



Axcient Business Recovery Cloud Web Application User 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

Preface	4
Intended Audience	4
Introduction	5
Architecture and Terminology	5
Administration	5
Web Application Walkthrough	7
Logging in to the Axcient Web Application	7
Web Application Dashboard	9
Services Page	11
Service Details Page	12
Sites Page	14
Sites Details Page	15
Devices Page	17
Device Details Page	19
Job Details Page	21
Exclude Files from a Job	23
Users Page	26
Reports Page	30
Cloud Failover	34
Starting the Virtual Office	35
The Virtual Office Page	38
Configure Virtual Office	40
Network Settings	41
Virtual Private Network (VPN) Settings	43
Port Forwarding	53
DHCP Settings	55
Site to Site Open VPN Settings	57
IPSec Site to Site VPN Settings	61

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, appliances, and devices in the organization.

Architecture and Terminology

The Axcient Web Application is designed to provide summary information of, and access to, all levels of the Axcient Protection Solution.

The Axcient Protection Solution includes the following elements:

- **Web Application**—the highest view of the Axcient protection solution hierarchy. You can monitor, manage, protect, and perform disaster recovery tasks from the Web Application.
- **Site(s)**—specific locations or organizations with Axcient services.
- **Service(s)**—Axcient services registered to your account.
- **Appliance(s)**—the physical or virtual machines located at a Site that run the Axcient service and protect devices.
- **Device(s)**—the machines that are protected by the Axcient appliance.

Administration

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

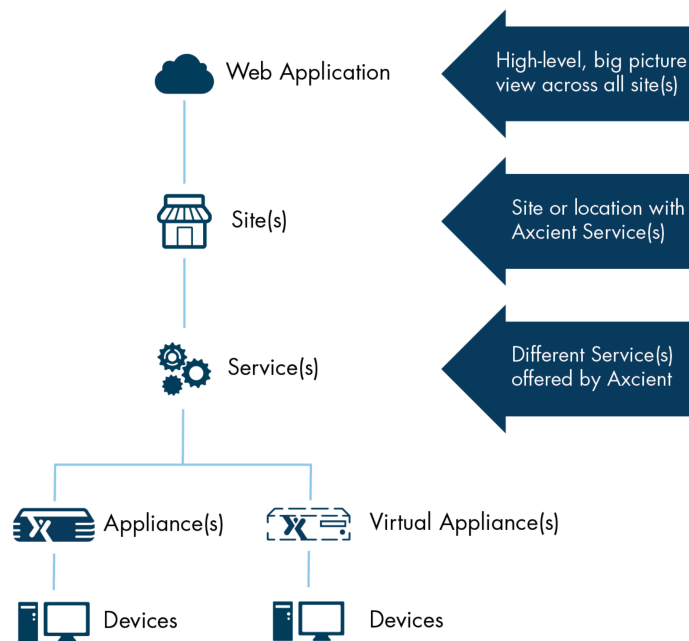
The Axcient Web Application includes the following pages:

- **Dashboard**—displays summary information across all Sites, including health status information, activities of interest, and other relevant notifications.
- **Services**—summary list view of all registered Services. You can click a Service to view the *Service Details* page, where you can perform management, recovery, and configuration actions.
- **Sites**—summary view of all registered Sites. Click a Site to view the *Site Details* page, where you can perform management, recovery, and configuration actions.
- **Events**—a detailed and searchable view of all events that occur across all Sites, Services, and devices.

- **Users**—list of all user accounts with access to the Axcient Web Application. The master user 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.

Figure 1 - Axcient Architecture and Terminology



Web Application Walkthrough

Logging in to the Axcient Web Application

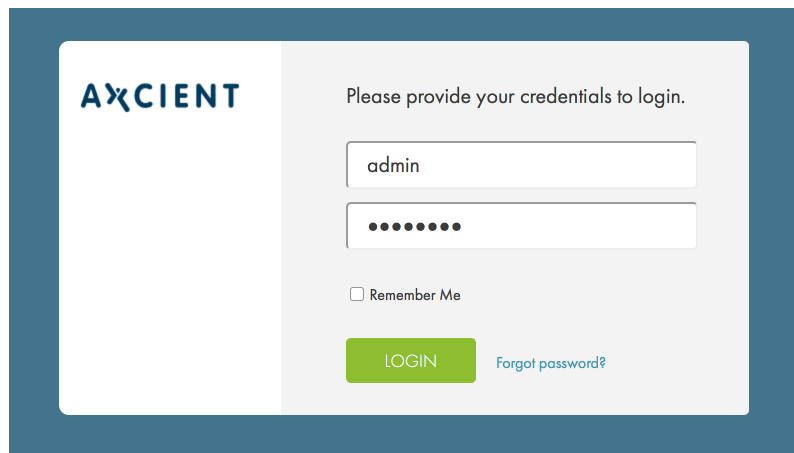
After you register with Axcient, Axcient Support will send an email containing information necessary for you to begin leveraging the Axcient protection solution.

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

To log in to the Axcient Web Application:

1. In your preferred browser, navigate to <https://my.axcient.net> (US) or <https://ca.axcient.net> (Canada).
2. Log in to the Axcient Web Application using the log in credentials provided by Axcient Support.

Figure 2 - Login Screen



Axcient

Please provide your credentials to login.

admin

.....

Remember Me

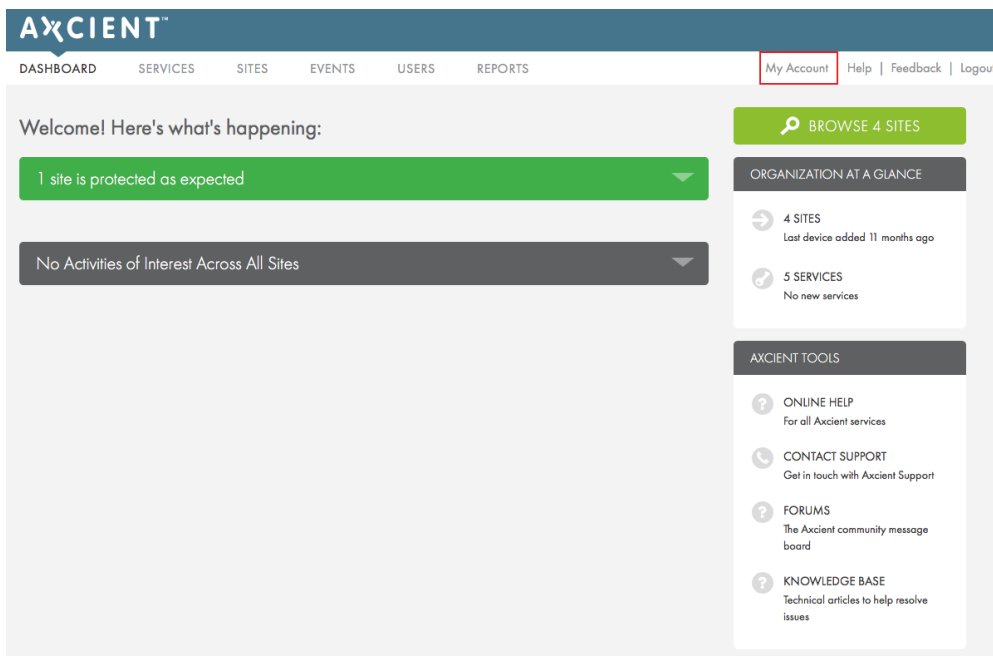
LOGIN [Forgot password?](#)

Note: For security reasons, Axcient recommends changing the password for the Web Application from the default password.

To change the password:

1. On the Axcient Web Application, click the **My Account** link.
2. Update the password.
3. Click the **Save** button.

Figure 3 - Location to Change Password

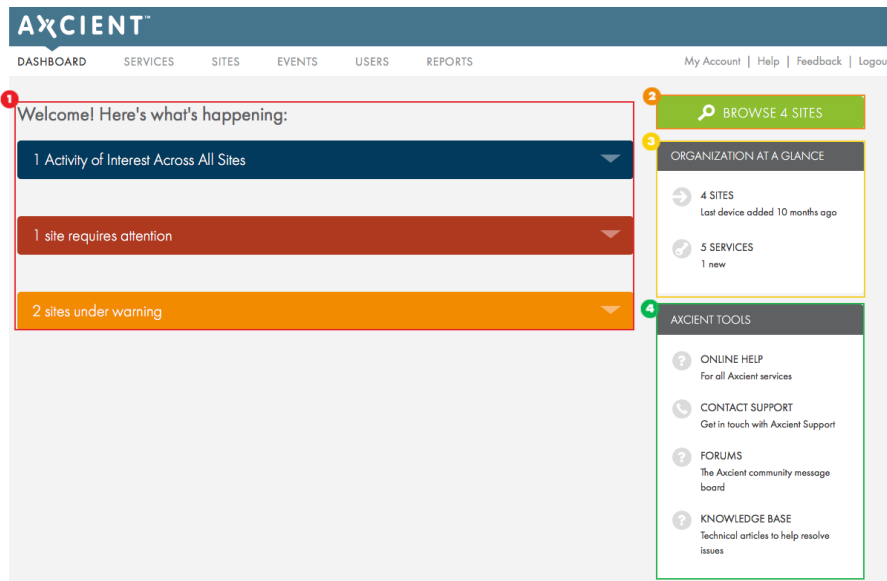


Web Application Dashboard

The Axcient Web Application Dashboard embodies Axcient’s Manage by Exception philosophy.

The Manage by Exception philosophy emphasizes the need to surface alerts, notifications, and activities that most urgently require your attention. In this way, you are able to resolve the most critical issues first, and ensure devices stay fully protected.

Figure 4 - Web Application Dashboard



1 Site Health Status Display

This panel displays the health status, alerts, notifications, and activity across all Sites and Services are displayed. A complete list of health status descriptions can be found below.

2 Browse Sites

Click the **Browse Sites** button to view the *Sites* page, which lists all Sites provisioned under the user.

3 Organization at a Glance

This panel displays a summary view of all Sites and Services registered to your account with direct links to the *Sites* and *Services* pages.

4 Axcient Tools

This panel provides links to Axcient's online documentation, support pages, and a link to the [Axcient Support](#) page.

Site Health Status Descriptions

- **Activities of Interest**—this panel lists important activities across all Sites and Services. Each individual alert includes direct links to the corresponding activity.
- **Requires Attention**—this panel, which is also referred to as *Troubled*, displays a list of devices that have fallen out of the protection threshold as configured in the Protection Policy. Devices that have failed the Cloud replication will be listed here as well. Each individual alert includes direct links to the corresponding device.
- **Warning**—this panel lists appliances or devices that have lost connectivity for an extended period of time as configured in the Protection Policy. This panel will also display alerts when a local or Cloud replication job completes with warnings. Each individual alert includes direct links to the corresponding device or appliance.
- **Protected as Expected**—this panel lists devices that are healthy and do not need attention at this time. Expand the alert and click **Browse** to view each protected Sites.

Services Page

The *Services* page provides a summary of all Axcient physical and virtual appliances registered to your account. The list view offers at-a-glance information such as health status, tunnel status, and important identifying information.

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

- Tunnel Status
- Service Alias
- Package (Service Type)
- Service ID
- Health
- Site

Click a **Service** to view the *Service Details* page.

