

Axcient

BRC Recovery Guide

NOTICE

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

Axcient assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. This document contains information that is property of Axcient, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine-readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Axcient.

The information contained in this document is subject to change without notice.

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

Table of Contents

Introduction	4
Recovery of Encrypted Files	4
Foreign Characters Support	4
Unsupported Files	4
Deduplication	5
Granular File Restore (Local)	6
Granular File Restore (Cloud)	12
Bare Metal Restore	18
BMR to a Virtual Machine	24
Manual Partition	29
Discarding the Image Lock	32
Failover VM (Local)	34
Test VM Screen Shot Validation	34
Recovery Steps	34
Viewing the Local Failover Details	40
Accessing the Local Failover VM	42
Export to VMDK	45
Generating the .vmdk Files	45
VMDK Alert Messages	49
Creating the VM using Export to VMDK	51
Cloud Failover	59
Starting the Virtual Office	60
The Virtual Office Page	64
Configure Virtual Office	66
Network Settings	67
Virtual Private Network (VPN) Settings	69
Port Forwarding	80
DHCP Settings	82
Site to Site Open VPN Settings	83
IPSec Site to Site VPN Settings	86
Additional Failover Steps for Windows Server 2008 SP1	88
Failing Over a Device with 5+ Drives	89
Runbooks	90
Create a New Runbook	90

Start a Runbook 96
Edit a Runbook 98
Delete a Runbook 99

You can leverage Axcient's business continuity tools in the event of data loss or disaster. Axcient recommends you leverage the local appliance whenever possible to ensure the quickest recovery time possible. In the event the local appliance is not available, you can utilize Axcient's cloud disaster recovery and business continuity tools, including:

- Granular File Restore (Local and Cloud)
- Bare Metal Restore (BMR)
- Failover Virtual Machine (Local and Cloud)
- Export to VMDK

Recovery of Encrypted Files

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

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

Foreign Characters Support

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

Unsupported Files

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

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

An unsupported file is one of the following:

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

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

Before performing any recovery actions, please make sure that the `/dev` file has been excluded from the replication job by following the steps in the File Exclusion section of the [Axcient Protection Guide](#).

Deduplication

Axcient does not support deduplication for Windows 2012.

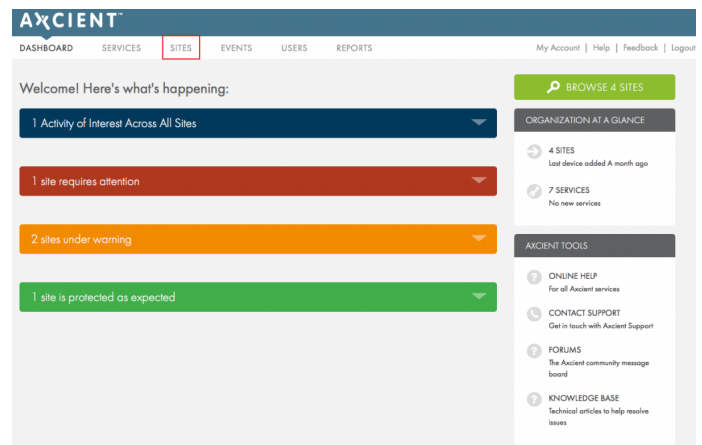
Fusion supports protection and recovery of encrypted files. You will be able to successfully recover encrypted data with the Fusion platform. Fusion is not currently compatible with external encryption solutions.

Granular File Restore (Local)

The local Granular File Restore recovery tool allows you to restore files, folders, and even entire directories from the local Axcient appliance. This process can be performed by clicking the **Recover** button where available on the Web Application. In this example, it will be performed from the *Site Details* page.

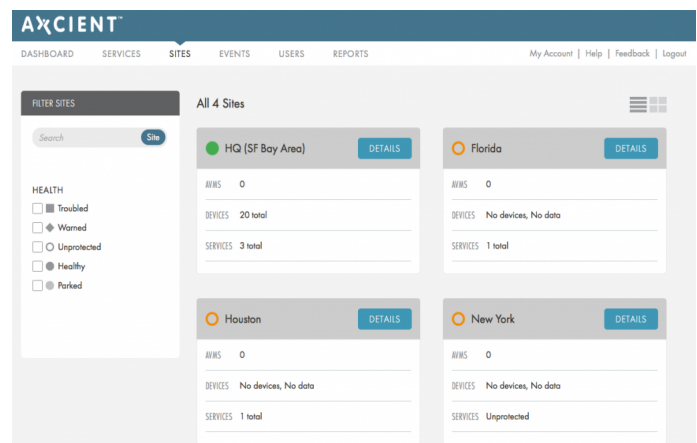
STEP 1

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



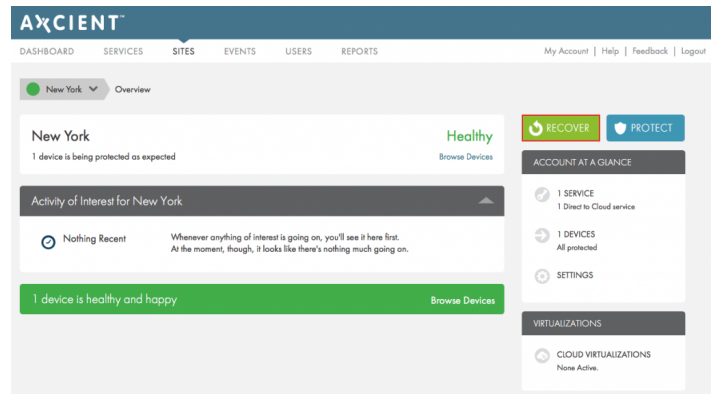
STEP 2

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



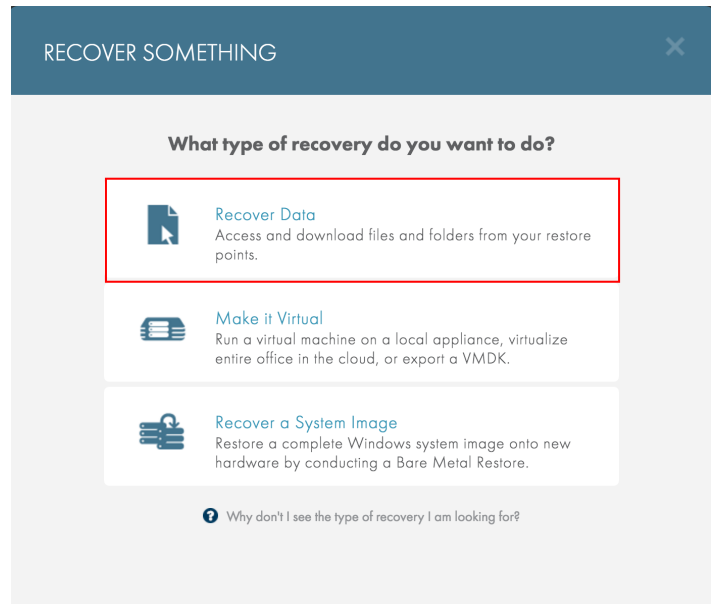
STEP 3

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



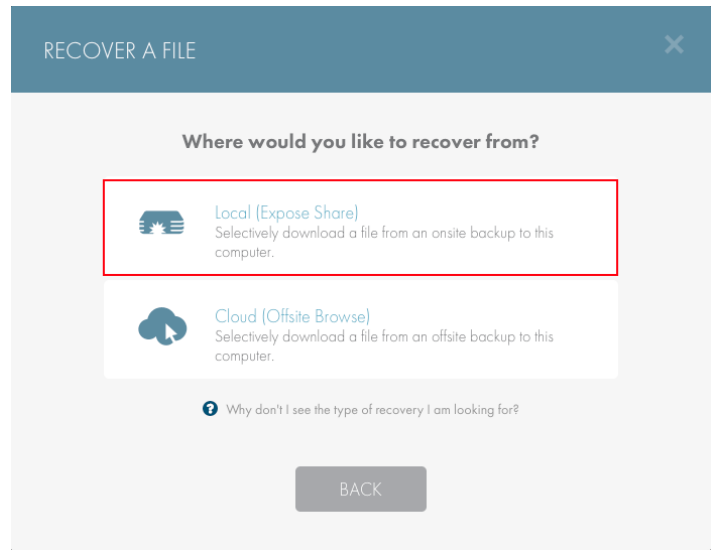
STEP 4

On the *Recover Something* screen, click the **Recover Data** button.



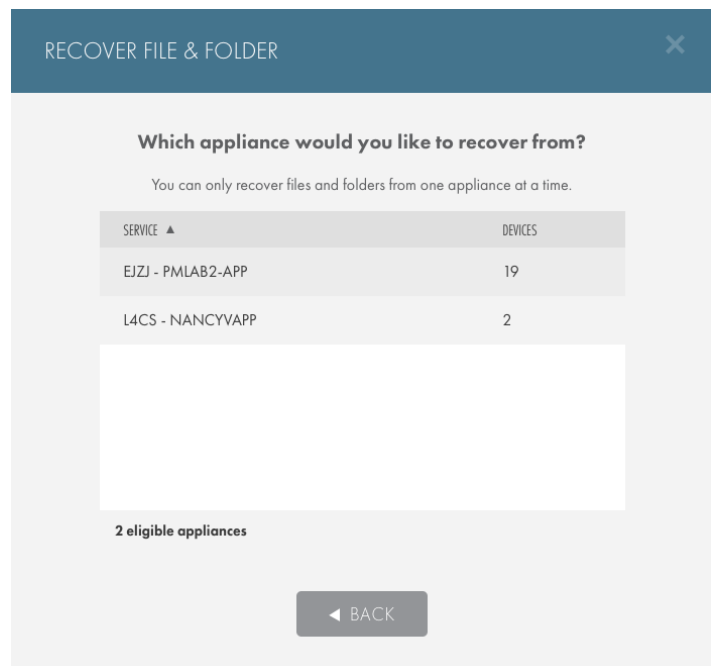
STEP 5

On the *Recover a File* screen, click the **Local (Express Share)** button.



STEP 6

Select the **Service** protecting the target device. If you are performing this step from the *Service Details* page or *Device Details* page, skip to the next step.



STEP 7

Select the device from which you would like to restore and click the **Next** button.

RECOVER FILE & FOLDER

Which device would you like to recover from?

You can only recover files and folders from one device at a time.

STATUS	DEVICE NAME ▲	DEVICE TYPE	APPLIANCE	LAST SUCCESSFUL ONSITE
●	Accounting	SERVER	PmLab2-App	2 hours ago
●	Backup01	SERVER	PmLab2-App	12 hours ago
●	CEO	LAPTOP	PmLab2-App	3 hours ago
●	Exchange 2007	SERVER	PmLab2-App	44 minutes ago
●	Finance	SERVER	PmLab2-App	2 hours ago

One eligible device [Why don't I see the device I'm looking for?](#)

BACK NEXT

STEP 8

Select the desired recovery point and click the **Recover** button.

The screenshot displays the 'RECOVER FROM ACCOUNTING' interface. At the top, there is a title bar with the text 'RECOVER FROM ACCOUNTING' and a close button (X). Below the title bar, the main content area is titled 'Select a point in time to recover from.' and includes a help icon and the text 'Why don't I see the recovery point I'm looking for?'. A date selector shows '12/29/2014'. Below this, a calendar view shows the days from DEC 26 to DEC 29, 2014. The days are labeled with their respective point counts: DEC 26 (6 Points), DEC 27 (6 Points), DEC 28 (6 Points), and DEC 29 (3 Points). The DEC 29 card is highlighted. Below the calendar, a vertical timeline shows three recovery points: 12:00 AM, 4:00 AM, and 8:01 AM. Each time point has a corresponding 'RECOVER' button. At the bottom of the interface, there is a 'BACK' button.

STEP 9

The UNC mount point is now generated. Copy and paste the generated path into the File Explorer to access the restored files.

Set the UNC mount expiration timer to give yourself enough time to complete the recovery actions.

The screenshot shows a dialog box titled "RECOVER FROM ACCOUNTING" with a close button in the top right corner. The main content area has a dark blue header with the text "Excellent! Here's the path to those files:". Below this is a blue document icon with a white arrow pointing right. A red box highlights the following text:

For Windows:
\\192.168.99.253\34-38-C+sessId-484c357a70094c649b097240bc604428

For Macs:
smb://192.168.99.253/34-38-C+sessId-484c357a70094c649b097240bc604428

Below the paths, there is a note: "Local recovery is achieved through a file, so you can get to the files directly on this computer by following the provided path. Note that it may take up to five minutes for the path to be operable." Another red box highlights the "Unmount share after:" section, which features a horizontal slider. The slider is positioned at the "24 HOURS" mark, with "1 HOUR" on the left and "7 DAYS" on the right. At the bottom of the dialog, there is a green "DONE" button and a link "Recover Something Else".

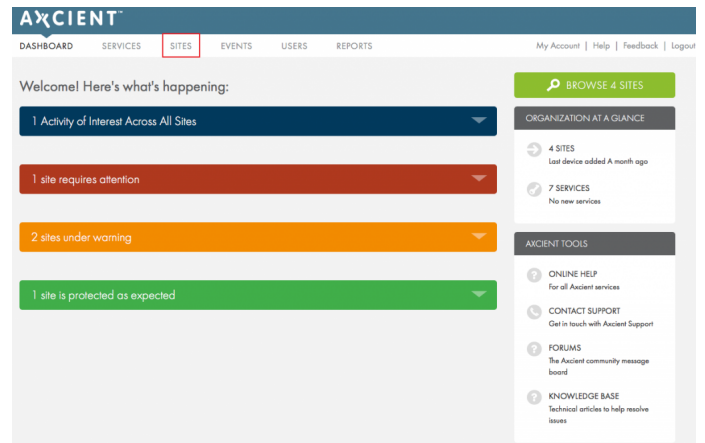
Granular File Restore (Cloud)

In the event the local appliance is not available, you can restore files and folders from the Axcient Cloud.

The selected files and folders will be downloaded locally to the device performing the recovery task. You will then be able to distribute the data as needed.

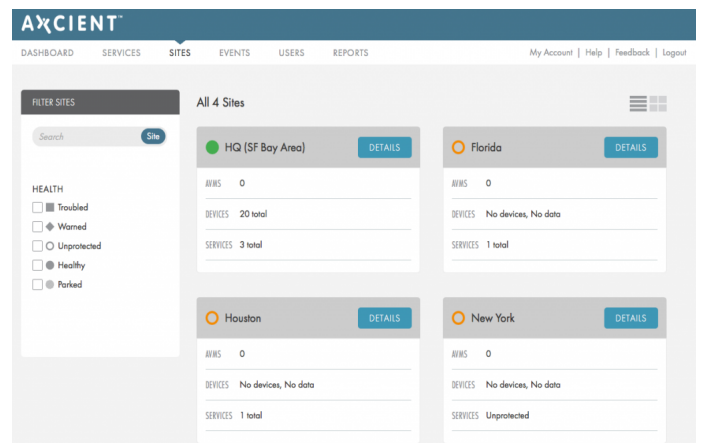
STEP 1

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



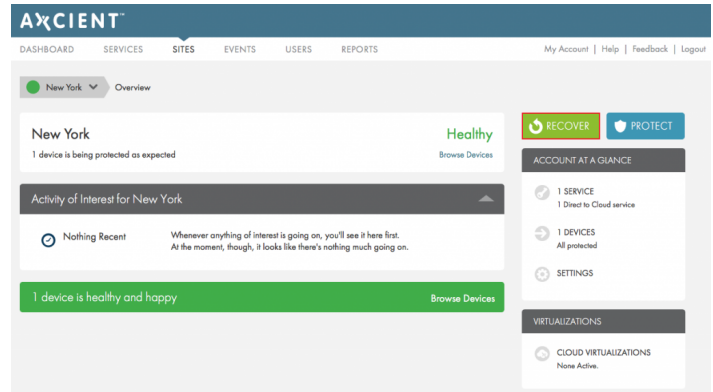
STEP 2

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



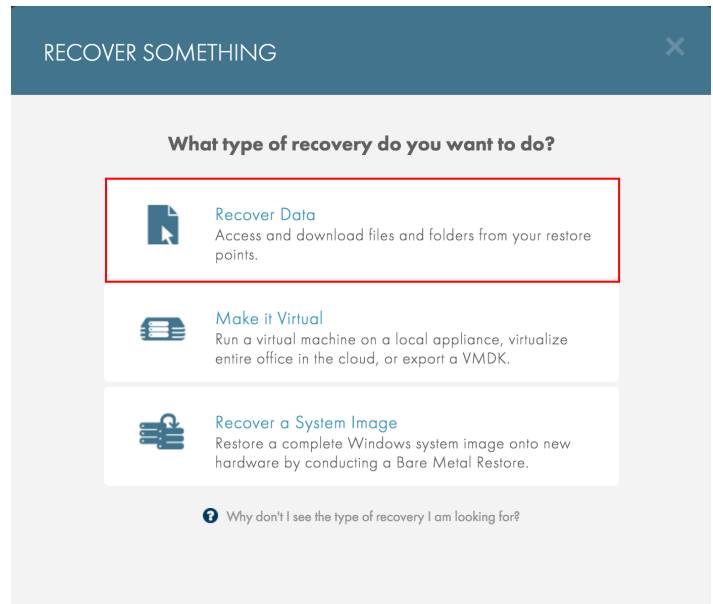
STEP 3

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



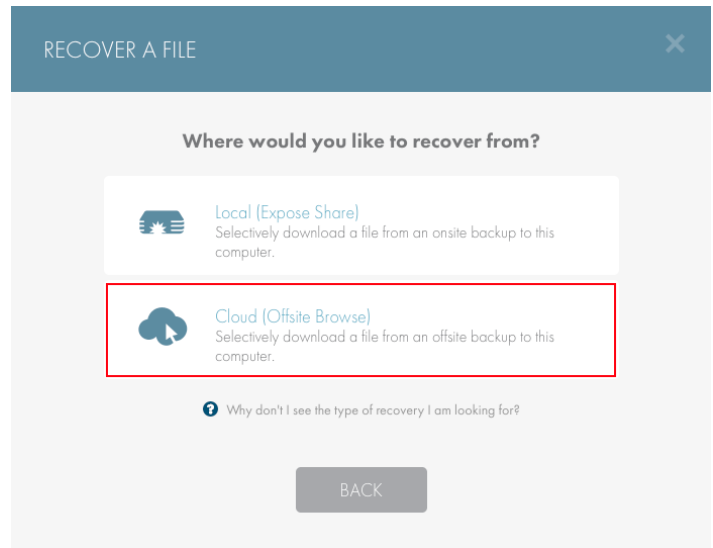
STEP 4

In the *Recover Something* screen, select the **Recover Data** button.



