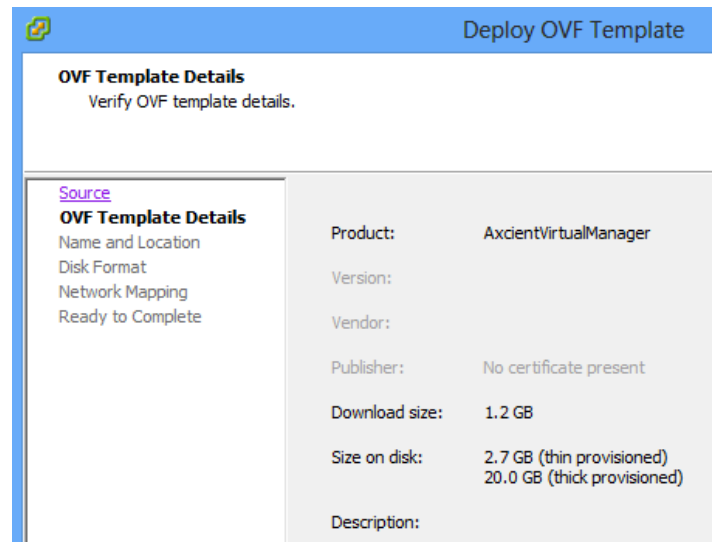
### STEP 4

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



### STEP 5

On the *OVF Template Details* page, review the specific OVF template details.  
Click **Next** to continue.



## STEP 6

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

Click **Next** to continue.

## 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.

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.

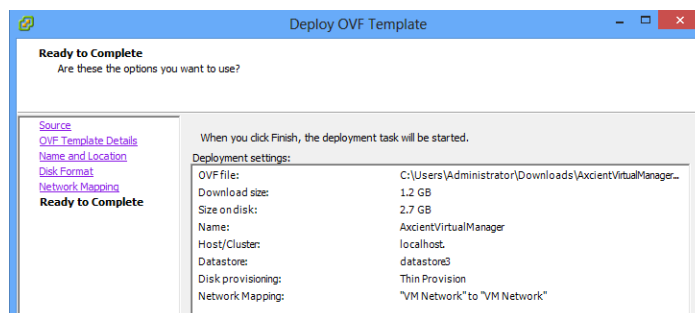
Click **Next** to continue.

## STEP 9

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.

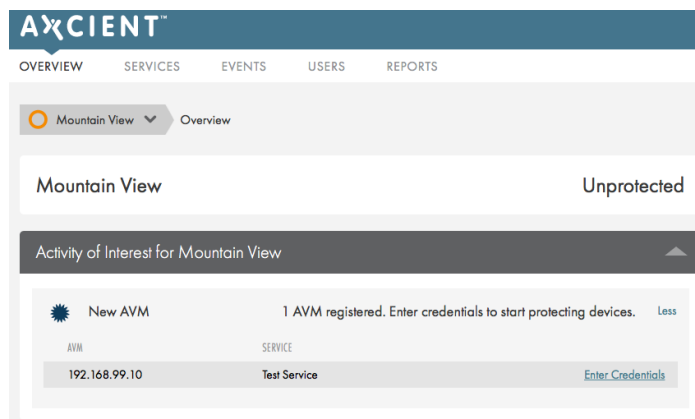


## STEP 10

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.



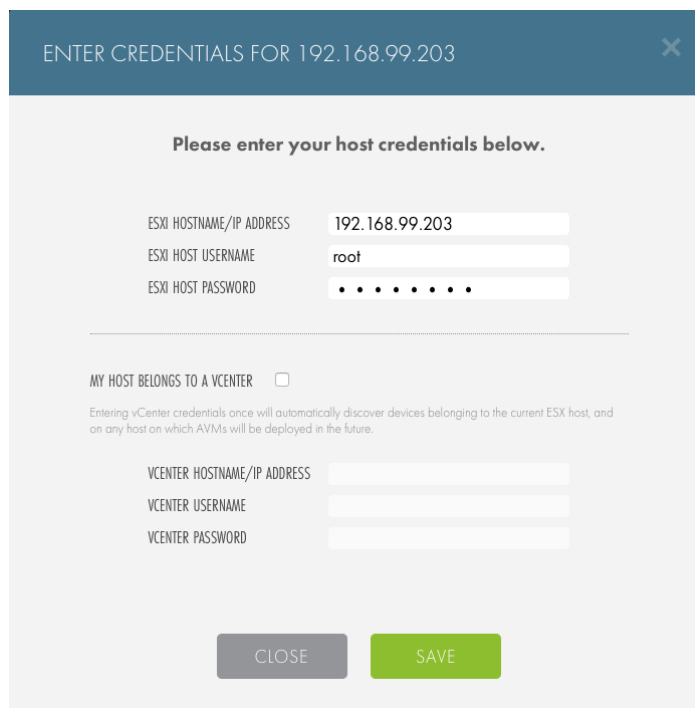
## STEP 11

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.