Figure 5 - Services Page

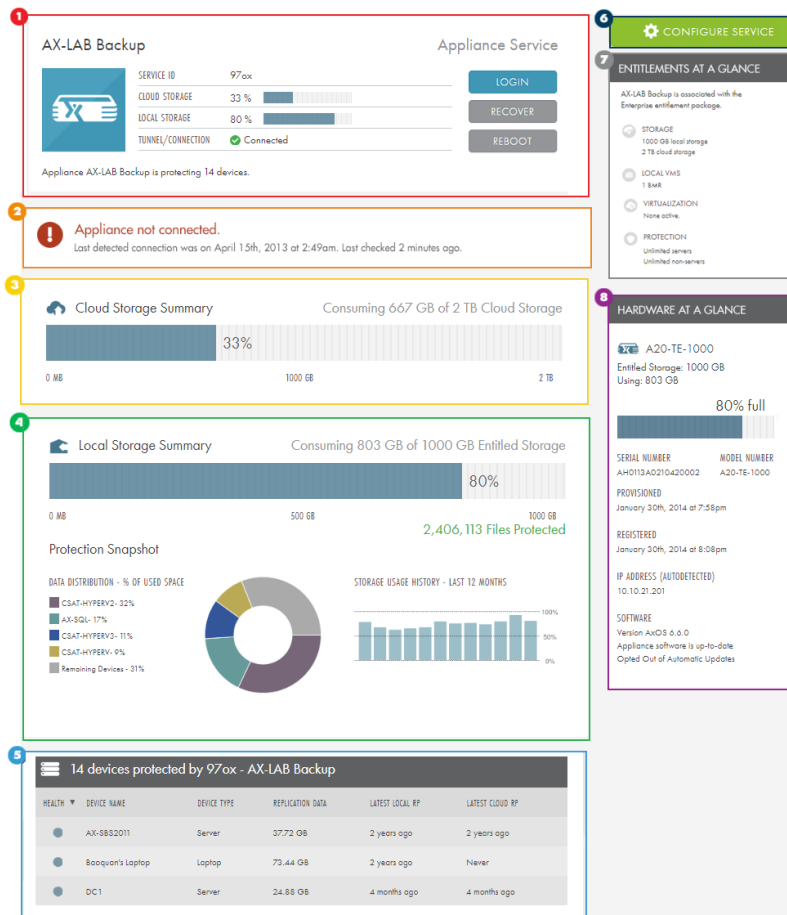
The screenshot shows the Services Page interface. On the left is a 'FILTER SERVICES' sidebar with a search bar, a 'Service' button, and filter sections for 'SITE' and 'SERVICE TYPE'. The main area shows 'All 2 Services' in a table.

TUNNEL	SERVICE ALIAS	PACKAGE	SERVICE ID	HEALTH	SITE ▲
✓	AX-LAB Backup	Enterprise	97ox	■	Axcient Internal Usage
!	AX-LAB VApp	Enterprise	3i99	■	Axcient Internal Usage

Service Details Page

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

Figure 6 - Service Details Page



1 Appliance Details

This panel displays summary information for the Service, including the ability to log in to the appliance UMC, recover devices, protect devices, and reboot the appliance.

2 Connectivity Alert

This panel displays a dated alert when the appliance loses connection.

3 Cloud Storage Summary

This panel displays summary of the appliance's Cloud storage usage. This section will show the most recent cloud replication attempt and the most recent successful Cloud replication.

4 Local Storage Summary

This panel displays a summary of the local storage usage with a breakdown of total files protected and storage used per device.

5 Device List

This panel displays a summary list of devices being protected by the appliance. Click a device to view the [Device Details](#) page.

Configure Service

This button launches the *Configure Service* page, where you can configure service settings, alerts, replication schedules, and software updates. For more information, please reference the [Axcient BRC Protection Guide](#).

Entitlements at a Glance

This panel displays entitlements allotted to the Service, including appliance protection type, the amount of storage available, the total virtualized machines running, and the total number of devices that can be protected.

Hardware at a Glance

This panel displays hardware summary information, including the IP address, the serial number, hardware capacities, and the current AxOS software version.

Sites Page

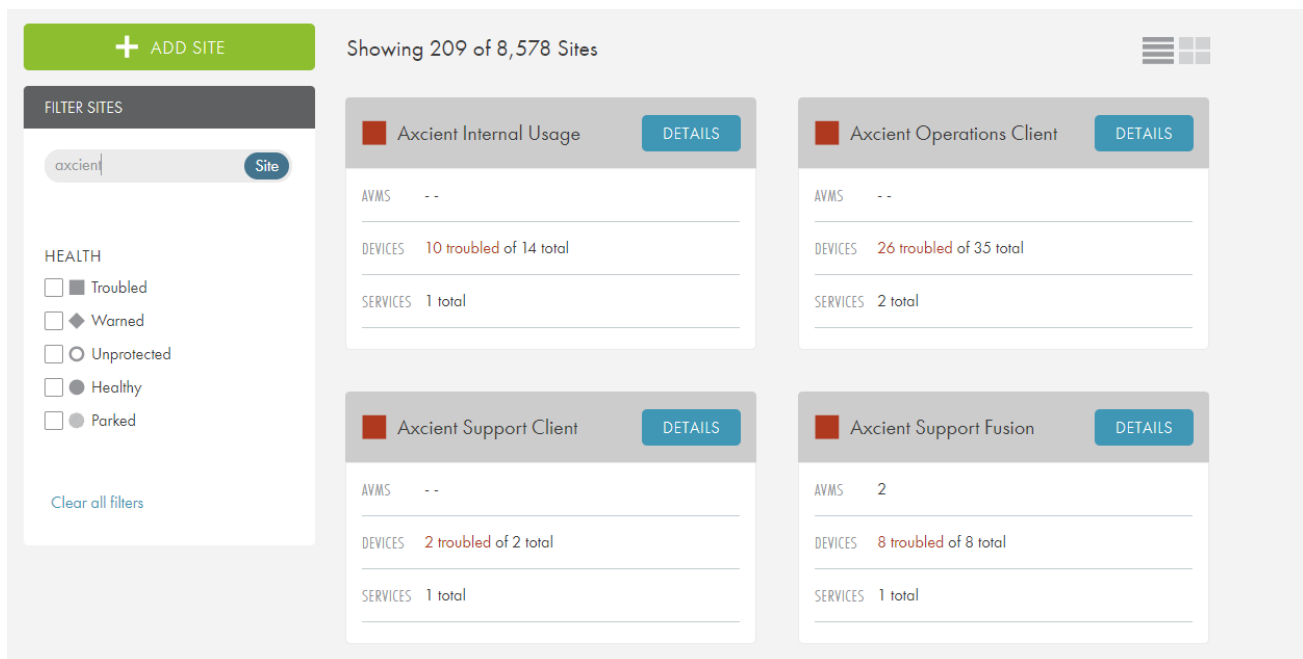
The *Sites* page displays each Site, which can be physical locations or companies, based on your preferences as the administrator. The *Sites* page shows summary information about each Site, including:

- Health status
- Total number of devices protected
- Total number of Services for the Site

Sites can be filtered using the *Filter Sites* panel on the left side of the page. Sites can be filtered by health status or searched by name.

If you are viewing the page in *Grid view*, click the **Details** button to view the *Site Details* page for the specified Site. Alternatively, if you are viewing the page in *List view*, click the **View Site** button to view the *Site Details* page.

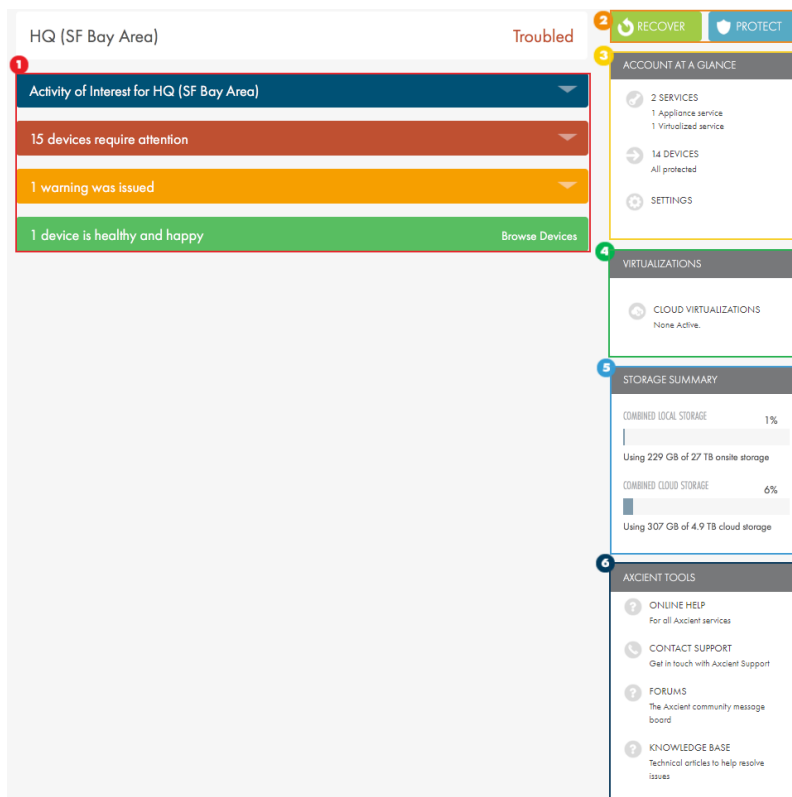
Figure 7 - Sites Page (Grid View)



Sites Details Page

The *Site Details* page displays a detailed view of the health status of protected devices and also provides tools to help you recover and protect devices.

Figure 8 - Site Details Page



1 Device Health Status Display

This panel displays the health status, alerts, notifications, and activities across the Site. A complete list of health status descriptions can be found below.

2 Recover and Protect

This panel includes tools to help you protect new devices or recover protected devices.

3 Account at a Glance

Click the **Settings** button to configure the Protection Policy. You can also use this panel to view all devices and Services associated with the Site by clicking the appropriately titled links.

4 Virtualizations

This panel displays all currently running virtualizations, both locally and in the Cloud.

5 Storage Summary

This panel displays a combined storage capacity summary across all appliances associated with the Site, both locally and in the Cloud.

6 Axcient Tools

This panel displays links to online support resources, including online help, support contact information, forums, and the knowledge base.

Device Health Status Descriptions

- **Activities of Interest**—this panel lists important activities across all Sites and Services. Each individual alert includes direct links to the corresponding activity.
- **Requires Attention**—this panel, which is also referred to as *Troubled*, displays a list of devices that have fallen out of the protection threshold as configured in the Protection Policy. Devices that have failed the Cloud replication will be listed here as well. Each individual alert includes direct links to the corresponding device.
- **Warning**—this panel lists appliances or devices that have lost connectivity for an extended period of time as configured in the Protection Policy. This panel will also display alerts when a local or Cloud replication job completes with warnings. Each individual alert includes direct links to the corresponding device or appliance.
- **Protected as Expected**—this panel lists devices that are healthy and do not need attention at this time. Expand the alert and click **Browse** to view each protected Sites.

Devices Page

The *Devices* page can be accessed by clicking the **Browse Devices** link where available. This page lists all devices protected under the Site and allows you to recover devices and protect new devices.

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

- Health status
- Device name
- Service protected under
- Total replicated data
- Last successful local replication
- Last successful Cloud replication

The Device List also allows you to view devices based on health status. You can then quickly isolate and address devices with issues that need to be resolved.