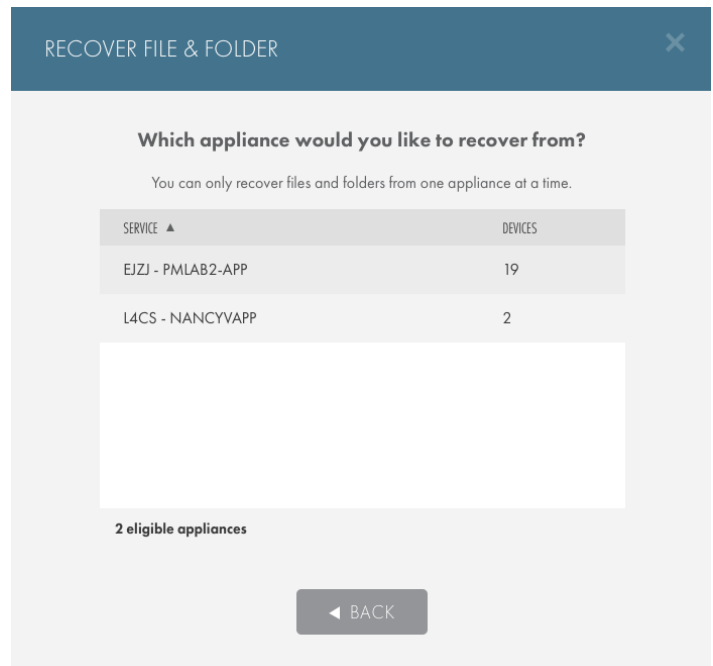
STEP 5

In the *Recover a File* screen, select the **Cloud (Offsite Browse)** option.



STEP 6

Select the **Service** protecting the target device. If performing this step from the *Service Details* page, or *Device Details* page, skip to the next step.



STEP 7

Select the device from which you would like to recover and click the **Next** button.

✕
RECOVER FILE & FOLDER

Which device would you like to recover from?

You can only recover files and folders from one device at a time.

STATUS	DEVICE NAME ▲	DEVICE TYPE	APPLIANCE	LATEST LOCAL RP
●	Accounting	SERVER	PmLab2-App	5 days ago
●	Backup01	SERVER	PmLab2-App	3 hours ago
●	CEO	LAPTOP	PmLab2-App	15 minutes ago
●	Exchange 2007	SERVER	PmLab2-App	4 hours ago
●	Finance	SERVER	PmLab2-App	An hour ago
●

19 eligible devices ? Why don't I see the device I'm looking for?

◀ BACK

STEP 8

Select the desired recovery point and click the **Recover** button.

The screenshot displays the 'RECOVER FROM ACCOUNTING' interface. At the top, there is a title bar with the text 'RECOVER FROM ACCOUNTING' and a close button (X). Below the title bar, the main content area is titled 'Select a point in time to recover from.' and includes a help icon and the text 'Why don't I see the recovery point I'm looking for?'. A date selector shows '12/29/2014' with a calendar icon. Below this, a calendar view shows the days of the month: DEC 26 (6 Points), DEC 27 (6 Points), DEC 28 (6 Points), and DEC 29 (3 Points). The 29th is highlighted with a blue arrow pointing down. Below the calendar, a vertical timeline shows three recovery points: 12:00 AM, 4:00 AM, and 8:01 AM. Each time point has a corresponding green 'RECOVER' button. At the bottom of the interface, there is a grey 'BACK' button.

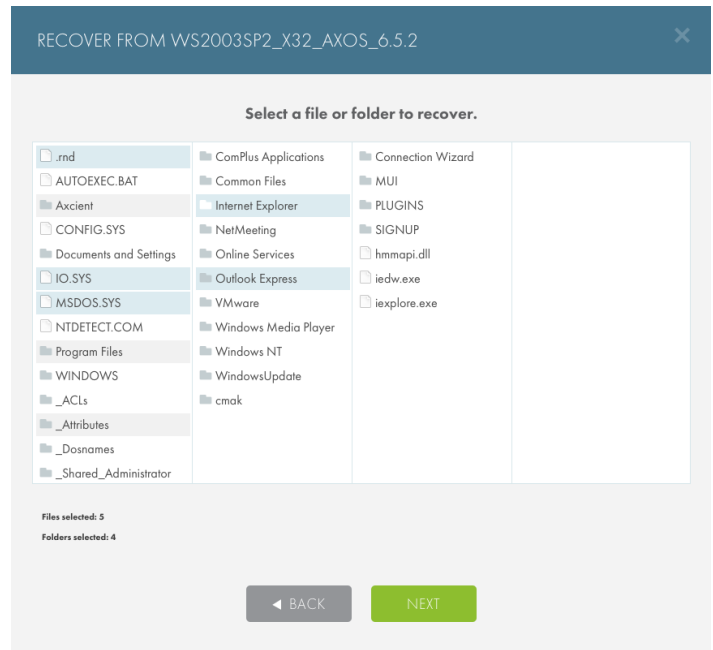
STEP 9

Select the files and folders to be restored.

Please note that selecting a file within a folder will only recover the selected file, not the containing folder.

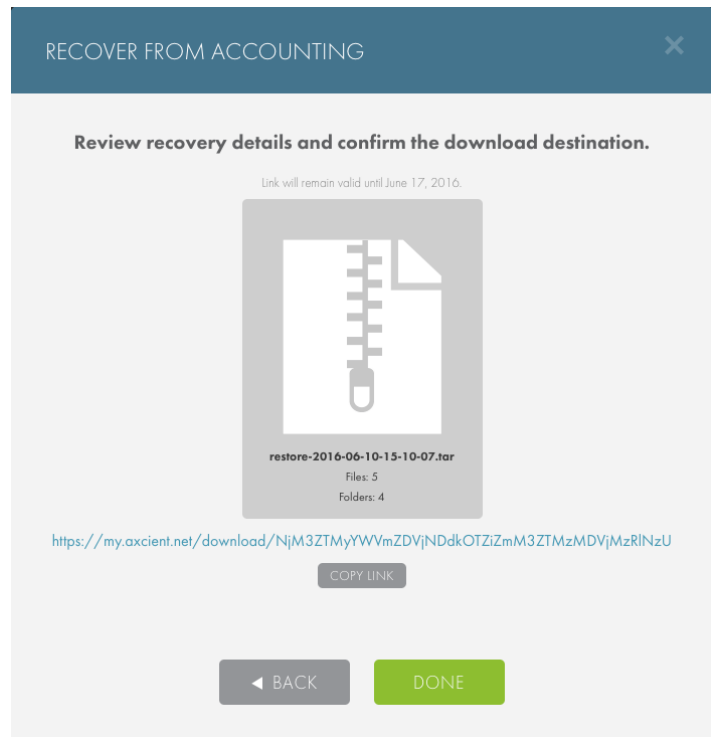
Reference the lower left-hand corner to view a tally of how many files and folders are being recovered.

Click the **Next** button when the target data has been selected.



STEP 10

Review the file recovery details and copy the URL. Paste this URL into a preferred browser to download the recovered data.

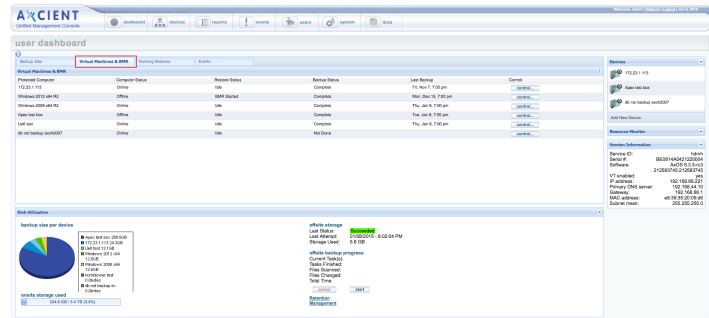


Bare Metal Restore

A Bare Metal Restore (BMR) allows you to apply a system image to new or existing devices rather than spending time and resources rebuilding an entire device.

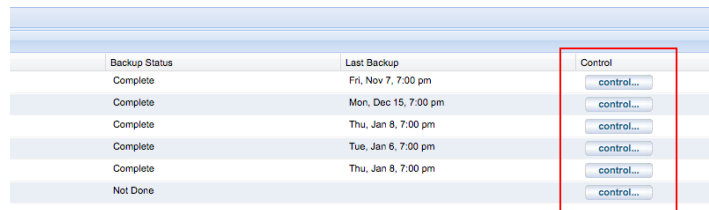
STEP 1

In the UMC Dashboard of the appliance protecting the desired device, click the **Virtual Machine & BMR** tab.



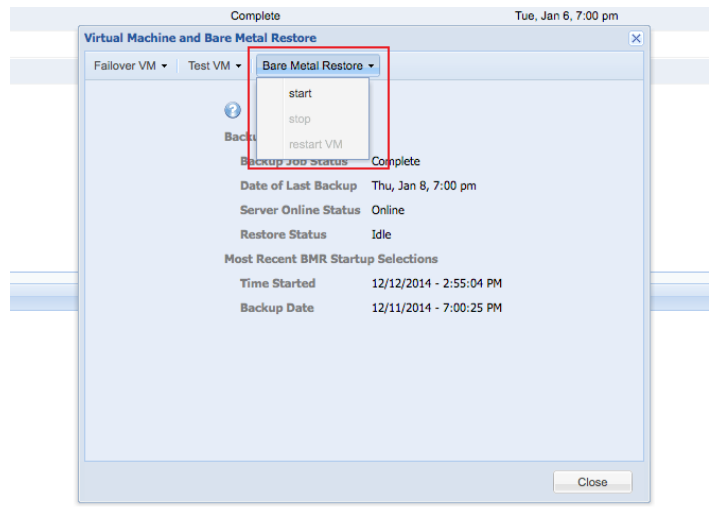
STEP 2

Click the **Control** button next to the appropriate device.



STEP 3

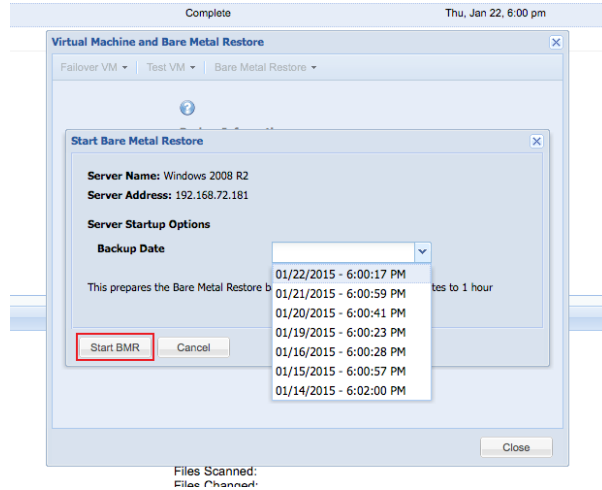
In the *Bare Metal Restore* drop-down menu, click **Start**.



STEP 4

Select the recovery point and click the **Start BMR** button.

You have now *locked the system* image for the BMR process.



STEP 5

On the [Downloads](#) page, download the appropriate BMR ISO to a bootable media.

To convert a USB to a bootable media, please refer to the [Format USB as BMR ISO Guide](#) for more information.

NOTE: If performing a BMR on an HP Proliant G9 device, you must use the *HP Proliant G9 BMR Boot ISO*. Otherwise, the BMR will not complete successfully.

Additionally, if device drivers need to be installed, add them to the bootable device before beginning the BMR.

Axcient provides the following download files. To download a file, do the following:

- Select the desired link.
- Right click the mouse and select "save target as" (Internet Explorer), "save link as" (Firefox), or "save download linked file as" (Safari).
- Select a target location and download the file.

Bare Metal Restore (BMR)

Recover a 32-bit or 64-bit system image. Download and burn the BMR boot file (bmr.iso) onto a CD to create an Axcient Bare Metal Restore Recovery Disk CD.

- [BMR Boot ISO](#)
- [BMR ISO Verification File \(bmr.md5\)](#)

HP G9 Proliant G9 Bare Metal Restore (BMR)

Recover a 32-bit or 64-bit system image. Download and burn the BMR boot file (bmr.iso) onto a CD to create an Axcient Bare Metal Restore Recovery Disk CD.

- [HP Proliant G9 BMR Boot ISO \(bmr.iso\)](#)
- [HP Proliant G9 BMR Verification File \(bmr.md5\)](#)

STEP 6

Plug in and boot from the bootable media. A GRUB menu displays. Select the **Windows** option.



STEP 7

Enter the **IP address** and **login credentials** for the UMC of the Axcient appliance and then click the **Connect** button.

Any additional configurations, such as loading drivers, renewing the DHCP lease, or setting a static IP address, can be completed here.

Note: For users who upgraded from AxOS 6.3.7 to AxOS 6.4.8:

- You will need to manually partition the disks by clicking the **Utils/Tools** option for a recovery point made using AxOS 6.3.7.
- In AxOS 6.5.3, you will need to manually partition the disk volumes if the device has multiple volumes on a single disk. The BMR Utility will be unable to appropriately replicate the partition schema.

Failure to manually partition the disks might disrupt the BMR process or create problems with the restored device.

In both instances, please refer to the [Manual Partition](#) section for more information.



STEP 8

Select the recovery point and configure the BMR. The following options can be configured:

- Select **User Source Device Network Settings** to apply the device's original network settings.
- Select **Use Existing Partition Table** to override the existing partition table and use the table configured in the Tools section of the BMR.
- The **Use 2nd NIC** option is only available for physical devices and assumes there is a direct connection to the appliance rather than a network connection.

Click the **Start BMR** button to begin the BMR process.



STEP 9

Towards the end of the BMR process, you will be prompted to install boot-critical device drivers. Select from the following options:

- Select the **Install boot-critical drivers** option to automatically install boot critical devices.
- Select the **Install additional boot-critical drivers** option to manually install drivers from the bootable media as instructed above.
- Select the **Return** option to continue after the drivers have been installed.

The BMR will complete and the device will reboot automatically. Remove the bootable device upon reboot so the device can boot from the OS.



STEP 10

The boot-critical drivers will be installed and the BMR process will run until completion.

When the BMR is complete, the device will restart. Disconnect the bootable to let the target device boot from the operating system.

Power on the newly stored device and confirm that the BMR process has completed successfully.



BMR to a Virtual Machine

This section of the guide [assumes that you have already locked the image](#) with which you would like to perform the BMR. This section outlines the necessary steps required to perform a BMR on a virtual machine (VM).

STEP 1

On the [Downloads](#) page, download the appropriate BMR ISO to a host datastore.

NOTE: If you are performing a BMR on an HP Proliant G9 device, you must use the *HP Proliant G9 BMR Boot ISO*. Otherwise, the BMR will not complete successfully.

Additionally, if device drivers need to be installed, add them to the bootable device before beginning the BMR.

Axcient provides the following download files. To download a file, do the following:

- Select the desired link.
- Right click the mouse and select "save target as" (Internet Explorer), "save link as" (Firefox), or "save download linked file as" (Safari).
- Select a target location and download the file.

Bare Metal Restore (BMR)

Recover a 32-bit or 64-bit system image. Download and burn the BMR boot file (bmr.iso) onto a CD to create an Axcient Bare Metal Restore Recovery Disk CD.

- [BMR Boot ISO](#)
- [BMR ISO Verification File \(bmr.md5\)](#)

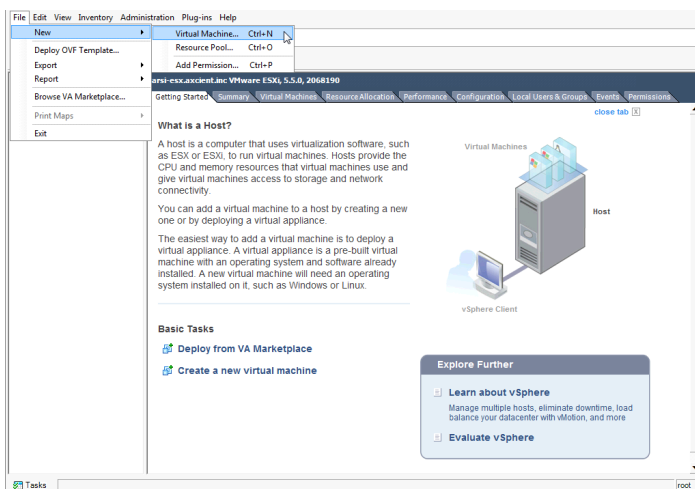
HP G9 Proliant G9 Bare Metal Restore (BMR)

Recover a 32-bit or 64-bit system image. Download and burn the BMR boot file (bmr.iso) onto a CD to create an Axcient Bare Metal Restore Recovery Disk CD.

- [HP Proliant G9 BMR Boot ISO \(bmr.iso\)](#)
- [HP Proliant G9 BMR Verification File \(bmr.md5\)](#)

STEP 2

Create a new virtual machine.

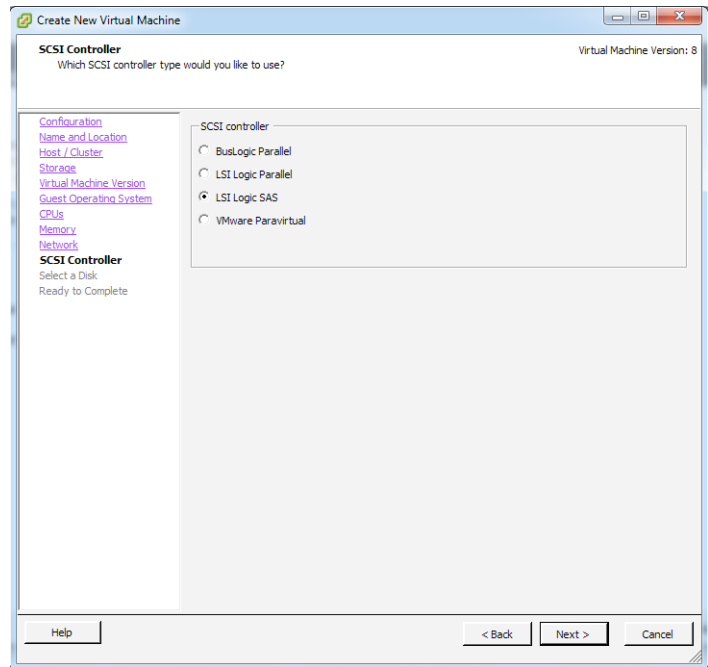


STEP 3

In the *SCSI Controller* screen, select the appropriate SCSI controller:

- Select **LSI Logic Parallel** for Windows 2003 environments.
- Select **LSI Logical SAS** for 2008 and 2012 Windows environments.

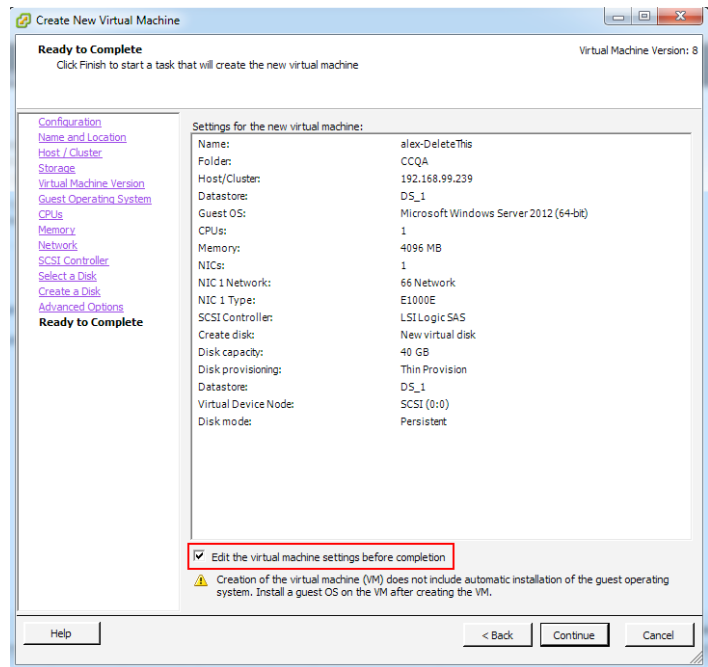
Click the **Next** button to continue.



