Axcient

Fusion Web Application User 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

Preface

The *Axcient Web Application User Guide* describes how to monitor the protection solution in an organization through a single Axcient Web Application (Web App).

Intended Audience

This guide is intended for administrators who manage or monitor Axcient services.

Introduction

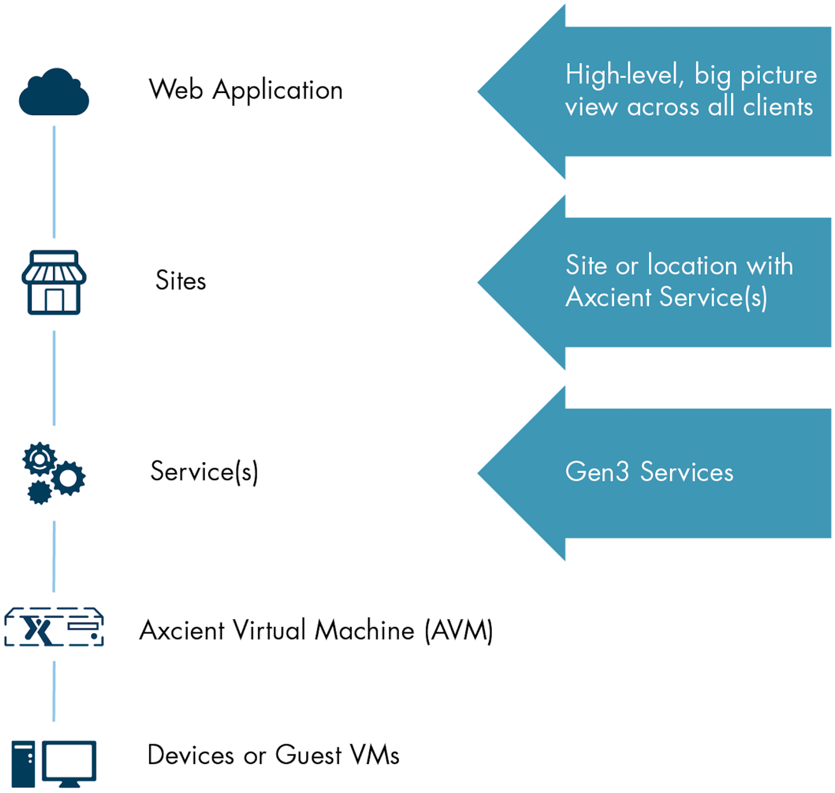
This chapter describes how the Axcient Web Application fits in to the Axcient data protection solution. The Axcient Web Application is a web-based management portal that allows you to manage and monitor all Sites, Services, Axcient Virtual Managers (AVMs), and devices in the organization.

The architecture of the Axcient Web Application is designed to give you the simplest and most expansive view with access to all levels of the Axcient Protection Solution.

As a first step, you should consider the following core components of the Axcient solution:

- **Web Application**—the highest view of the Axcient protection solution hierarchy. You can use the Axcient Web Application to monitor, manage, protect, and perform disaster recover processes.
- **Site(s)**—refers to specific locations or organizations.
- **Service(s)**—refers to the different Axcient services registered to your account.
- **Axcient Virtual Machine (AVM)**—a Virtual Machine deployed on the same ESX has as the target devices.
- **Device(s)**—the machines which are protected by Axcient.

Figure 1 **-** Axcient Terminology


Web Application
High-level, big picture view across all clients
Sites
Site or location with Axcient Service(s)
Service(s)
Gen3 Services
Axcient Virtual Machine (AVM)
Devices or Guest VMs

What is the Axcient Virtual Machine?

The Axcient Virtual Machine (AVM) is a VM that is deployed on the same ESX host as the protected devices. A single AVM can only protect a single ESX host and its VMs. If there are multiple ESX hosts that need to be protected, you must deploy an AVM on each host. A single AVM cannot protect multiple ESX hosts.

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 acts as a middle man between the protected devices and the Axcient Cloud. The AVM relays the replicated data of the protected devices to the Axcient Cloud.

Administration

The Axcient Web Application includes various management and administration screens to help you easily facilitate management of the Axcient protection solution.

The Axcient Web Application includes the following:

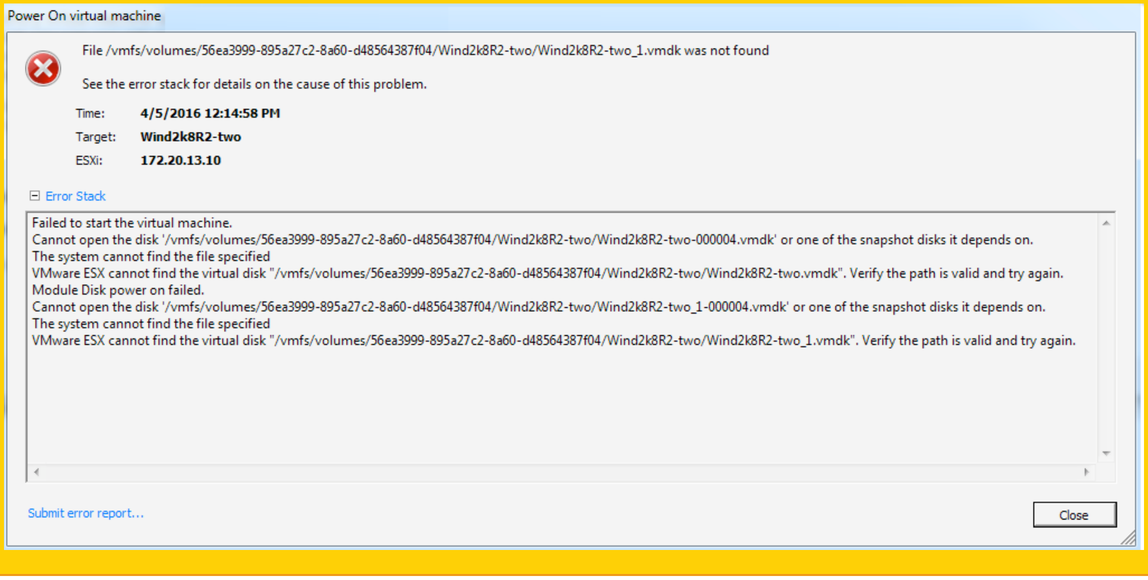
- **Dashboard**—displays summary information across all Sites, including health status information, activities of interest, and other relevant notifications.
- **Services**—displays a summary list view of all registered Services. From this page, you can access the Service Details page of a specific Service where management, recovery, and configuration actions can be taken.
- **Sites**—displays a summary view of all Sites registered to your account. From this page, you can access the Site Details page of a specific Site where management, recovery, and configuration actions can be taken.
- **Events**—provides a view of events across all Sites, Services, and devices. You can view the type of event, a description of the event, and the AVM, device, and time that the event occurred.
- **Users**—lists of all user accounts with access to the Axcient Web Application. The Organization Admin accounts can create, delete, edit, and deactivate accounts as necessary.
- **Reports**—generate configurable reports detailing replication job analysis, hardware usage, network activity, and more.

All Axcient appliances are served and managed by the Axcient Web Application regardless of software version.

CAUTION!

Do not delete an AVM from the ESX host environment while a replication job is in progress. It is possible that one of the client machines' disks may still be attached and this associated disk can be lost. A disk lost in this manner will cause damage that is **not recoverable** to the affected VM(s).

You will see the following ESX error if the AVM has been deleted while a replication job is in progress:



File /vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk was not found

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**

```
Failed to start the virtual machine.
Cannot open the disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two-000004.vmdk' or one of the snapshot disks it depends on.
The system cannot find the file specified
VMware ESX cannot find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two.vmdk". Verify the path is valid and try again.
Module Disk power on failed.
Cannot open the disk '/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1-000004.vmdk' or one of the snapshot disks it depends on.
The system cannot find the file specified
VMware ESX cannot find the virtual disk "/vmfs/volumes/56ea3999-895a27c2-8a60-d48564387f04/Wind2k8R2-two/Wind2k8R2-two_1.vmdk". Verify the path is valid and try again.
```

Web Application Walkthrough

Logging in to the Axcient Web Application

After you register with Axcient, Axcient Support will send an email containing information necessary for you to begin leveraging the Axcient protection solution.

In this email, you will find default login credentials for the Axcient Web Application. If you did not receive this email, please contact [Axcient Support].

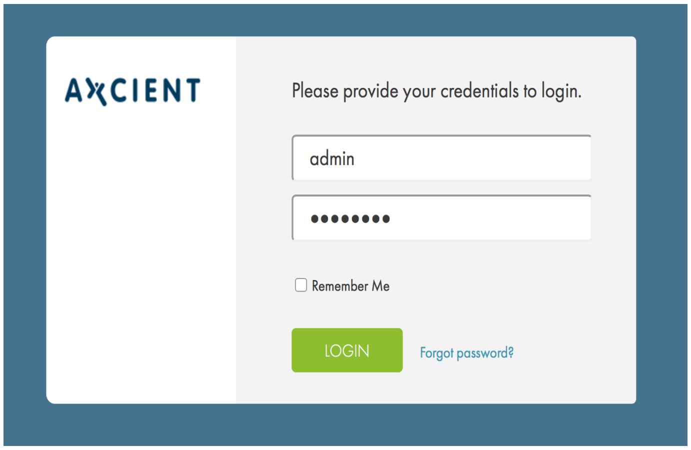
> **Note**: For security reasons, we recommend changing the password for the Web Application.

To change the password:

STEP 1

In your preferred browser, navigate to https://my.axcient.net (US) or https://ca.axcient.net (Canada).

Log in to the Axcient Web Application using the login credentials provided by Axcient Support.



Please provide your credentials to login.

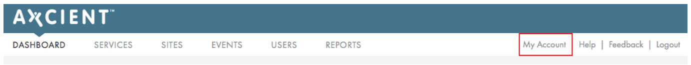
admin

••••••••

STEP 2

On the Axcient Web Application, click the **My Account** link.

Update the password and click the **Save** button.



Web Application Dashboard

The Axcient Web Application Dashboard acts as the landing page in the Axcient Web Application. The *Dashboard* best embodies Axcient’s *Manage by Exception* philosophy.

The *Manage by Exception* philosophy is built around the idea of surfacing alerts, notifications, and activities that require your attention most urgently. You, as the administrator, can therefore identify these issues quickly, ensuring that problems are resolved promptly and devices stay fully protected.

❶Sites Health Status Display

Displays the health status, alerts, notifications, and activities across all Sites and Services are displayed.

❷Browse Sites

Provides access to all provisioned Sites. Click this button to access the *Sites* page

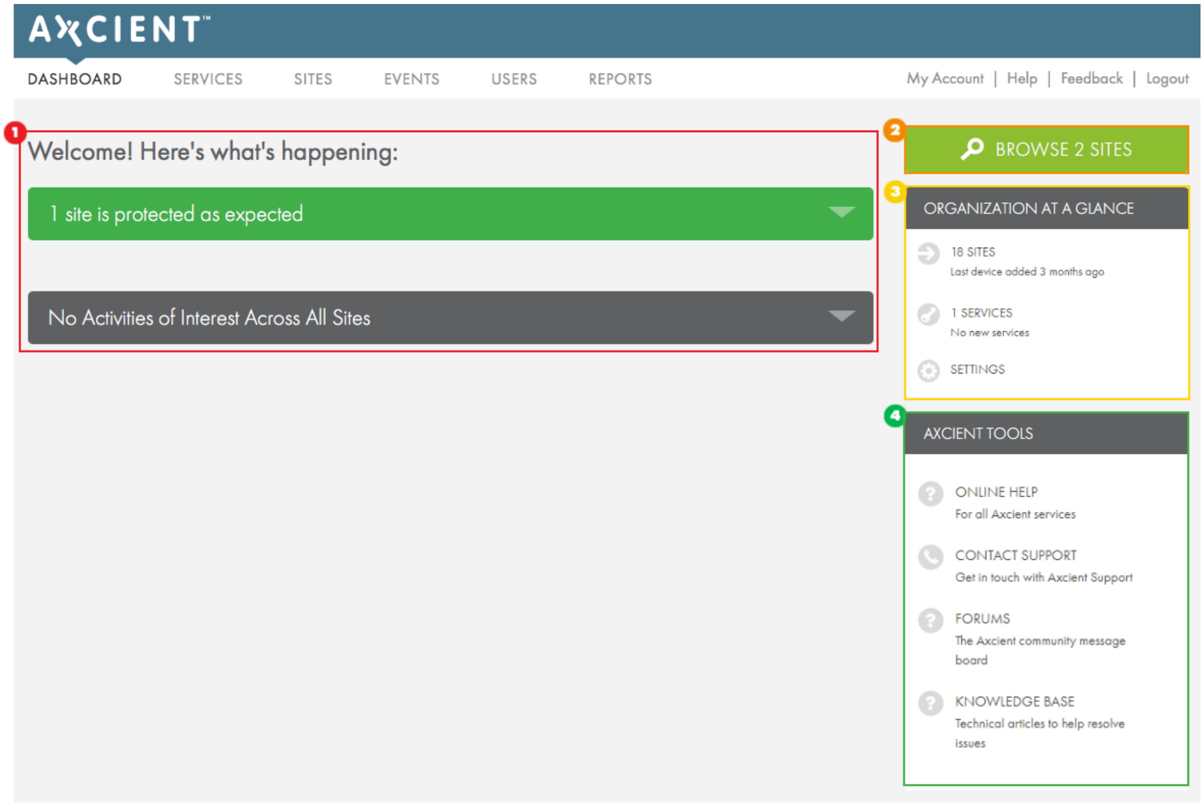
❸Organization at a Glance

A summary view of all Sites and Services registered to your account with direct links to the *Sites, Services*, and *Settings* pages.

❹Axcient Tools

Links to Axcient's online documentation and support pages, as well as a link to the Axcient Support page.

Figure 2 **-** Web Application Dashboard



AXCIENT™
DASHBOARD
SERVICES
SITES
EVENTS
USERS
REPORTS
My Account | Help | Feedback | Logout
1
Welcome! Here's what's happening:
1 site is protected as expected
No Activities of Interest Across All Sites
2
BROWSE 2 SITES
3
ORGANIZATION AT A GLANCE
18 SITES
Last device added 3 months ago
1 SERVICES
No new services
SETTINGS
4
AXCIENT TOOLS
ONLINE HELP
For all Axcient services
CONTACT SUPPORT
Get in touch with Axcient Support
FORUMS
The Axcient community message board
KNOWLEDGE BASE
Technical articles to help resolve issues

Site Health Status Descriptions

- Activities of Interest—the first alert displayed showing important activities across all Sites, Services, AVMs, and devices. All individual activities include direct links to the corresponding activity.
- Requires Attention—the highest positioned health status alert. Also referred to as *Troubled*, these are Sites containing AVMs and devices that have fallen out of the protection threshold as configured in the Protection Policy. The expanded list includes individual entries with direct links to help you resolve the issue.
- Warning—signifies a Site containing AVMs or devices that have lost connectivity for an extended period of time as configured in the Protection Policy. Devices that have completed a Cloud replication job with warnings will be listed here as well. The expanded list includes individual entries with direct links to help you resolve the issue.
- Protected as Expected—these are Sites that are healthy and do not need attention at this time. Expand the alert and click **Browse** to view all the protected Sites.