- **Troubled**—devices that are outside of the Protection Policy Threshold for the freshest recovery point. These devices are marked with 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. These devices are marked with an orange health status symbol.
- **Healthy**—devices that are within the Protection Policy Threshold and have had no Cloud replication issues. These devices are marked with a green health status symbol.
- **Parked**—devices that have been previously protected and are still registered by the appliance, but no replication jobs are currently running. These devices are essentially on standby.
- **All Protected**—devices protected by the Service regardless of health status.
- **Local VMs**—all running Local VMs with the ability to start, stop, and discard.
- **Unprotected Devices**—devices registered to the appliance but not currently protected.

Click a device to view the [Device Details](#) page.


Figure 9 - Device List Page

aplotnikov_site Devices RECOVER

	3 Troubled	Warned	Healthy	Parked	3 All Protected	Local VMs	Unprotected
HEALTH ▲	DEVICE NAME	SERVICE		REPLICATION DATA	LATEST LOCAL RP	LATEST CLOUD RP	
■	ws_2008	ssbe - aplotnikov_sjc24_t...		44 GB	3 months ago	3 months ago	
■	ws_2003	h0e3 - vijitha_dema_app...		3.3 GB	4 days ago	A month ago	

ws_2003

■ Troubled



JOB HEALTH/NAME	JOB TYPE	LATEST LOCAL RP	LATEST CLOUD RP	
■ Image2003	Image	4 days ago	A month ago	VIEW DEVICE LOGIN
■ FF2003Demo	File & Folders	4 days ago	A month ago	

■	ws_2008r2	h0e3 - vijitha_dema_app...		31 GB	A month ago	A month ago	
---	-----------	----------------------------	--	-------	-------------	-------------	--

Device Details Page

The *Device Details* page displays a detailed view of the health status and protection summaries. This page also allows you to recover data and configure custom notifications for the device.

1 Device Details

This panel displays information about the device, including current health status, device type, OS, Service, and the hostname or IP address.

2 Health Status History

This panel displays the health status history of the device for the last 30 days. Red and yellow blocks display if the device has experienced health issues.

3 Onsite Protection Summary

This panel displays local data usage for the device.

4 Protection Schedule

This panel displays the replication jobs scheduled for the device. A device can have one or more replication schedules.

Click on a job to view the [Job Details](#) page.

5 Recover

This button allows you to perform data recovery actions for the device.

6 Protection at a Glance

This panel displays custom alerting for the device. These alerts will override the pre-existing alerting policy for the device.

Figure 10 - Device Details Page

●
172.20.10.166
Healthy

DEVICE TYPE	DESKTOP
OS	WINDOWS
SERVICE	qdzj - axcientapp2
HOSTNAME OR IP	172.20.10.166

LOGIN

↻ RECOVER

PROTECTION AT A GLANCE

172.20.10.166 is protected by 1 job

ALERTING
Local threshold - 36 hours
Cloud log threshold - 36 hours

2
+
Device Health Status History - Last 30 Days

3
+
Local Protection Summary — Using 15 GB of 12 TB

< 1%

4
+
1 Backup Job

HEALTH	JOB NAME ▲	JOB TYPE	LATEST LOCAL RP	LATEST CLOUD RP
●	172.20.10.166 Policy	Image	Never	Never

Job Details Page

The *Job Details* page gives you a detailed breakdown about the specified job, including:

1 Job Details

This panel provides information about the job, including job type, the device protected by the job, the Service, and the hostname/IP address of the device.

2 Threshold Alert

This panel displays alerts when the device being protected has fallen out of the protection threshold for the specified job. If the device is within threshold, no message will appear.

3 Most Recent Protection Activity

This panel displays a progress bar for the current or most recent scheduled replication job. When a replication job is running, this bar displays the replication job status.

4 Job Health Status History

This panel displays the health history of the replication job over the last 30 days.

5 Recover

Click this button to perform recovery actions.

6 Job at a Glance

This panel displays the local and Cloud Protection Policy, as well as excluded files, folders, or directories.

7 Job Settings

This panel displays custom configuration settings for the job.

Exclude Files from a Job

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

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

To exclude a drive, folder, or file:

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

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

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

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

<Drive Letter>:/

Example: *E:/*

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

<Drive Letter>:/<Folder Name>

Example: *C:/Documents*

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

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

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

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

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

<Drive Letter>:/<Folder Name>

Example: *E:/Music*

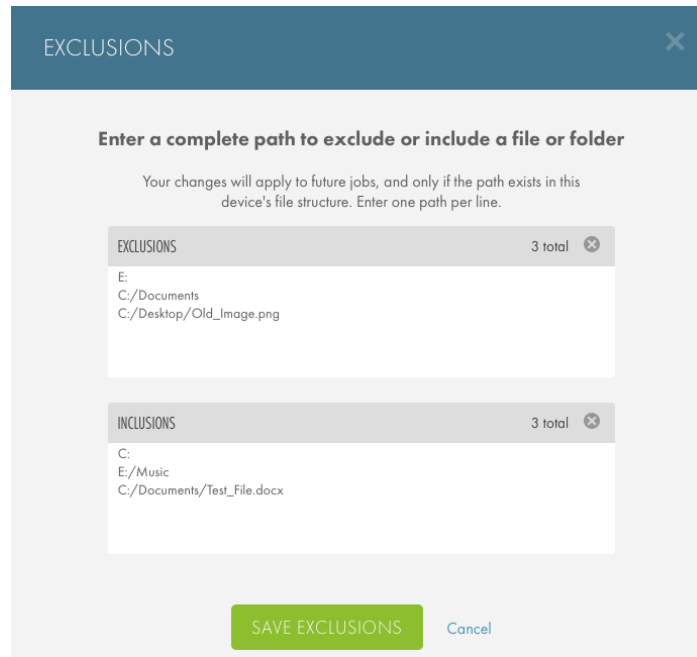
- To include a specific file from an excluded folder, enter the drive letter along with the target folder and the specific file in the following format:

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

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

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

Figure 12 - Exclusions Screen



Additional Exclusion and Inclusion Notes

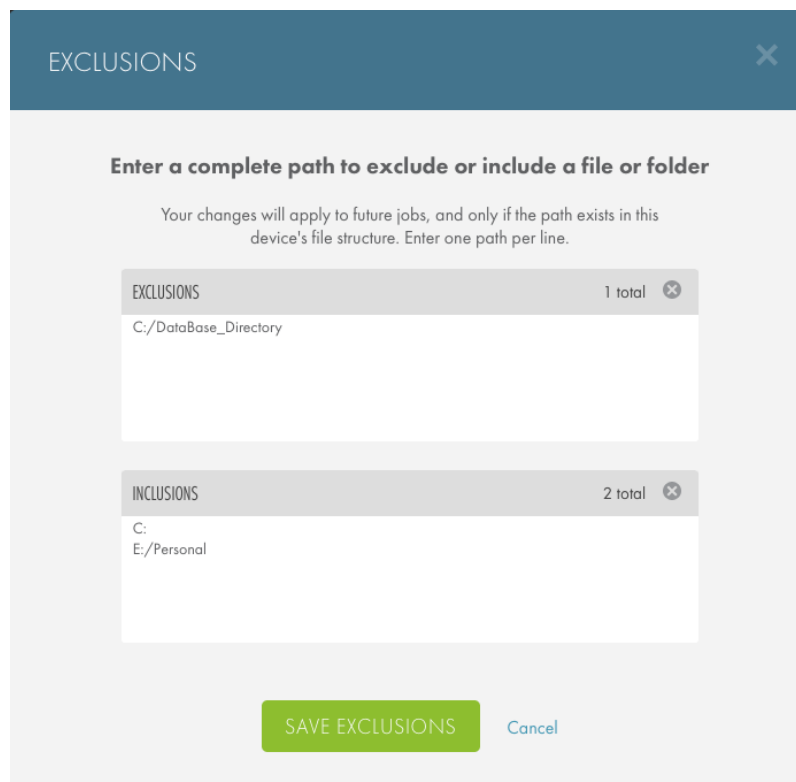
- When a device is added, all detected drives will populate the *Inclusions* section of *Exclusions* dialog box.
- Axcient recommends that you **do not** delete a drive from the *Inclusions* field in order to exclude it from the replication job.

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

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

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

Figure 13 - Exclusion Example



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 14 - Users Page

The screenshot displays the 'Users Page' interface. On the left, there is a sidebar with several filter sections:

- ADD USER:** A green button with a plus sign and the text '+ ADD USER'.
- FILTER USERS:** A search input field with the placeholder 'Search' and a blue 'User' button.
- USER ROLE:** A dropdown menu currently set to 'All'.
- STATUS:** Two radio button options: 'Active' (which is selected) and 'Inactive'.

 The main content area shows a table with the heading 'Showing 2 of 2 Users'. The table has five columns: 'ACTIVE', 'USERNAME', 'NAME', 'EMAIL', and 'ROLE'.

ACTIVE	USERNAME	NAME	EMAIL	ROLE
✓	axciu	axciu	[REDACTED]	Site User
✓	adoring@efolder.net	Anne Doring	[REDACTED]	Org Admin

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.

You can select from the following roles:

- An Organization Admin can view, create, and edit Services, devices, and jobs. Organization Admin accounts can add new devices to protect and use the Axcient business continuity features.
- An Organization Manager can view existing Services, devices, and jobs.

Figure 15 - Add User Screen

The screenshot shows a modal window titled "ADD USER" with a close button (X) in the top right corner. The form contains the following fields and controls:

- USERNAME***: A text input field with a small icon on the right.
- ROLE**: A dropdown menu currently showing "Org Admin" with a downward arrow. The dropdown is open, showing "Org Admin" (highlighted in blue) and "Org Manager".
- NAME**: A text input field.
- EMAIL***: A text input field.
- PASSWORD***: A text input field with a password icon on the right.
- CONFIRM PASSWORD***: A text input field with a password icon on the right.

At the bottom of the form, there are two buttons: a green "SAVE" button and a grey "Cancel" button.

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.