STEP 4

In the *Ready to Complete* screen, select the **Edit the virtual machine settings** checkbox.

Click the **Continue** button to finish configuring the VM.



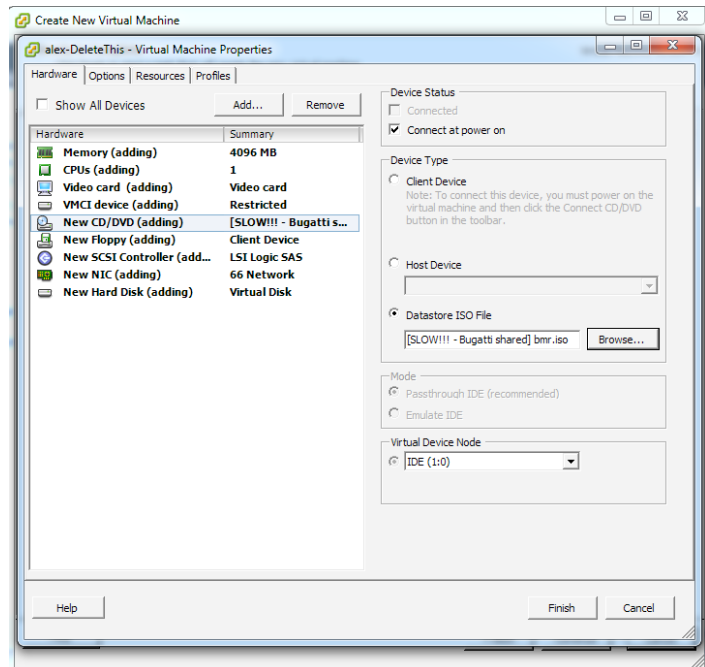
STEP 5

In the *Hardware* section, select the **New CD/DVD** option and update the following settings:

- In the *Device Status* section, select the **Connect at power on** checkbox.
- In the *Device Type* section, select the **Datastore ISO file** radio button. Then click the **Browse** button to browse the datastore and select the downloaded `bmr.iso` file.

Click the **Finish** button.

The VM can now be powered on, and you can continue with the BMR process.



STEP 6

Power on the VM. A GRUB menu displays. Select the **Windows** option.



STEP 7

Enter the IP address and login credentials for the UMC Axcient appliance, and then click the **Connect** button.

Additional configurations, such as loading drivers, renewing the DHCP lease, or setting a static IP address can be updated during this process.

Note: For users who upgraded from AxOS 6.3.7 to AxOS 6.4.8:

You will need to manually partition the disks by clicking the **Utils/Tools** option for a recovery point made using AxOs 6.3.7.

Failure to manually partition the disks might disrupt the BMR process or create problems with the restored device.



STEP 8

Select the recovery point and configure the BMR using the following options:

- Select **User Source Device Network Settings** to apply the device's original network settings.
- Select **Use Existing Partition Table** to override the existing partition table and use the table configured in the Tools section of the BMR.
- The **Use 2nd NIC** option is only available for physical devices, and will assume there is a direct connection, rather than a network connection.

Click **Start BMR** to begin the BMR process.

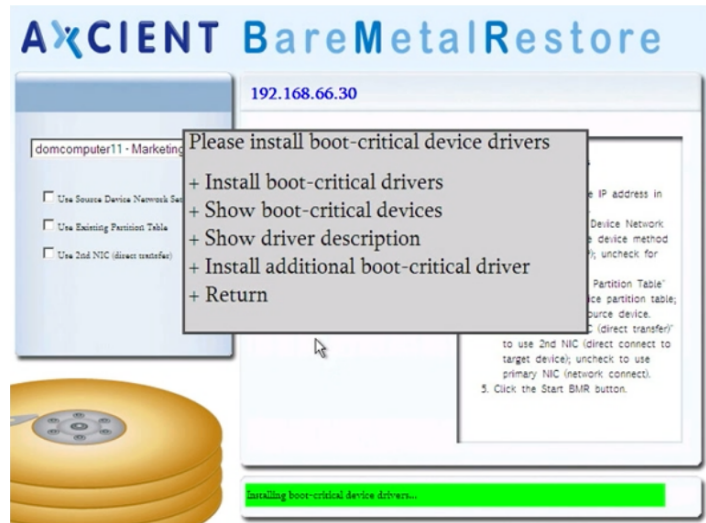


STEP 9

Towards the end of the BMR process, you will be prompted to install boot-critical device drivers.

- Select the **Install boot-critical drivers** option to automatically install boot critical devices.
- Select the **Install additional boot-critical drivers** option to manually install drivers from the bootable media as instructed above.
- Select the **Return** option to continue after the drivers have been installed.

The BMR process will complete and the device will reboot automatically. Remove the bootable device upon reboot so the device can boot from the OS.



STEP 10

The boot-critical drivers will be installed and the BMR process will run until completion.

When the BMR is complete, the device will restart. Disconnect the bootable to let the target device boot from the operating system.

Power on the newly stored device and confirm that the BMR has completed successfully.



Manual Partition

You will need to manually partition the disk(s) for a device being recovered using the BMR tool. This applies to the following types of devices:

- Any device replicated using AxOS 6.4.8 and later
- Any device replicated using AxOS 6.5.3 with multiple volumes

Recovering a Device with Multiple Volumes

If you are recovering a device with multiple volumes, the BMR Utility will be unable to preserve the partitioning and will be restored as an extended partition. You will be unable to convert these extended partitions back in to a primary partition. To avoid this, you should partition disks manually using the Diskpart commands or by using the BMR Disk Partitioner.

To manually partition the disk(s):

STEP 1

Click the **Utils/Tools** option before logging in to the Axcient appliance.



STEP 2

Select a preferred partitioning method:

- Select the **Manually partition disk** option to partition using a GUI. If you select this option, continue to *Step 3*.
- Select the **DOS Window** option to partition the disks using Diskpart commands. If you select this option, a DOS window will display.

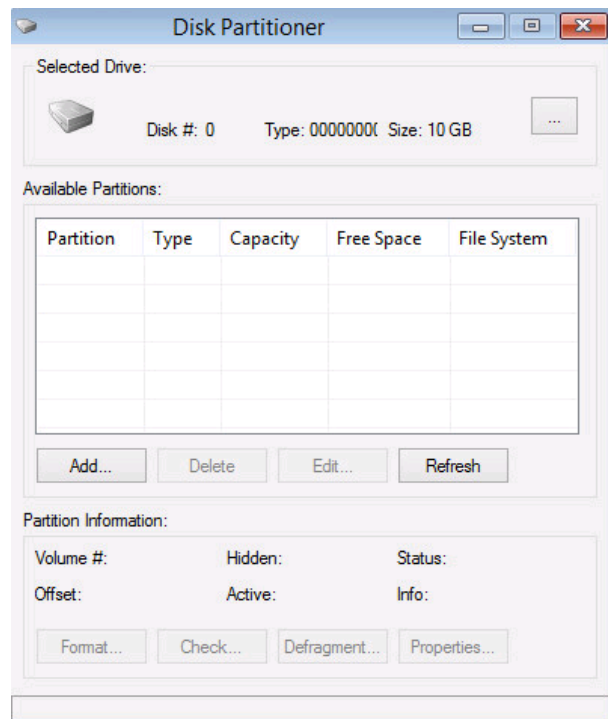
Consult the System Administrator for the exact commands to correctly partition the disks.



STEP 3

On the *Disk Partitioner* screen, click the **Add...** button to add partitions to the disk.

Click the ... button on the top-left corner to select the specific disk to be partitioned.

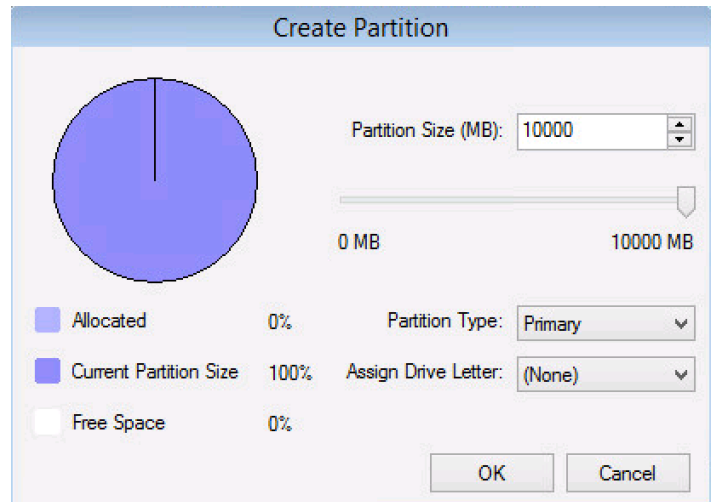


STEP 4

On the *Create Partition* screen, configure the following:

- In the *Partition Size (MB)* field, configure the size of the partition in MB.
- In the *Partition Type* field, configure the type of partition (including primary or extended).
- In the *Assign Drive Letter* field, assign the drive letter to the partition.

Click the **OK** button to save these changes. Repeat *Step 3* and *Step 4* until all disks are correctly partitioned.

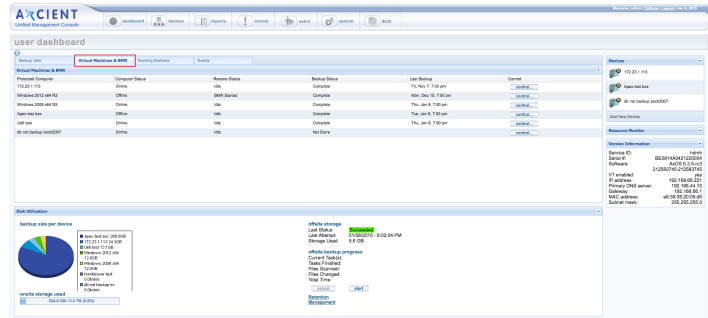


Discarding the Image Lock

When the BMR has successfully completed, you must discard the image lock on the device. If you do not remove the system image lock, backups will not continue to run on the device.

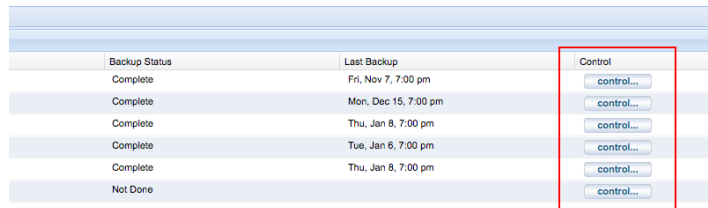
STEP 1

On the UMC Dashboard, click the **Virtual Machines & BMR** tab.



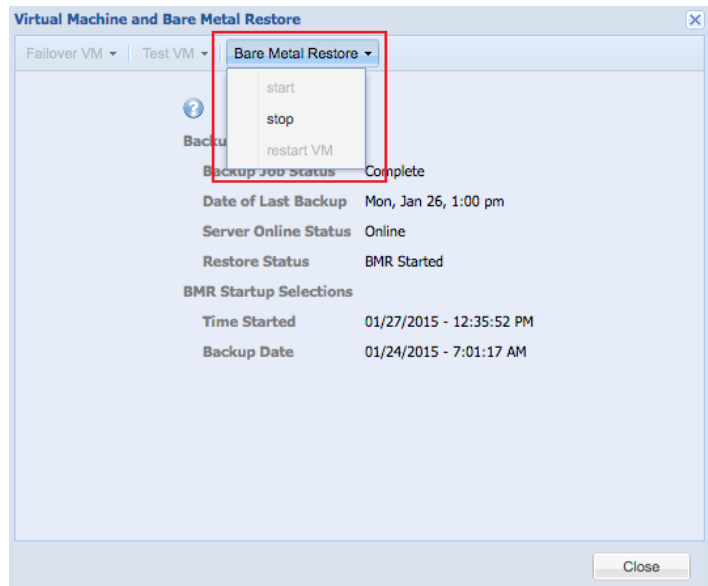
STEP 2

Click the **Control** button to view the lock for the BMR.



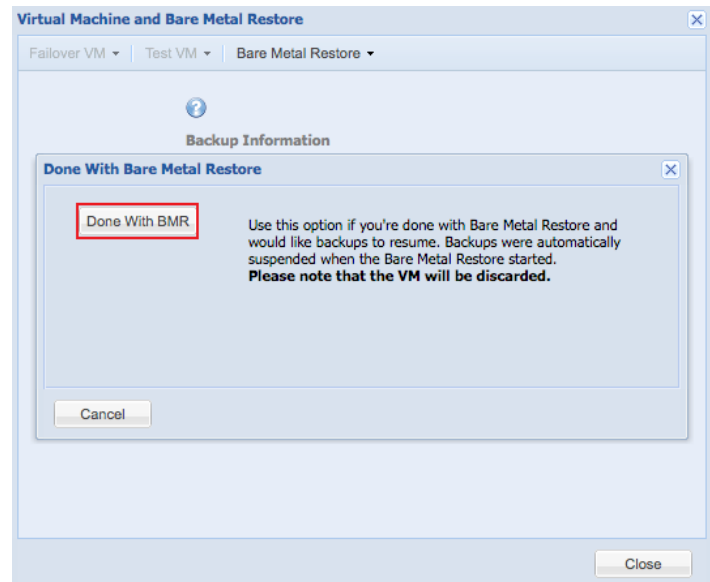
STEP 3

In the *Bare Metal Restore* drop-down menu, click **Stop**.



STEP 4

On the confirmation screen, click the **Done with BMR** button to discard the system image lock.



Failover VM (Local)

Axcient's Failover Virtual Machine (VM) allows you to start a virtual machine on the local Axcient appliance in the event a protected device is lost or fails. Although the Failover VM can run indefinitely, it is not intended as a long-term replacement for a permanent server. The server functions should be transferred back to a primary device as soon as possible.

Test VM Screen Shot Validation

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

To ensure that screen shot validations can be successfully performed, please set the *Screen Sleep Timeout option* to **30 minutes** or longer. When a Test VM is being deployed, minimal resources are allocated to the deployment so that they can be used by other processes on the appliance, resulting in a longer deployment process. If the Test VM enters sleep mode during the deployment, a screen shot created during this validation will depict a black screen and will result in a failed validation.

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

Recovery Steps

Warning!

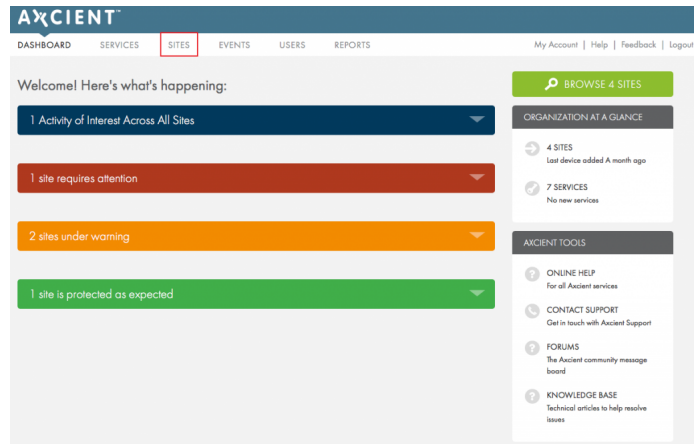
When protecting a device with the Windows Server 2008 SP1 operating system, you must confirm that **the 955430 package has been installed on the target device** before performing the recovery. Please refer to the [Microsoft KB955430](#) article for more information and to download the package.

Without the 955430 package, WS2008 will be unable to install GPLPV drivers due to Windows not trusting the certificates used to sign drivers.

This will mean that you will not be able to deploy a local failover VM for the device if it has more than 4 drives.

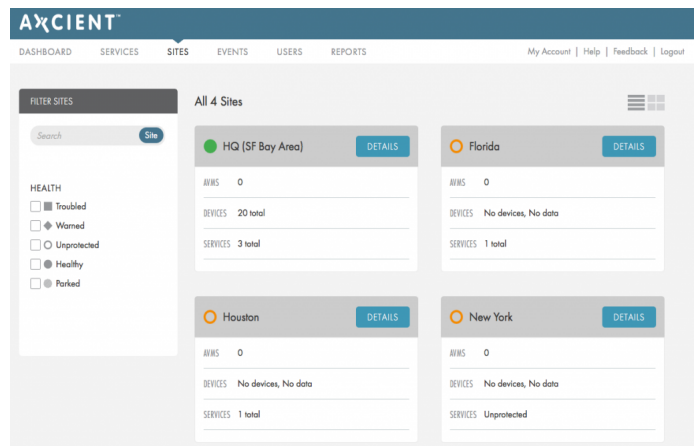
STEP 1

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



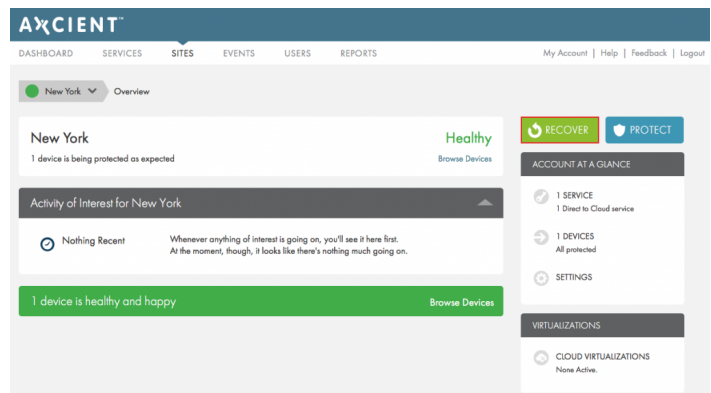
STEP 2

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



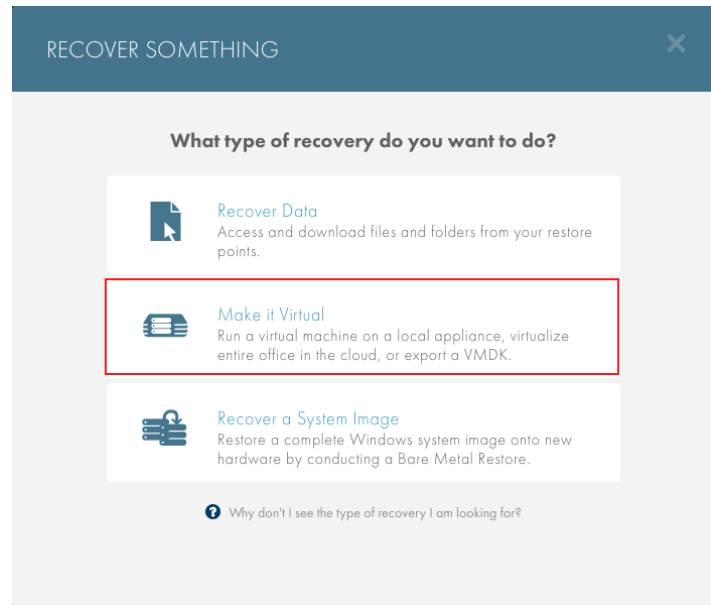
STEP 3

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



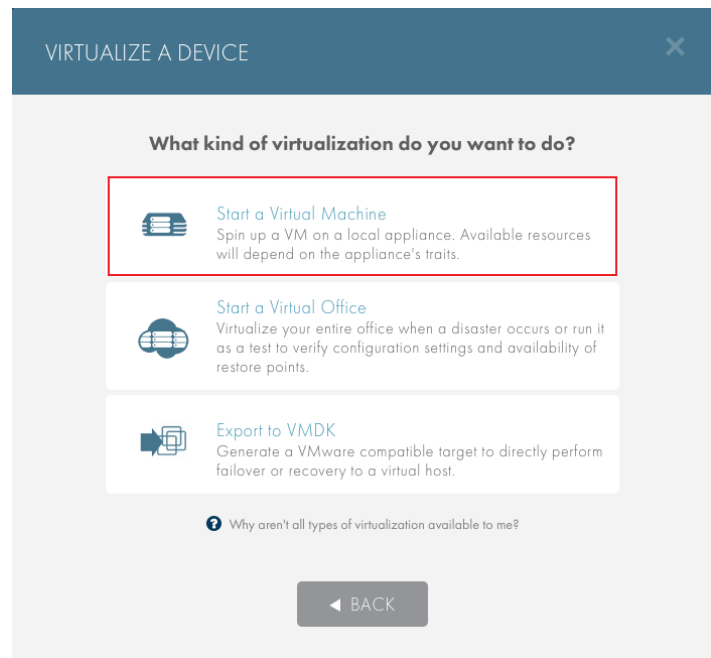
STEP 4

On the *Recover Something* screen, select the **Make it Virtual** option.