Services Page

The *Services* page is a list summary of the Axcient services registered to your account. The list view offers at-a-glance information such as health status, tunnel status, and important identifying information.

The *Services* list section of the page, which lists all the Services registered to your account, allows you to view:

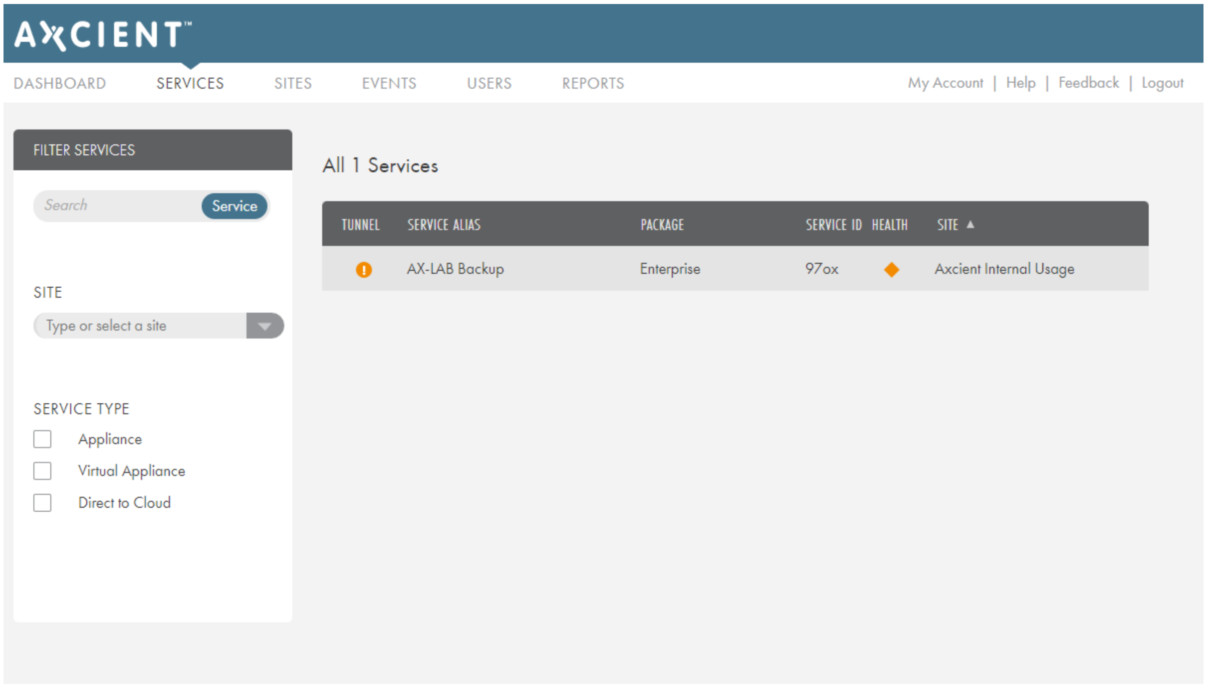
- Tunnel,
- Service Alias,
- Package,
- Service ID,
- Health, and
- Site under which the Service is registered.

On the left-hand side is a search and filter tool to sort through the Services list. The Services list can be sorted by:

- Service search,
- Site search, and
- Service type.

You can click to expand a Service to view more details. You can also click the **View Service** button to access the *Service Details* page.

Figure 3 - Services Page



All 1 Services

TUNNEL	SERVICE ALIAS	PACKAGE	SERVICE ID	HEALTH	SITE ▲
!	AX-LAB Backup	Enterprise	97ox	◆	Axcient Internal Usage

Service Details Page

The *Service Details* page allows you to take protection and recovery actions, view storage summaries, view Service entitlements, and view a hardware description of the appliance.

1 Service Details

Provides general information about the Service, including the Service key and a link to download the AVM agent. You can also take recovery and protection actions by clicking the **Recover** and **Protect** buttons, respectively.

2 AVM List

Lists all AVMs registered under the Service. The list shows the AVM alias, number of devices protected, and last successful Cloud replication. Click an AVM in the list to expand and show a more detailed information about the AVM, including the ESXi and AVM versions, and list of protected devices.

3 Configure Service

Configure the Service. This includes Service Settings, Alerts and Thresholds, Protection Policy Defaults, Bandwidth, Business Hours, and Time Zone.

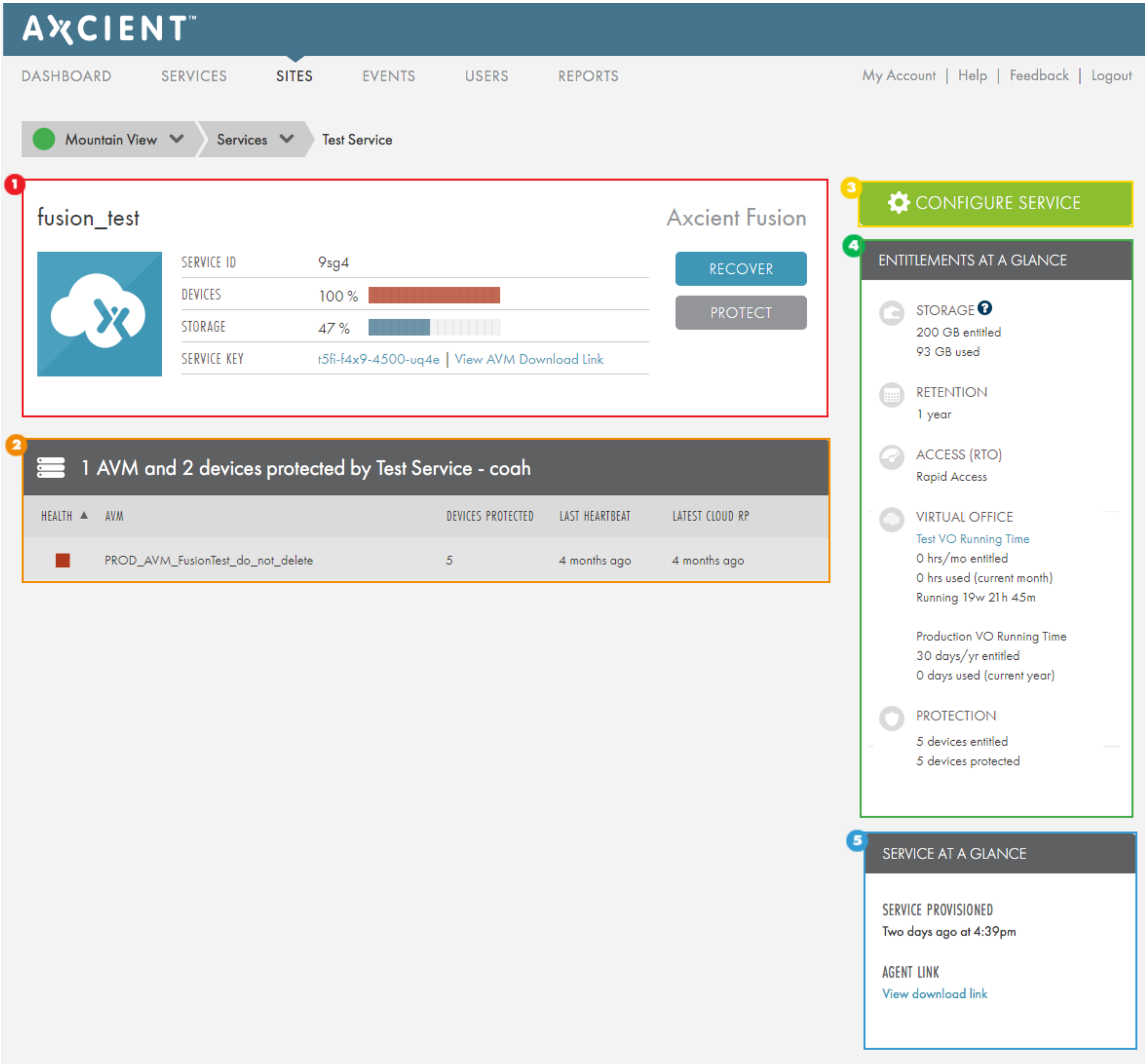
4 Entitlements at a Glance

View the entitlements allotted to the Service. This includes storage, data retention, protection details, and a link to the Virtual Office (when deployed).

5 Service at a Glance

Summary information about the Service, including the date the Service was provisioned, and a link to download the AVM agent.

Figure 4 - Service Details Page



fusion_test

Axcient Fusion

SERVICE ID	9sg4
DEVICES	100 %
STORAGE	47 %
SERVICE KEY	t5fi-f4x9-4500-uq4e | View AVM Download Link

1 AVM and 2 devices protected by Test Service - coah

HEALTH ▲	AVM	DEVICES PROTECTED	LAST HEARTBEAT	LATEST CLOUD RP
🟥	PROD_AVM_FusionTest_do_not_delete	5	4 months ago	4 months ago

ENTITLEMENTS AT A GLANCE

STORAGE
200 GB entitled
93 GB used

RETENTION
1 year

ACCESS (RTO)
Rapid Access

VIRTUAL OFFICE
Test VO Running Time
0 hrs/mo entitled
0 hrs used (current month)
Running 19w 21h 45m

Production VO Running Time
30 days/yr entitled
0 days used (current year)

PROTECTION
5 devices entitled
5 devices protected

SERVICE AT A GLANCE

SERVICE PROVISIONED
Two days ago at 4:39pm

AGENT LINK
View download link

Axcient Virtual Manager Details Page

The Axcient Virtual Manager (AVM) is the VM agent that acts as an intermediary between the protected device and the Axcient Cloud.

The initial AVM configuration occurs during the setup process, and multiple AVM agents can be deployed using this same configuration. However, there might be a scenario where the AVM details may need to be viewed and the configuration changed.

In this case, you will need to navigate to the *AVM Details*:

1 AVM Details

Displays information about the AVM including health status, IP address, Service ID, ESXi host IP address, and ESXI version.

2 AVM Health Status History

Displays the health history of the AVM.

3 Device List

The summary list of devices being protected by the appliance. You can click to expand a device to view details and optionally recover, park, or navigate to the *Device Details* page.

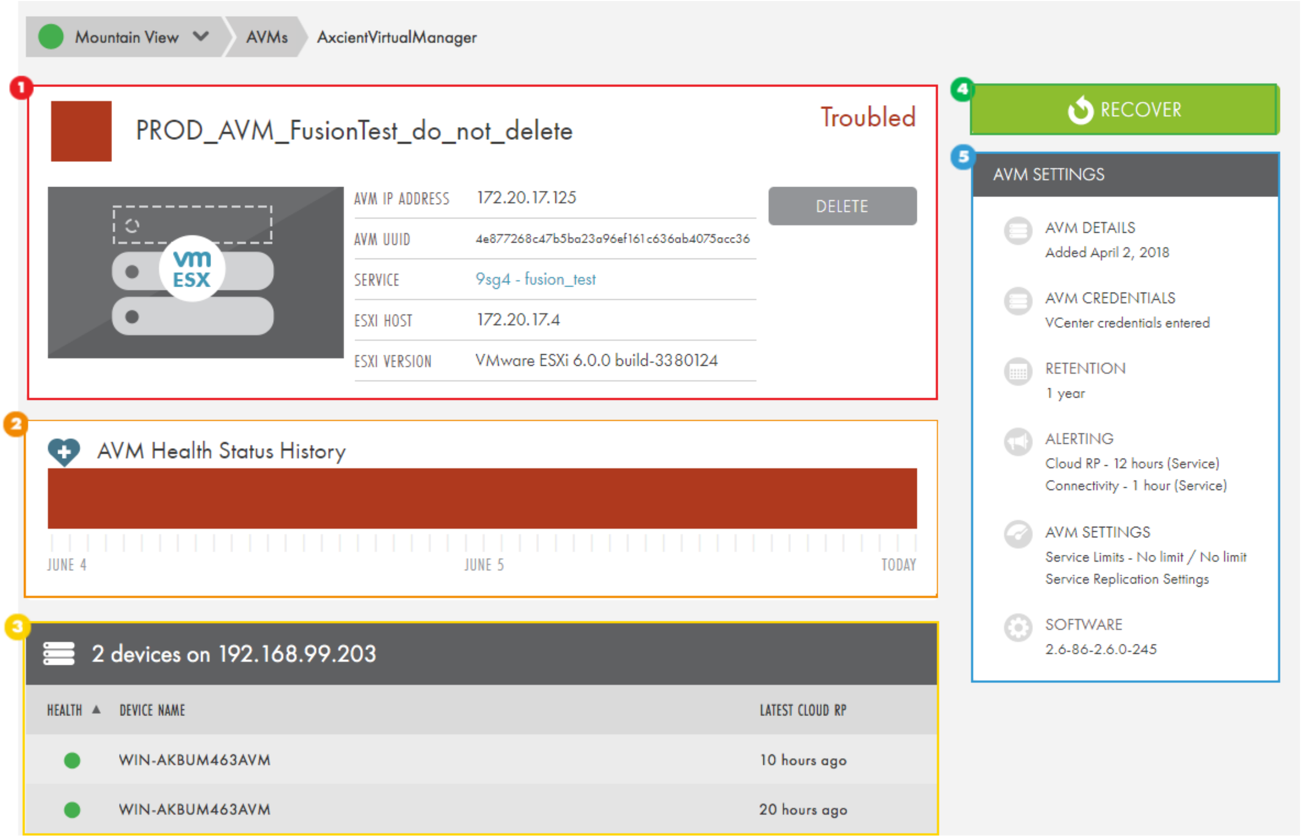
4 Recover

Take recovery actions by clicking the **Recover** button.

5 AVM Settings

Displays the configured AVM settings. You can view AVM details, update AVM credentials, and edit AVM settings.