- **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:

## STEP 1

On the *Service Details* page, find the appropriate AVM, click the drop-down arrow, and select **View AVM**.

## STEP 2

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

## STEP 2

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](#).

☒ Enable Custom Bandwidth Limits

During business hours

1 MBPS | | | 50 MBPS | | | NO LIMIT

During non-business hours

1 MBPS | | | | | | | NO LIMIT

☒ Enable Custom Replication Settings

Run replication every 12 Hours

☒ at all times

☐ on specific days and times

SUN MON TUE WED THU FRI SAT

10:00 PM to 05:00 AM

You may need to adjust your Alert Thresholds to accommodate this schedule.

SAVE CUSTOM LIMITS Cancel



# 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.

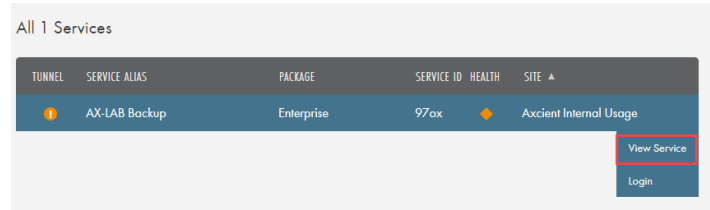
Configurations are not permanent and can be changed at any time to accommodate a dynamic environment.

To access the *Service Configuration* page:

## STEP 1

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

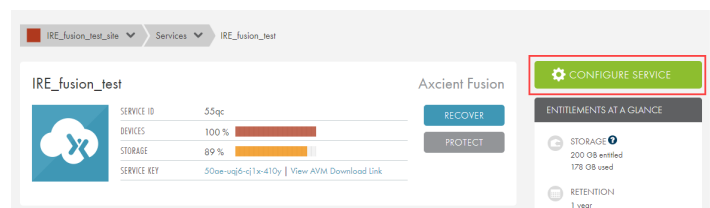
On the *Services* page, find the service to be configured, click the drop-down menu, and select **View Service**.