STEP 5

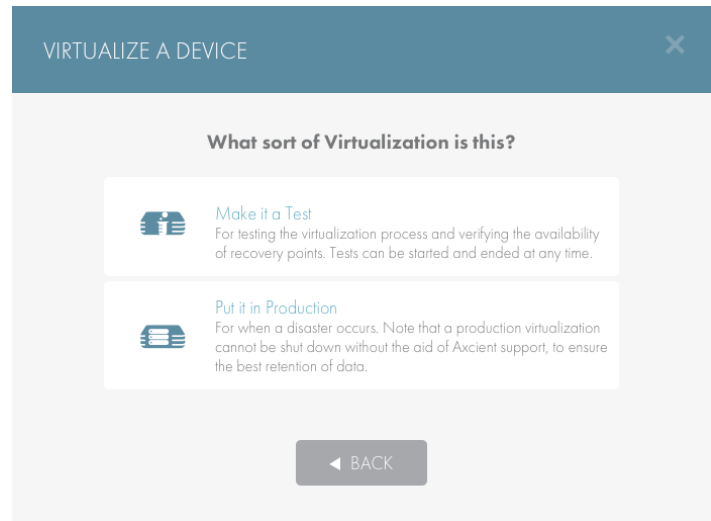
On the *Virtualize a Device* screen, select the **Start a Virtual Machine** option.



STEP 6

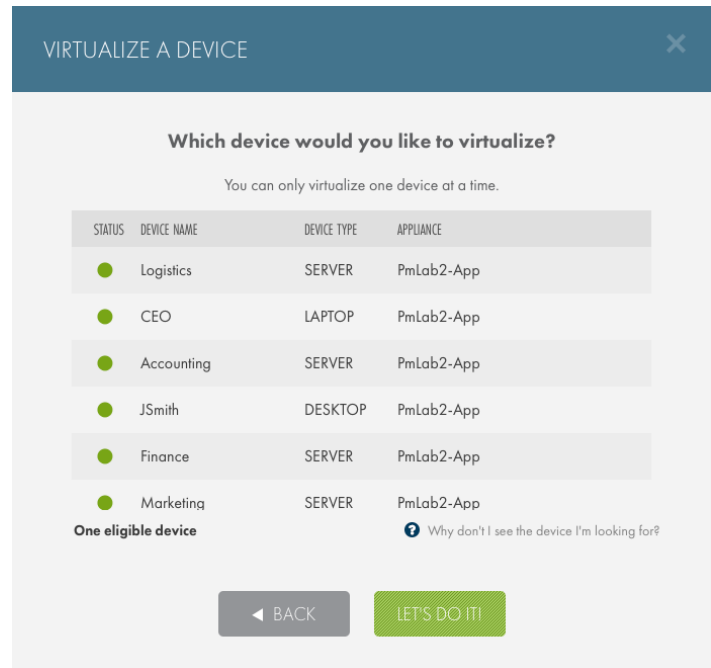
Select the type of local virtualization to deploy:

- 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 7

Select the device to virtualize and click **Let's Do It!**.



STEP 8a: Test VM

If this is a test, configure the Test VM:

- In the *Recovery Point* drop-down menu, select the **recovery point time**.
- Using the *RAM* slider, allocate virtual RAM.
- Using the *CPU* slider, allocate virtual CPU cores.
- In the *Use Current Address* field, enable or disable the option to use the device IP address.
- In the *VNC* field, enable or disable the option to allow a VNC connection (this option is only available when manually configuring the IP address).
- In the *VNC Password* field, enter the **VNC password** (only if the VNC connection is enabled).
- In the *IP Address* field, enter the **IP address** (only if the *Use Current Address* field is disabled).

Click the **Looks Good** button to continue.

Please note that a Test Failover VM cannot communicate with any other device. A Test VM cannot be accessed through RDP.

VIRTUALIZE ACCOUNTING ✕

Configure your local Virtual Machine.

RECOVERY POINT June 05, 2016 at 8:00am ▼

RAM 2 GB

512 MB | | 14.5 GB | | 28.6 GB

CPU 1

1 | | 5 | | 8

USE CURRENT ADDRESS NO

VNC ENABLED

VNC PASSWORD Test123

IP ADDRESS 192.168.99.100

◀ BACK
LOOKS GOOD

STEP 8b: Production VM

If this is production, configure the production VM:

- In the *Recovery Point* drop-down menu, select the **recovery point time**.
- Using the *RAM* slider, allocate virtual RAM.
- Using the *CPU* slider, allocate virtual CPU cores.
- In the *Use Current Address* field, enable or disable the option to use the device IP address.
- In the *VNC* field, enable or disable the option to allow a VNC connection (this option is only available when manually configuring the IP address).
- In the *VNC Password* field, enter the **VNC password** (only if the VNC connection is enabled).
- In the *IP Address* field, enter the **IP address** (only if the *Use Current Address* field is disabled).

Click the **Looks Good** button to deploy the local Production VM failover.

✕
VIRTUALIZE ACCOUNTING

Configure your local Virtual Machine.

RECOVERY POINT ▼ June 05, 2016 at 8:00am

RAM 512 MB

512 MB | | 14.5 GB | | 28.6 GB

CPU 1 CPU

1 | | 5 | | 8

VNC ENABLED

VNC PASSWORD

IP ADDRESS domcomputer5

◀ BACK
LOOKS GOOD

Viewing the Local Failover Details

You can view the local failover information for the device after the failover VM is running.

STEP 1

On the *Web Application Dashboard*, expand the *Activities of Interest* section, click **Local Virtualizations**, and then click the **Manage VMs** link.

The screenshot displays the 'Overview' page for 'HQ (SF Bay Area)'. The status is 'Healthy' with '16 devices are being protected as expected'. A 'RECOVER' button is visible in the top right. The 'Activity of Interest for HQ (SF Bay Area)' section shows 'Local Virtualizations' with 'Running 1 test VM'. A table lists the virtualization details:

TYPE	STATUS	
Test	1 VM running	Manage VMs

Below the table, a green bar states '16 devices are healthy and happy'. The right sidebar shows 'ACCOUNT AT A GLANCE' with 20 devices (5 unprotected), 2 services (1 appliance service, 1 virtualized service), and 'VIRTUALIZATIONS' with 1 local VM (Test) and no active cloud virtualizations.

STEP 2

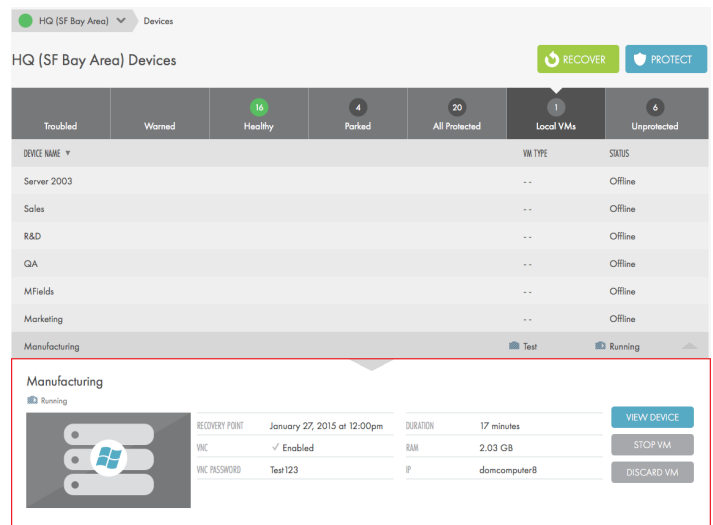
The Local VMs section of the *Client's Device List* page displays.

Click to expand the device and view information about the failover VM, including:

- **Recovery Point** - The recovery point selected in the failover deployment.
- **VNC** - Whether VNC is enabled or disabled.
- **VNC Password** - The configured VNC password.
- **Duration** - Length of time the failover VM has been running.
- **RAM** - The amount of RAM allocated in the failover deployment.
- **IP** - The IP address or domain name of the failed over VM.

The following administrative buttons can also be used to manage the device:

- Click the **View Device** button to visit the *Device Details* page for the specified device.
- Click the **Stop VM** button to change the VM status from *Running* to *Ready*.
- Click the **Discard VM** button to completely discard the local failover VM.



Accessing the Local Failover VM

The local failover VM can be accessed in two different ways: VNC and Remote Desktop Protocol.

Method 1: VNC

A VNC agent can be used to connect to both Test and Production failover VMs. Axcient recommends using the UltraVNC Viewer.

For a single local failover VM:

1. Open the VNC agent.
2. In the *VNC Server* field, enter the **IP address** of the appliance.
3. Enter the **VNC password** if configured.

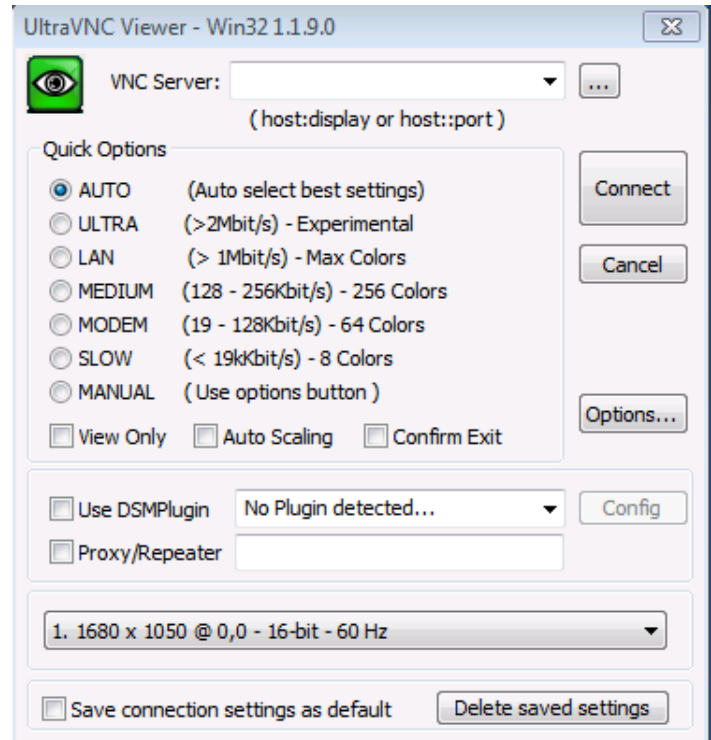
For multiple failover VMs:

1. Open the VNC agent.
2. In the *VNC Server* field, enter the **IP address** of the appliance, along with the **port number** of the failover VM.

VM ports are numbered in sequential order of when they were deployed, starting with 5901.

Example: 192.168.99.234:59001

3. Enter the **VNC password** if configured.

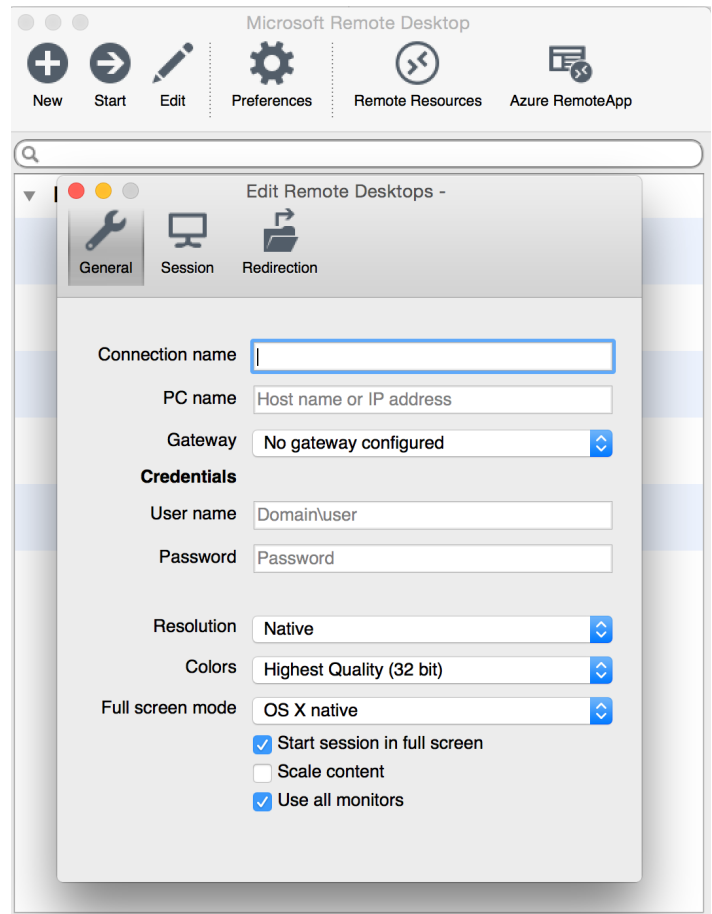


Method 2: Remote Desktop Protocol

Use the Remote Desktop Protocol (RDP) tool to connect to the local failover VM. RDP can only be used to connect to Production failover VMs.

To access the failover VM using an RDP agent:

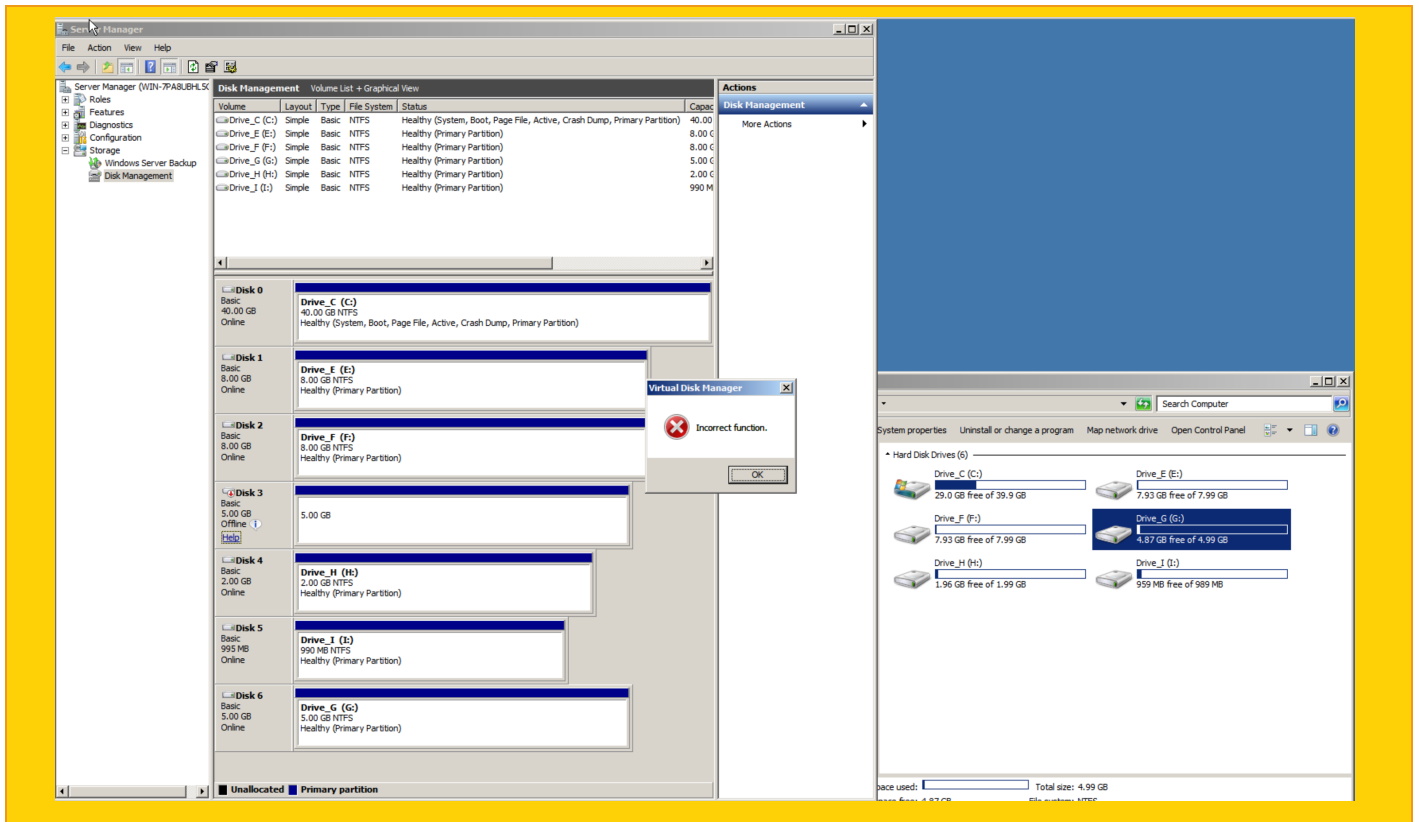
1. Open the RDP agent.
2. Create a new RDP connection using the production IP address and the administrator login credentials.
3. Connect to the local failover VM.



Warning!