Figure 5 **-** AVM Details Page



Mountain View › AVMs › AxcientVirtualManager

1

PROD_AVM_FusionTest_do_not_delete

Troubled

AVM IP ADDRESS	172.20.17.125
AVM UUID	4e877268c47b5ba23a96ef161c636ab4075acc36
SERVICE	9sg4 - fusion_test
ESXI HOST	172.20.17.4
ESXI VERSION	VMware ESXi 6.0.0 build-3380124

2

AVM Health Status History

3

2 devices on 192.168.99.203

HEALTH ▲	DEVICE NAME	LATEST CLOUD RP
●	WIN-AKBUM463AVM	10 hours ago
●	WIN-AKBUM463AVM	20 hours ago

4

5

AVM SETTINGS

AVM DETAILS
Added April 2, 2018

AVM CREDENTIALS
VCenter credentials entered

RETENTION
1 year

ALERTING
Cloud RP - 12 hours (Service)
Connectivity - 1 hour (Service)

AVM SETTINGS
Service Limits - No limit / No limit
Service Replication Settings

SOFTWARE
2.6-86-2.6.0-245

Sites Page

The *Sites* page displays all the Sites currently registered to your account. These can be physical locations or companies, based on your needs and preferences. The *Sites* page shows summary information about each Site, including:

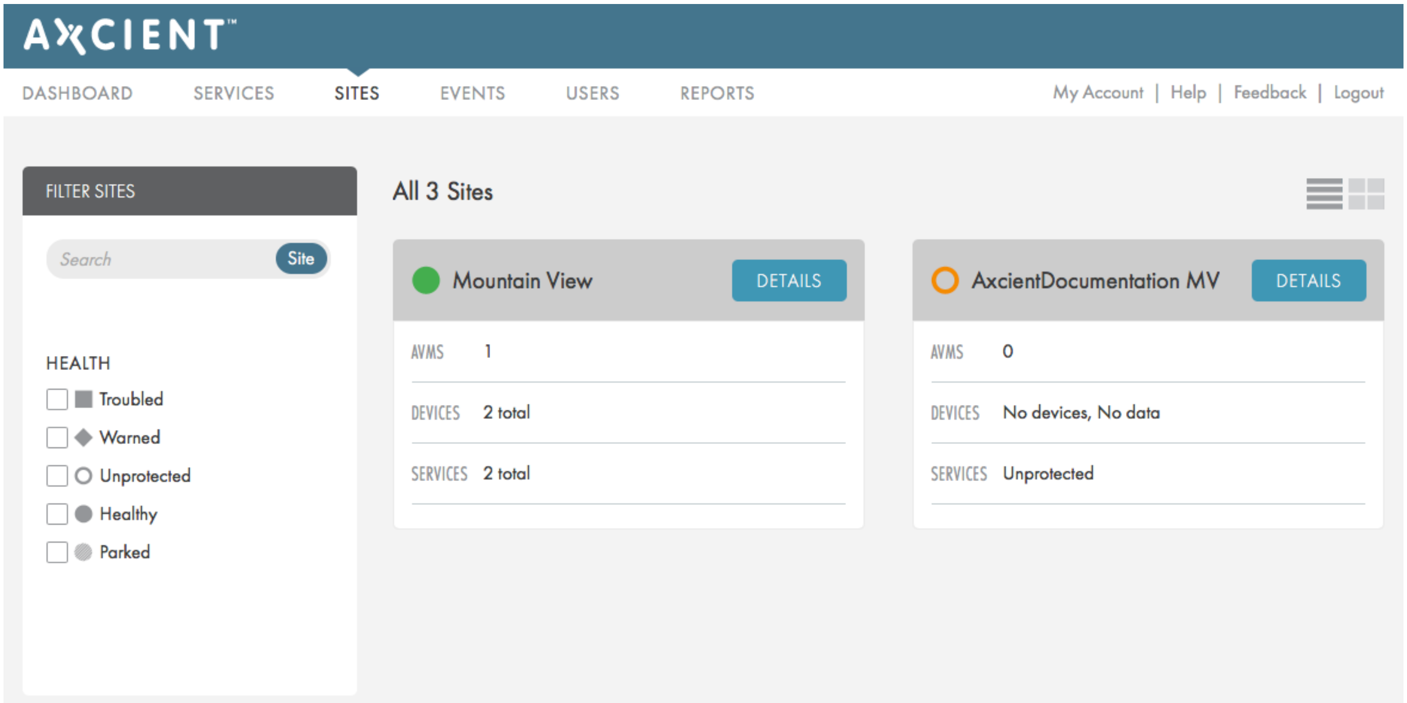
- Health status of the Site. This will reflect the same Health Status displayed in the Web App *Dashboard*.
- Total number of AVMs deployed.
- Total number of devices protected under the Site.
- Total number of Services registered under the Site.

Sites can be filtered by using the Filter tool on the left-hand side of the page. Sites can be filtered based on:

- Site name, and
- Health status.

Click a **Details** button to access the *Site Details* page for the specified Site.

Figure 6 **-** Sites Page



All 3 Sites

● Mountain View

AVMS	1
DEVICES	2 total
SERVICES	2 total

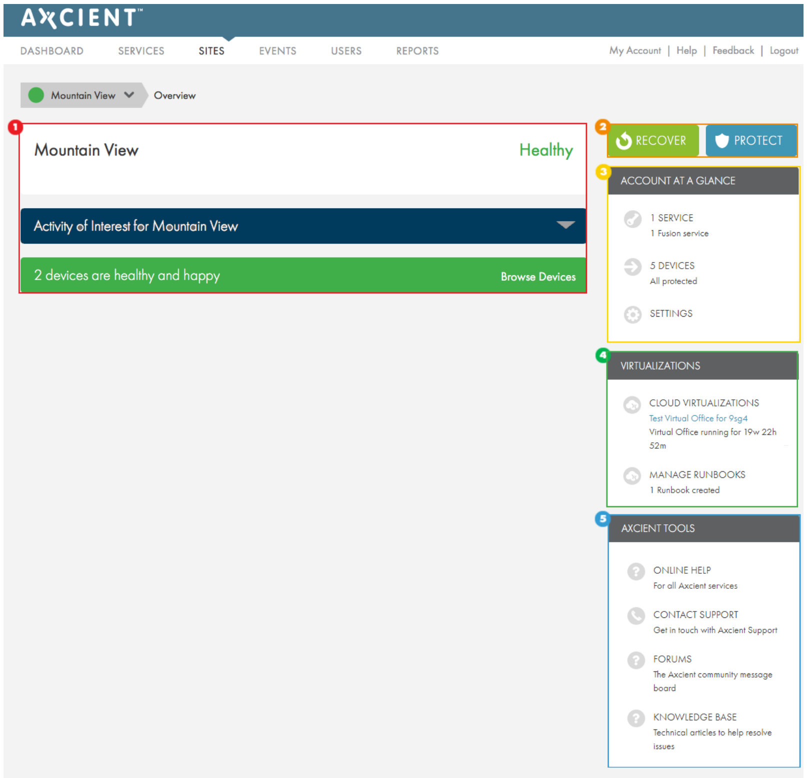
○ AxcientDocumentation MV

AVMS	0
DEVICES	No devices, No data
SERVICES	Unprotected

Site Details Page

The *Site Details* page provides a detailed view of the health status of protected devices, allowing you to recover and protect devices, and helping you view managerial summaries and configurable settings.

***Figure 7* -** Site Details Page



Mountain View

Healthy

Activity of Interest for Mountain View

2 devices are healthy and happy

ACCOUNT AT A GLANCE

1 SERVICE
1 Fusion service

5 DEVICES
All protected

SETTINGS

VIRTUALIZATIONS

CLOUD VIRTUALIZATIONS
Test Virtual Office for 9sg4
Virtual Office running for 19w 22h 52m

MANAGE RUNBOOKS
1 Runbook created

AXCIENT TOOLS

ONLINE HELP
For all Axcient services

CONTACT SUPPORT
Get in touch with Axcient Support

FORUMS
The Axcient community message board

KNOWLEDGE BASE
Technical articles to help resolve issues

❶Device Health Status Display

Where the health status, alerts, notifications and activities across the Site are displayed.

❷Recover and Protect

Protect new devices or recover protected devices by clicking on the appropriate button.

❸Account at a Glance

Click the **Services** button to view registered Services under the Site . Click the **Devices** button to view all devices protected under the Site. Click the **Settings** button configure the Protection Policy.

❹Virtualizations

View all running virtualizations in the Cloud.

5 **Axcient Tools**

Links to online support including links the End-User Documentation page, forums, knowledge base, and methods by which to contact Axcient Support.

Site Health Status Descriptions

- **Activities of Interest**—the first alert displayed, showing important activities across the Site. All individual activities include direct links to the corresponding activity.
- **Requires Attention**—the highest positioned health status alert. Also referred to as *Troubled*, these are devices that have fallen out of protection threshold as configured in the Protection Policy. Devices that have failed Cloud replication will be alerted here as well. The expanded list includes individual entries with direct links to help you resolve the issue.
- **Warning**—signifies a device that has lost connectivity for an extended period of time as configured in the Protection Policy. Additionally, devices that completed a Cloud replication job with warnings will be listed here. The expanded list includes individual entries with direct links to help you resolve the issue.
- **Protected as Expected**—these are devices that are healthy and do not need attention at this time. Expand the alert and click the **Browse Devices** button to view the *Devices* page, which lists all devices protected under the Site.

Devices Page

You can access the *Devices* page by clicking the **Devices** link in any *Site Details* page. This list includes all devices protected under the Site with the ability to recovery devices and protect new devices.

The Device List shows summary information about each device, including:

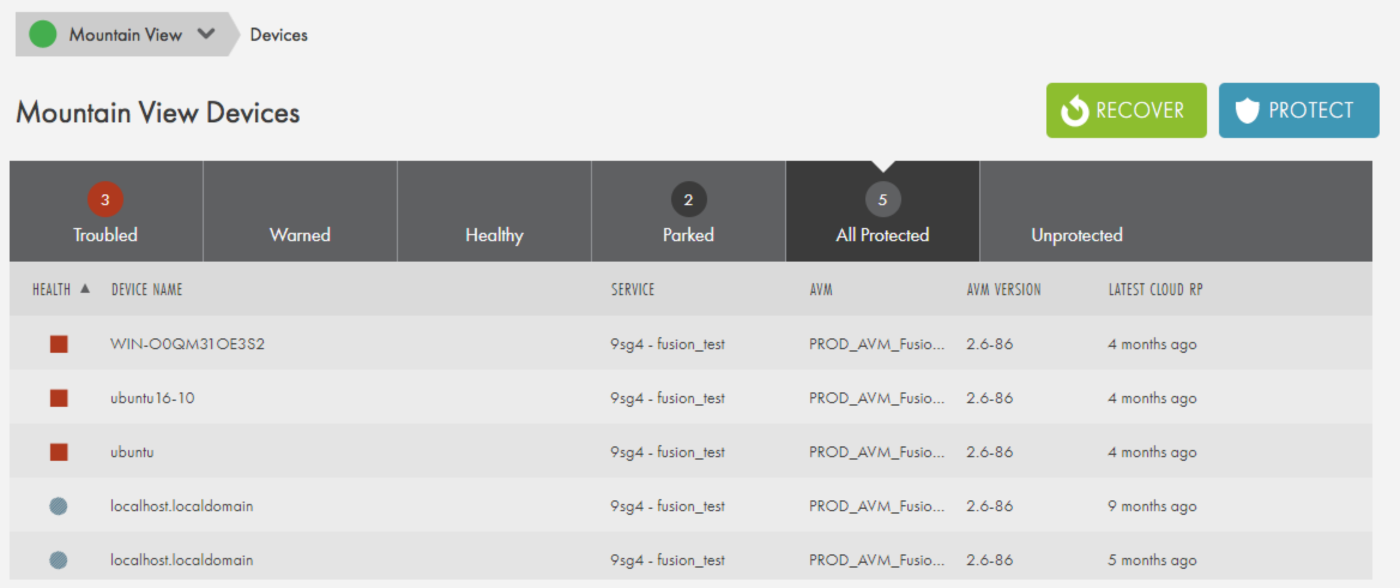
- Health status,
- Device name,
- Service protected under,
- Name of AVM protecting the device,
- AVM version, and
- Last successful Cloud replication.

The *Device List* page provides a view of devices organized by their health status, allowing you to quickly isolate and address devices with issues that need to be resolve. Categories include:

- **Troubled**—devices that are outside of the Protection Policy Threshold for the latest recovery point. This category is signified by a **Red** health status symbol.
- **Warned**—devices that are outside of the Protection Policy Threshold for loss of connectivity, or the most recent cloud replication occurred with errors. This category is signified by an **Orange** health status symbol.
- **Healthy**—devices that are within the Protection Policy Threshold and have no Cloud replication issues. This category is signified by a **Green** health status symbol.
- **Parked**—devices that have been previously protected and are stilled registered by the appliance, but no replication jobs are currently running. These devices are essentially on standby.
- **All Protected**—all devices protected by the Service regardless of health status.
- **Unprotected Devices**—list of devices registered with the appliance but are currently not protected.

Click a device to view the *Device Details* page.

Figure 8 - Device List Page



Mountain View > Devices

Mountain View Devices

Troubled (3)	Warned	Healthy	Parked (2)	All Protected (5)	Unprotected

HEALTH ▲	DEVICE NAME	SERVICE	AVM	AVM VERSION	LATEST CLOUD RP
🟥	WIN-O0QM31OE3S2	9sg4 - fusion_test	PROD_AVM_Fusio...	2.6-86	4 months ago
🟥	ubuntu16-10	9sg4 - fusion_test	PROD_AVM_Fusio...	2.6-86	4 months ago
🟥	ubuntu	9sg4 - fusion_test	PROD_AVM_Fusio...	2.6-86	4 months ago
●	localhost.localdomain	9sg4 - fusion_test	PROD_AVM_Fusio...	2.6-86	9 months ago
●	localhost.localdomain	9sg4 - fusion_test	PROD_AVM_Fusio...	2.6-86	5 months ago

Device Details Page

The *Device Details* page allows you to view a detailed list of the health status and protection summaries of each device. It also provides the ability to recover data and configure custom notifications.

❶Device Details

Information about the device, including current health status, the device type, OS, Service, and the hostname or IP address.

❷Health Status History

Shows the health status history and recent events. Red and Yellow blocks will display if the device experienced health status issues.

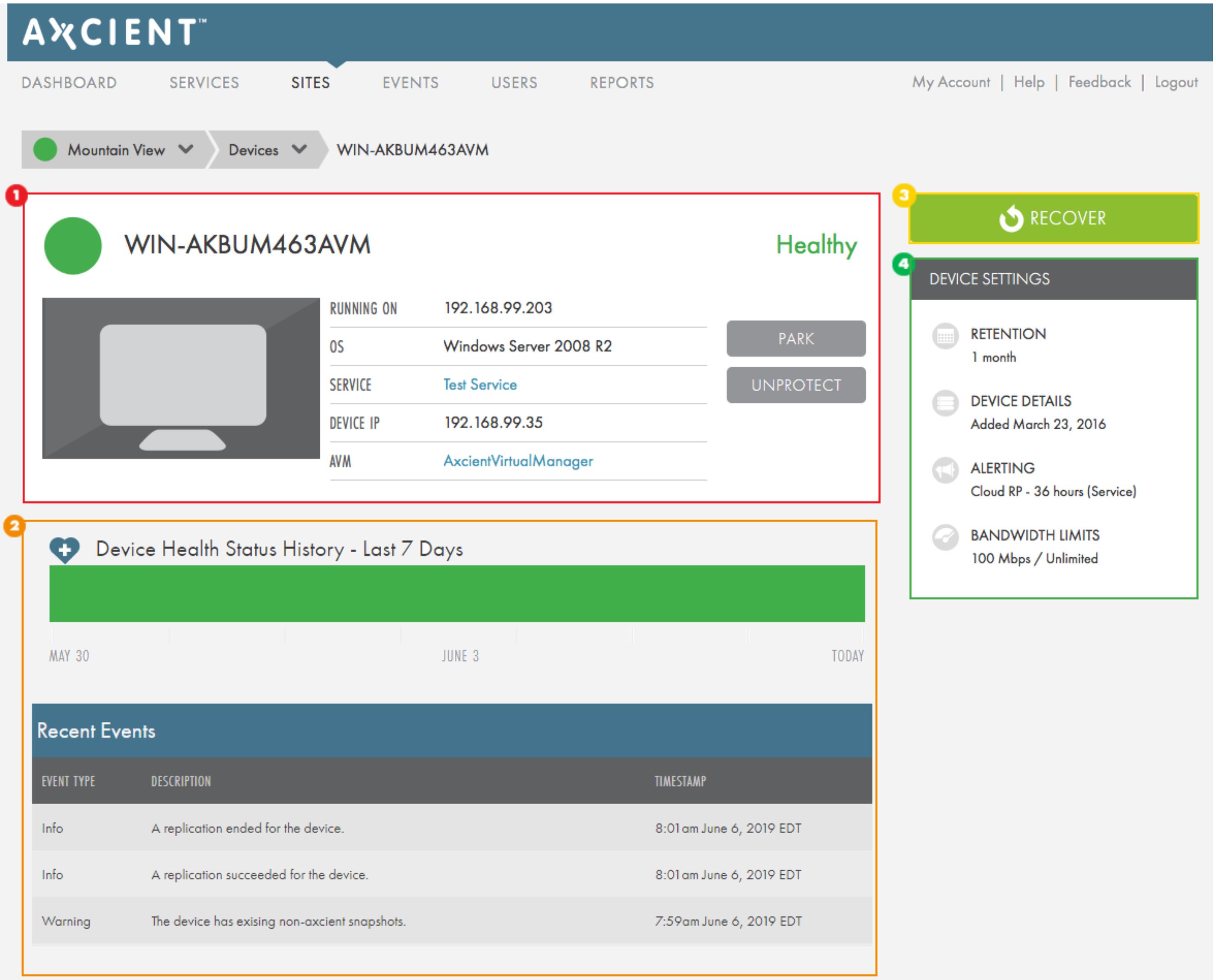
❸Recover and Edit

Click the **Recover** button to perform any recovery actions for the device.