## 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

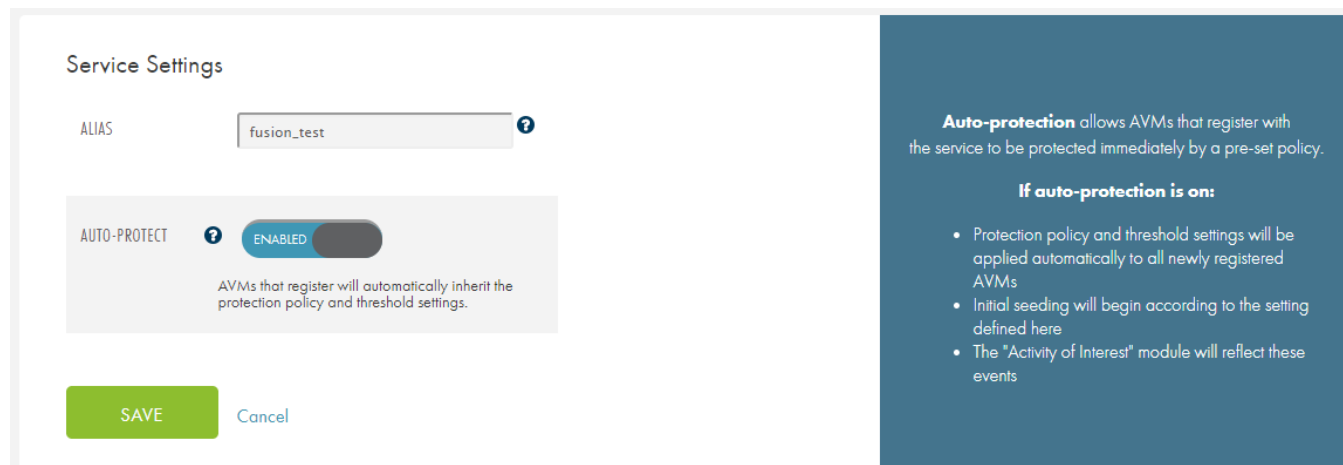


## Service Settings

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

- **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



The image shows a 'Service Settings' configuration window. It has a title bar 'Service Settings'. Below the title bar, there is a section for 'ALIAS' with a text input field containing 'fusion\_test' and a help icon. Below that is a section for 'AUTO-PROTECT' with a toggle switch set to 'ENABLED' and a help icon. Below the toggle switch, there is a description: 'AVMs that register will automatically inherit the protection policy and threshold settings.' At the bottom left, there are two buttons: 'SAVE' (green) and 'Cancel' (blue). On the right side of the window, there is a blue sidebar with white text. The sidebar contains the text: 'Auto-protection allows AVMs that register with the service to be protected immediately by a pre-set policy.' Below this, it says 'If auto-protection is on:' followed by a bulleted list: 'Protection policy and threshold settings will be applied automatically to all newly registered AVMs', 'Initial seeding will begin according to the setting defined here', and 'The "Activity of Interest" module will reflect these events'.

**Service Settings**

ALIAS  ?

AUTO-PROTECT ? ☒ ENABLED

AVMs that register will automatically inherit the protection policy and threshold settings.

**Auto-protection** allows AVMs that register with the service to be protected immediately by a pre-set policy.

**If auto-protection is on:**

- Protection policy and threshold settings will be applied automatically to all newly registered AVMs
- Initial seeding will begin according to the setting defined here
- The "Activity of Interest" module will reflect these events

## 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

### Service-Wide Alerts & Thresholds

**Configurable thresholds:**

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

1 HOUR

24 HOURS

■ Device's most recent recovery point is older than:

12 HOURS

24 HOURS

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

◆ Device's best recent restore point within threshold **completed with warnings**.

SAVE

Cancel

#### HOW THRESHOLDS WORK

Thresholds are service wide and will be used to determine when a device's or AVM's health status changes. Base them on your overall standard of protection and recovery point objectives (RPO).

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

RESET TO DEFAULTS

## 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 snapshot 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 crash-consistent snapshot will ignore them.

Figure 3 - Protection Policy Default Configuration Screen

### Service-Wide Protection Policy

CLOUD RETENTION

Cloud
 

1 Year

1 WEEK2 WEEKS1 MONTH3 MONTHS1 YEAR3 YEARS5 YEARS7 YEARS10 YEARS

INITIAL SEED

☐ **Start seeding immediately**  
 Start jobs as soon as possible, as resources allow

☒ **Delay seeding to a later time**  
 Seed jobs after hours, over the weekend, or on a particular day
 

START ON

Friday

9:00

PM

Replications will start anytime within an hour from when they are scheduled.

RUN PROTECTION EVERY

1 Hour

☒ at all times
 ☐ on specific days and times

AVM REPLICATION SETTING

☒ **Application-consistent when possible**
☐ **Crash-consistent only**

Learn more about application and crash consistent snapshots [here](#).

SAVE

Cancel

Configuring retention will allow you to choose how long you'd want to store your data and are limited by your entitlements.

Initial seed settings give you an option to either start the replication jobs immediately or to delay them to a later date. Customizing protection frequency gives you the flexibility to configure how often a replication job should run. Jobs will start based on initial seed setting and run based on protection frequency setting.

## 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.

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

**Bandwidth / QoS (Quality of Service)**

**WAN**

QoS values selected below will apply to every AVM protected by this service. AVMs with custom bandwidth limits will not be affected

**During business hours**

1 MBPS | 50 MBPS | NO LIMIT

**During non-business hours**

1 MBPS | 50 MBPS | NO LIMIT

**SAVE** **Cancel**

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

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

**RESET TO DEFAULTS**

## 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 [Time Zone](#) and [Protection Policy Default](#) 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 ▼	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 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 [Business Hours](#) and [Protection Policy Defaults](#) 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 Configuration Screen

### Time Zone

SERVICE TIME ZONE (GMT-08:00) Pacific Time (US & Canada) ?

RESULTING LOCAL TIME 10 Jun, 2019 12:35 PM

UTC 10 Jun, 2019 7:35 PM

SAVE Cancel

All application data is shown using the global time zone.

However, because your service may be deployed in multiple locations, you can choose to have QoS and Business Hours honor the local device's time zone instead.

Note that changing the time zone restarts the replication service. Do not change the time zone while any replications 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.

### Notification Configuration

Health digest notifications configuration

Get a health overview of your devices and services every day

NOTIFICATION TYPE
EMAIL

+ Add Another

SAVE Cancel

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 threshold and connectivity settings defined on the Service Configuration page for each service.

- ◆ **WARNED** Action may need to be taken to prevent the replications from becoming troubled
- **TROUBLED** The most recent recovery point is older than 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.