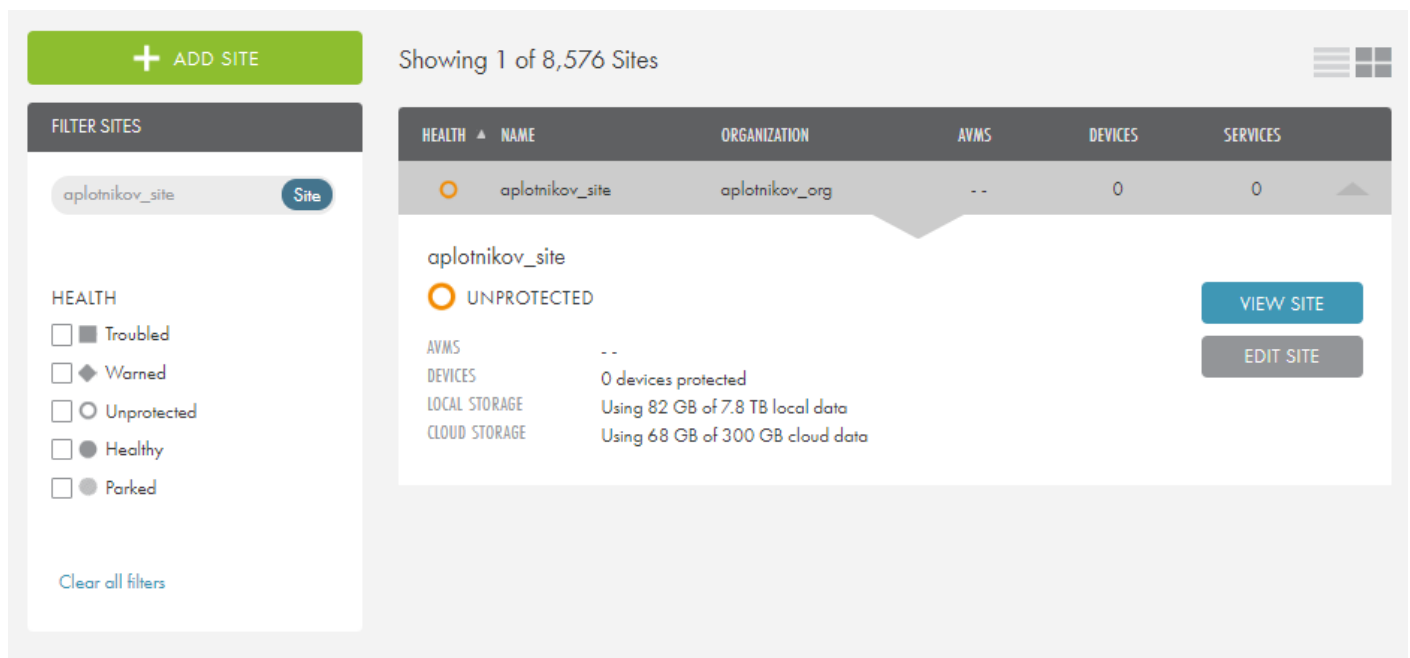
Note

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

To create a Site-specific login:

1. Log in to the Web App as a user with Organization Admin privileges.
2. Click the **Site** tab.
3. On the *Site* page, click the **List View** icon, which is depicted with four parallel lines.
4. Locate the target Site and click to expand the Site.
5. Click the **Edit Site** button.
6. Enter the appropriate information requested in the *Edit User* screen.

Figure 16 - Navigate to the Edit User Screen



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.

Figure 17 - Edit User Screen

The screenshot shows a modal window titled "EDIT USER" with a close button (X) in the top right corner. The form contains five input fields, each with a label to its left:

- USERNAME**: A text input field with a yellow highlight.
- USER FULL NAME**: A text input field.
- EMAIL**: A text input field.
- PASSWORD**: A text input field.
- CONFIRM PASSWORD**: A text input field.

At the bottom of the form, there are two buttons: a green "SAVE" button and a blue "Cancel" button.

Reports Page

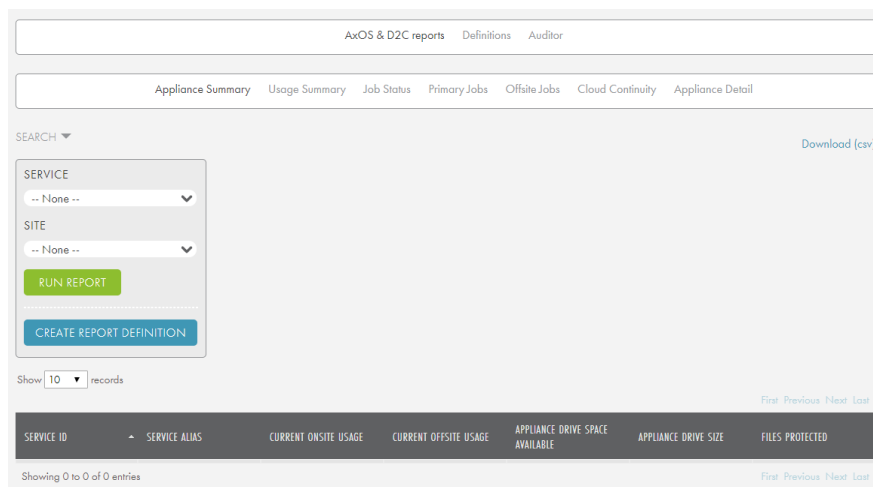
Within the Axcient Web Application, you can generate reports detailing replication job analysis, hardware usage, network activity, and more.

Axcient offers the following reports:

- The *Appliance Summary* report summarizes general usage across Axcient Services or Sites.
- The *Usage Summary* report summarizes service information, package information, and usage information.
- The *Job Status* report summarizes the status of jobs.
- The *Primary Jobs* report summarizes local jobs that run across an Axcient Services or Sites.
- The *Offsite Jobs* report summarizes all Cloud replication jobs that run across Axcient Services or Sites.
- The *Cloud Continuity* report summarizes failovers in the Cloud. This report provides an easy way to keep track of Cloud business continuity usage.
- The *Appliance Detail* report provides details of a specific Axcient appliance.
- The *Auditor* report summarizes activities based on action taken, time, entity, and user.
- The *Definitions* report summarizes a list of predefined configurations or parameters.

All reports can be downloaded as CSV files.

Figure 18 - Reports Page



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.

Figure 19 - Create Report Definition Screen

The screenshot shows a modal window titled "CREATE REPORT DEFINITION" with a close button (X) in the top right corner. The form contains the following fields:

- NAME:** A text input field containing "Report Definition Example".
- DELIVERY TYPE:** A dropdown menu with "Weekly" selected.
- ACTIVE:** An unchecked checkbox.
- EMAIL ADDRESS:** A text input field containing "adoring@axcient.com, admin@axcient.com". Below this field is a note: "Add up to 10 email addresses separating them by a comma."

At the bottom of the form, there is a green "SAVE" button and a blue "Cancel" button.

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 dropdown 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.

Figure 20 - Reports Definition Page

The screenshot displays the AXCIENT Reports Definition Page. At the top, the navigation bar includes 'My Account' (highlighted with a red box), 'Help', 'Feedback', and 'Logout'. Below the navigation bar is a breadcrumb trail: 'Appliance Summary > Usage Summary > Job Status > Primary Jobs > Offsite Jobs > Cloud Continuity > Appliance Detail > Auditor > Definitions'. A table lists report definitions with columns for Name, Type, Delivery Type, Active, and Actions. The table contains two entries: 'Report Definition Example' (Usage Report, Weekly, Active) and 'Test' (Appliance Summary, Daily, Inactive). The 'Test' entry has 'Edit', 'Delete', and 'View' actions. The page also shows 'Showing 1 to 2 of 2 entries' and pagination controls.

NAME	TYPE	DELIVERY TYPE	ACTIVE	ACTIONS
Report Definition Example	Usage Report	Weekly	Yes	
Test	Appliance Summary	Daily	No	Edit Delete View

Cloud Failover

In the event the local appliance is not available in a disaster situation, the Cloud failover feature in the Web Application allows you to start virtual machines (VMs) in the Axcient Cloud of one or more protected devices. For complete instructions, please reference the [Axcient Recovery Guide](#).

The Axcient Cloud failover solution allows you to do the following:

- Create a Virtual Office running in the Axcient data center that matches existing server configurations
- Configure network settings for the virtual office, including:
 - Provide secure access to the Virtual Office by configuring VPN
 - Configure Site to Site Open VPN, allowing multiple remote networks to connect to the Virtual Office
 - Allow VMs to access the Internet by enabling outbound connections (disabled by default)
 - Establish Port Forwarding rules
- Start the Virtual Office VMs of each server from separate restore points

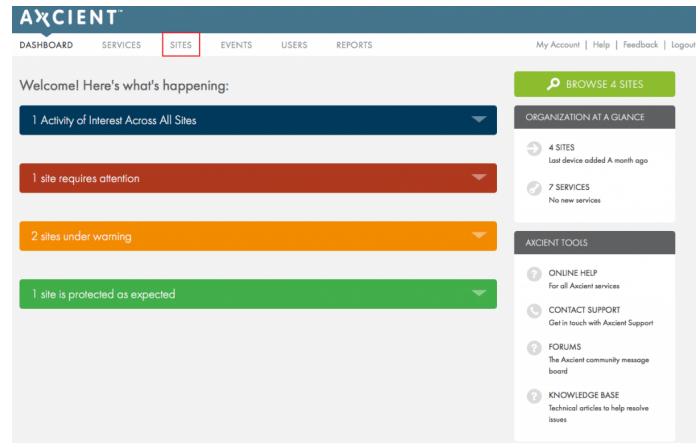
This section of the guide will cover the various Virtual Office interfaces.

Starting the Virtual Office

To start the Virtual Office:

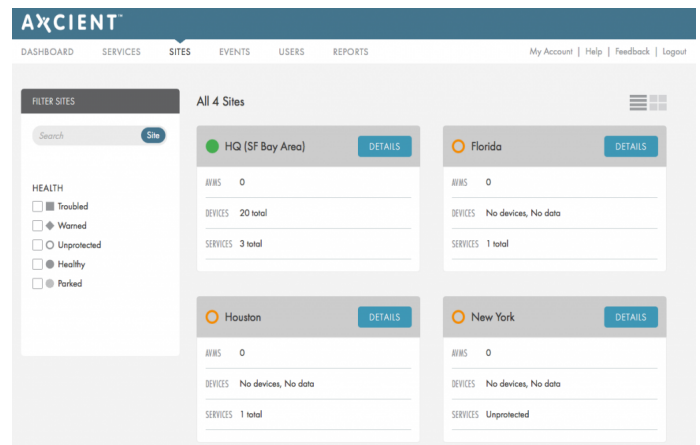
STEP 1

On the Axcient Web Application, click **Sites**.



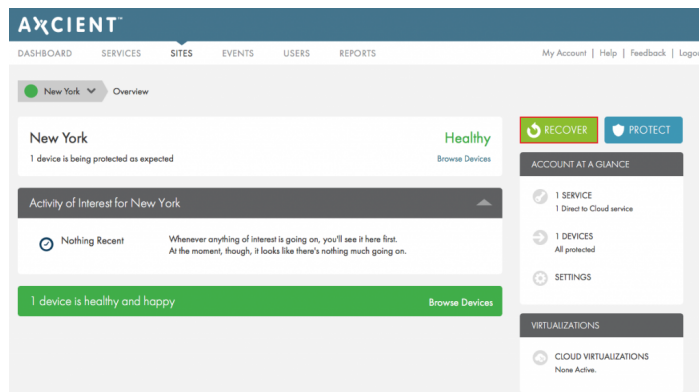
STEP 2

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



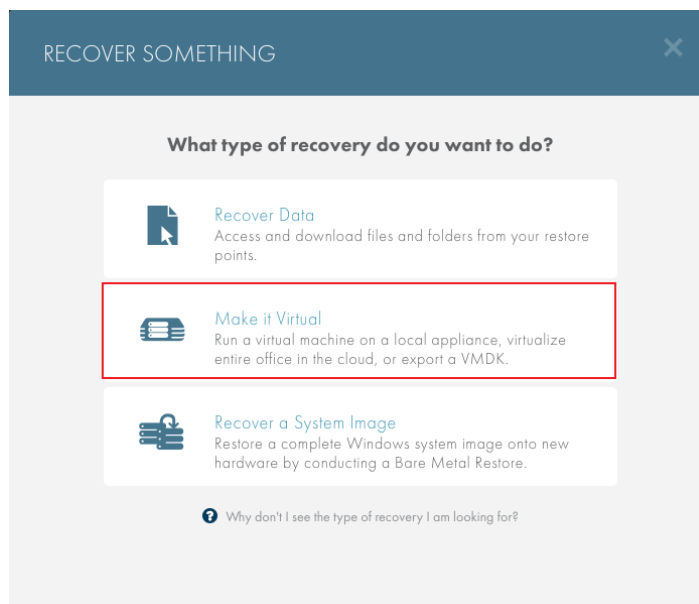
STEP 3

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



STEP 4

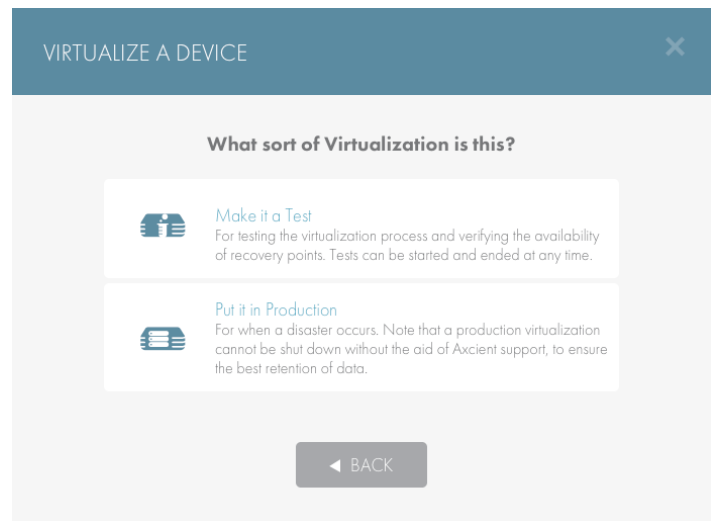
On the *Recover Something* screen, click the **Make it Virtual** option and then select the **Start a Virtual Office** option.