When failing over a device with 5 drives or more in either a test or production environment, you might see an extra disk displayed in the *Disk Management/Device Manager* after launching. This extra disk will not show up in *My Computer*, and you will receive an *Incorrect Function* error when attempting to bring the disk online.

This extra disk will not affect the failover or any other recovery-related process associated with the failover VM.



Export to VMDK

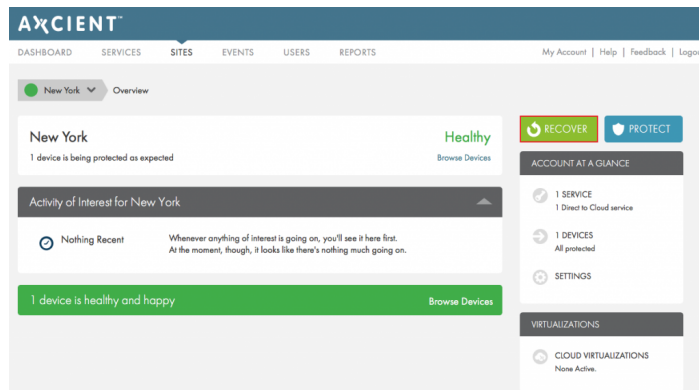
The Export to VMDK tool allows you to deploy VMware-specific, identical virtual machine replicas of physical devices.

The Export to VMDK recovery feature is only available for devices backed up by an Axcient Appliance *using AxOS 6.4 or later*. To view the AxOS version the Axcient Appliance, refer to the [Service Details page of the Web Application User Guide](#).

Generating the .vmdk Files

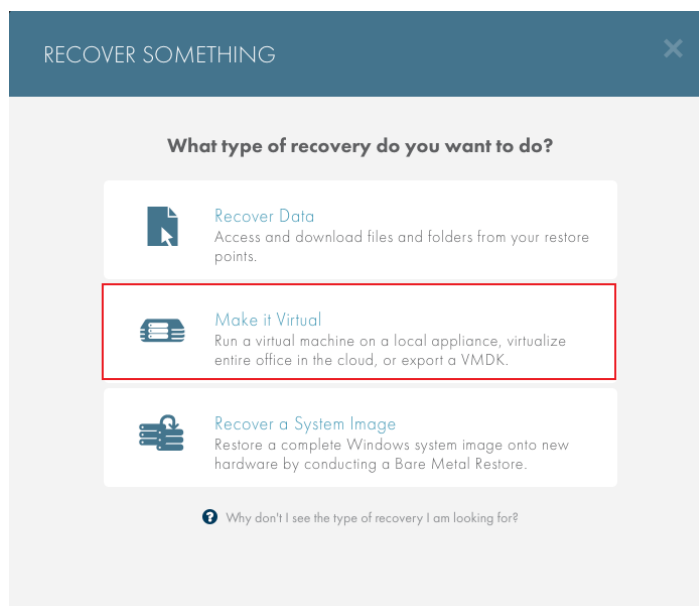
STEP 1

On the Web Application, click the **Recover** button.



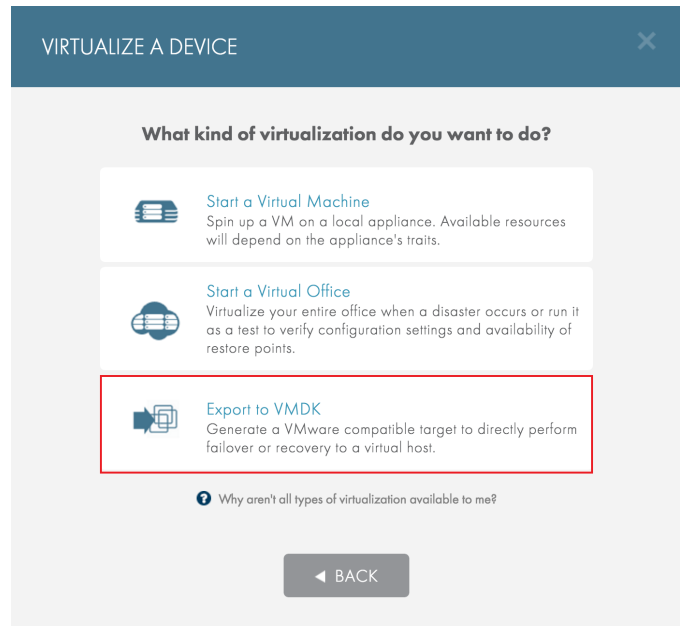
STEP 2

On the *Recover Something* screen, click the **Make it Virtual** option.



STEP 3

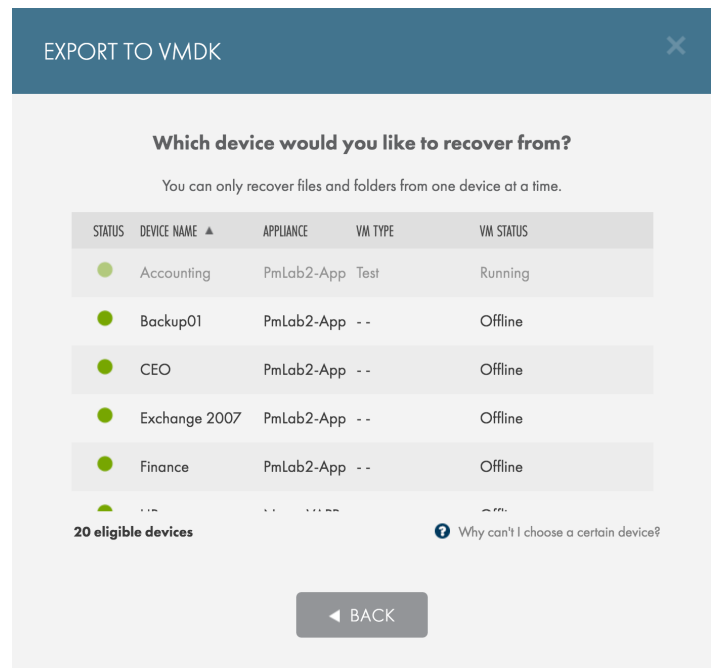
On the *Virtualize a Device* screen, select the **Export to VMDK** option.



STEP 4

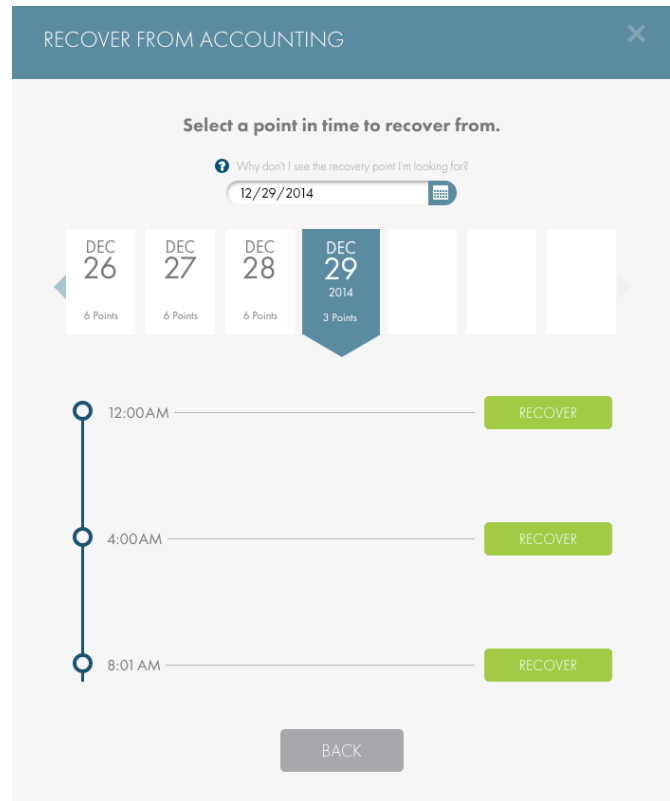
On the *Export to VMDK* screen, select the desired device and click the **Next** button.

A device with a *Running* VM Status indicates that a VM is currently running for that device. You can still continue with the recovery process, but you will be prompted to stop the VM to continue. See the [VMDK Alert Messages](#) section for more information about alerts you might encounter when selecting a device.



STEP 5

On the *Recover From* screen, select the desired recovery point and click the **Recover** button.



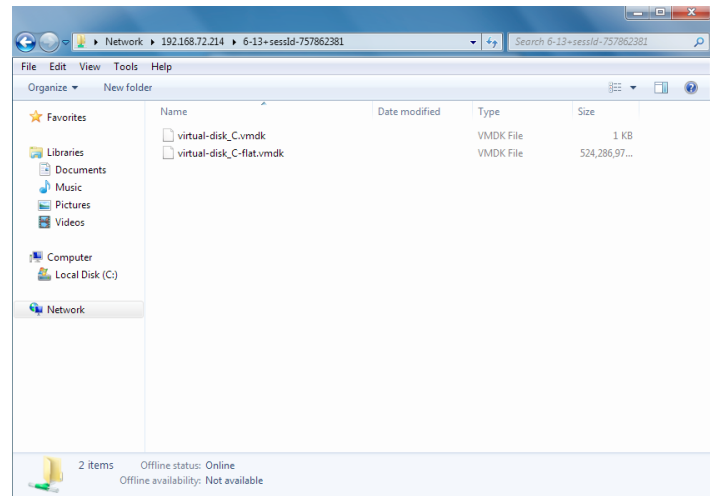
STEP 6

A UNC mount point will generate. Copy the UNC mount path and set the UNC mount expiration timer.



STEP 7

Paste the UNC mount path into a File Explorer window. Two .vmdk files will display.



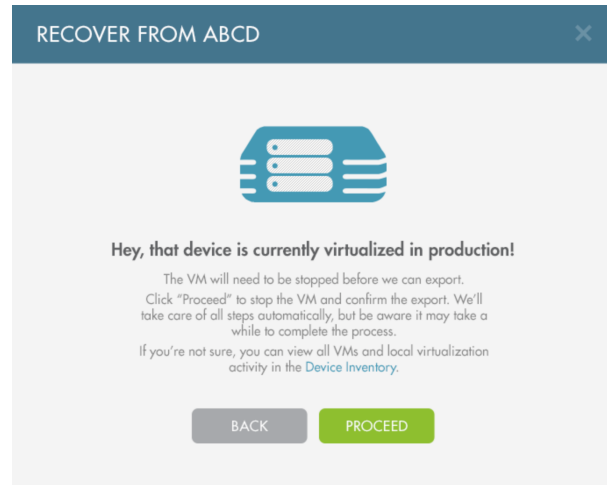
VMDK Alert Messages

You might encounter one of the following alert messages after selecting a device. Below are descriptions of each alert.

Alert: Virtualized Device in Production

You will receive this alert when the selected device is currently virtualized in a Production environment.

Click the **Proceed** button to stop the VM and generate the VMDK for the selected device.

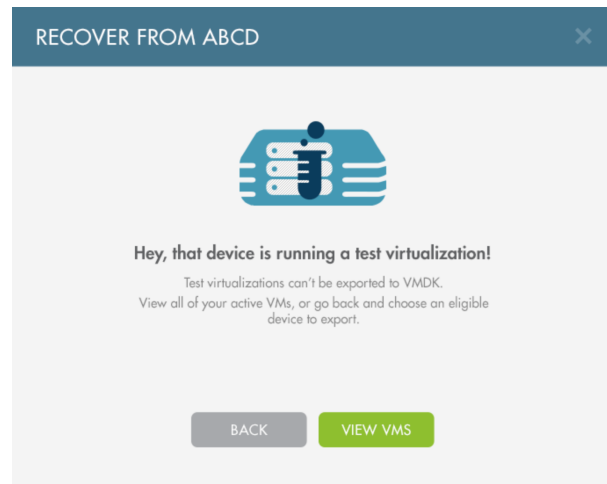


Alert: Virtualized Device in Test

You will receive this alert when the selected device is currently virtualized in a Test environment.

Currently, Axcient does not support Exporting to VMDK from a Test failover.

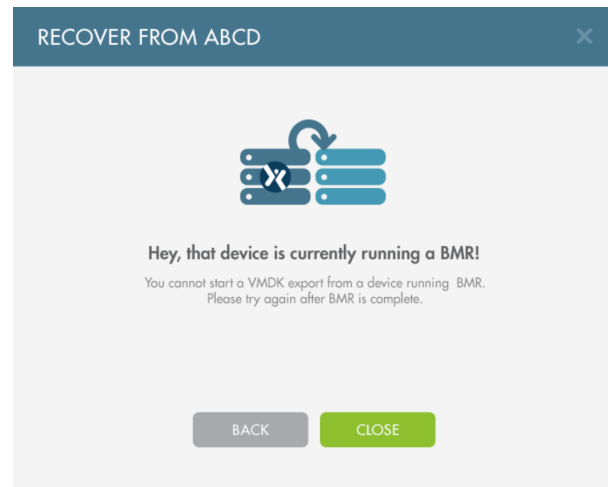
You will need to manually shut down the Test VM or select a different device.



Alert: Running BMR

You are unable to use the Export to VMDK feature for a device currently running a BMR.

You will need to wait until the BMR has completed before exporting to VMDK.

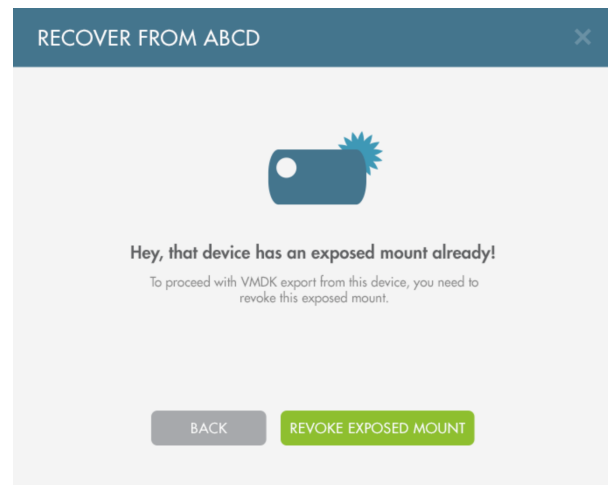
**Alert: Exposed Mount**

The Export to VMDK feature has already been performed on the selected device, exposing a UNC Mount point containing the VMDK files.

Click the **Revoke Exposed Mount** button to erase the previous UNC mount and generate a new one.

Alternatively, click the **Back** button to select a different device.

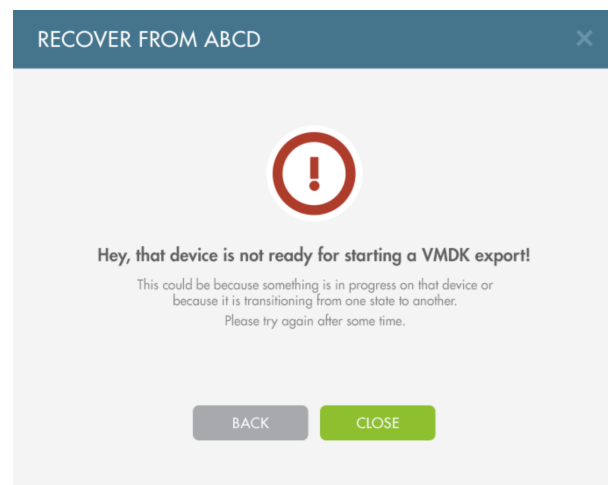
Check the *Activities of Interest* on the *Web App Dashboard* or *Site Details* page to view the currently exposed UNC Mount point.

**Alert: Device Not Ready**

The device is unable to perform the Export to VMDK recovery process because the selected device is currently in use, or is otherwise unavailable.

Click the **Close** button to exit the Export to VMDK process, or press the **Back** button to select a different device.

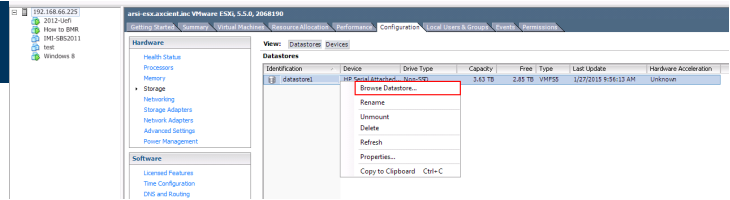
You will need to wait for the device to become available before trying again. You can investigate the device to check if there are any actions that can be taken to make the device available.



Creating the VM using Export to VMDK

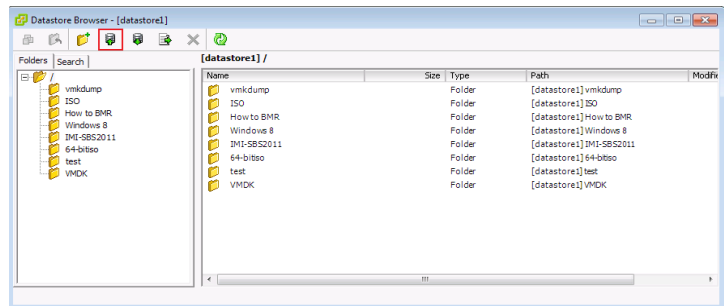
STEP 1

In the VMware vSphere, select the **Host Machine**, click the **Configuration** tab, and then right click the datastore and select the **Browse Datastore** option.



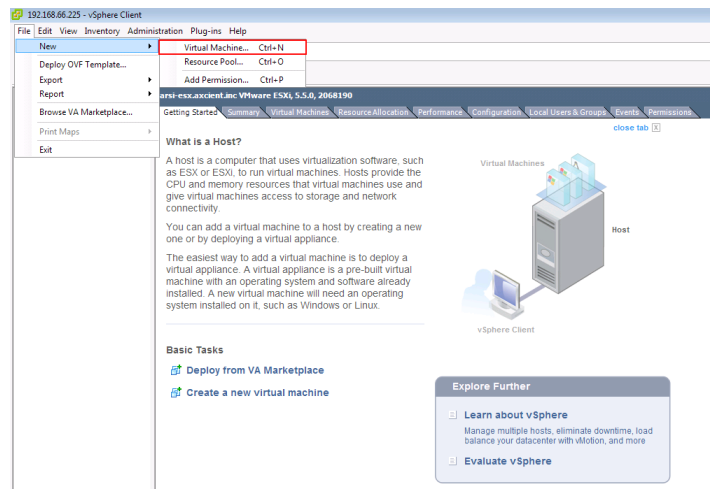
STEP 2

Click the **Upload** button and upload both .vmdk files from the UNC mount point generated above.