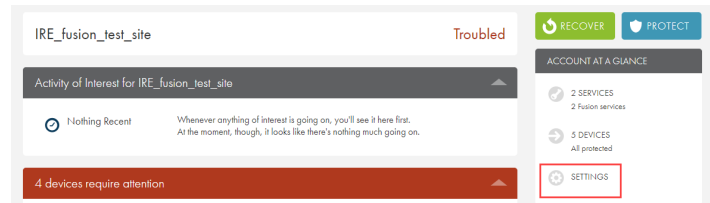


## STEP 2

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.

Figure 7 - Notification Configuration Section

## Notification Configuration

Outgoing notifications will be sent by these methods:

	LOCAL/D2C JOBS	CLOUD JOBS	CONNECTIVITY	
INFO	◆	◆	◆	
Email	◆	◆	◆	●
admin@partner.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
support@partner.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

+ Add another

Configure your chosen PSA tool in the section below.

SAVE

Cancel

Notifications are outgoing messages intended to keep you informed of significant changes in the status of a site's devices without having to be logged in to the application. Their triggers are based on Alert Configurations set above, and the settings are site-wide.

RESET TO DEFAULTS

## 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

SAVE

Cancel

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.

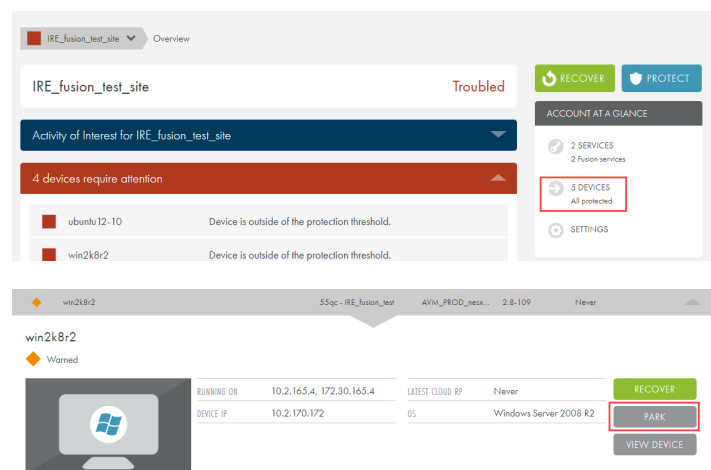
To park a device:

## 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 **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.

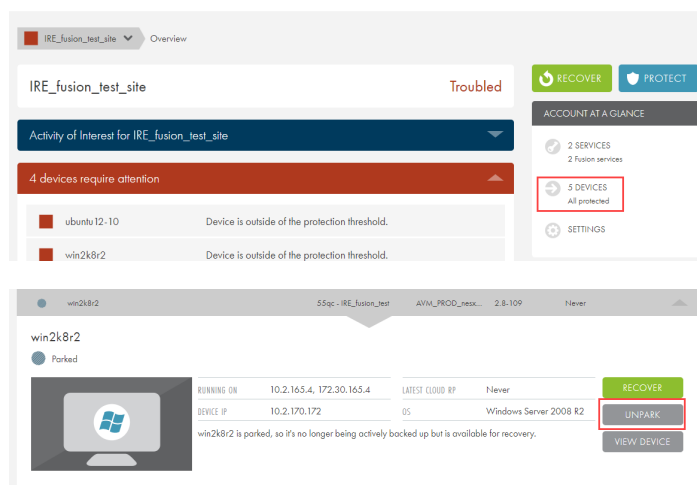
To unpark a device:

### 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.



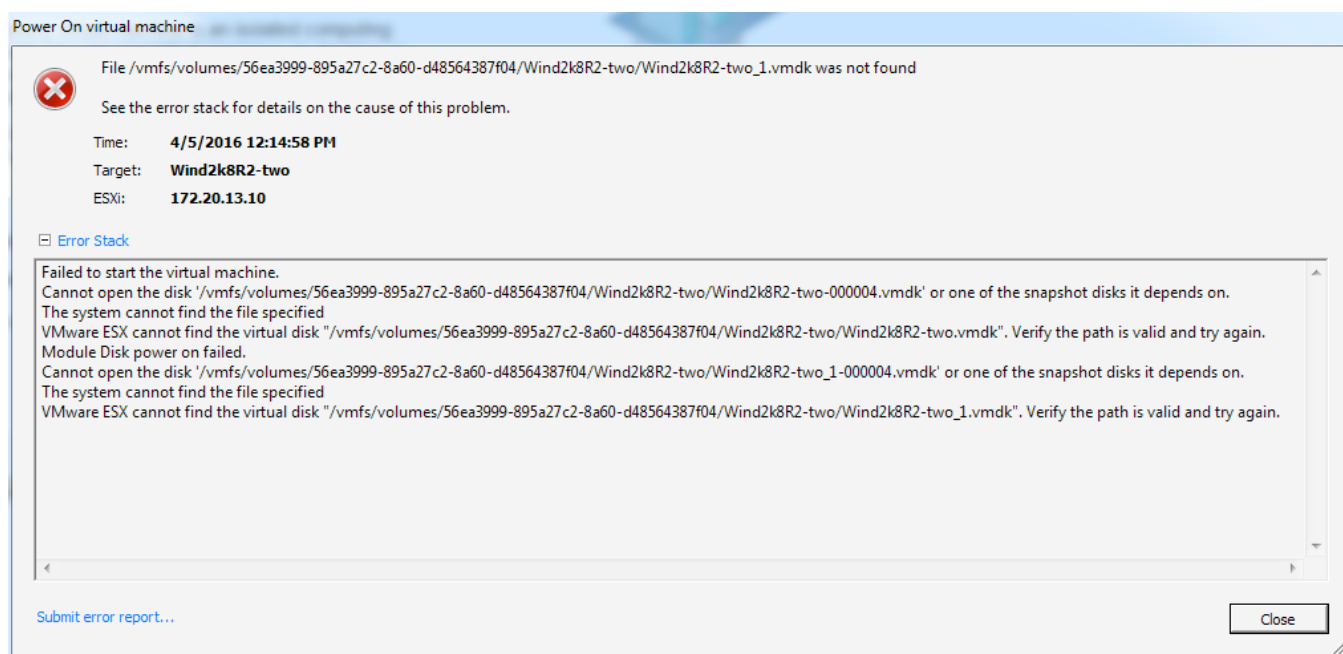
# Delete an AVM

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*



# 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

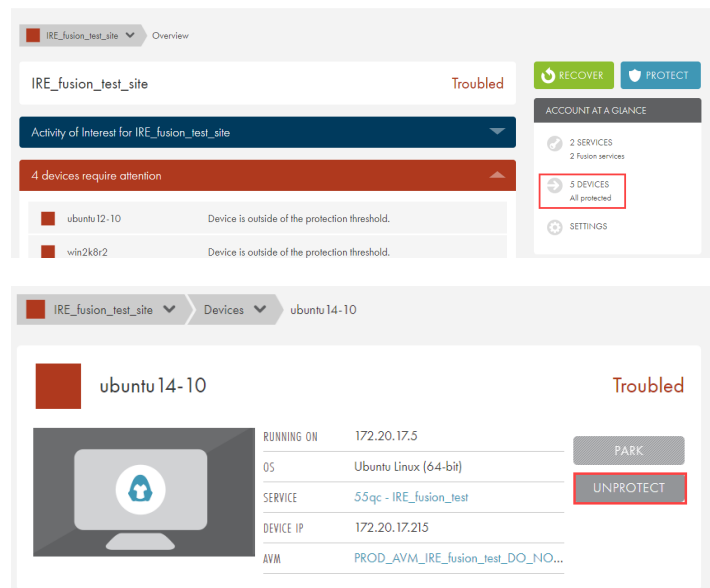
On the *Site Details* page, click the **Devices** link under the *Account at a Glance* section.

### 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.



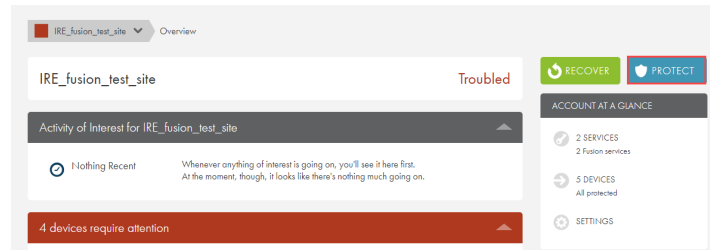
## Re-protect a Device

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:

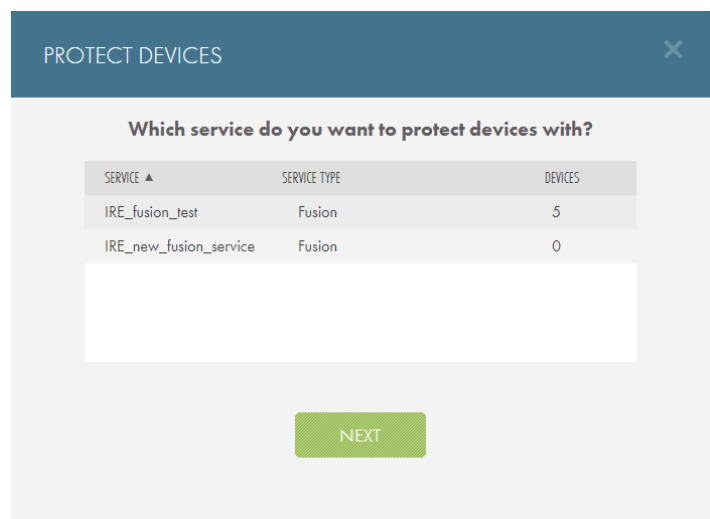
### STEP 1

On the *Site Details* page, click the **Protect** button.



### STEP 2

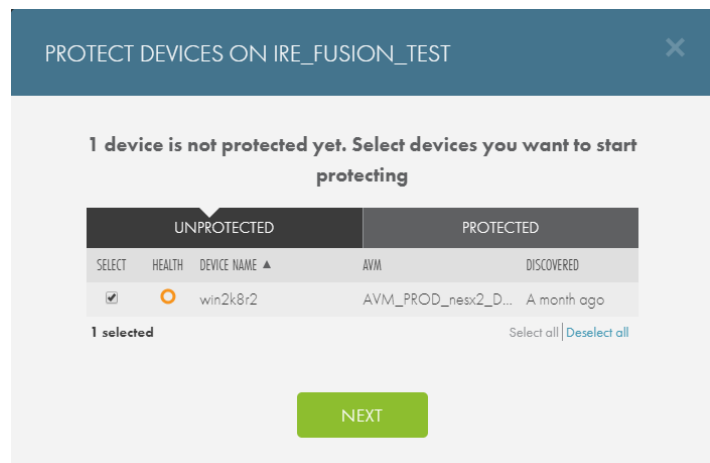
On the *Protect* screen, select the appropriate Fusion service if prompted and then click the **Next** button.



### STEP 3

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

Click the **Next** button to continue.





## STEP 4

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

Click the **Next** button to continue.

PROTECTION SETTINGS FOR SELECTED DEVICES

**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	<div>50 Mbps</div> <div>500 Mbps</div>
SEEDING START TIME	Start seeding immediately

BACK

NEXT

## STEP 5

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

PROTECTION UNDERWAY

**Here we go!**  
**Now protecting win2k8r2.**

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](#).

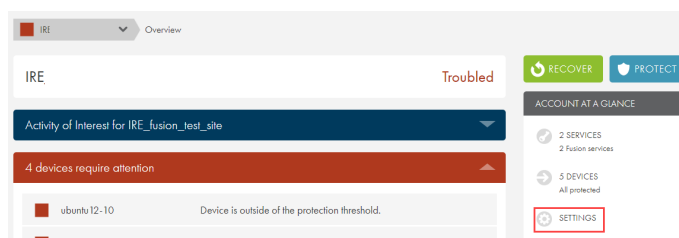
# Autotask Integration with the Axcient Web Application

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

To integrate with the Autotask PSA Tool:

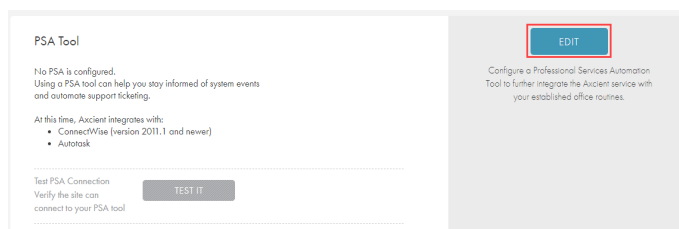
## STEP 1

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.

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 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 drop-down 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

RESOURCE MANAGEMENT

Save & Close

Save

Save & Copy

Cancel

Tabs with \* contain required fields

General \*

Security \*

HR \*

Approvers \*

Associations \*

Skills

Attachments

CREDENTIALS

Username \*

☒ Active

Password \*

.....

Confirm Password \*

.....

Security Level \*

API User (system)

☐ Allow Resource to access links to Datto pages from within Autotask (Datto Integration must be enabled)

☐ 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](#).

☐ Resource is not required to Submit Timesheets

Outsourcing Permissions \*

None

TWO-FACTOR AUTHENTICATION

☐ Require Two-Factor Authentication for this Resource

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 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](#)

Option 2 - CRYPTOCARD Tokens

Option 3 - TOTP (Google Authenticator, etc.)