❹Device Settings

View configured device settings. To update device settings, you will need to configure the Service settings in the Service Details page.

Figure 9 - Device Details Page



WIN-AKBUM463AVM Healthy

RUNNING ON	192.168.99.203
OS	Windows Server 2008 R2
SERVICE	Test Service
DEVICE IP	192.168.99.35
AVM	AxcientVirtualManager

DEVICE SETTINGS

RETENTION
1 month

DEVICE DETAILS
Added March 23, 2016

ALERTING
Cloud RP - 36 hours (Service)

BANDWIDTH LIMITS
100 Mbps / Unlimited

Device Health Status History - Last 7 Days

Recent Events

EVENT TYPE	DESCRIPTION	TIMESTAMP
Info	A replication ended for the device.	8:01am June 6, 2019 EDT
Info	A replication succeeded for the device.	8:01am June 6, 2019 EDT
Warning	The device has exising non-axcient snapshots.	7:59am June 6, 2019 EDT

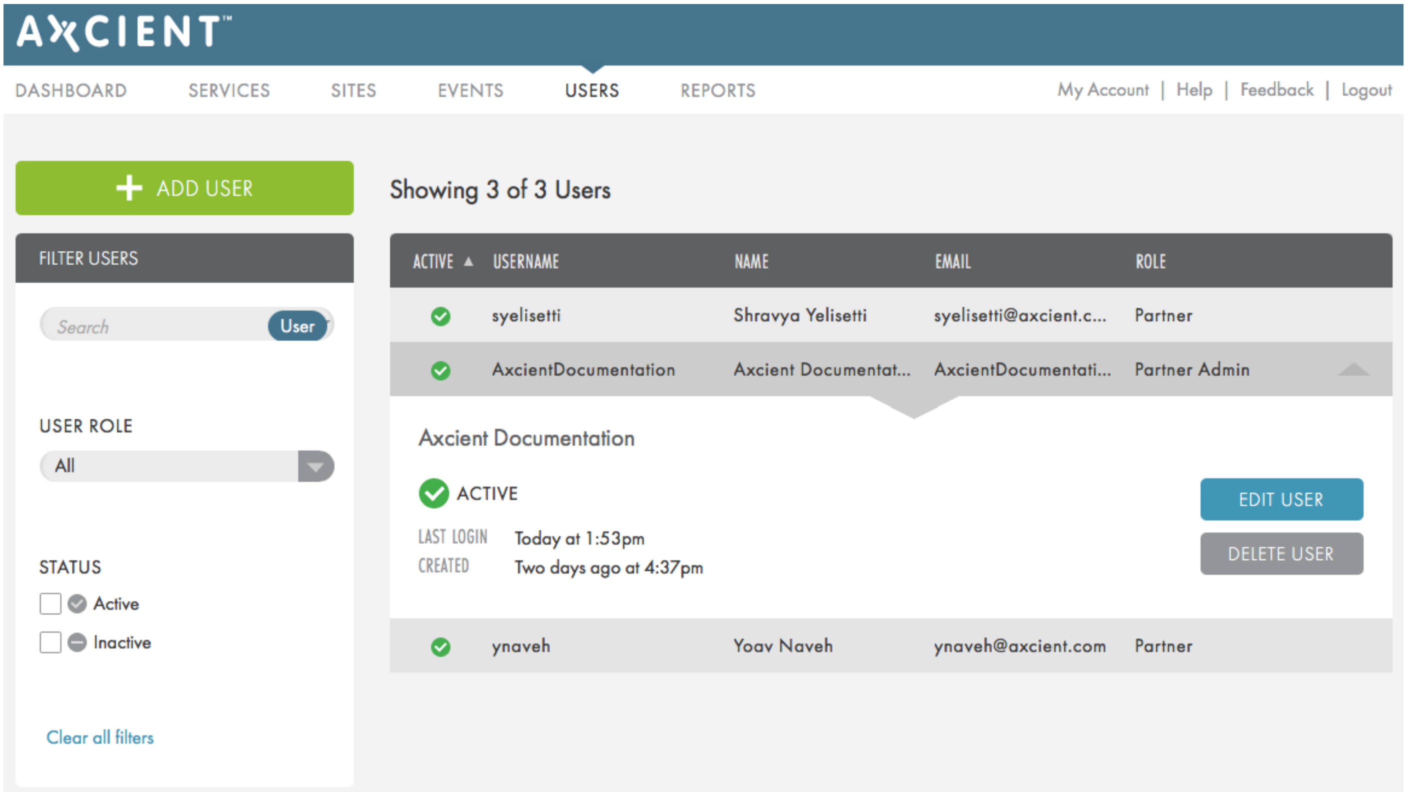
Users Page

You can create multiple users with different authorization levels within the Axcient Web Application. This feature can be useful for large organizations that have many system administrators with varying access needs.

It is important to only give access to trusted and trained colleagues. We recommended that all users go through the Axcient ACE Certification program before being given Organization Admin level access.

New users can be added by clicking the **Add User** button and filling out the required information. Existing user accounts can be edited or deleted at any time.

Figure 10 **-** Users Page



Showing 3 of 3 Users

ACTIVE ▲	USERNAME	NAME	EMAIL	ROLE
✓	syelisetti	Shravya Yelisetti	syelisetti@axcient.c...	Partner
✓	AxcientDocumentation	Axcient Documentat...	AxcientDocumentati...	Partner Admin
✓	ynaveh	Yoav Naveh	ynaveh@axcient.com	Partner

Axcient Documentation

✓ ACTIVE

LAST LOGIN Today at 1:53pm
CREATED Two days ago at 4:37pm

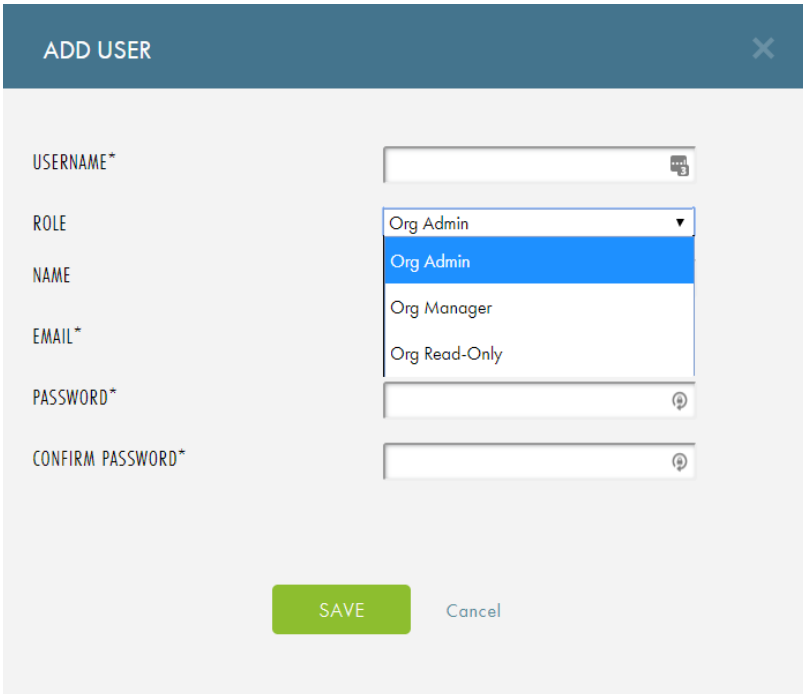
Adding a New Web App User

Organization Admin users are able to create login credentials, allowing full or limited access to the Web Application. After clicking the **Add User** button, new user account information can be entered and the role set. The administrator will need to define:

- A *username* for logging in to the Web Application.
- A *role* that determines what the user can or cannot do within the Web Application.
- A *name* of the User for identification purposes.
- An *email* associated with the account.
- A *password* to be used when logging in to the Web Application.

- An Organization Admin can view and edit Sites, Services, devices, and AVMs, and can add new devices.
- An *Organization Manager* can view and edit existing Sites, Services, devices, and AVMs.
- An *Organization Read-Only* can view existing Sites, Services, devices, and AVMs.

Figure 11 **-** Add Users Screen



ADD USER

USERNAME*

ROLE: Org Admin

NAME

EMAIL*

PASSWORD*

CONFIRM PASSWORD*

Adding a Site-Specific User

You can create Site-specific login credentials so that the user only has access to a certain Site, rather than to the entire Web Application.

This functionality is only available when logged in to the Web Application as a user with Organization Admin privileges.

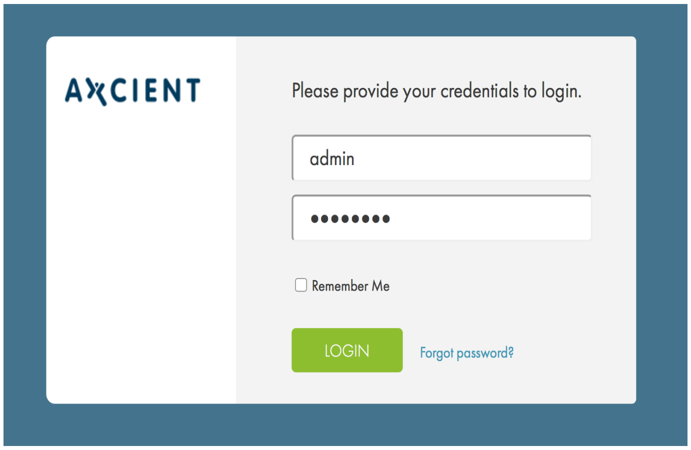
Note

Only one Site-specific login can be created per Site.

To create a Site-specific login:

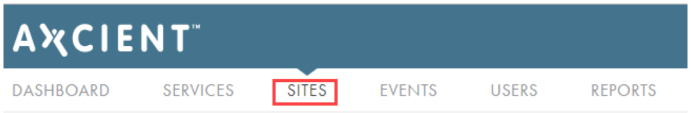
STEP 1

Log in to the Web Application as a user with Organization Admin privileges.



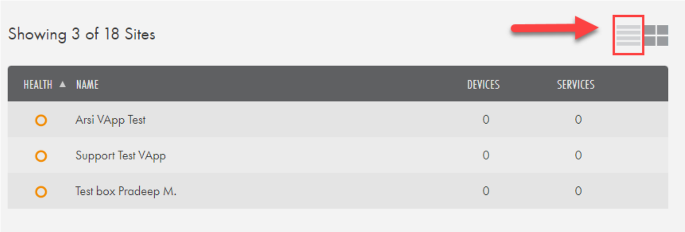
STEP 2

Click the **Site** tab. The *Sites* page displays, listing all Sites registered to your account.



STEP 3

On the *Sites* page, click the **List View** icon, which is depicted with four parallel lines.

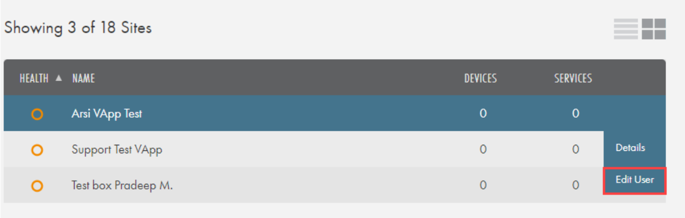


Showing 3 of 18 Sites

HEALTH ▲	NAME	DEVICES	SERVICES
○	Arsi VApp Test	0	0
○	Support Test VApp	0	0
○	Test box Pradeep M.	0	0

STEP 4

Locate the target Site, click the drop-down arrow, and select the **Edit User** Option.



Showing 3 of 18 Sites

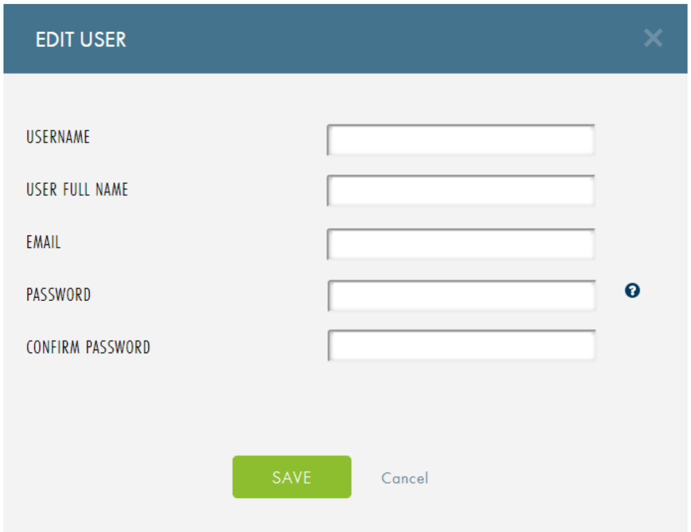
HEALTH ▲	NAME	DEVICES	SERVICES
○	Arsi VApp Test	0	0
○	Support Test VApp	0	0
○	Test box Pradeep M.	0	0

STEP 5

In the *Edit User* pop-up window, enter the appropriate information and click the **Save** button.

The user *will not* receive a confirmation email. Instead, you must manually distribute the login credentials to the new user.

When logged in to the Web App using these credentials, the user will only be able to interactive with the Site to which he has been assigned.