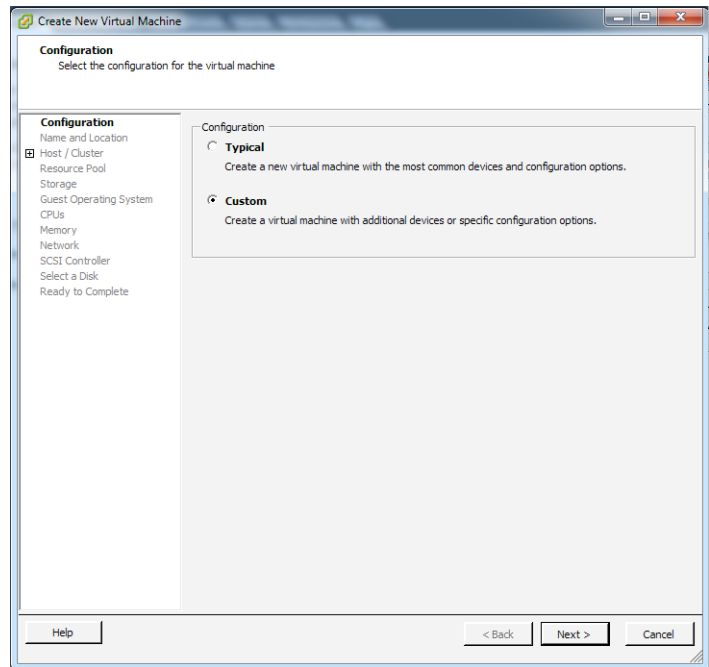
STEP 3

Create a new virtual machine and configure it as needed.



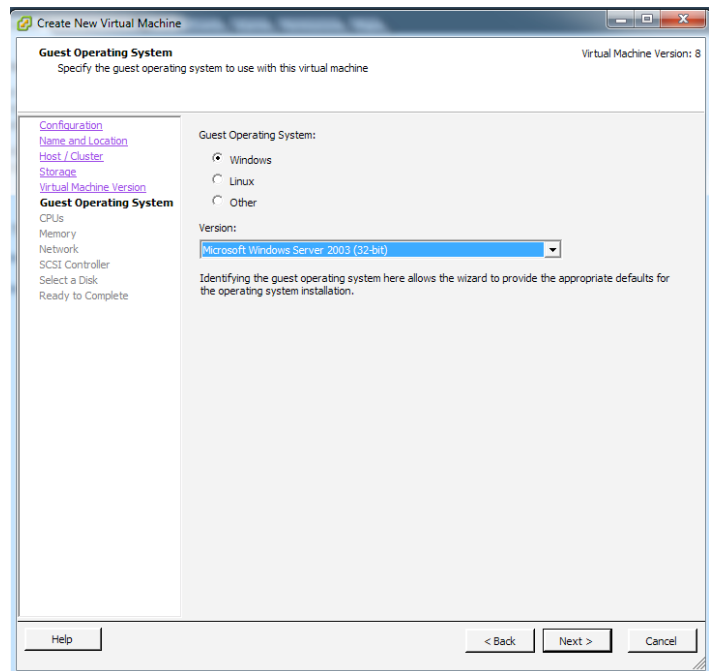
STEP 4

On the *Configuration* screen, select the **Custom** option and continue with configuring the VM as needed.



STEP 5

On the *Guest Operating System* screen, select the appropriate OS from the drop-down menu. The OS should match that of the device from which the Export to VMDK process was performed. Click **Next** to continue configuring the VM as needed.

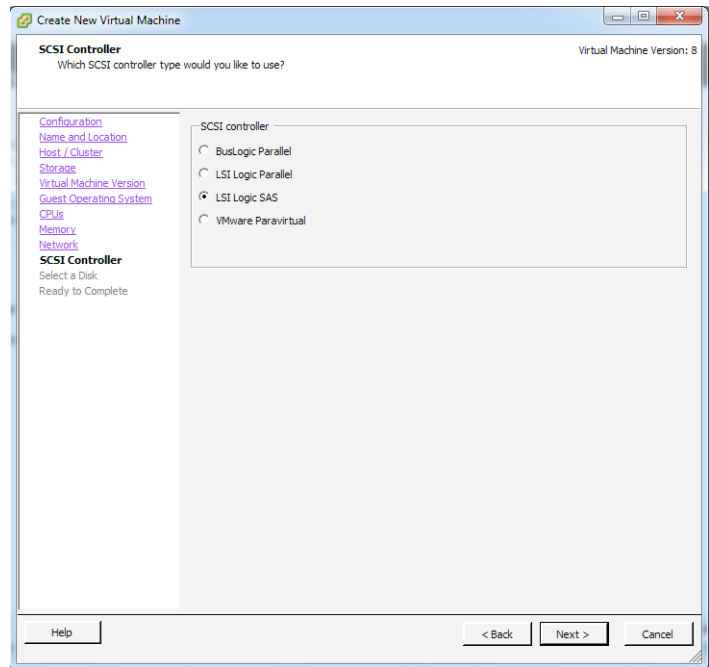


STEP 6

On the *SCSI Controller* screen, select the SCSI controller:

- Select the **LSI Logic Parallel** radio button for a Windows 2003 OS.
- Select the **LSI Logical SAS** radio button for every other Windows OS.

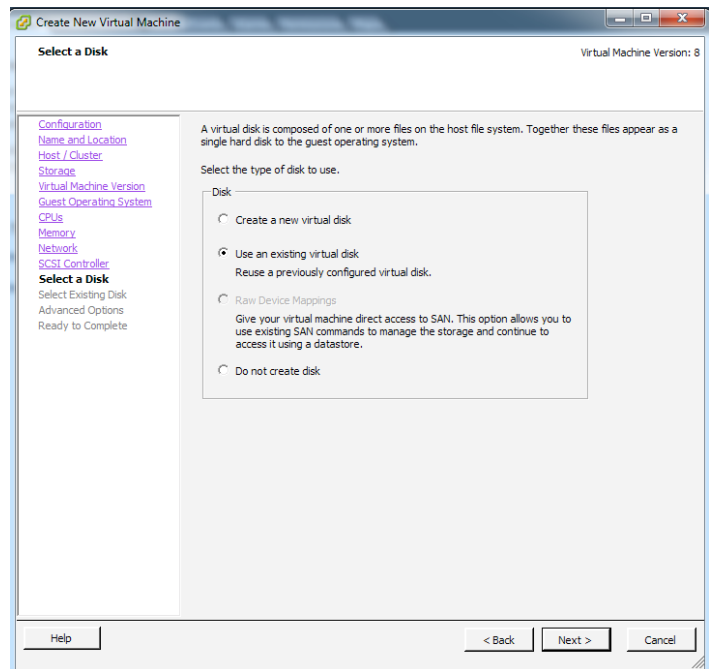
Click the **Next** button to continue.



STEP 7

On the *Select a Disk* screen, select the **Use an existing virtual disk** option.

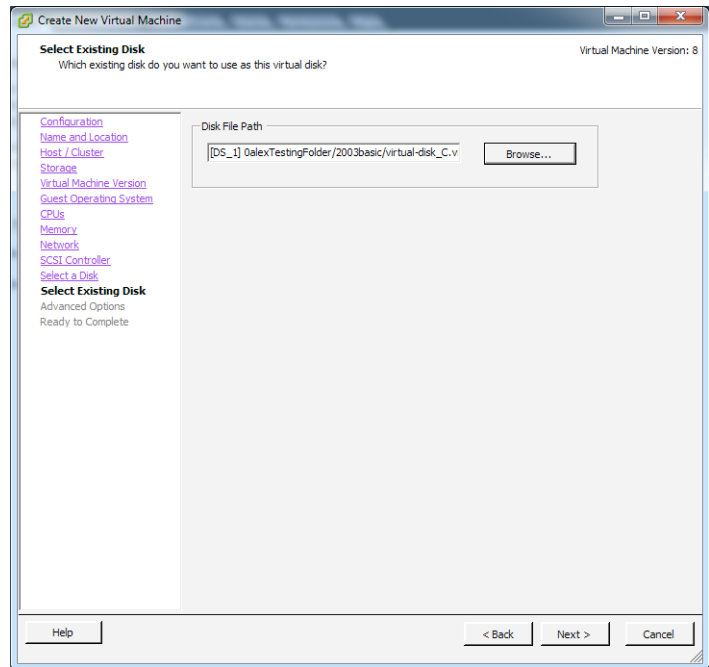
Click the **Next** button to continue.



STEP 8

On the *Select Existing Disk* screen, click the **Browse** button to browse the datastore and select the exported VMDK.

Click the **Next** button to continue.

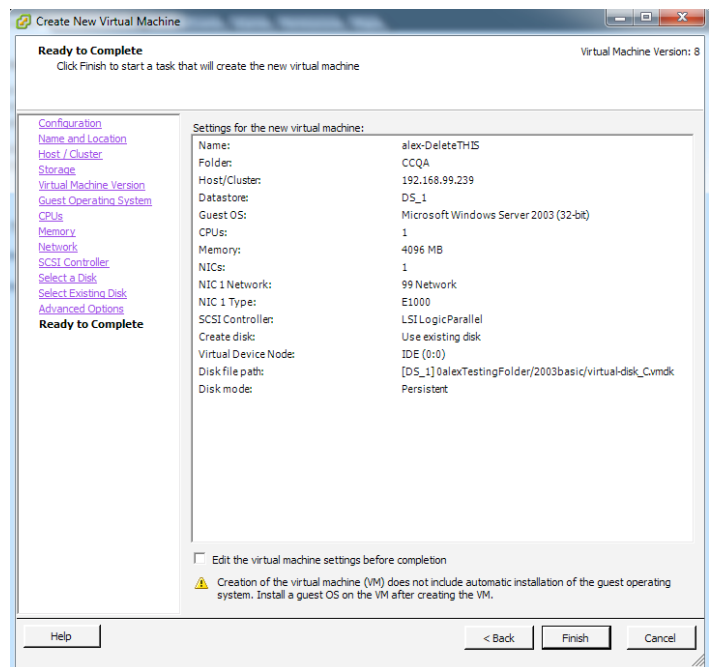


STEP 9

Review the VM configuration. When ready, click the **Finish** button.

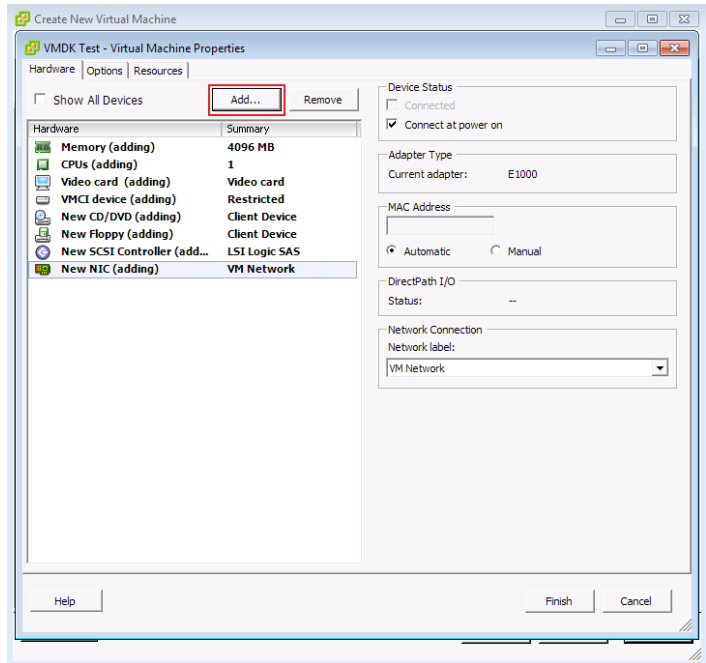
If there are no more hard disks, the VM can now be powered on.

If more hard disks need to be added, check the **Edit the virtual machine settings before completion** box and continue to the section below.



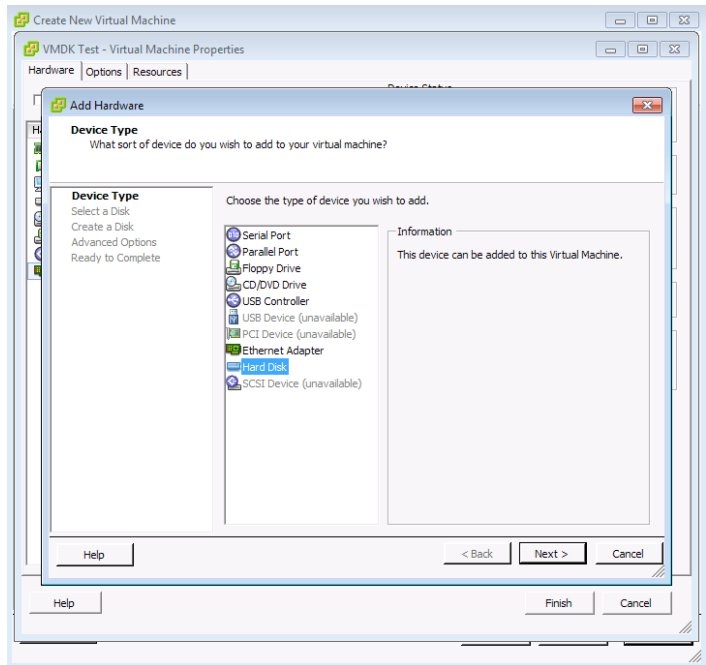
STEP 1 (Add Additional Disk)

On the same *Virtual Machines Properties* screen, click the **Add** button.



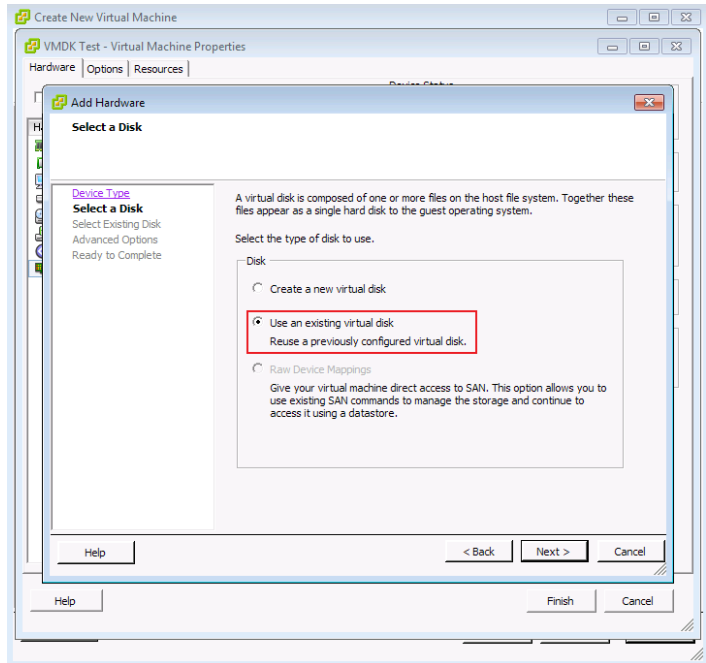
STEP 2 (Add Additional Disk)

You will now need to go through the *Add Hardware* process. On the *Device Type* screen, select the **Hard Disk** option from the menu and click the **Next** button.



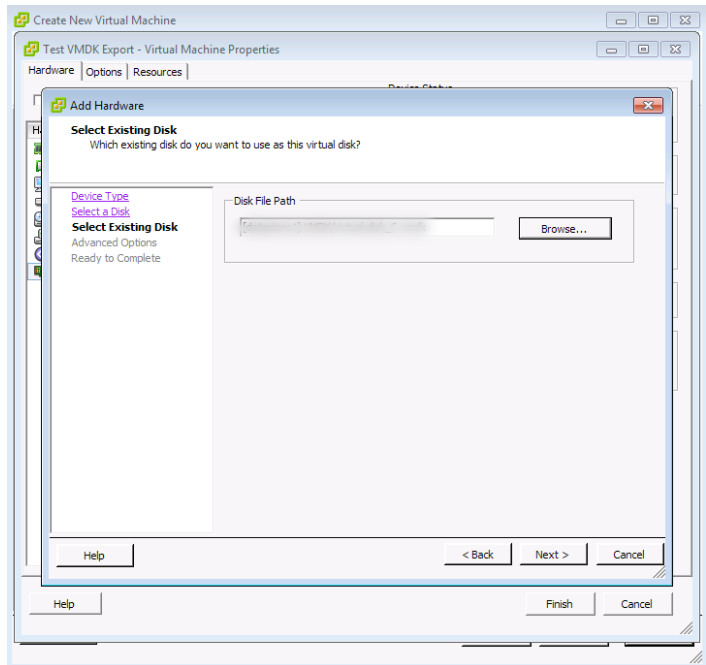
STEP 3 (Add Additional Disk)

On the *Select a Disk* screen, select the **Use an existing virtual disk** option, and then click the **Next** button.



STEP 4 (Add Additional Disk)

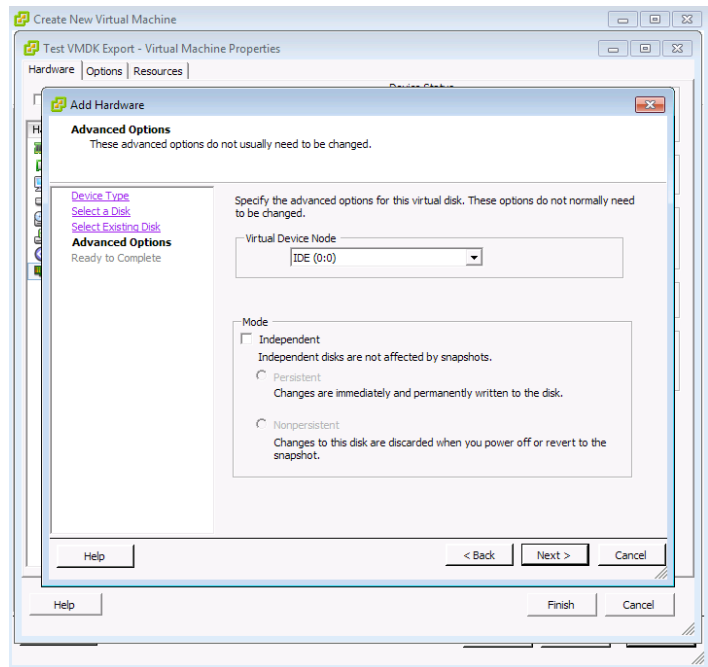
On the *Selecting Existing Disk* screen, click **Browse** and navigate to the .vmdk files uploaded above. Although two files were uploaded, you will only see one large .vmdk file.



STEP 5 (Add Additional Disk - Optional)

If necessary, configure any advanced options on the *Advanced Options* screen.

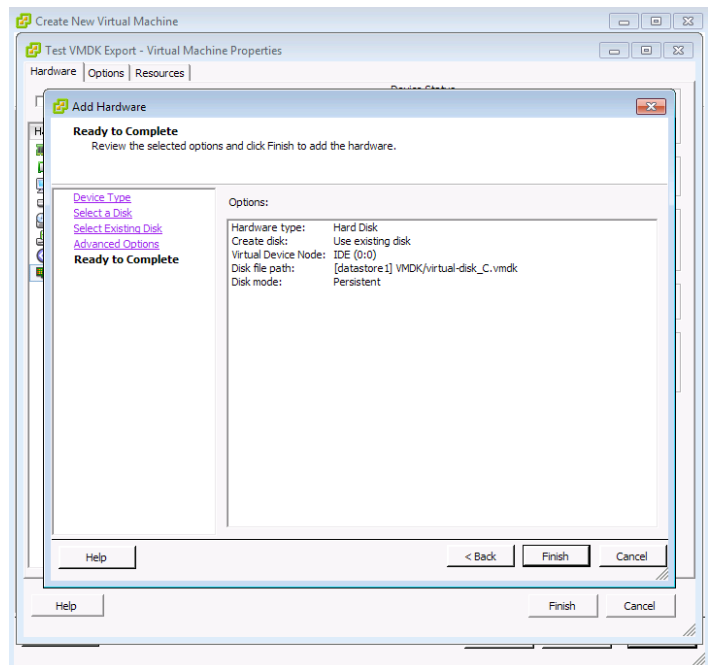
In most instances, no further action is needed unless required on the specific virtual machine environment. Click the **Next** button to continue.