Time-based one-time password

API TRACKING IDENTIFIER

API version 1.6 & later require the use of an API tracking identifier. Once assigned, this cannot be changed.

☐ None

☒ Integration Vendor

☐ Custom (Internal Integration)

Generate

© 2020 Axcient, Inc. All Rights Reserved.

47

## 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

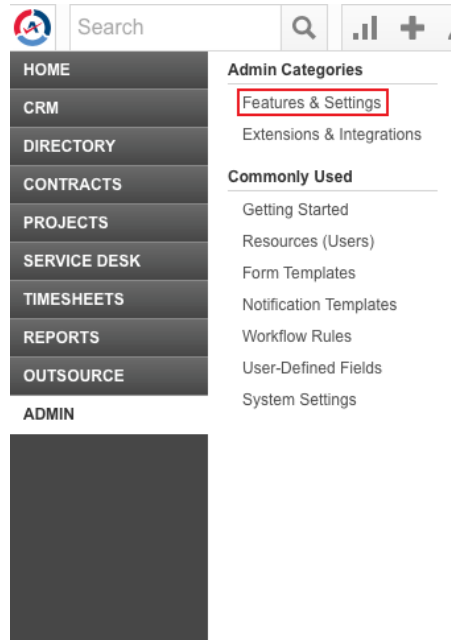
The screenshot displays the Autotask CRM interface. On the left, the 'MY ACCOUNTS' section shows a list of accounts. A search filter is applied, showing results like '12-18-13 - API PRTEST', 'ABC123', 'Amcheck Ottawa', etc. A right-click context menu is open over the 'Anchor Network Solutions' account, with the 'View Account' option highlighted. The main area shows the 'ACCOUNT - Anchor Network Solutions (ID: 30243651) | Active Customer' details. The 'Account ID' is clearly visible as 30243651. The account manager is Steve Perry. The page also shows various tabs like 'Edit', 'New', 'Tools', 'Report', and 'LiveLinks'. A message at the bottom states: 'There are no items to display from the last 6 months. To view activity older than 6 months, use the menu in the top-left corner and select "Notes", or click here'.



## Obtain the Queue ID

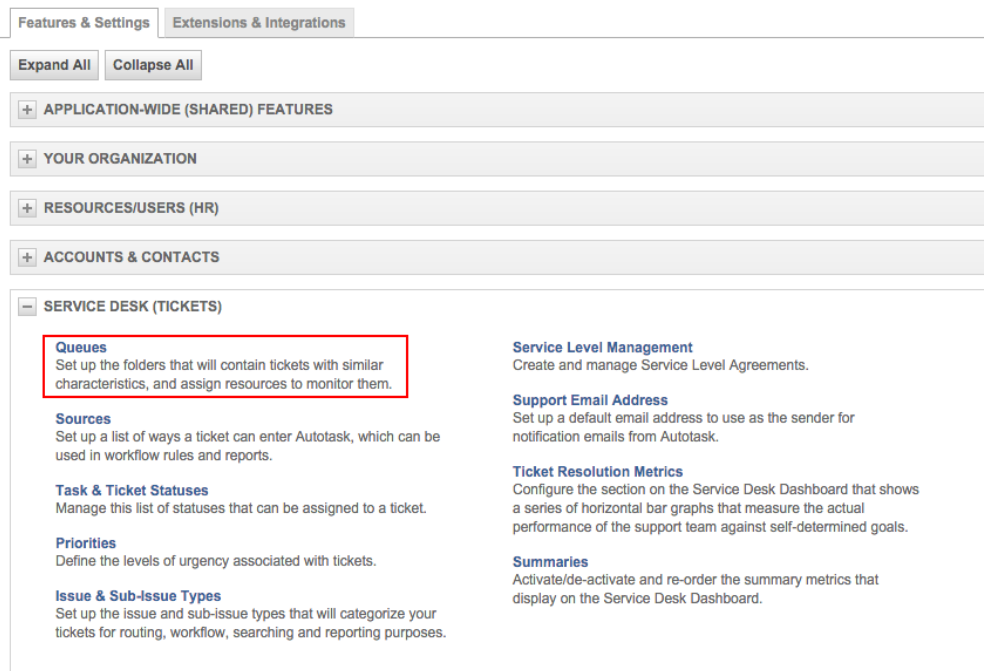
The Queue ID is found in the *Queue Details* page of the appropriate Service Desk Queue, located in the *Features & Settings* section. To obtain the Queue ID:

Figure 12 - Autotask Features & Settings Option



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

Figure 13 - Queues Option in the Service Desk Section



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

Figure 14 - Edit Queue Details Option

←

SERVICE DESK QUEUES

Set up the folders that will contain tickets with similar characteristics, and assign resources to monitor them.