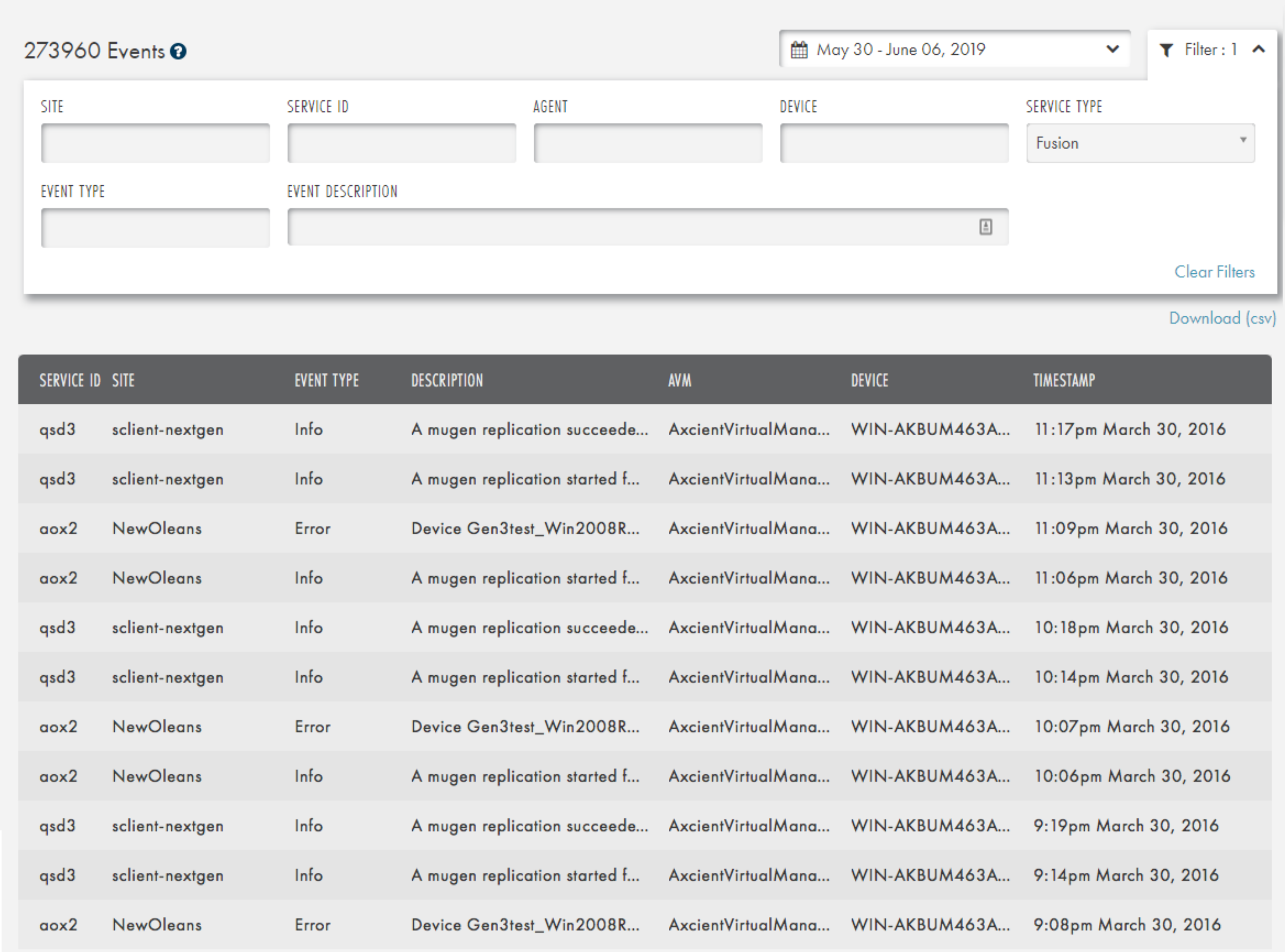
Events Page

The *Events* page lists all events that have occurred across Services registered under your account. Events are recorded chronologically, listing the Site, Service ID, Device, Description, Event Category, and AVM where the specific event occurred. You can click a specific event to read a more detailed description.

You have access to two filter tools:

- **Date Search**—search events based on configurable date ranges. You can select one of the default time frames or use the calender tool to select specific dates.
- **Filter Tool**—search events based on specific event categories. These include:
  - **Site**—select the Site name.
  - **Service ID**—select the Service ID.
  - **Agent**—select the AVM.
  - **Device**—select the device name.
  - **Service Type**—select the type of Service. If there are multiple Service types registered under a Site, they will be listed here.
  - **Event Type**—select the event category.
  - **Event Description**—type a description of the event.

Figure 12 - Events Page



273960 Events

SERVICE TYPE: Fusion

SERVICE ID	SITE	EVENT TYPE	DESCRIPTION	AVM	DEVICE	TIMESTAMP
qsd3	sclient-nextgen	Info	A mugen replication succeede...	AxcientVirtualMana...	WIN-AKBUM463A...	11:17pm March 30, 2016
qsd3	sclient-nextgen	Info	A mugen replication started f...	AxcientVirtualMana...	WIN-AKBUM463A...	11:13pm March 30, 2016
aox2	NewOleans	Error	Device Gen3test_Win2008R...	AxcientVirtualMana...	WIN-AKBUM463A...	11:09pm March 30, 2016
aox2	NewOleans	Info	A mugen replication started f...	AxcientVirtualMana...	WIN-AKBUM463A...	11:06pm March 30, 2016
qsd3	sclient-nextgen	Info	A mugen replication succeede...	AxcientVirtualMana...	WIN-AKBUM463A...	10:18pm March 30, 2016
qsd3	sclient-nextgen	Info	A mugen replication started f...	AxcientVirtualMana...	WIN-AKBUM463A...	10:14pm March 30, 2016
aox2	NewOleans	Error	Device Gen3test_Win2008R...	AxcientVirtualMana...	WIN-AKBUM463A...	10:07pm March 30, 2016
aox2	NewOleans	Info	A mugen replication started f...	AxcientVirtualMana...	WIN-AKBUM463A...	10:06pm March 30, 2016
qsd3	sclient-nextgen	Info	A mugen replication succeede...	AxcientVirtualMana...	WIN-AKBUM463A...	9:19pm March 30, 2016
qsd3	sclient-nextgen	Info	A mugen replication started f...	AxcientVirtualMana...	WIN-AKBUM463A...	9:14pm March 30, 2016
aox2	NewOleans	Error	Device Gen3test_Win2008R...	AxcientVirtualMana...	WIN-AKBUM463A...	9:08pm March 30, 2016

When you click inside a field a drop-down menu displays, providing a list of available inputs. When entering filter rules, the tool will automatically filter available inputs based on the category populated before it.

For example, if you select a Site in the Site field, the Service field will only display Services registered under the indicated Site.

Multiple inputs can be entered in any field.

Reports Page

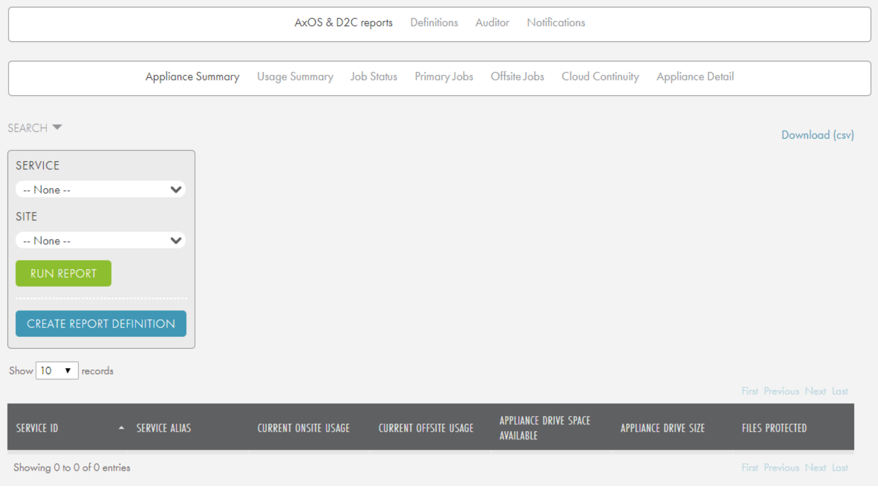
Within the Axcient Web Application, you can generate reports detailing replication job analysis, hardware usage, network activity, and more.

Axcient offers the following reports:

- The *Virtual Office* report displays all Virtual Offices that have run between the specified start and end dates.
- The *VO Devices* report lists all devices virtualized in a Virtual Device for the specified Site within the given date range.
- The *Sites* report summarizes information about the specified Site. You can only select one Site per report.
- The *Services* report allows you to view the details of a specific Service.
- The *Health Status Summary* report queries all devices protected under the designated Site, and creates a report summarizing the total health statuses of the devices. This report presents the health status summary of the devices at the time the report is run and does not present health status summary data over a period of time.
- The *AVM* report lists information about all AVMs deployed under the specified Axcient Fusion service. This report lists high-level descriptive information about the AVM, including the Site and Service under which is it protected, version, build number, and other important protection information.
- The *Devices* report lists devices under the selected Site and Service. You can use this report to view data about each device.
- The *Replication* report allows you to view the replication status for the Site.
- The *Definitions* page summarizes a list of predefined configurations or parameters.
- The *Auditor* report summarizes activities based on action taken, time, entity, and user.
- The *Notifications* page provides details on each notification generated in the system, including name, type, start timestamp, end timestamp, and status.

All reports can be downloaded as CSV files.

Figure 13 - Reports Page



SERVICE: -- None --

SITE: -- None --

Show 10 records

SERVICE ID	SERVICE ALIAS	CURRENT ONSITE USAGE	CURRENT OFFSITE USAGE	APPLIANCE DRIVE SPACE AVAILABLE	APPLIANCE DRIVE SIZE	FILES PROTECTED

Showing 0 to 0 of 0 entries

Report Definitions

You can create and save specific report definitions, or parameters, about appliance use and backup history. Report definitions eliminate the need for you to configure the same report multiple times.

Report definitions are unique to each user.

1. When a report definition is configured, click the **Create Report Definition** button. The *Create Report Definition* screen displays.

2. Update the following configurations and click the **Save** button when finished:
   - In the *Name* field, enter a **name** for the report definition.
   - In the *Delivery Type* drop-down menu, select the **frequency** the report is delivered. You can choose from *daily*, *weekly*, or *monthly*.
   - Select the **Active** checkbox to activate the report. When this box is checked, the report is automatically delivered based on the *Delivery Type* selected. If this box is left blank, the report definition will be saved but will not be delivered automatically.
   - In the *Email Address* field, enter one or more **email addresses** where the report will be delivered. Separate each individual email address with a comma. By default, this field is pre-populated with the email address associated with your account.
3. Optionally, click the **Definitions** button to view all created report definitions. In this screen, you can view the following information about each definition:
   - Name
   - Type
   - Delivery Type
   - Active Status
4. Optionally, using the *Actions* column, you can expand a drown down menu to **Edit**, **Delete** or **View** the specific report definition.

Recipient Email Address

Each active report definition will be automatically delivered to the email address(es) defined in the *Email Address* field. By default, the *Email Address* field is automatically pre-populated with the email address associated with your account, although you can edit and update this field as necessary.

You can optionally view or update the email address associated with your account. To view or update your email address:

1. Click the **My Account** button on the top right of the Web Application. The *My Account* page displays.
2. Review the *Email* field. The email address displayed in this field will serve as the default email address for automatically delivered reports.

Cloud Failover (Virtual Office)

In the event one or more protected devices fails, the Cloud Failover feature in the Web Application allows you to start virtual machines (VMs) in the Axcient Cloud for one or more protected devices. The Axcient Cloud failover solution allows you to:

- Create a Virtual Office running in the Axcient data center that matches existing server configurations.
- Configure the network settings for the Virtual Office, including:
  - Provide secure access to the Virtual Office by configuring the VPN.
  - Configure multiple subnets for the Virtual Office.
  - Configure Site to Site VPN settings, allowing multiple remote networks to connect to the Virtual Office.
  - Allow VMs to access the Internet by enabling outbound internet connections, or keep them isolated for development and testing purposes.
  - Configure remote desktop for the Virtual Office.
  - Establish Port Forwarding rules.
- Configure the restore point, vCPU cores, and vRAM for each device in the Virtual Office.
- Create Runbooks (Automated Orchestration) to automatically fail over or start large numbers of VMs in the Virtual Office.

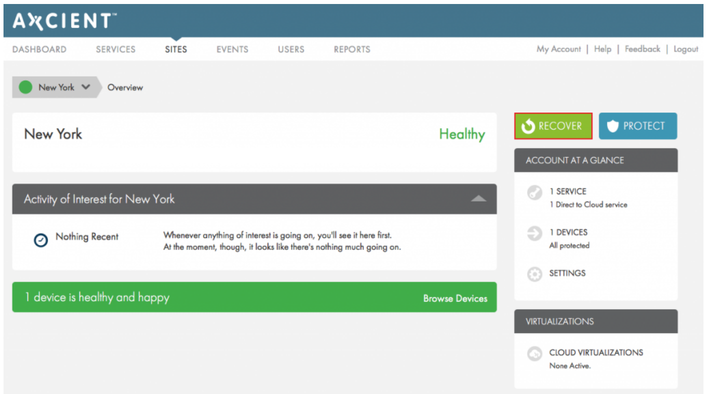
This section of the guide will cover how to deploy and configure the Virtual Office, as well as how to prepare, start, access, and shut down the devices.

Start the Virtual Office

To start the Virtual Office:

STEP 1

From the *Site Details* page, click the **Recover** button.



New York Healthy

Activity of Interest for New York

Nothing Recent — Whenever anything of interest is going on, you'll see it here first. At the moment, though, it looks like there's nothing much going on.

1 device is healthy and happy

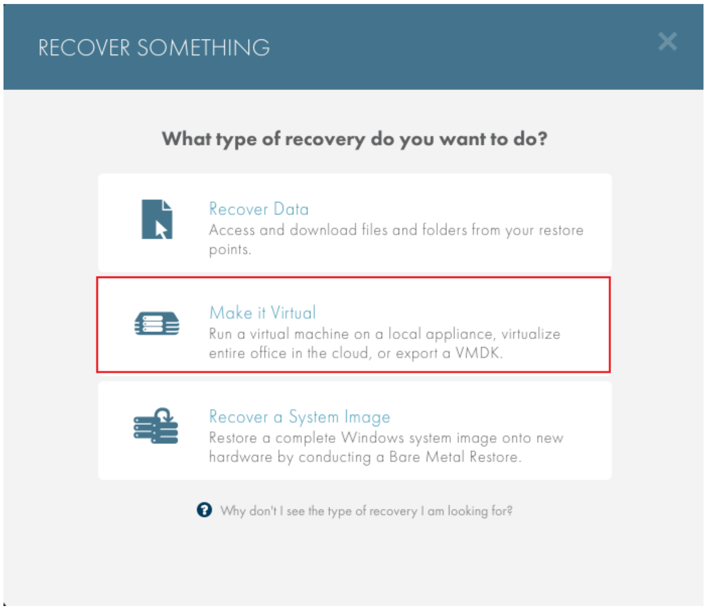
1 SERVICE
1 Direct to Cloud service

1 DEVICES
All protected

CLOUD VIRTUALIZATIONS
None Active.

STEP 2

On the *Recover Something* screen, click the **Make it Virtual** option, and then select the **Start a Virtual Office in the Cloud** option.



What type of recovery do you want to do?

Recover Data
Access and download files and folders from your restore points.

Make it Virtual
Run a virtual machine on a local appliance, virtualize entire office in the cloud, or export a VMDK.