STEP 6 (Add Additional Disk)

Review the selected options. When ready, click the **Finished** button.

The new disk has now been added. Repeat this process for as many disks as required.



Notes

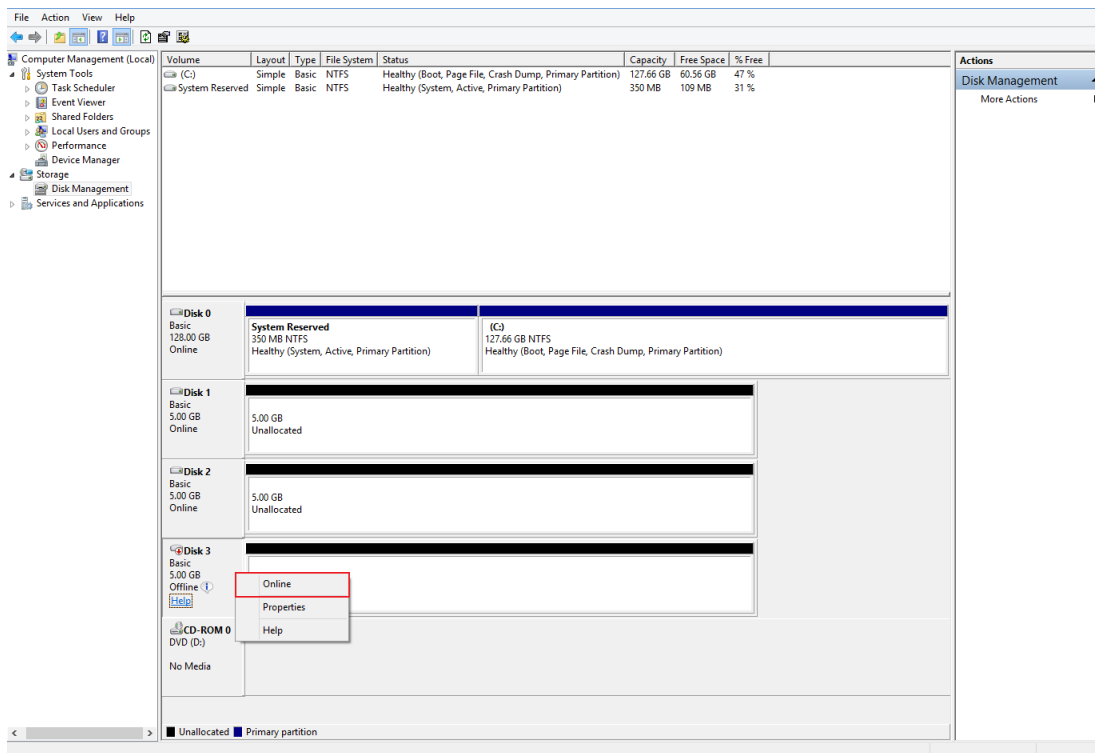
- Occasionally, when a customer deploys a VMDK for a Windows 2003, 2008 or 2012 device, the network settings might not be preserved.

You must manually configure the IP address for the device using the generated VMDK. You can use any preferred method of configuring an IP address for the device.

- Occasionally, when a customer deploys a VMDK for a Windows 2008 R2 device, one disk might be listed as *offline* when using any number of extended disks.

To resolve this issue:

- Ensure the device created using the generated VMDK is powered on.
- Navigate to the Disk Management utility (sometimes called Computer Management).
- Right click the offline drive.
- Select the **Online** option.
- Exit the Disk Management (or Computer Management) utility.



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. 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

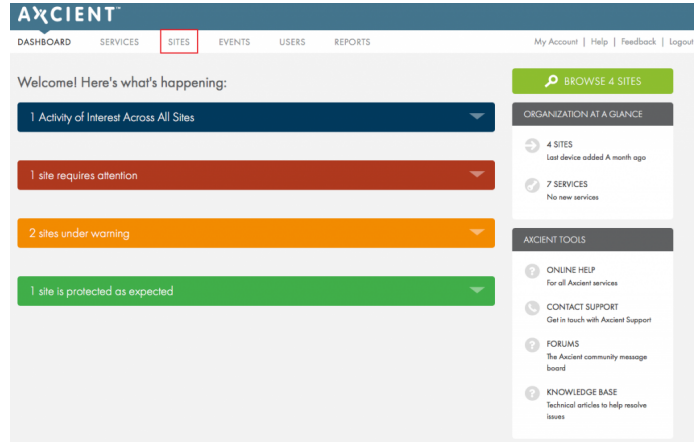
This section of the guide will cover the various Virtual Office interfaces.

Starting the Virtual Office

To start the Virtual Office:

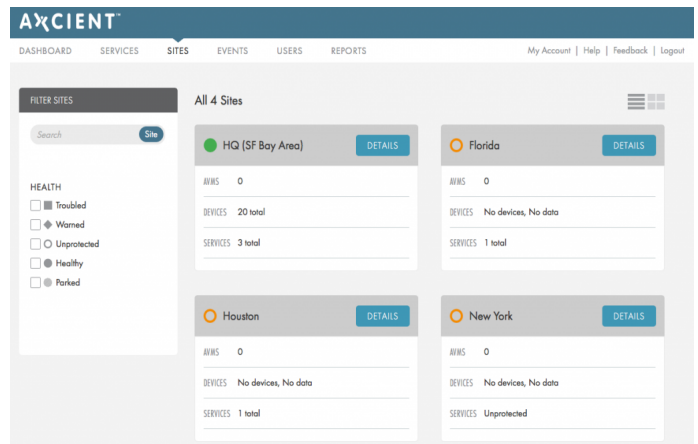
STEP 1

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



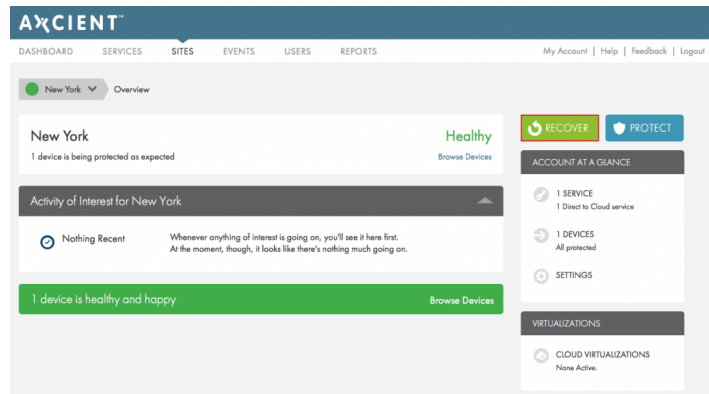
STEP 2

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



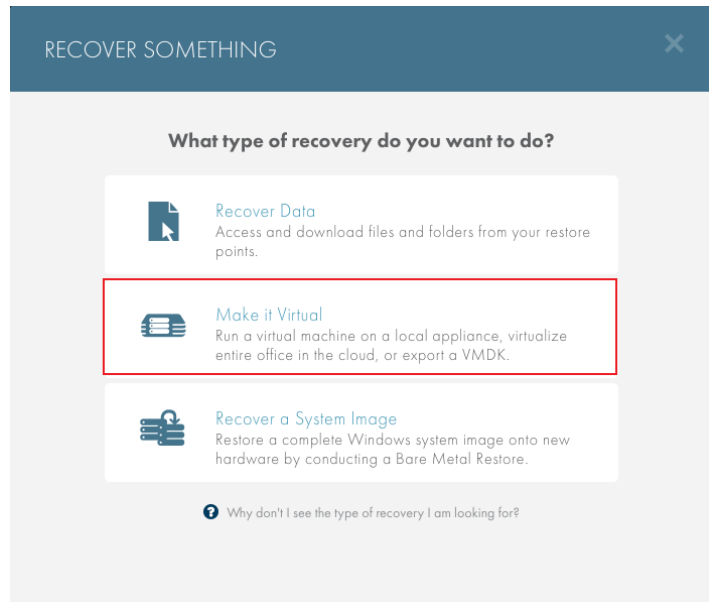
STEP 3

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



STEP 4

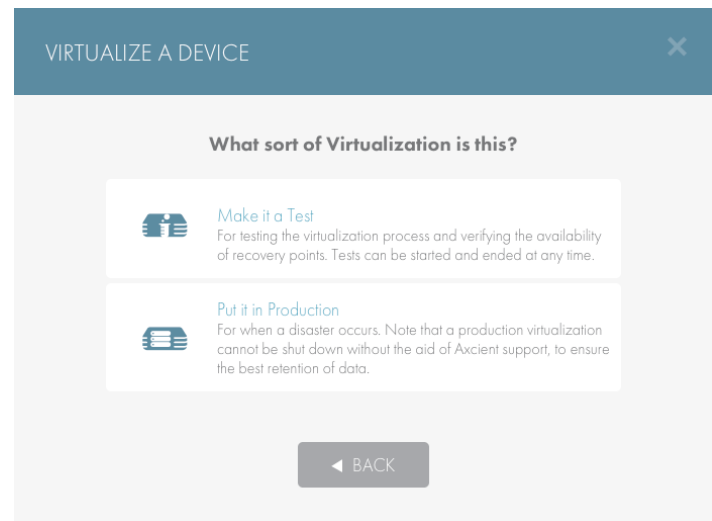
On the *Recover Something* screen, click the **Make it Virtual** option and then select the **Start a Virtual Office** option.



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

On the *Start Virtual Office (Failover)* screen, select the services and configure settings:

- In the *Services* field, use the checkboxes to select the appropriate **service(s)**.
- If you would like to set up a subnet for the Virtual Office, configure the *Gateway* and *Netmask* fields:
 - In the *Gateway* field, enter the **gateway IP address**. This address should be the same as the default gateway on the physical network that the Virtual Office is trying to replicate. For example, if devices are on the 192.168.1.xxx network, the gateway will most likely be 192.168.1.1.
 - In the *Netmask* field, enter the **netmask value**.
- Optionally, to add a new subnet for the Virtual Office, click the **+ Add Another** link. 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, click the red **Delete** icon.

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

START VIRTUAL OFFICE (FAILOVER)

Set up the virtual environment for testing.

SITE Axcient Internal Usage

SERVICES AX-LAB Backup – Service ID 97ax AX-LAB VApp – Service ID 3199

GATEWAY NETMASK

+ Add Another

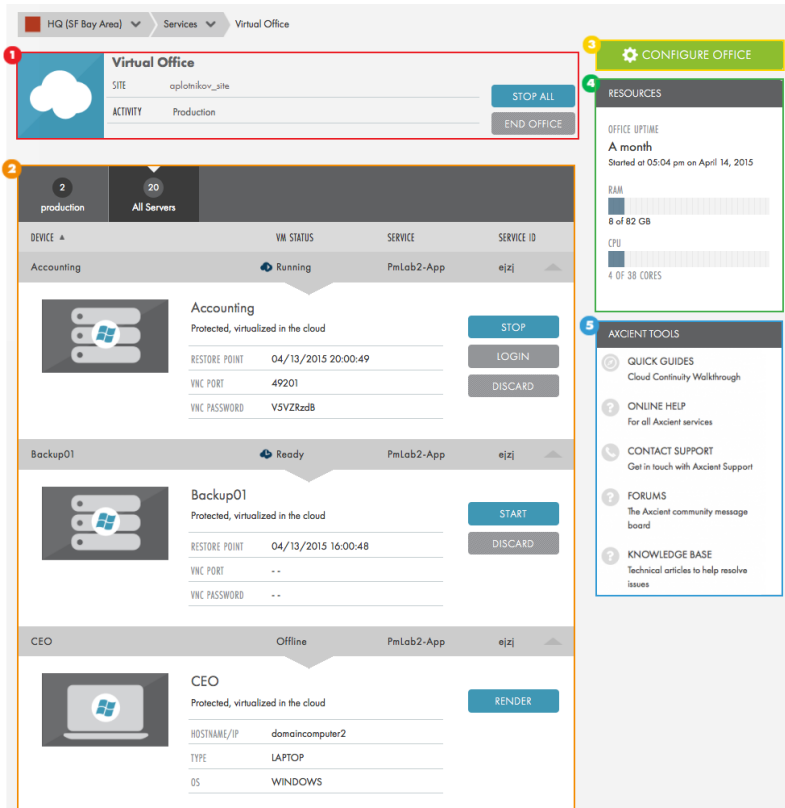
◀ BACK START VIRTUAL OFFICE

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:

Figure 1 - Virtual Office Page



1 Virtual Office Summary

This section provides a summary of the Virtual Office, showing which Clients 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.

Virtual Machine States

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

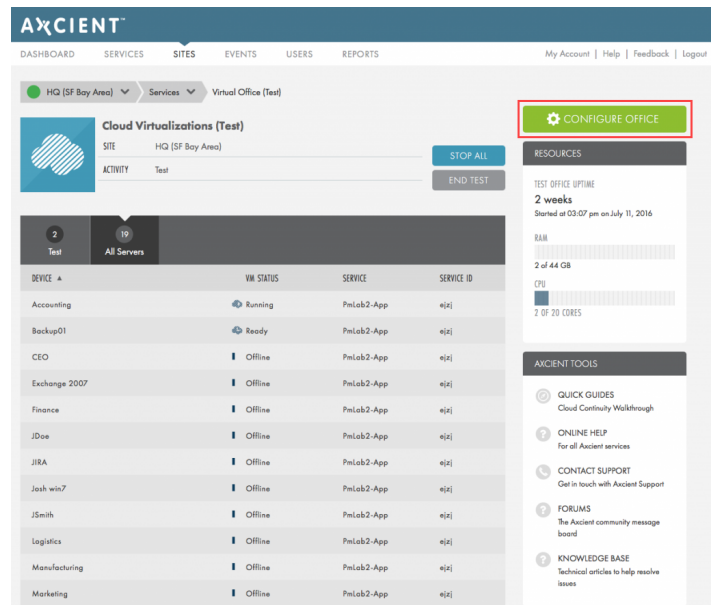
- The **Offline** state indicates that the VMs have yet to be rendered. To render a device, click the **Render** button.
- The **Ready** state indicates that the VMs have been rendered. This means that you have allocated CPU cores and RAM to the VM. You can optionally click the **Start** button to start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

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.

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

VPC IP 172.18.7.1
OUTBOUND ACCESS Disabled

Subnets	
GATEWAY	NETWORK
172.18.7.1	255.255.255.0
172.18.9.1	255.255.255.0

EDIT

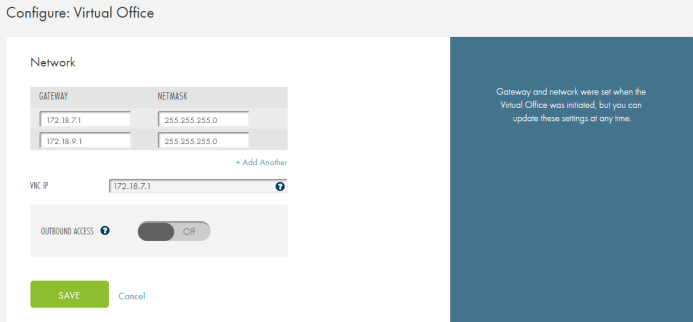
Configure the network environment for the virtual office. These can mimic the physical office settings.

STEP 2

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

- 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 Internet connectivity 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.



Configure: Virtual Office

Network

GATEWAY	NETMASK
172.18.7.1	255.255.255.0
172.18.9.1	255.255.255.0

+ Add Another

VNC IP: 172.18.7.1

OUTBOUND ACCESS: Off

SAVE Cancel

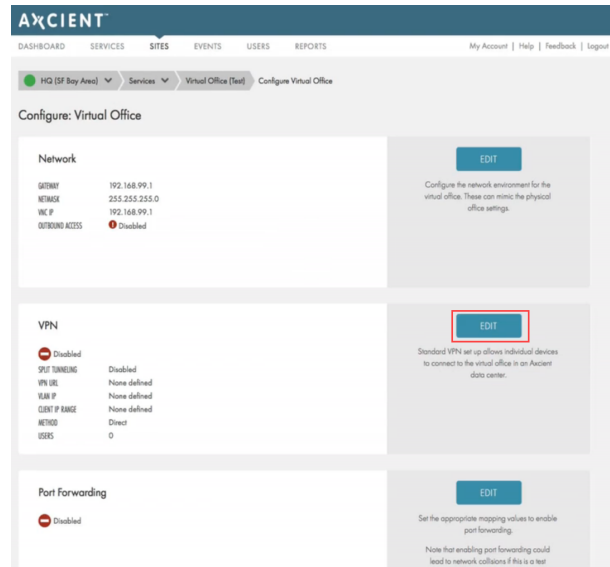
Gateway and network were set when the Virtual Office was initiated, but you can update these settings at any time.

Virtual Private Network (VPN) Settings

To configure or edit VPN settings:

STEP 1

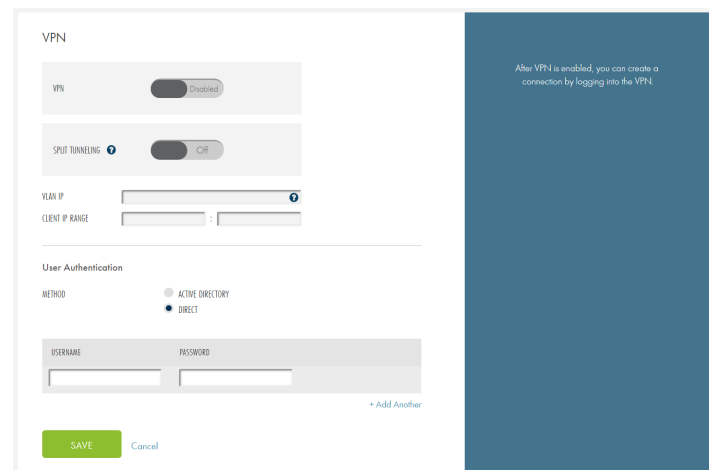
On the *Configure: Virtual Office* page, click the **Edit** button in the VPN section.



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**.



VPN

VPN Disabled

SPLIT TUNNELING Off

VLAN IP

CLIENT IP RANGE :

User Authentication

METHOD

ACTIVE DIRECTORY

DIRECT

USERNAME

PASSWORD

+ Add Another

SAVE Cancel

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

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.

The screenshot shows a configuration window titled "User Authentication". It has two main sections: "METHOD" and "CONNECTION TYPE".