STEP 5

Select the type of local virtualization to deploy:

- Select the **Make it a Test** option to test the virtualization process and verify the availability of recovery points in case of an emergency.
- 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.



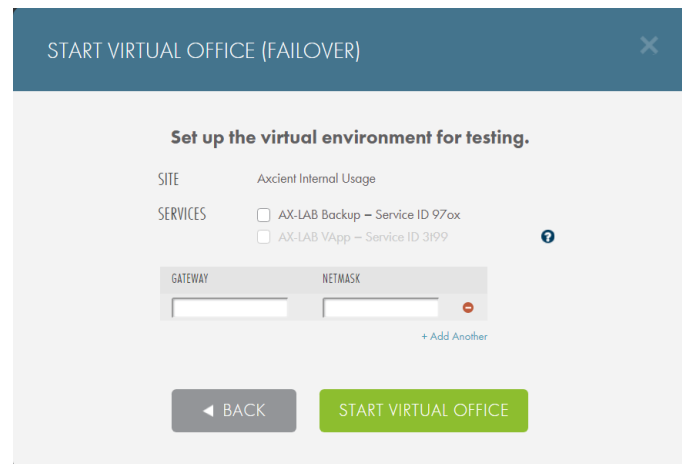
STEP 6

Select the services you would like to fail over and configure the network settings.

When configuring the network settings for the Virtual Office, the gateway should be the same as the default gateway on the physical network that the Virtual Office is trying to replicate.

Example: If all the devices are on the 192.168.1.xxx network, the gateway will most likely be 192.168.1.1.

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



The Virtual Office Page

The *Virtual Office* page is accessible when a Virtual Office has been started. This page is the administrative page for the Virtual Office. From here, you can take any managerial and configuration actions for the Virtual Office.

There are five main sections to the Virtual Office View page:

1 Virtual Office Summary

This section provides a 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 and take steps to discard the Virtual office.

2 Device List

This section displays all protected devices under the Client as well as the device states. The three device states are explained below.

3 Configure Office

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

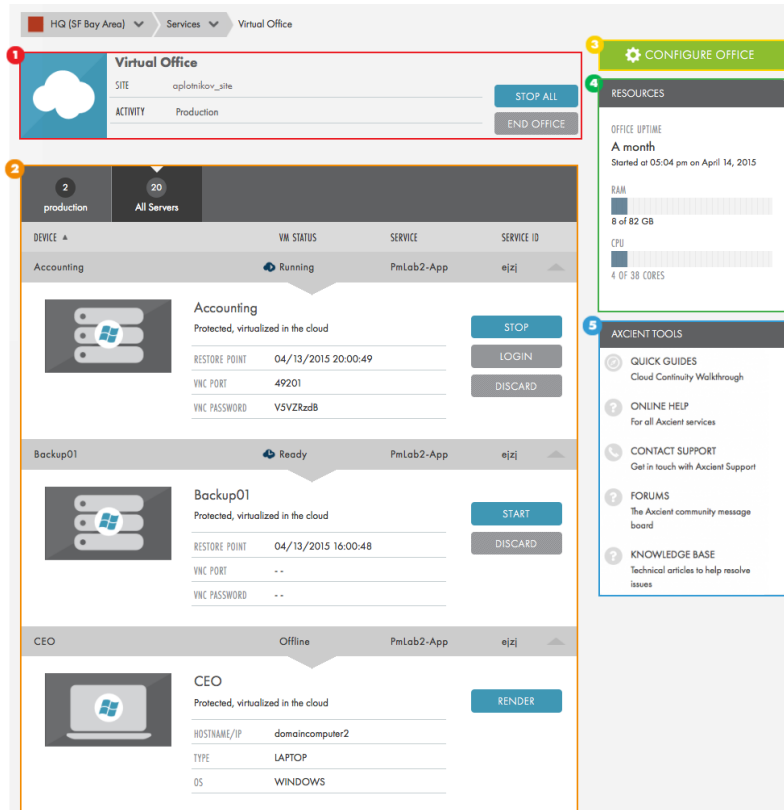
4 Resources

This section displays used and available resources across all live VMs, and information about how long the Virtual Office has been running.

5 Axcient Tools

This section displays links to Axcient support documentation and Axcient Technical Support.

Figure 21 - Virtual Office Page



Virtual Machine States

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

- The **Offline** state indicates that the VMs have yet to be rendered. To render a device, click the **Render** button.
- The **Ready** state indicates that the VMs have been rendered. This means that you have allocated CPU cores and RAM to the VM. You can optionally click the **Start** button to start a device and make it accessible.
- The **Running** state indicates that the VMs are live and accessible. You can optionally click the **Stop** button to return the device to a *Ready* state, log in to access the VM, or click the **Discard** button to return the device to an *Offline* state.

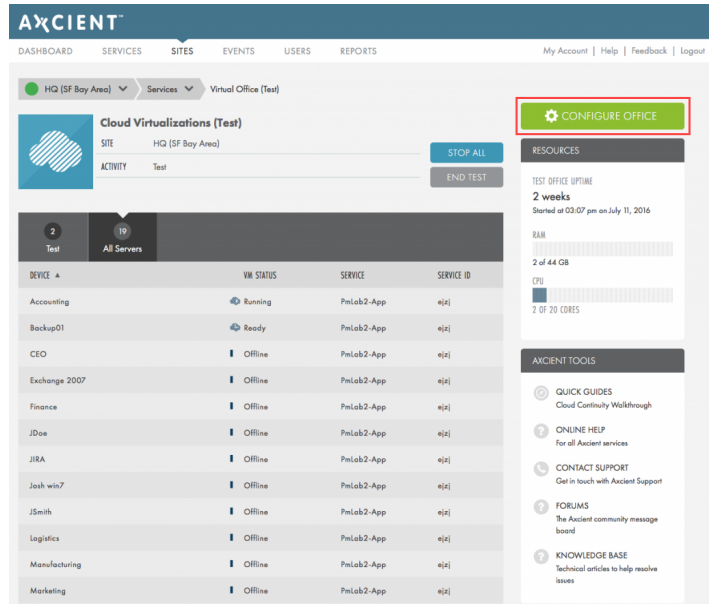
Configure Virtual Office

While inside the Virtual Office, you can configure the cloud failover environment as needed. To configure these options:

STEP 1

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

On the *Configure: Virtual Office* page, you can configure the various network options.



Network Settings

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

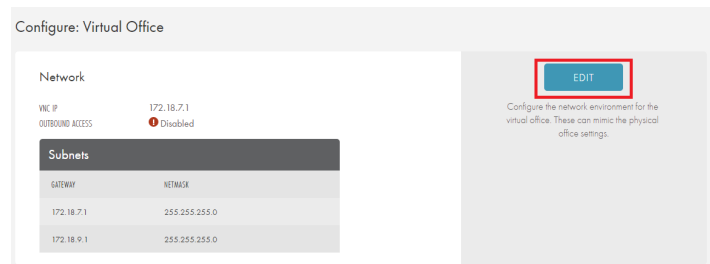
Please note the following restrictions related to subnets:

- You can add no more than ten subnets.
- Subnets must not overlap with each other.
- The DHCP IP range should be determined from one subnet.
- Port forwarding IPs should fall within one of the subnets.

To edit the network settings:

STEP 1

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

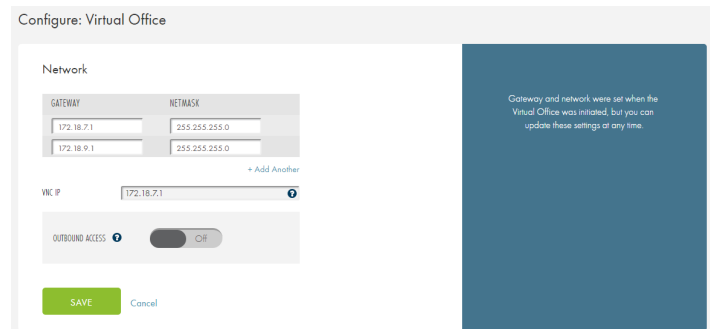


STEP 2

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

- In the *Gateway* field, enter a **gateway IP address**.
- In the *Netmask* field, enter the **netmask value**.
- Optionally, click the **+Add Another** link to add an additional subnet. Please note that you can add up to ten subnets. Subnets must not overlap with other subnets on the Virtual Office. To delete a subnet, hover your mouse over the appropriate row and click the red **Delete** icon.
- Optionally, in the *VNC IP* field, enter the **IP address** for the VNC clients, which can be any available (unused) IP address in the Virtual Office. VNC clients typically use the Virtual Office Gateway address, so a separate IP address is not necessary. However, when testing a Cloud Failover while the original gateway is still active, an alternative IP address should be specified.
- Optionally, enable the *Outbound Access* option to allow outbound access to the Internet. Enabling this option allows both outbound and inbound messages between external devices and the server VMs in the Virtual Office. Disabling outbound access means that only devices within the Virtual Office can communicate with each other.