+ New

Save

Cancel

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

Edit Queue
 

**Edit Queue Details**

 Inactivate Queue
  Delete Queue

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

Figure 15 - Queue Number Location

<https://ww2.autotask.net/autotask/popups/administration/QueueDetails.aspx?objectId=29878555&type=queue>

QUEUE SUMMARY

Save & Close

Cancel

Summary

Resources

Queue Name\*

Anchor HD

☒ Active

Queue Location\*

British Columbia

+

Queue Number

29878555

Queue Description

Tier 1 Helpdesk Requests

☒ Appears in Client Portal

When this is not checked, tickets in this queue will not display in the Client Portal

Queue Location

British Columbia

# ConnectWise Integration in the Axcient Web Application

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

To integrate with the ConnectWise PSA tool:

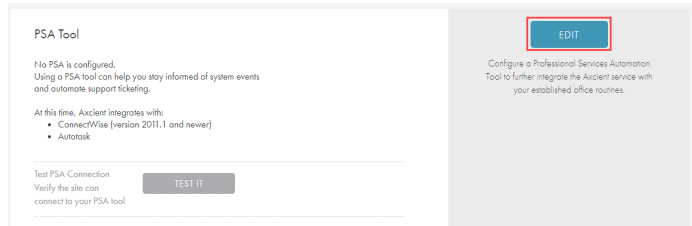
## STEP 1

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 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

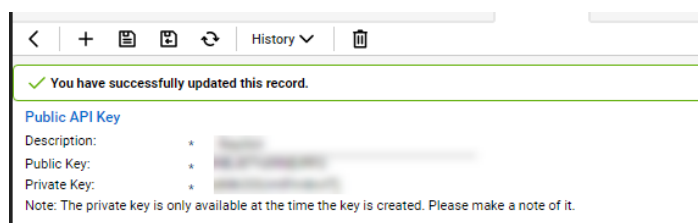
You can obtain API information within the ConnectWise service. For the purposes of integrating ConnectWise with the Axcient protection solution, you will need to create a new API key.

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.

Figure 17 - 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 18 - 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 19 - 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
<input type="text"/>	<input type="text"/>	<input type="text"/>
<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 20 - 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

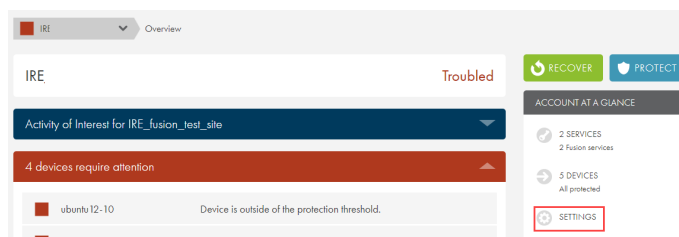
You must configure which alerts will be published to the PSA tool. If you successfully integrate a PSA tool but neglect to configure alerting, then **no alerts will be published to the PSA tool**.

## Configure PSA Tool Alerting in the Web Application

To configure alerting and notifications in the Axcient Web Application:

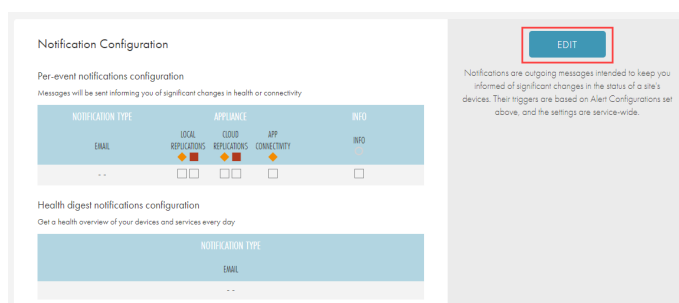
### STEP 1

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



### STEP 2

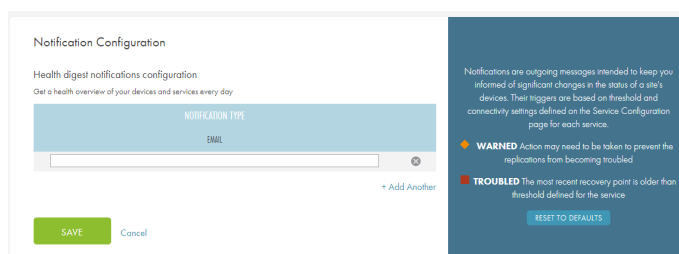
In the *Notifications* section, click the **Edit** button.



### 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.