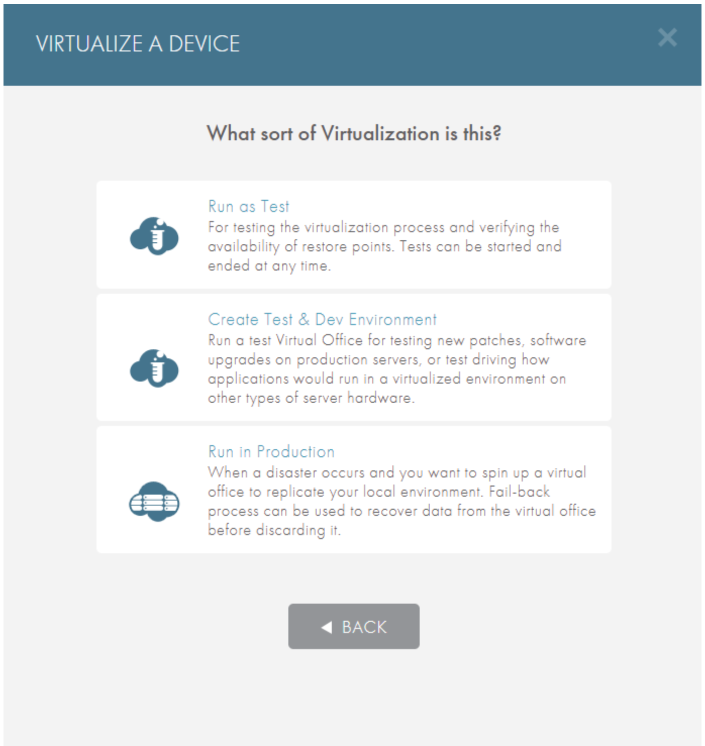
Recover a System Image
Restore a complete Windows system image onto new hardware by conducting a Bare Metal Restore.

Why don't I see the type of recovery I am looking for?

STEP 3

Select the type of local virtualization to deploy:

- Select the **Run as Test** option to test the virtualization process and verify the availability of recovery points in case of an emergency.
- Select the **Test & Dev Environment** option to test new patches, software upgrades on production servers, or test drive how applications would run in a virtualized environment.
- Select the **Put it in Production** option in the event of a disaster. This local failover VM can be used to temporarily replace production devices until a permanent replacement is ready.


VIRTUALIZE A DEVICE

What sort of Virtualization is this?

Run as Test
For testing the virtualization process and verifying the availability of restore points. Tests can be started and ended at any time.

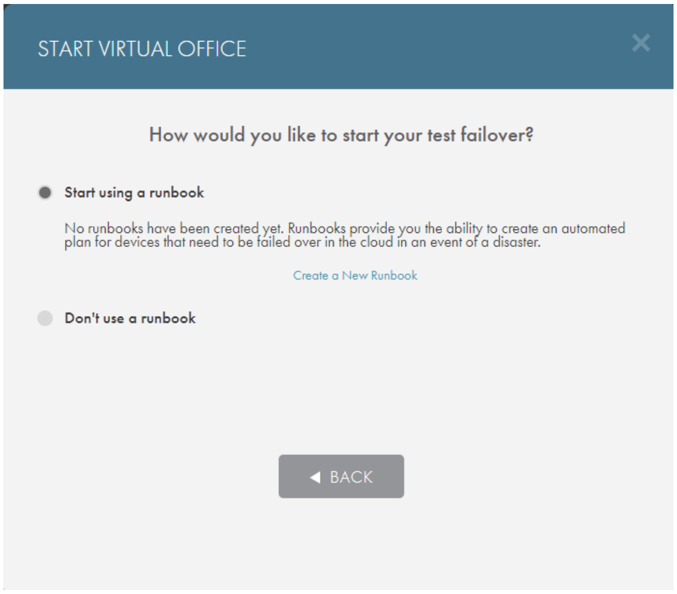
Create Test & Dev Environment
Run a test Virtual Office for testing new patches, software upgrades on production servers, or test driving how applications would run in a virtualized environment on other types of server hardware.

Run in Production
When a disaster occurs and you want to spin up a virtual office to replicate your local environment. Fail-back process can be used to recover data from the virtual office before discarding it.

STEP 4

Select whether you want to start the Virtual Office using a Runbook. Runbooks enable orchestration and automation in Axcient Fusion, letting you configure an automatic deployment plan for virtualized devices in the Virtual Office.

- Click the **Start using a runbook** radio button to use a runbook, and then select your preferred runbook. If a runbook does not yet exist, click the **Create a New Runbook** link to create a new runbook.
- Alternatively, click the **Don't use a runbook** radio button if you prefer to configure settings manually.


START VIRTUAL OFFICE

How would you like to start your test failover?

● Start using a runbook

No runbooks have been created yet. Runbooks provide you the ability to create an automated plan for devices that need to be failed over in the cloud in an event of a disaster.

Create a New Runbook

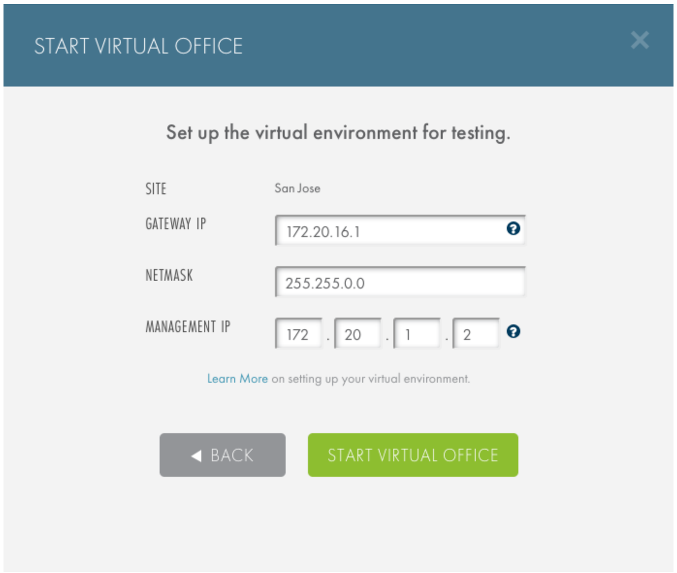
○ Don't use a runbook

STEP 5

Select the services you would like to fail over and configure the primary Virtual Office network settings:

- In the *Gateway IP* field, configure the **gateway IP** of the Virtual Office. This IP address must be on the same network as the devices that will be virtualized in the Virtual Office.
- In the *Netmask* field, configure the **netmask** of the Virtual Office. At most this is a 16-bit netmask.
- In the *Management IP* field, configure the **management IP** of the Virtual Office. This IP address cannot be on the same network as the gateway IP or any subnets created in the Virtual Office. For example, if the Management IP address is 172.20.1.2, the gateway IP or the subnet configured in the Virtual Office cannot be on the 172.10.1.X network.

Click the **Start Virtual Office** button when finished.



START VIRTUAL OFFICE

Set up the virtual environment for testing.

SITE San Jose

GATEWAY IP 172.20.16.1

NETMASK 255.255.0.0

MANAGEMENT IP 172 . 20 . 1 . 2

Learn More on setting up your virtual environment.

Warning!

The primary Virtual Office network settings cannot be changed once they have been configured during the initial deployment process. If the network settings of the Virtual Office need to be changed, the original Virtual Office must be discarded, and a new Virtual Office must be deployed. You cannot deploy two Virtual Offices at one time.

Warning!

The management IP address cannot be the same as the **subnets** in the Virtual Office. If multiple subnets will be created in the Virtual Office, make note of the Management IP address to ensure that a duplicated subnet is not created.

Virtual Office Page

The *Virtual Office* page is accessible when a Virtual Office has been started. The *Virtual Office* page is the administrative page for the Virtual Office, where you can take various managerial actions.

The *Virtual Office* page includes the following sections:

1 Virtual Office Summary

This section displays the summary of the Virtual Office, showing which Sites are being virtualized and the type of virtualization (test or production).

Additionally, you can stop all running VMs or take steps to discard the Virtual Office.

2 Device List

This section displays all protected devices under the selected Service. The device states are explained in the section below.

3 Configure Office

This button launches the *Virtual Office Configuration* page where you can configure various aspects of the Virtual Office.

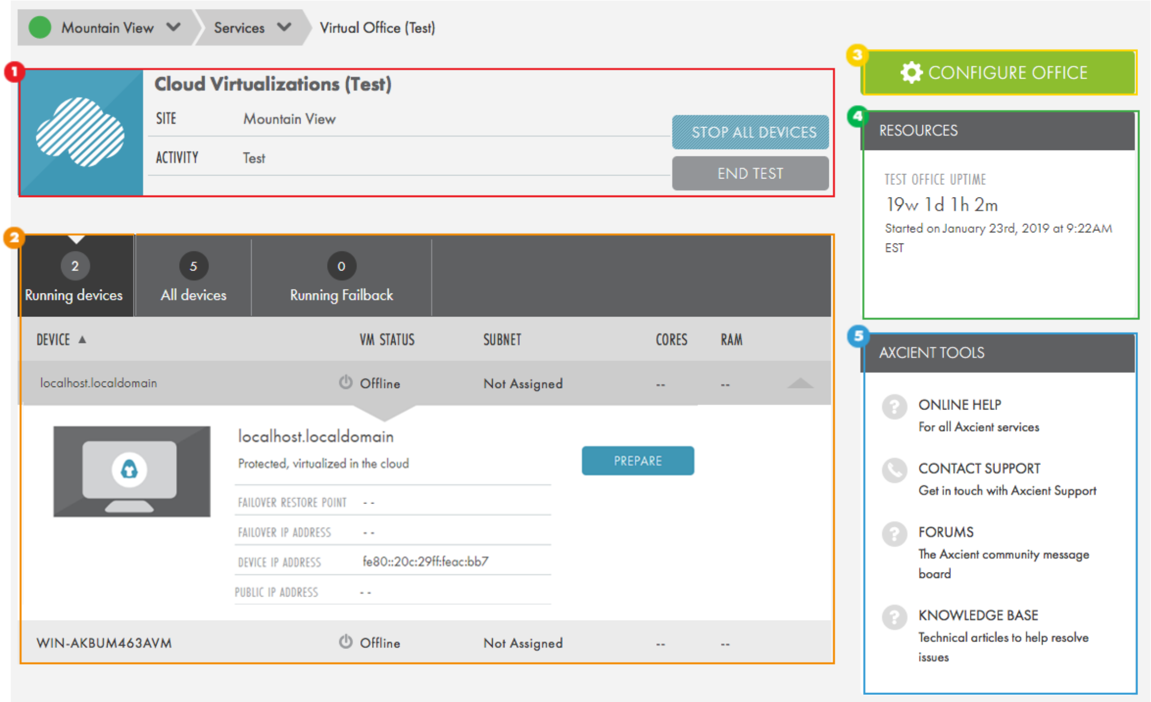
4 Resources

This section displays information on how long the Virtual Office has been running.

5 Axcient Tools

This section provides links to the Axcient support documentation and Axcient Technical Support.

Figure 14 - Virtual Office Page



Cloud Virtualizations (Test)

SITE Mountain View

ACTIVITY Test

DEVICE ▲	VM STATUS	SUBNET	CORES	RAM
localhost.localdomain	Offline	Not Assigned	--	--
WIN-AKBUM463AVM	Offline	Not Assigned	--	--

localhost.localdomain

Protected, virtualized in the cloud

FAILOVER RESTORE POINT	- -
FAILOVER IP ADDRESS	- -
DEVICE IP ADDRESS	fe80::20c:29ff:feac:bb7
PUBLIC IP ADDRESS	- -

TEST OFFICE UPTIME

19w 1d 1h 2m

Started on January 23rd, 2019 at 9:22AM EST

ONLINE HELP
For all Axcient services

CONTACT SUPPORT
Get in touch with Axcient Support

FORUMS
The Axcient community message board

KNOWLEDGE BASE
Technical articles to help resolve issues

Virtual Machine States

A VM will be listed in one of the following states:

- **Offline**—VMs that have yet to be rendered. To render a device, click the **Prepare** button.
- **Preparing**—VMs that are currently being prepared. The Virtual Office is rendering them and allocating virtual resources for the VM.
- **Prepared**—VMs that have been prepared, but are not yet running. This means that you have allocated CPU cores and RAM to the VM. To start a device and make it accessible, click the **Start** button.
- **Starting**—VMs that are in the process of starting after clicking the **Start** button.
- **Running**—live VMs that are accessible through an RDP agent. Click the **Stop** button to return the device to a *Ready* state, or click the **Discard** button to return to the device to an *Offline* state.
- **Stopping**—VMs that are shutting down after clicking the **Stop** button. These devices will revert back to the *Prepared* state.
- **Terminated**—VMs that have been shut down.

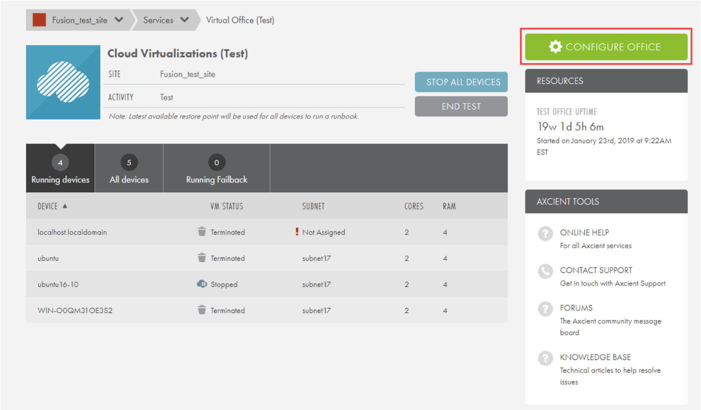
Configure Virtual Office

While inside the Virtual Office, you can configure the cloud failover environment as needed.

To access and configure these options:

STEP 1

On the *Virtual Office* page, click the **Configure Office** button.



Cloud Virtualizations (Test)

SITE Fusion_test_site

ACTIVITY Test

Note: Latest available restore point will be used for all devices to run a runbook.

DEVICE ▲	VM STATUS	SUBNET	CORES	RAM
localhost.localdomain	Terminated	! Not Assigned	2	4
ubuntu	Terminated	subnet17	2	4
ubuntu16-10	Stopped	subnet17	2	4
WIN-O0QM31OE3S2	Terminated	subnet17	2	4

TEST OFFICE UPTIME

19w 1d 5h 6m

Started on January 23rd, 2019 at 9:22AM EST

ONLINE HELP
For all Axcient services

CONTACT SUPPORT
Get in touch with Axcient Support

FORUMS
The Axcient community message board

KNOWLEDGE BASE
Technical articles to help resolve issues

Network Settings

The *Network* section allows you to configure subnets under the primary Virtual Office network.

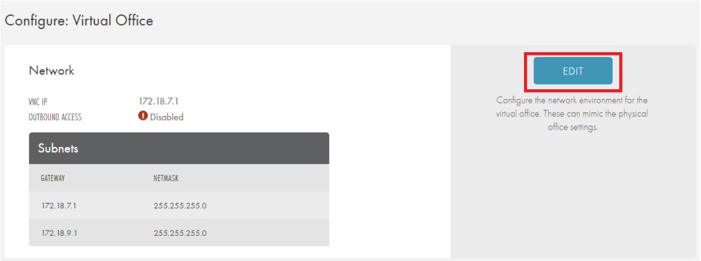
You must configure **at least one subnet** in the Virtual Office. This will be required when preparing a device.