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

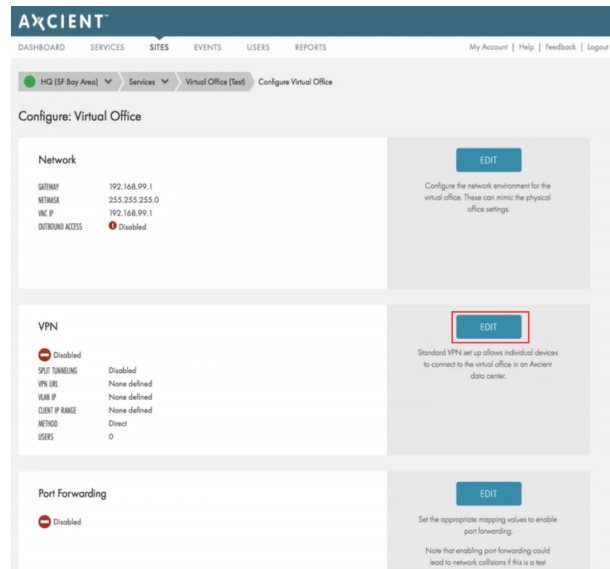


Virtual Private Network (VPN) Settings

To configure or edit VPN settings:

STEP 1

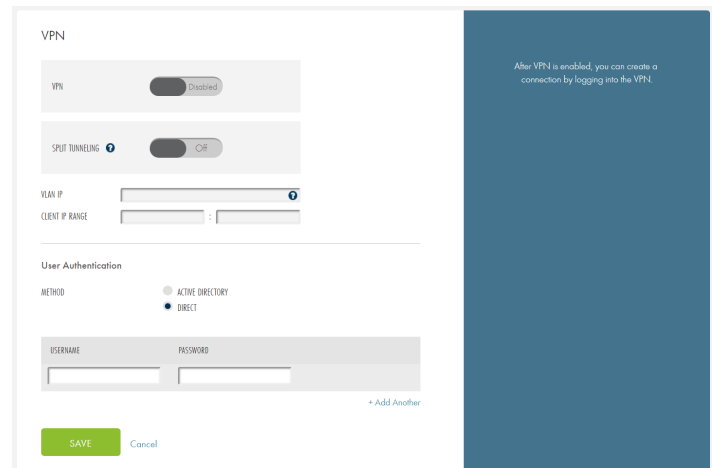
On the *Configure: Virtual Office* page, click the **Edit** button in the VPN section.



STEP 2

In the *VPN* section of the screen, enter a value for one or more of the following fields:

- Enable the *VPN* setting to turn on VPN.
- Enable the *Split Tunneling* setting to route the VPN user’s Internet access through their device. Alternatively, disable to route all Internet traffic through the Virtual Office.
- In the *VLAN IP* field, enter the **IP address** that gets assigned to the virtual network interface inside the failover network. This address *must* be an unused IP address.
- In the *Client IP Range* field, enter the **range of available IP addresses** that are assigned to connecting VPN users. This range must not conflict with any devices in the Virtual Office.
- In the *User Authentication* section of the screen, select the preferred method of **VPN authentication**.

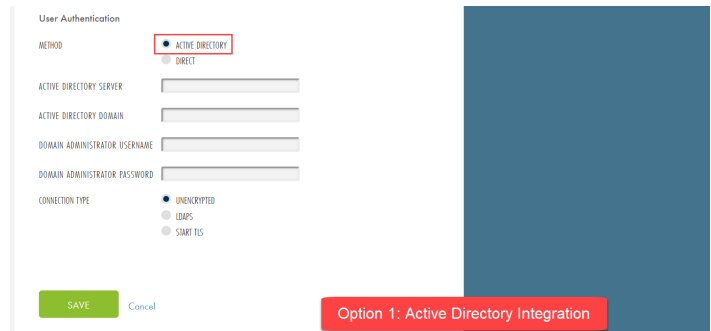


STEP 3a

Click the **Active Directory** radio button to integrate with Active Directory, which enables users to connect through VPN using their known Active Directory credentials. If you select this option, you will be prompted to configure the following fields:

- In the *Active Directory server* field, enter the **IP address** of the Active Directory server.
- In the *Active Directory Domain* field, enter the **domain name** of the Active Directory server.
- In the *Domain Administrator Username* field, enter the **username** of the Active Directory administrative user.
- In the *Domain Administrator Password* field, enter the **password** of the Active Directory administrative user.
- In the *Connection Type* field, use the radio buttons to select your preferred connection type, including: **Unencrypted**, **LDAPS**, or **Start TLS**.

Please note that if you select *LDAPS* or the *Start TLS* method, you must also configure the *Active Directory Certificate Services* role on the domain controller. For more information, please reference the [**Configuring Active Directory Certificate Services Settings**](#) section below.

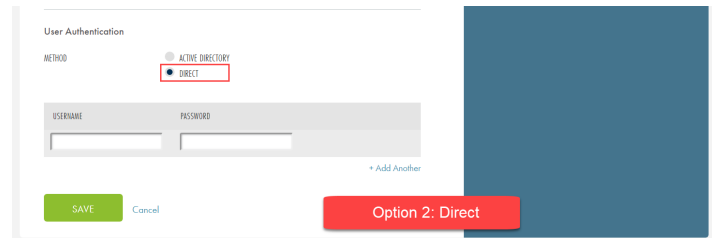


STEP 3b

Alternatively, in the *User Authentication* section of the screen, click the **Direct** radio button to manually create login credentials for users to connect through VPN. If you select this option, you will be required to configure the following fields:

- In the *Username* field, enter a **username** needed for users to connect through VPN.
- In the *Password* field, enter a **password** needed for users to connect through VPN.

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



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:

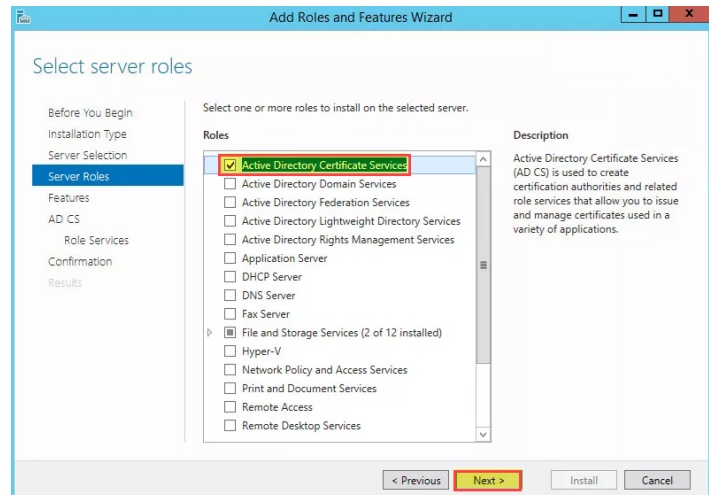
STEP 1

On the domain controller, start the *Service Manager* and select **Add Roles and Features**. The *Add Roles and Features Wizard* displays.



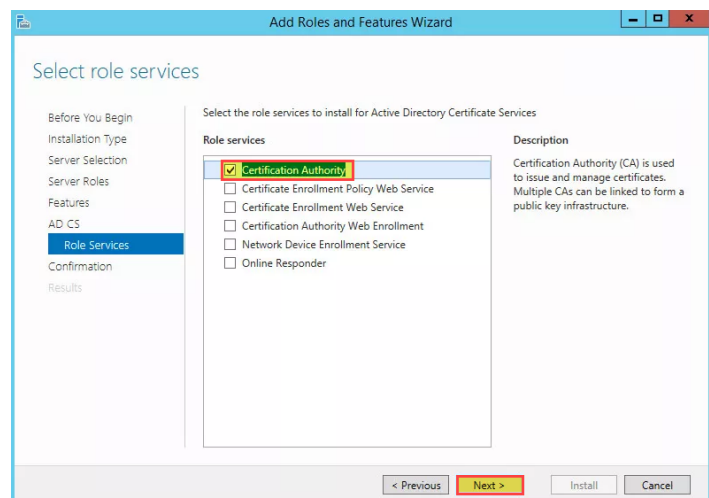
STEP 2

In the Wizard, click the series of **Next** buttons until you reach the *Select server roles* screen. On the *Select server roles* screen, click the **Active Directory Certificate Services** checkbox and then click the **Next** button to continue.



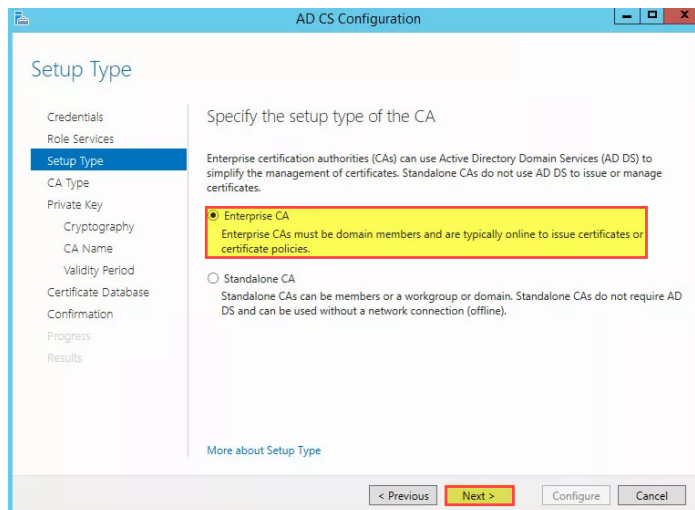
STEP 3

Continue through the Wizard until you reach the *Select role services* screen. On the *Select role services* screen, click the **Certification Authority** checkbox and then click the **Next** button to continue.



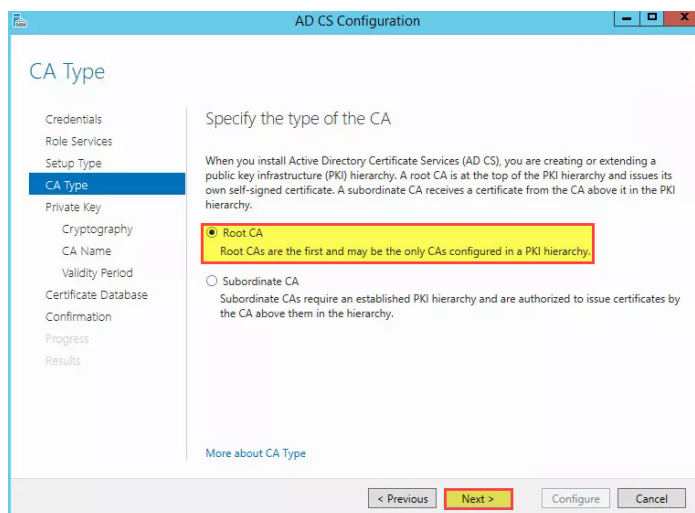
STEP 4

On the *Setup Type* screen, click the **Enterprise CA** radio button and then click the **Next** button to continue.



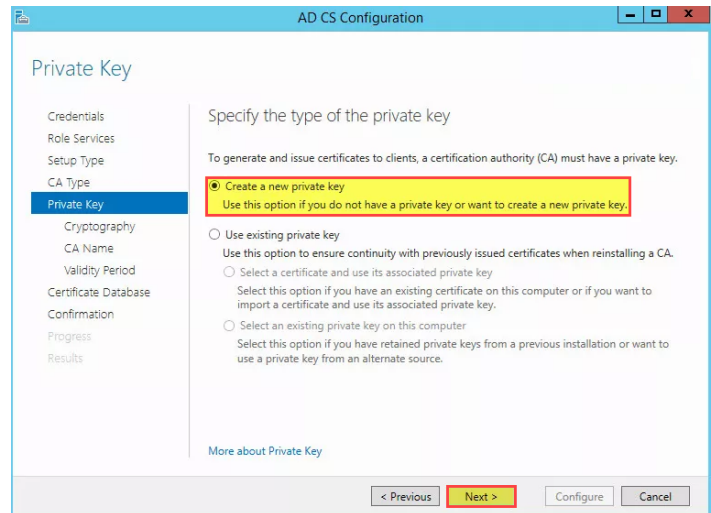
STEP 5

On the *CA Type* screen, click the **Root CA** radio button and then click the **Next** button to continue.



STEP 6

On the *Private Key* screen, click the **Create a new private key** radio button and then click the **Next** button to continue.

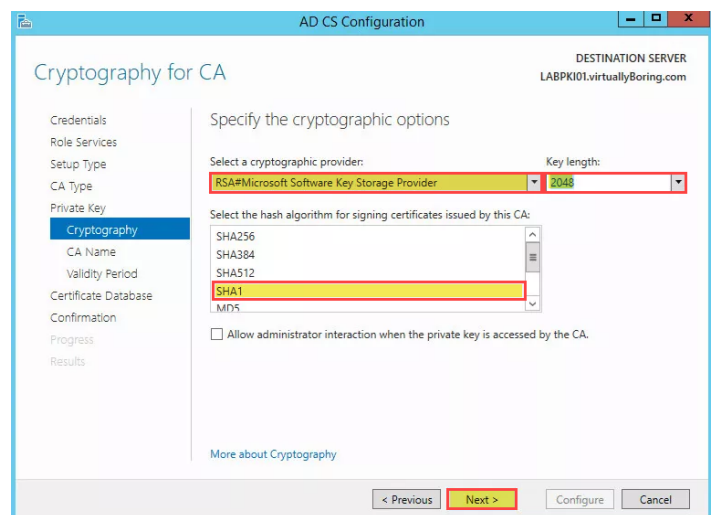


STEP 7

On the *Cryptography for CA* screen, configure the following settings:

- In the *Select a cryptographic provider* drop-down menu, select **RSA #Microsoft Software Key Storage Provider**.
- In the *Key length* drop-down menu, select **2048**.
- In the *Select the hash algorithm* scroll-down menu, select **SHA1**.

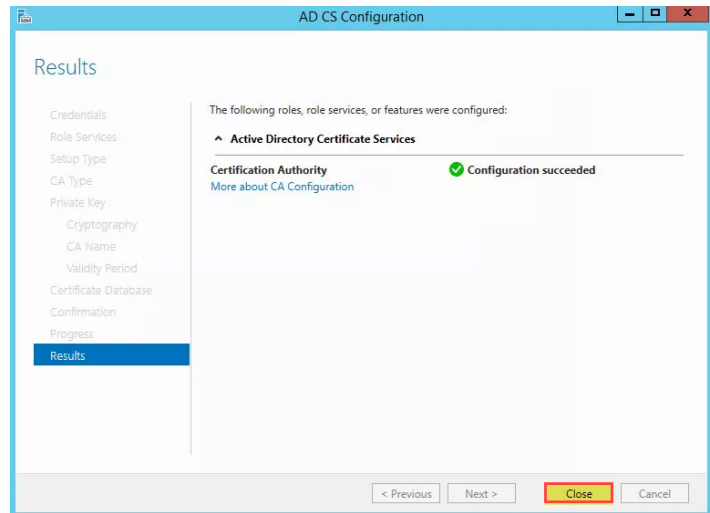
Click the **Next** button to continue.



STEP 8

On the *CA Name* screen, configure settings for the certificate authority (CA). Click the **Next** button to continue.

Continue through the Wizard until you successfully configure the *Active Directory Certificate Services* role, and then click the **Close** button when you are finished.



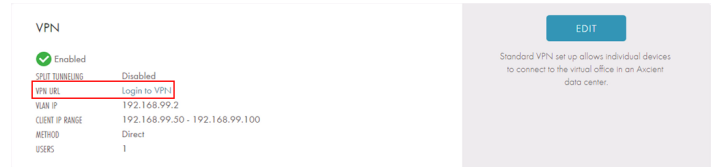
For alternative instructions, please reference the [LDAP over SSL \(LDAPS\) Certificate](#) Microsoft TechNet article.

Connecting to 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.

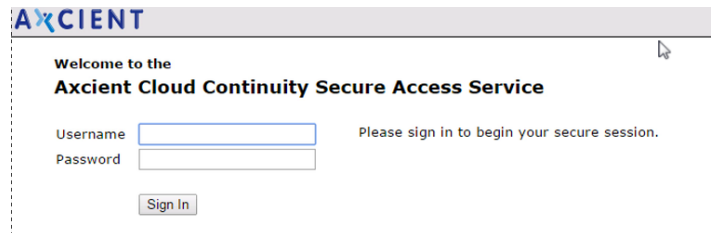
STEP 1

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



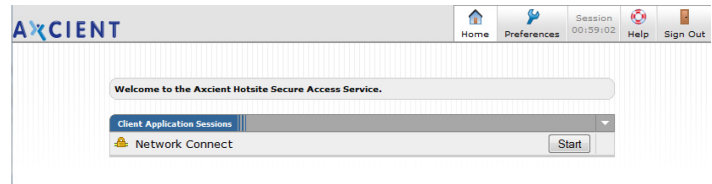
STEP 2

On the *VPN Access* page, enter login credentials. These are the same credentials created in the *User Authentication* field on the *VPN* screen.



STEP 3

After logging in, click the **Start** button to connect to the VPN and follow the prompted connection steps.



Note

The latest version of Java *must* be installed. If not already done so, you will be prompted to download a java plug-in that is required to complete the VPN connection process. If you are prompted to download the plug-in, install the plug-in and then begin the VPN connection process from the beginning.

If your browser blocks Java applets, you can connect through an alternative VPN client, such as the Windows 10 (built-in) VPN client. For more information, please reference the [Axcient Recovery Guide](#).

Port Forwarding

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

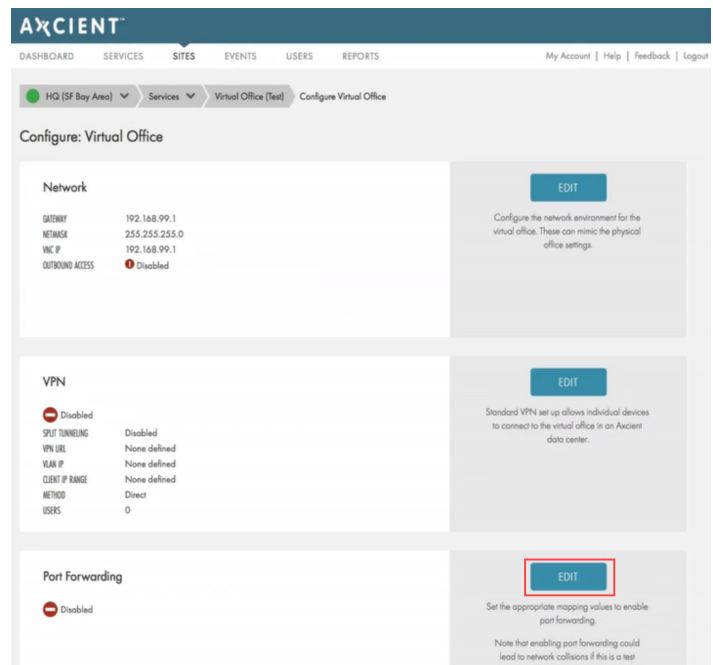
Enabling port forwarding could lead to network collisions if configured on a test Virtual Office. Do *not* enable and configure port forwarding for a test Virtual Office as productivity and data loss might occur.

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.



STEP 2

On the *Port Forwarding* screen, update the following fields:

- Enable the *Port Forwarding* option.
- Enter the appropriate values to set the port forwarding rules:
 - In the *Ext Port* field, enter the **external port number** to be forwarded.
 - In the *Internal IP* field, enter the **internal IP address**. The internal IP address must fall inside one of the Virtual Office's subnets.
 - In the *Int Port* field, enter the **internal port number**.
- Click the **Add Another** button to add additional entries. Repeat these steps as many times as necessary.

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

Port Forwarding

PORT FORWARDING Disabled

Public IP: None Assigned

EXT PORT	INTERNAL IP	INT PORT
<input type="text"/>	<input type="text"/>	<input type="text"/>

+ Add Another

Public IP: None Assigned

EXT PORT	INTERNAL IP	INT PORT
<input type="text"/>	<input type="text"/>	<input type="text"/>

+ Add Another

SAVE Cancel

CAUTION

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

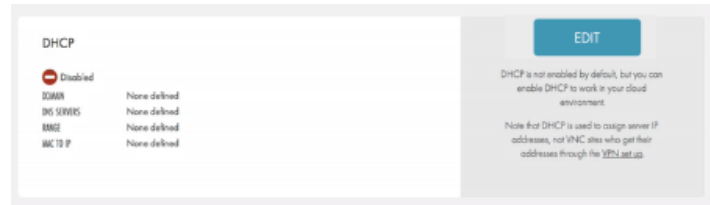
DHCP Settings

DHCP is not enabled by default but can be configured to work in the Virtual Office environment. Please note that the DHCP applies only to virtualized devices and not for remote user IP addresses that are assigned through the [VPN settings](#).

To configure or edit the DHCP settings:

STEP 1

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



STEP 2

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

- Enable the *DHCP* option.
- In the *Domain* field, enter the **domain name**.
- In the *DNS Servers* field, enter the **host name** or IP address of the DNS server. Click the **Add Another** button to add additional DNS servers.
- In the *Range* field, enter a **range of IP addresses** that can be used by the DHCP. The range must reside inside one of the Virtual Office's subnets.
- Optionally, in the *MAC to IP* field, assign an **IP address** to a server by entering the MAC address and the desired IP address.
- Click the **Add Another** button to add more entries.

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

DHCP

DHCP Disabled

DOMAIN

DNS SERVERS + Add Another

RANGE :

MAC TO IP : + Add Another

SAVE Cancel

Note that DHCP is used to assign server IP addresses, not VNC clients who get their addresses through the VPN set up.

Site to Site Open VPN Settings

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

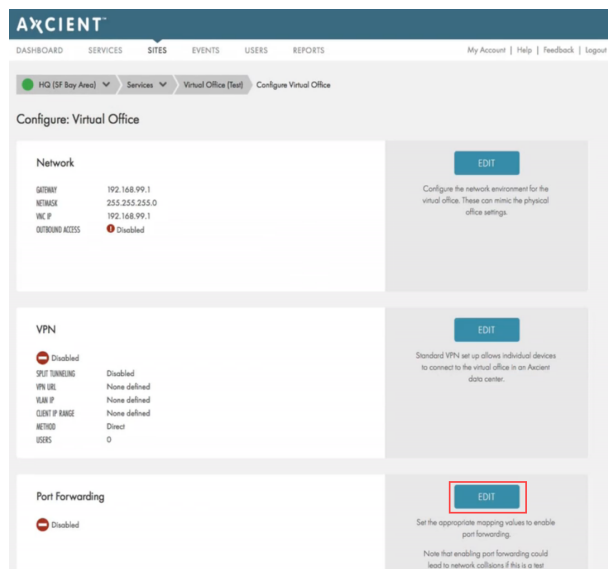
Using Site to Site Open VPN is not recommended in a test environment. However, during a disaster, it can provide valuable services in the following situations:

- 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 recreates the corporate network for the unavailable physical site.
- When a site is being rebuilt after a disaster and users can physically use the site itself, but not the servers. A Site-to-Site VPN connection can be configured as a replacement while the servers are being rebuilt.

For the Site to Site Open VPN feature to work, Port Forwarding must be enabled. When it is enabled, you can continue to configure the Site to Site Open VPN.

STEP 1

Enable the Port Forwarding feature according to the instructions listed in the [Port Forwarding](#) section.