If the original environment has multiple subnets, you can emulate this configuration in the Virtual Office. The *Network* settings section allows you to create multiple subnets in order to replicate the original environment.

To edit the network settings:

STEP 1

On the *Configure: Virtual Office* page, click the **Edit** button in the *Network* section.



Configure: Virtual Office

Network

VNC IP 172.18.7.1

OUTBOUND ACCESS ! Disabled

GATEWAY	NETMASK
172.18.7.1	255.255.255.0
172.18.9.1	255.255.255.0

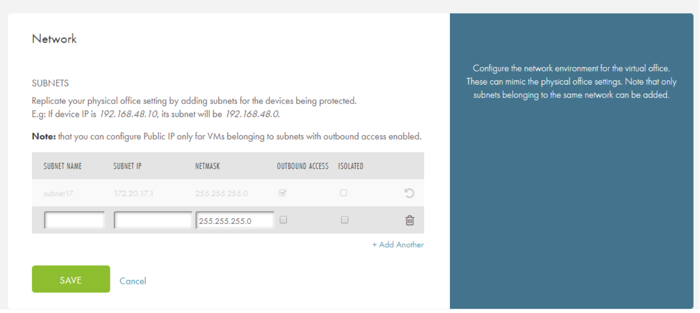
Configure the network environment for the virtual office. These can mimic the physical office settings.

STEP 2

On the *Network* screen, enter a value for one or more of the following fields:

- **Subnet Name**—enter the name for the subnet.
- **IP Address**—enter the IP address for the subnet.
- **Netmask**—enter the netmask for the subnet.
- **Outbound Access**—check this box to allow the subnet outbound access. This is not recommended for a Test Virtual Office.
- **Isolated**—check this box to isolate the subnet from all other subnets in the Virtual Office. This is recommended for a Test Virtual Office, or when performing a test or developmental work in a Production Virtual Office.
- Click the **Add Another** link to add multiple subnets.

Click the **Save** button to save any new configurations.



Network

SUBNETS

Replicate your physical office setting by adding subnets for the devices being protected.
E.g: If device IP is *192.168.48.10*, its subnet will be *192.168.48.0*.

Note: that you can configure Public IP only for VMs belonging to subnets with outbound access enabled.

SUBNET NAME	SUBNET IP	NETMASK	OUTBOUND ACCESS	ISOLATED	
subnet17	172.20.17.1	255.255.255.0	☑	□	
		255.255.255.0	□	□	

Configure the network environment for the virtual office. These can mimic the physical office settings. Note that only subnets belonging to the same network can be added.

Configuring Active Directory Certificate Services Settings

When configuring VPN connection settings, you can optionally integrate with Active Directory for authentication purposes. This option requires that you select a connection type, including *Unencrypted*, *LDAPS* (LDAP over SSL/TLS), or *Start TLS*. *LDAPS* and *Start TLS* connection types both require that you set up the *Active Directory Certificate Services* role on the domain controller.

Please note that *LDAPS* (LDAP over SSL/TLS) is automatically enabled when you install an Enterprise Root CA on a domain controller.

To set up the *Active Directory Certificate Services* role on the domain controller:

For alternative instructions, please reference the LDAP over SSL (LDAPS) Certificate Microsoft TechNet article.

Virtual Private Network (VPN)

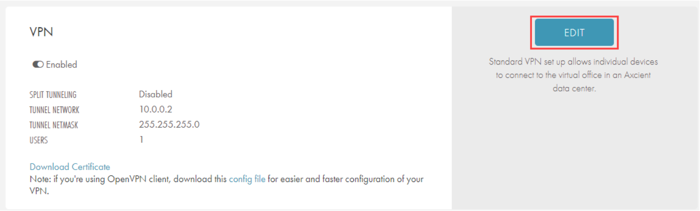
You can configure a VPN to create a secure connection over the public Internet so that outside devices can connect.

You can configure the network settings for the VPN, as well as configure specific user logins.

To edit VPN settings:

STEP 1

On the *Configure: Virtual Office* page, click the **Edit** button in the *VPN* section.



VPN

Enabled

SPLIT TUNNELING Disabled
TUNNEL NETWORK 10.0.0.2
TUNNEL NETMASK 255.255.255.0
USERS 1

Download Certificate
Note: if you're using OpenVPN client, download this config file for easier and faster configuration of your VPN.

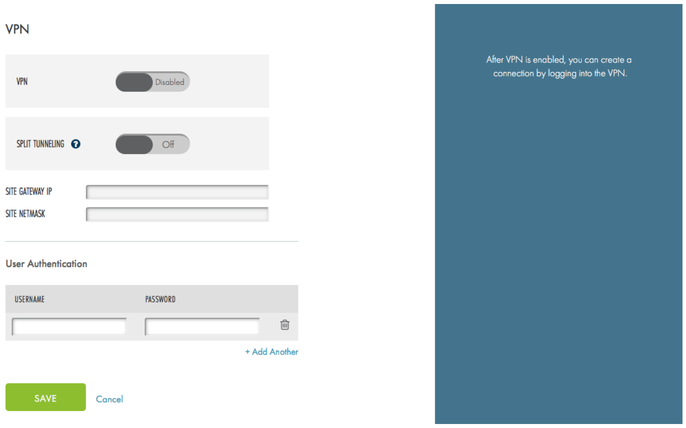
Standard VPN set up allows individual devices to connect to the virtual office in an Axcient data center.

STEP 2

On the *VPN* screen, configure the following fields:

- **Split Tunneling**—enable split tunneling to route the VPN user’s Internet access through their device. Disable to route all Internet traffic through the Virtual Office.
- **Site Gateway IP**—set the Virtual Office gateway IP address. The *Site Gateway IP* address establishes a network tunnel between the user's device and the Virtual Office. It should meet the following guidelines:
    - Cannot be on the same network as the Virtual Office.
    - Cannot be on the same network as the device performing connecting to the Virtual Office.
    - Should be a private IP address, such as:
        - **Class A**—10.X.X.X
        - **Class B**—172.16.16.X - 172.16.31.X
        - **Class C**—192.168.X.X
- **Site Netmask**—enter the primary Virtual Office netmask. Axcient recommends a small netmask, such as 255.255.255.X.
- **User Authentication**—create login credentials for users to access the VPN. Click the **Add Another** button to create multiple user logins.

Click the **Save** button to save any new configurations.



VPN

VPN: Disabled

SPLIT TUNNELING: Off

After VPN is enabled, you can create a connection by logging into the VPN.

When the VPN has been configured, the Virtual Office will generate a link that allows you to connect to the VPN. This link can be copied and sent to the desired recipients.

Connecting to VPN

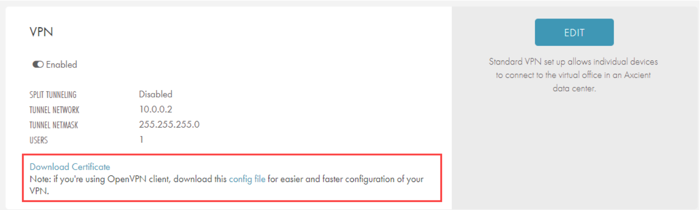
When a VPN network has been configured in the Virtual Office, you will need to connect to the VPN network using a preferred VPN agent. This procedure will use **OpenVPN** as the VPN agent for demonstration purposes. You can, however, use any preferred VPN agent.

To connect to the VPN network:

STEP 1

On the *Configure: Virtual Office* page, find the *VPN* section. Select from the following options:

- **Using OpenVPN Agent**—when the VPN has been configured successfully, click the **config file** link to download the required file. These must be downloaded to the config folder of the OpenVPN agent.
- **Using Other VPN Agents**—for other VPN agents, click the **Download Certificate** link to download the VPN certificate. The file name should be `ca.crt`. While the actual file name is not important, you must enter this file name when creating the configuration file in the steps below. Be sure to download this file to the appropriate folder for the VPN agent to connect to the VPN.



VPN

Enabled

SPLIT TUNNELING	Disabled
TUNNEL NETWORK	10.0.0.2
TUNNEL NETMASK	255.255.255.0
USERS	1

Download Certificate
Note: if you're using OpenVPN client, download this config file for easier and faster configuration of your VPN.

Standard VPN set up allows individual devices to connect to the virtual office in an Axcient data center.

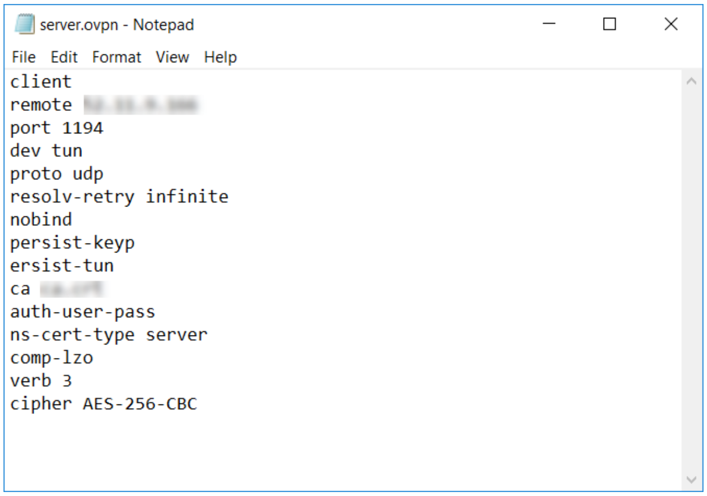
STEP 2a

If you are using the OpenVPN option, the configuration file should be automatically configured with the appropriate information; however you may want to confirm this.

Using a preferred text editor, open the configuration file for the VPN agent. The configuration file **must be saved** in the following format: `File Name.ovpn`.

Confirm that the following text exists in the configuration file:

```
client
remote Public IP of Virtual Office
port 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
ca Certificate File filename
auth-user-pass
ns-cert-type server
comp-lzo
verb 3
cipher AES-256-CBC
```

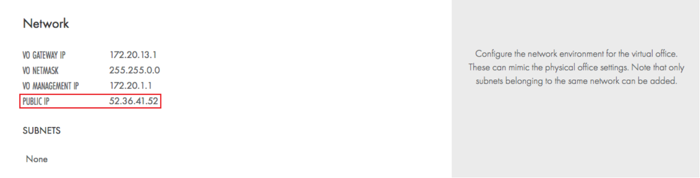


```
client
remote [redacted]
port 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-keyp
ersist-tun
ca [redacted]
auth-user-pass
ns-cert-type server
comp-lzo
verb 3
cipher AES-256-CBC
```

STEP 2b

If you are using an alternative VPN option, locate the configuration file for the VPN agent. Configure the file using the correct information:

- **Public IP Address of the Virtual Office**—this can be found in the Network section of the *Virtual Office Configuration* page.
- **Certificate File Name**—this is the Certificate File name that was downloaded in the steps above.



Network

VO GATEWAY IP	172.20.13.1
VO NETMASK	255.255.0.0
VO MANAGEMENT IP	172.20.1.1
PUBLIC IP	52.36.41.52

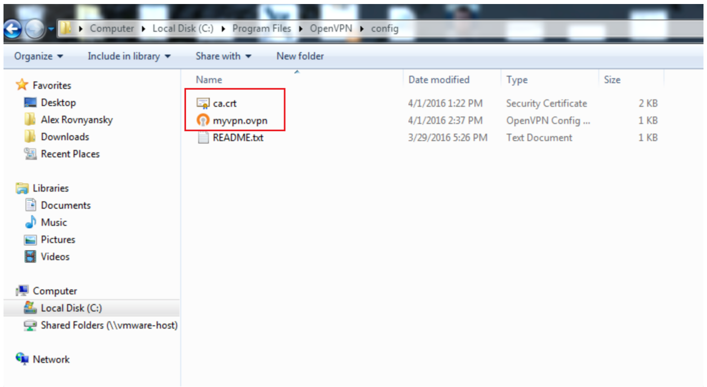
SUBNETS

None

Configure the network environment for the virtual office. These can mimic the physical office settings. Note that only subnets belonging to the same network can be added.

STEP 3

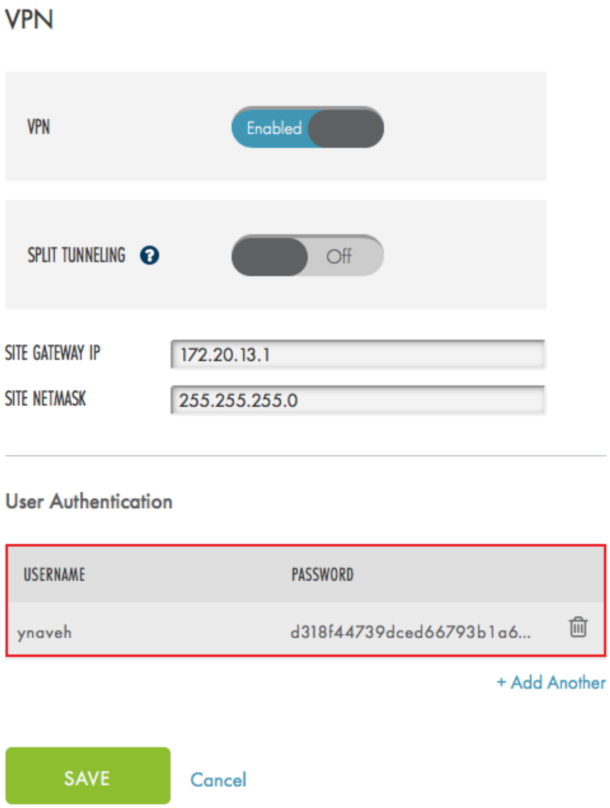
Save the changes to the configuration file. Make sure the `ca.crt` file and the configuration file are both saved in the config folder of the VPN agent.



Name	Date modified	Type	Size
ca.crt	4/1/2016 1:22 PM	Security Certificate	2 KB
myvpn.ovpn	4/1/2016 2:37 PM	OpenVPN Config ...	1 KB
README.txt	3/29/2016 5:26 PM	Text Document	1 KB

STEP 4

You can now run the agent and connect to the VPN. Use the username and password configured in the VPN section to access the VPN. The administrating user who originally creates the logins should make note of the passwords when creating them. Once saved, the passwords are hashed for your protection. In the event a password is forgotten, simply delete the user and create new login credentials.



VPN

VPN: Enabled

SPLIT TUNNELING: Off

SITE GATEWAY IP: 172.20.13.1

SITE NETMASK: 255.255.255.0

User Authentication

USERNAME	PASSWORD
ynaveh	d318f44739dced66793b1a6...

Port Forwarding

Port Forwarding is not enabled by default but can be configured to work in the Virtual Office.

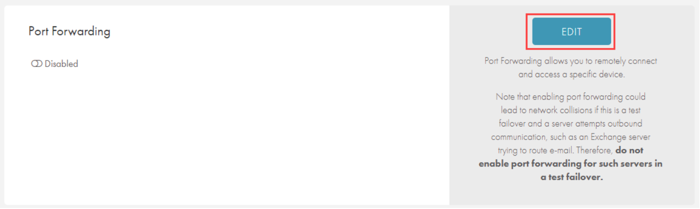
Enabling Port Forwarding could lead to a network collision if configured on a Test Virtual Office. Do not enable and configure Port Forwarding for a Test Virtual Office as productivity and data loss may occur.

Additionally, Port Forwarding must be enabled for [Site to Site Open VPN] to function.

To configure or edit the Port Forwarding settings:

STEP 1

On the *Configure: Virtual Office* page, click the **Edit** button in the *Port Forwarding* section.



Port Forwarding

Disabled

EDIT

Port Forwarding allows you to remotely connect and access a specific device.

Note that enabling port forwarding could lead to network collisions if this is a test failover and a server attempts outbound communication, such as an Exchange server trying to route e-mail. Therefore, **do not enable port forwarding for such servers in a test failover.**

STEP 2

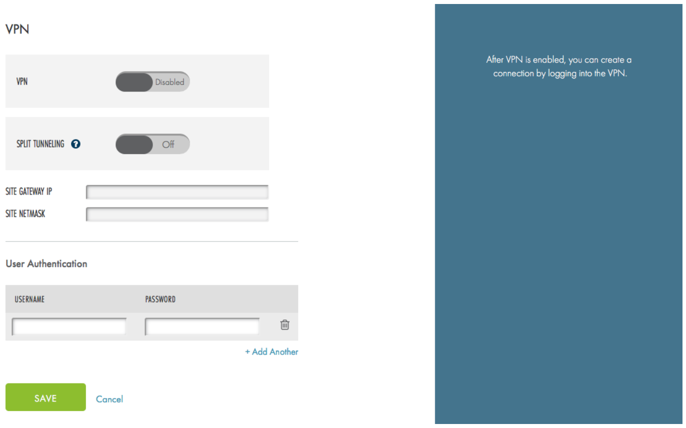
On the *Port Forwarding* screen, toggle the *Port Forwarding* field to **Enabled**.

Enter a value for one or more of the following fields:

- **Protocol**—specify the use of the port. The options are **TCP**, **UDP** and **ICMP**. **TCP** is the most common. If unsure which to specify, please consult your network administrator or contact [Axcient Support](#).
- **Ext IP**—select a public IP address to use. These IP addresses are automatically generated in the Axcient Cloud. This IP address will be used to access the Virtual Office environment from external devices.
- **Ext Port**—designate the external port number used to access a target internal port.
- **Int IP**—designate the internal IP address of the target device being forwarded to.
- **Int Port**—designate the internal port number of the target device being forwarded to.

Click the **Add Another** button to add any additional entries.

Click the **Save** button to save any new configurations.



VPN

VPN: Disabled

SPLIT TUNNELING: Off

SITE GATEWAY IP

SITE NETMASK

User Authentication

USERNAME	PASSWORD

After VPN is enabled, you can create a connection by logging into the VPN.

Public IP Settings

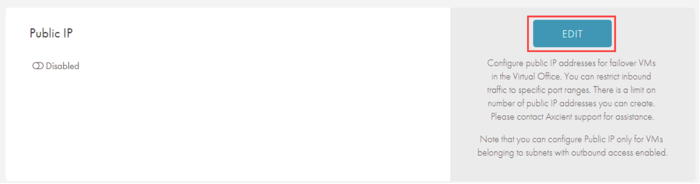
You can configure public IP addresses for failover VMs in the Virtual Office. You can also restrict inbound traffic to specific port ranges. Please note, however, that there is a limit on the number of public IP addresses you can create.

> **Note**
>
> Note that you can configure Public IP only for VMs belonging to subnets with outbound access enabled.

To configure a public IP address:

STEP 1

On the *Configure: Virtual Office* page, click the **Edit** button in the Public IP section.



Public IP

Disabled

Configure public IP addresses for failover VMs in the Virtual Office. You can restrict inbound traffic to specific port ranges. There is a limit on number of public IP addresses you can create. Please contact Axcient support for assistance.

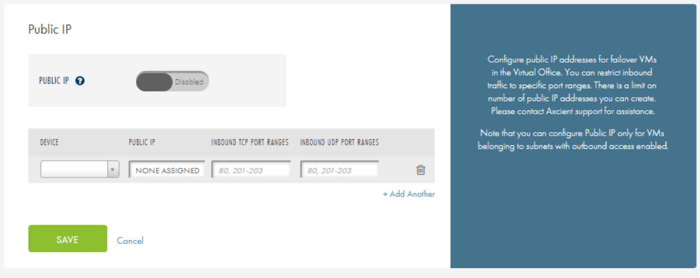
Note that you can configure Public IP only for VMs belonging to subnets with outbound access enabled.

STEP 2

On the Port Forwarding page, update the following fields:

- Click the *Public IP* field to enable the feature.
- Enter the appropriate values to set the port forwarding rules:
  - In the *Device* field, select the **IP Address** of the device.
  - In the *Public IP* field, enter the **public IP address**. Note that you can configure Public IP only for VMs belonging to subnets with outbound access enabled.
  - In the *Inbound TCP Port Ranges* field, enter the **TCP port range** that will accept inbound traffic.
  - In the *Inbound UDP Port Ranges* field, enter the **UDP port range** that will accept inbound traffic.
- Click the **Add Another** button to add additional entries.

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



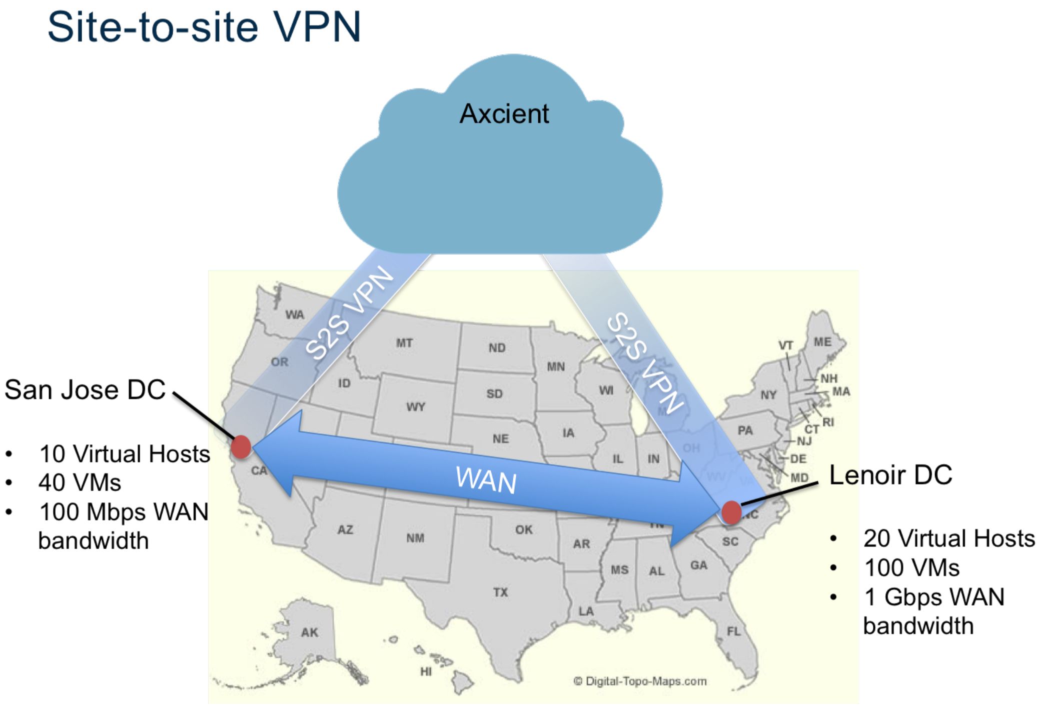
Configure public IP addresses for failover VMs in the Virtual Office. You can restrict inbound traffic to specific port ranges. There is a limit on number of public IP addresses you can create. Please contact Axcient support for assistance.

Note that you can configure Public IP only for VMs belonging to subnets with outbound access enabled.

Site to Site VPN

Site to Site VPN lets you create a single VPN endpoint for a local network through which any local user can connect to the Virtual Office. Once the Site to Site VPN endpoint has been configured, a virtual image is generated, which must be then downloaded and run on any VMware virtual machine software.

Figure 15 **-** Visualization of the Site-to-Site Endpoint Functionality



The image above represents a typical use case where the Site to Site VPN feature would be helpful.

Using Site to Site VPN is not recommended in a test environment. However, it can provide valuable services in the following situations:

- When a disaster occurs in an organization with two (or more) sites linked together in a corporate network. A Site-to-Site VPN connection can be configured that effectively recreates the corporate network for the unavailable physical site.
- When a site is being rebuilt after a disaster, such that users can physically use the site but the machine room is still in repair. The Site to Site VPN connection can be configured as a replacement while the machine and servers are being rebuilt.

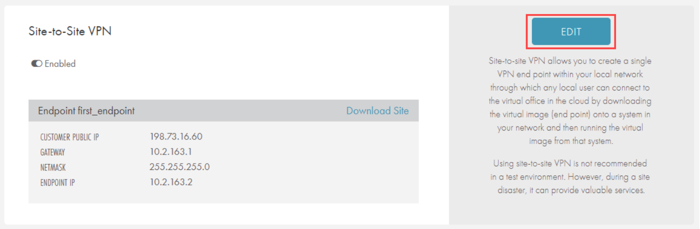
Note

For the Site to Site VPN feature to function, Port Forwarding must be enabled. Once enabled, you can continue to configure the Site to Site VPN.

To set up a Site to Site VPN:

STEP 1

On the *Configure: Virtual Office* page, click the **Edit** button in the *Site-to-Site VPN* section.



Site-to-Site VPN

Enabled

Endpoint first_endpoint

CUSTOMER PUBLIC IP	198.73.16.60
GATEWAY	10.2.163.1
NETMASK	255.255.255.0
ENDPOINT IP	10.2.163.2

Site-to-site VPN allows you to create a single VPN end point within your local network through which any local user can connect to the virtual office in the cloud by downloading the virtual image (end point) onto a system in your network and then running the virtual image from that system.

Using site-to-site VPN is not recommended in a test environment. However, during a site disaster, it can provide valuable services.

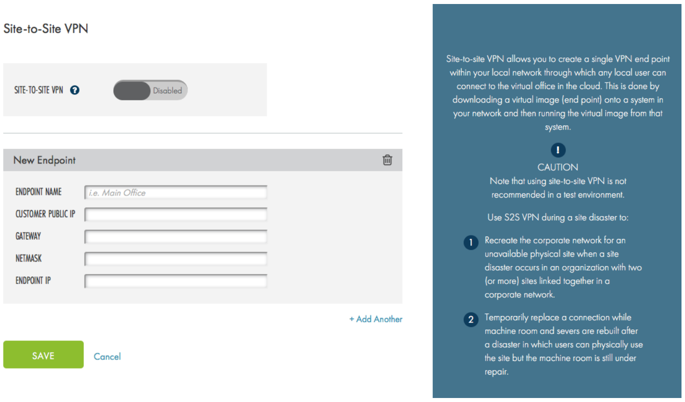
STEP 2

In the *Site-to-Site VPN* field, click to enable the feature.

In the *Endpoint* section, enter a value in the following fields:

- **Endpoint Name**—enter the desired name for the Endpoint.
- **Customer Public IP**—enter the public IP address of the site connecting to the Virtual Office.
- **Gateway**—enter the gateway IP address.
- **Netmask**—enter the netmask value.
- **Endpoint IP**—configure an IP address for the Endpoint. The IP address must be an empty IP in the subnet where the Endpoint will be deployed.
- Optionally, click the **Add Another** link to add additional endpoints.

Click the **Save** button to save any new configurations.



Site-to-Site VPN

SITE-TO-SITE VPN: Disabled

New Endpoint

ENDPOINT NAME	i.e. Main Office
CUSTOMER PUBLIC IP	
GATEWAY	
NETMASK	
ENDPOINT IP	

Site-to-site VPN allows you to create a single VPN end point within your local network through which any local user can connect to the virtual office in the cloud. This is done by downloading a virtual image (end point) onto a system in your network and then running the virtual image from that system.

CAUTION

Note that using site-to-site VPN is not recommended in a test environment.

Use S2S VPN during a site disaster to:

1. Recreate the corporate network for an unavailable physical site when a site disaster occurs in an organization with two (or more) sites linked together in a corporate network.
2. Temporarily replace a connection while machine room and severs are rebuilt after a disaster in which users can physically use the site but the machine room is still under repair.

How to Deploy the Site to Site VPN Endpoint

When Site to Site VPN is configured for the Virtual Office, you can then download the image of the Endpoint. This image should be deployed at the desired location using any VMware virtual machine software.

Note

When the VM endpoint is powered on, a console window should print out a message acknowledging the VPN connection. A message should also appear with network instructions to reconfigure the host machine on which the VM endpoint is being deployed. If you do not see the console windows, please contact Axcient Support.

The message will be formatted as follows:

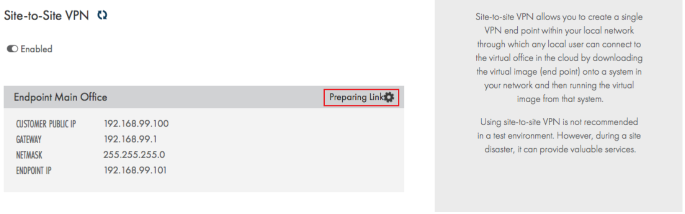
```
"Open VPN Connect *** ESTABLISHED ***"

Please add <Virtual Office Subnet> netmask <Host Machine Netmask> gw <Host Machine
Gateway> to your subnet router
```

To deploy the Site to Site VPN Endpoint:

STEP 1

On the *Configure: Virtual Office* page, find the *Network* section.

Click the **Download Client** link to download the image of the Endpoint. This image should be deployed at the desired location using any VMware virtual machine software.



Site-to-Site VPN

Enabled

Endpoint Main Office

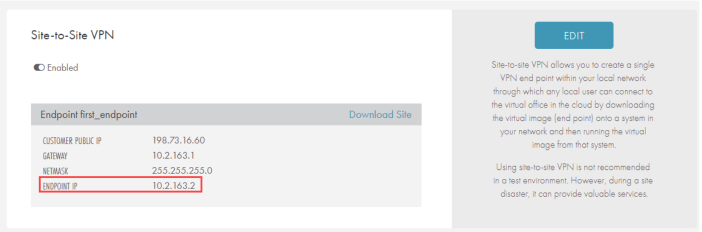
CUSTOMER PUBLIC IP	192.168.99.100
GATEWAY	192.168.99.1
NETMASK	255.255.255.0
ENDPOINT IP	192.168.99.101

Site-to-site VPN allows you to create a single VPN end point within your local network through which any local user can connect to the virtual office in the cloud by downloading the virtual image (end point) onto a system in your network and then running the virtual image from that system.

Using site-to-site VPN is not recommended in a test environment. However, during a site disaster, it can provide valuable services.

STEP 2

After the VM of the Endpoint has been deployed, all local devices must have their gateways changed to the **IP address of the Endpoint** configured in the steps above.



Site-to-Site VPN

Enabled

Endpoint first_endpoint

CUSTOMER PUBLIC IP	198.73.16.60
GATEWAY	10.2.163.1
NETMASK	255.255.255.0
ENDPOINT IP	10.2.163.2

Site-to-site VPN allows you to create a single VPN end point within your local network through which any local user can connect to the virtual office in the cloud by downloading the virtual image (end point) onto a system in your network and then running the virtual image from that system.

Using site-to-site VPN is not recommended in a test environment. However, during a site disaster, it can provide valuable services.