STEP 2

After Port Forwarding has been enabled, click the **Edit** button in the *Site to Site Open VPN* section.

STEP 3a

In the *Site to Site Open VPN* section, update the following fields:

- Enable the *Site to Site Open VPN* option.
- Optionally, in the *Whitelisted IPs* field, add an **IP address** that can access the Virtual Office. Only IP addresses from this list can access the Virtual Office. Click the **Add Another** button to whitelist additional IP addresses.
- Click the **Save** button when you are finished entering whitelisted IPs.

The screenshot shows the 'Site-To-Site VPN' configuration page. At the top, there is a 'Site-To-Site VPN' header with a 'Disabled' status indicator and a 'Whitelisted IPs' field currently set to 'None'. A 'SAVE' button is visible below the field. To the right, a text box explains that Site-to-site VPN allows creating a single VPN end point within a local network to connect to a virtual office in the cloud, and includes a caution about not recommending it in a test environment.

This screenshot shows the 'Site-To-Site VPN' configuration page with the 'Site-to-site VPN' toggle turned 'On'. Below it, the 'Whitelisted IPs' field is empty, and an 'Add Another' button is present. The 'Endpoint 1' configuration form is expanded, showing fields for 'Endpoint Name' (with a hint 'i.e. Main Office'), 'Key Password' (marked as optional), 'Configured Using' (with radio buttons for 'Static IP' and 'DHCP'), 'Gateway', 'Netmask', 'IP of Endpoint', and 'DNS'. An 'Add Endpoint' button is at the bottom of the form, and a 'DONE' button is at the bottom of the page. To the right, a text box explains the purpose of Site-to-site VPN and provides a two-step process for disaster recovery: 1. Recreate the corporate network for an unavailable physical site, and 2. Temporarily replace a connection while the machine room and servers are rebuilt.

STEP 3b

In the *Endpoint* section, update the following fields:

- In the *Endpoint Name* field, enter the desired **name for the Endpoint**.
- Optionally, in the *Key Password* field, set a **password** for the SSL RSA key. If configured, this password will be required to log in to the VPN.
- In the *Configuring Using* section, use the radio buttons to select whether to configure using a **Static IP address** or **DHCP**.
- In the *Gateway* field, enter the **gateway IP address**.
- In the *Netmask* field, enter the **netmask** value.
- In the *IP of Endpoint* field, enter the **IP address of the Endpoint** (static IP address only). This address should be on a different subnet than that of the Virtual Office. For example, if the Virtual Office IP address is 192.168.99.2, configure the endpoint address to 172.168.22.2.
- In the *DNS (Static IP Only)* field, enter the **IP address of the DNS server**.
- Once configured correctly, click the **Add Endpoint** button, or click the **Done** button.

Site-to-site VPN allows you to create a single VPN endpoint 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 servers are rebuilt after a disaster in which users can physically use the site but the machine room is still under repair.

STEP 4

When *Site-to Site VPN* settings are configured, click the **Download Client** link to download the virtual image. This image should be deployed at the desired location using any VMware virtual machine software.

When the virtual machine is deployed, all local devices must have their gateway changed to the *IP address of the endpoint*.

Site-To-Site VPN

Enabled

WHITELISTED IPS 44.22.55.68

yaav1		Download Client
KEY PASSWORD	*****	
CONFIGURED USING	Static IP	
GATEWAY	172.16.22.1	
NETMASK	255.255.255.0	
IP OF ENDPOINT	172.16.22.2	
DNS	8.8.8.8	

EDIT

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.

Note

When the VM endpoint is powered on, a console window will print out a message acknowledging the Open VPN connection. A message will also appear with network instructions to reconfigure the host machine on which the VM endpoint is being deployed. If you do not see these console windows, please visit www.axcient.com/support for additional resources.

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
```

IPSec Site to Site VPN Settings

The Internet Protocol Security (IPSec) Site to Site VPN feature allows you to establish IPSec VPN tunnels from the Virtual Office in the Axcient Cloud to any standard compliant IKEv2 IPSec VPN gateway on your local network. Specially, you can use this feature during a site disaster to:

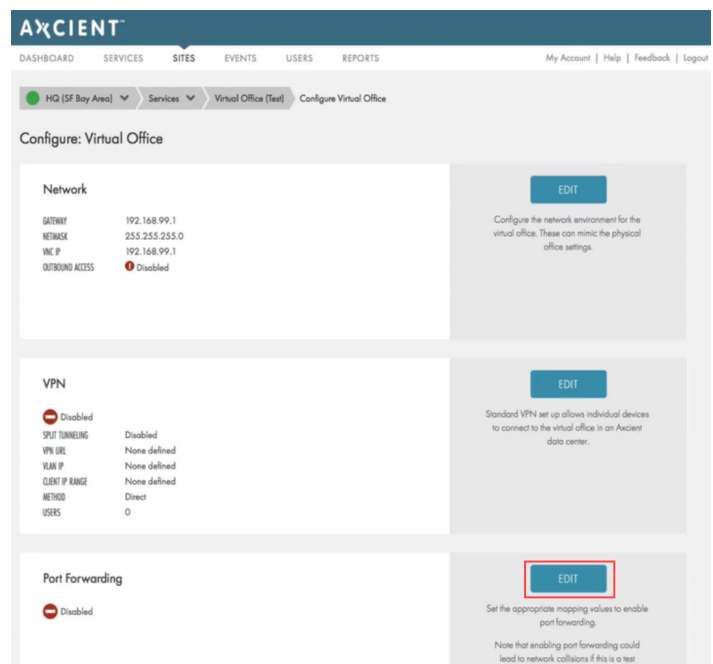
- Recreate the network in an organization with two or more sites linked together in a corporate network
- Temporarily replace a connection while a machine room is rebuilt after a disaster

Note: IPSec Site-to-Site VPN is not recommended in a test environment.

To set up an IPSec Site-to-Site VPN connection, you must turn on the feature in your Virtual Office and also configure settings on your gateway.

STEP 1

Enable the Port Forwarding feature according to the instructions listed in the [Port Forwarding](#) section.



STEP 2

After Port Forwarding settings have been configured, navigate to the *Site to Site IPSec VPN* section and click the **Edit** button. You can configure the following options:

- Click the **S2S IPSec** option to enable Site to Site IPSec VPN settings.
- In the *Site Public IP* field, enter the **public IP address** of the remote machine or hardware with IPSec software (for example, Cisco ASA).
- In the *Site Local Subnets* section, enter the **remote subnets** and associated **netmasks** for sharing with the Virtual Office subnets. Please note that these subnets do not need to intersect with the Virtual Office subnets.

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

Site to site IPSec VPN

S2S IPSEC Enabled

SITE PUBLIC IP

SITE LOCAL SUBNETS

SUBNET IP	NETMASK
<input type="text" value="172.20.17.0"/>	<input type="text" value="255.255.255.0"/>
<input type="text" value="172.20.19.0"/>	<input type="text" value="255.255.255.0"/>

[+ Add Another](#)

Gateway Settings

You can connect with any standard compliant IKEv2 IPSec VPN gateway.

Example 1: Configure IPSec on Debian Using strongSwan

When you configure IPSec Site to Site VPN settings using strongSwan, we recommend using *strongSwan version 5.2.1 or later*. Please reference the official [strongSwan](#) documentation for more information and additional configuration options.

1. Install strongSwan on Debian 8+.

```
$ sudo apt-get update
$ sudo apt-get install strongswan
```

2. Alternatively, install strongSwan on Debian 7, ensuring `/etc/apt/sources.list` contains following lines:

```
deb http://deb.debian.org/debian wheezy main
deb http://deb.debian.org/debian wheezy-backports main
```

Install strongSwan on Debian 7:

```
$ sudo apt-get update
$ sudo apt-get install libstrongswan=5.2.1-6+deb8u2~bpo70+1
strongswan-starter=5.2.1-6+deb8u2~bpo70+1 strongswan=5.2.1-
6+deb8u2~bpo70+1
```

3. Insert the secret key into the `/etc/ipsec.secrets` file.

```
: PSK <Secret Key>
```

4. Insert settings into the `/etc/ipsec.conf` file, where *left IP* refers to the local IP address where IPSec traffic is listened and *right IP* refers to the Virtual Office public IP.

```
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2
    authby=secret
    ike=aes256-sha1-modp1536,aes256-sha384-modp1536,aes256-sha256-
modp1536,aes256-sha384-modp2048!
    esp=aes256-sha1-modp1536
    mobike=no
    left=<left IP>
    leftsubnet=172.20.17.0/24,172.20.19.0/24
    leftid=@office
    leftfirewall=yes
    auto=start
    type=tunnel
conn 9192aff1-a4ee-4d92-a03a-f63757be083c
    right=<right IP>
    rightsubnet=172.18.7.0/24
conn 131c97ba-745b-4e3b-8347-2ef4aea245dd
    right=<right IP>
    rightsubnet=172.18.8.0/24
```

5. Enable IP forwarding.

```
$ sysctl net.ipv4.ip_forward=1
```

6. Apply IPSec settings.

```
$ ipsec restart
```

7. Test your configuration settings by trying to access the Virtual Office subnets.

Example 2: Configure IPSec on Cisco ASA

When you configure IPSec Site to Site VPN settings using Cisco ASA, please reference Cisco [configuration examples 1](#) and [configuration example 2](#) for additional information and instructions.

1. Configure IPSec Site to Site settings on your Cisco ASA device. In this example, please note the following:
 - *172.20.17.0/24* refers to the the network behind Cisco ASA
 - *172.18.7.0/24* refers to the remote network (e.g. inside of Virtual Office)
 - *162.22.33.44* refers to the public IP of remote gateway (the Virtual Office gateway)
 - *port1* refers to the outside port of Cisco ASA

```
object network local
    subnet 172.20.17.0 255.255.255.0
object network virtual_office
    subnet 172.18.7.0 255.255.255.0
access-list port1_cryptomap extended permit ip 172.20.17.0
255.255.255.0 172.18.7.0 255.255.255.0
crypto ipsec ikev2 ipsec-proposal aes256-sha256
    protocol esp encryption aes-256
    protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal aes256-sha384
    protocol esp encryption aes-256
    protocol esp integrity sha-384 sha-1

crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
crypto map port1_map 1 match address port1_cryptomap_1
crypto map port1_map 1 set peer 162.22.33.44
crypto map port1_map 1 set ikev2 ipsec-proposal aes256-sha256
aes256-sha384
crypto map port1_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_
```

```
CRYPTO_MAP
crypto map port1_map interface port1
crypto ikev2 policy 1
    encryption aes-256
    integrity sha
    group 5 2
    prf sha
    lifetime seconds 86400
crypto ikev2 enable port1
group-policy GroupPolicy_162.22.33.44 internal
group-policy GroupPolicy_162.22.33.44 attributes
    vpn-tunnel-protocol ikev2
tunnel-group 162.22.33.44 type ipsec-l2l
tunnel-group 162.22.33.44 general-attributes
    default-group-policy GroupPolicy_162.22.33.44
tunnel-group 162.22.33.44 ipsec-attributes
    ikev2 remote-authentication pre-shared-key <Secret key>
    ikev2 local-authentication pre-shared-key <Secret key>
```

2. In some instances, you might be required to add NAT rules:

```
nat (inside,port1) source static local local destination static
virtual_office virtual_office no-proxy-arp
```