- METHOD:** Two radio buttons are present: "ACTIVE DIRECTORY" (which is selected and highlighted with a red box) and "DIRECT".
- ACTIVE DIRECTORY SERVER:** A text input field.
- ACTIVE DIRECTORY DOMAIN:** A text input field.
- DOMAIN ADMINISTRATOR USERNAME:** A text input field.
- DOMAIN ADMINISTRATOR PASSWORD:** A text input field.
- CONNECTION TYPE:** Three radio buttons are present: "UNENCRYPTED" (selected), "LDAPS", and "START TLS".

At the bottom left, there are "SAVE" and "Cancel" buttons. On the right side of the image, there is a red callout box with the text "Option 1: Active Directory Integration".

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

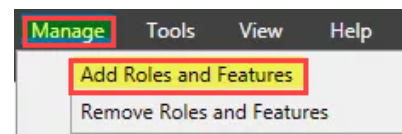
When configuring VPN connection settings, you can optionally integrate with Active Directory for authentication purposes. This option requires that you select a connection type, including *Unencrypted*, *LDAPS* (LDAP over SSL/TLS), or *Start TLS*. *LDAPS* and *Start TLS* connection types both require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

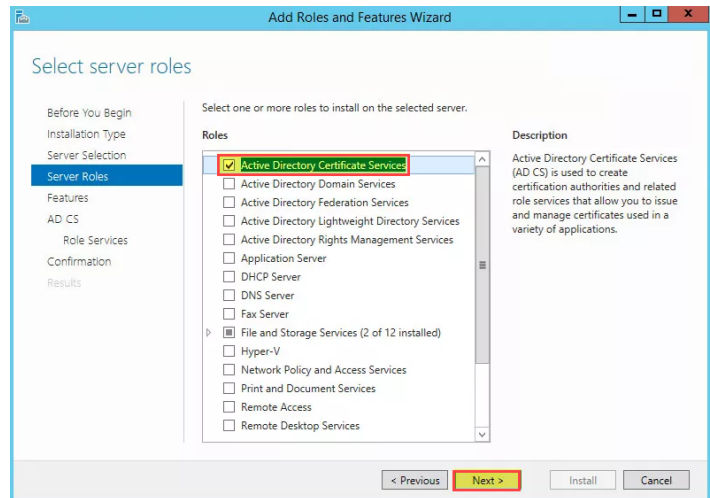
STEP 1

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



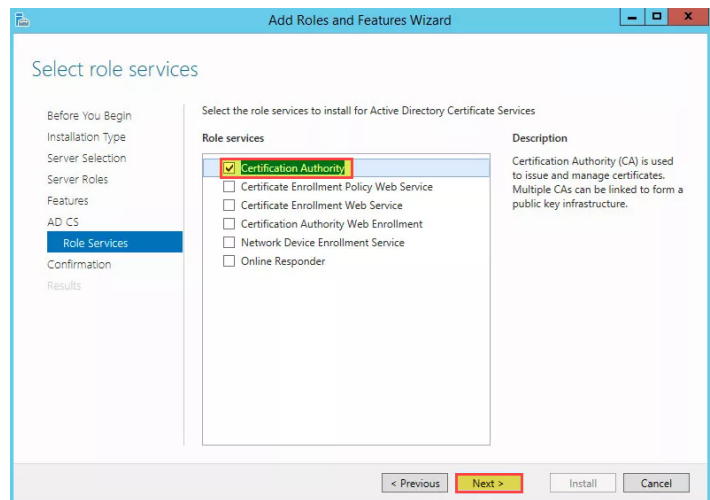
STEP 2

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.



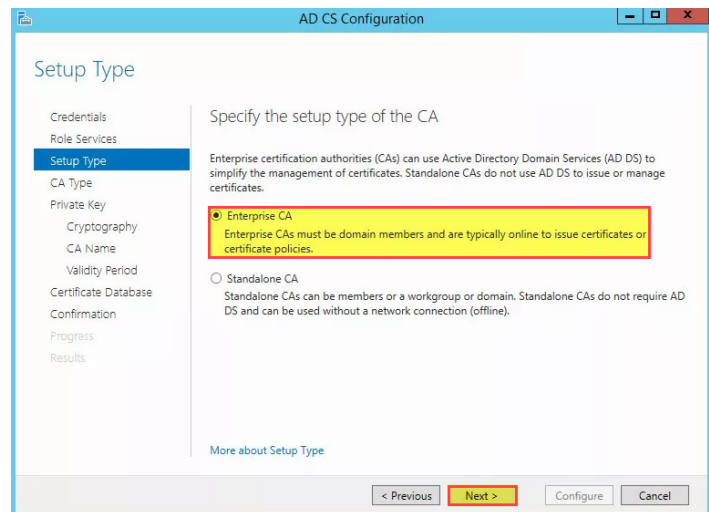
STEP 3

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.



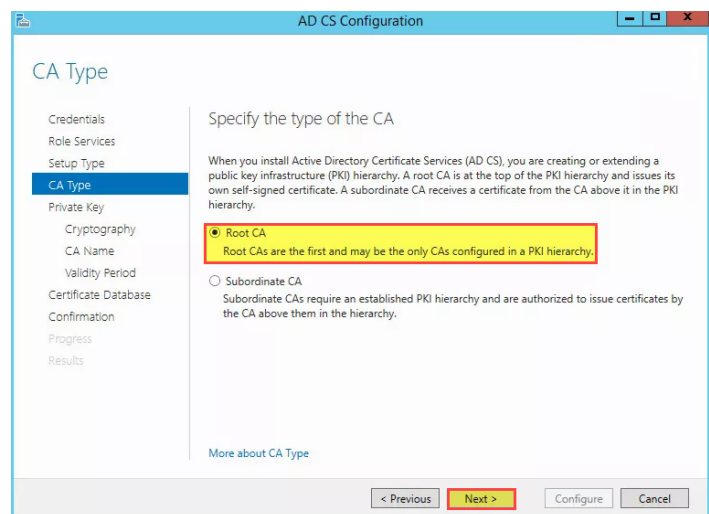
STEP 4

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



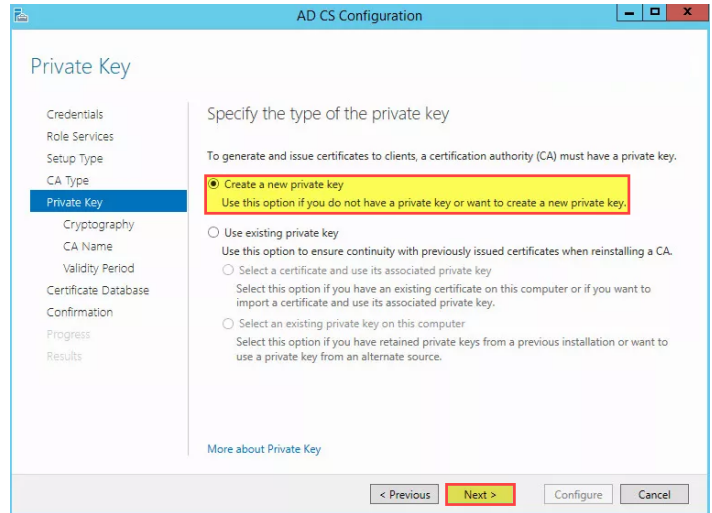
STEP 5

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.

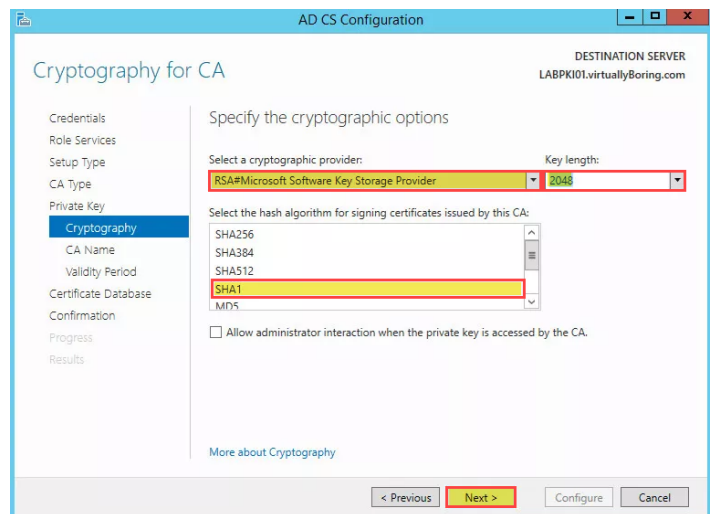


STEP 7

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**.

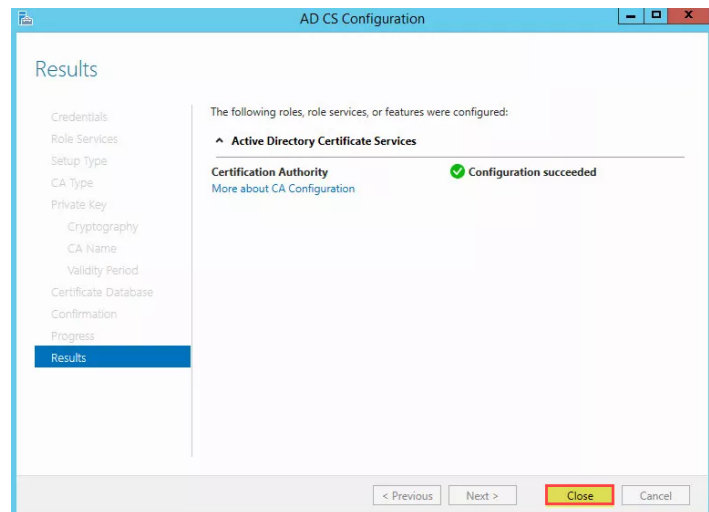
Click the **Next** button to continue.



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.



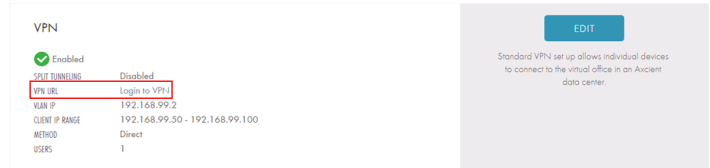
For alternative instructions, please reference the [LDAP over SSL \(LDAPS\) Certificate](#) Microsoft TechNet article.

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.

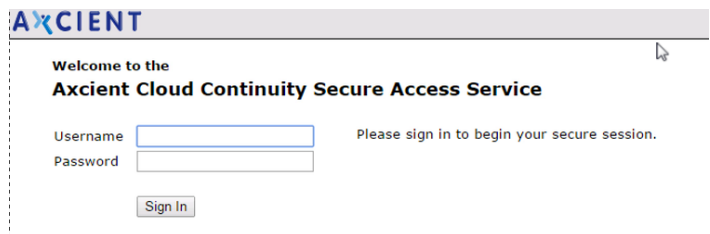
STEP 1

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



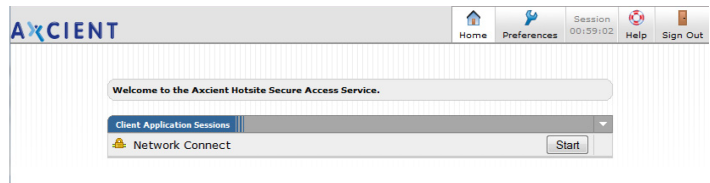
STEP 2

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 [Connecting to VPN Using an Alternative Connection Method](#) section below.

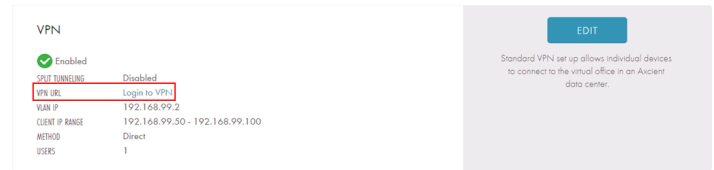
Connecting to VPN Using an Alternative Connection Method

Depending on browser type and settings, you might experience connection issues when attempting to connect to VPN, as described in the [Connecting to VPN](#) section. In these instances, an alternative VPN client can be utilized.

As an example, the following instructions provide steps for connecting through the Windows 10 VPN client (built-in).

STEP 1

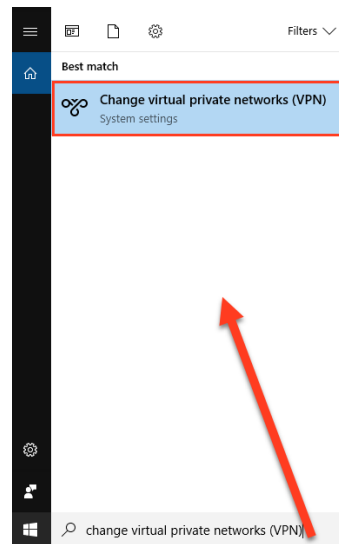
On the *Configure: Virtual Office* page, click the **Login to VPN** button in the VPN section.



STEP 2

From the local machine, download and install the *Pulse Secure* app from the [Microsoft Store](#).

When the *Pulse Secure* app is installed, click the **Windows Start** icon and enter *Change Virtual Private Networks (VPN)* in the search box. Then, click to launch *Change Virtual Private Networks (VPN)* settings.



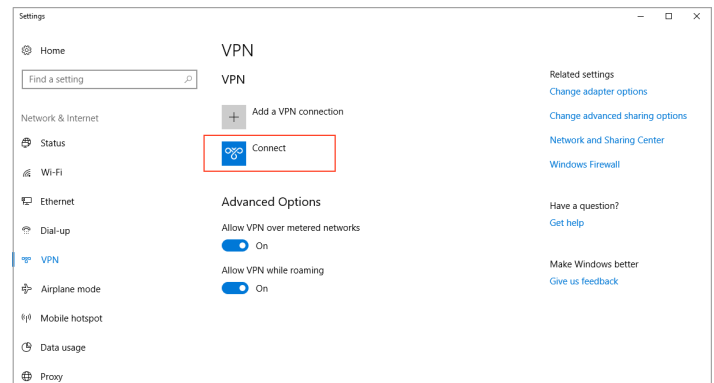
STEP 3

In the *VPN* window, click the **Add a VPN** button. Enter information into the *Add a VPN Connection* dialog box:

- In the *VPN Provider* field, select **Pulse Secure**.
- In the *Connection Name* field, enter a descriptive **connection name**.
- In the *Server Name or Address* field, paste the **VPN connection URL**.
- Click the **Save** button.

STEP 4

When the connection is configured, click the title of the new VPN connection to launch.



STEP 5

When prompted, enter the appropriate **user name** and **password** and then click the **OK** button to connect. These credentials are the same credentials created in the *User Authentication* field on the *VPN* screen.

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.

The screenshot shows the Axcient web interface for configuring a Virtual Office. The page title is "Configure: Virtual Office". It is divided into three main sections, each with an "EDIT" button:

- Network:** Shows settings for GATEWAY (192.168.99.1), NETMASK (255.255.255.0), VNC IP (192.168.99.1), and OUTBOUND ACCESS (Disabled). The "EDIT" button is located to the right.
- VPN:** Shows settings for a disabled VPN, with options for SPLIT TUNNELING (Disabled), VPN URL (None defined), VENDOR (None defined), CLIENT IP RANGE (None defined), METHOD (Direct), and USERS (0). The "EDIT" button is located to the right.
- Port Forwarding:** Shows the feature is currently Disabled. The "EDIT" button is highlighted with a red box. A note below states: "Note that enabling port forwarding could lead to network collisions if this is a test".

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](#)

CAUTION

Enabling port forwarding cloud 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.

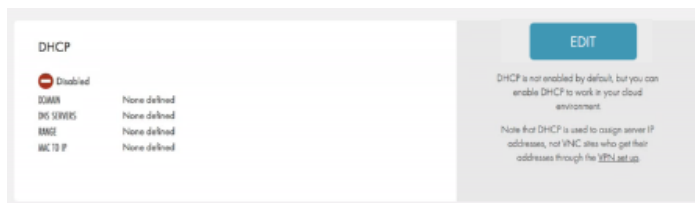
DHCP Settings

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.

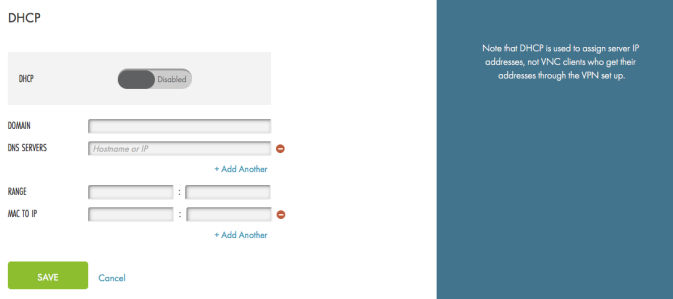


STEP 2

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.



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.

The screenshot shows the Axcient dashboard with the 'Configure: Virtual Office' page. The 'Port Forwarding' section is highlighted with a red box around the 'EDIT' button. The page includes sections for Network, VPN, and Port Forwarding, each with an 'EDIT' button.

Section	Status	Details
Network	Disabled	Gateway: 192.168.99.1, Network: 255.255.255.0, VEC IP: 192.168.99.1
VPN	Disabled	VPN URL: None defined, SUB IP: None defined, CLIENT IP RANGE: Direct, USERS: 0
Port Forwarding	Disabled	None

STEP 2

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

The screenshot shows the 'Site-To-Site VPN' settings page. The 'EDIT' button is highlighted with a red box. The page includes a 'WHITELISTED IPS' section with a value of 'None'.

Section	Status	Details
Site-To-Site VPN	Disabled	None
WHITELISTED IPS	None	None

STEP 3

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 **Add Another** to whitelist additional IP addresses.
- Configure the Endpoint, including:
 - 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

SITE-TO-SITE VPN Disabled

WHITELISTED IPS + Add Another

SAVE

Endpoint 1

ENDPOINT NAME

KEY PASSWORD ⓘ

CONFIGURED USING Static IP DHCP

GATEWAY

NETMASK

IP OF ENDPOINT

DNS

ADD ENDPOINT

DONE

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.

1

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.

The screenshot shows the Axcient management console interface. At the top, there is a navigation bar with 'Axcient' logo and menu items: DASHBOARD, SERVICES, SITES, EVENTS, USERS, REPORTS. Below the navigation bar, there is a breadcrumb trail: HQ (SF Bay Area) > Services > Virtual Office (Test) > Configure Virtual Office. The main content area is titled 'Configure: Virtual Office' and contains three configuration panels:

- Network:** Shows settings for GATEWAY (192.168.99.1), NETMASK (255.255.255.0), VNC IP (192.168.99.1), and OUTBOUND ACCESS (Disabled). An 'EDIT' button is present.
- VPN:** Shows settings for SPLIT TUNNELING (Disabled), VPN URL (None defined), VLAN IP (None defined), CLIENT IP RANGE (None defined), METHOD (Direct), and USERS (0). An 'EDIT' button is present.
- Port Forwarding:** Shows a status of Disabled. An 'EDIT' button is present and highlighted with a red box.

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. For examples and instructions, please reference the [Axcient Knowledge Base](#).

Additional Failover Steps for Windows Server 2008 SP1

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

Download the KB955430 Package

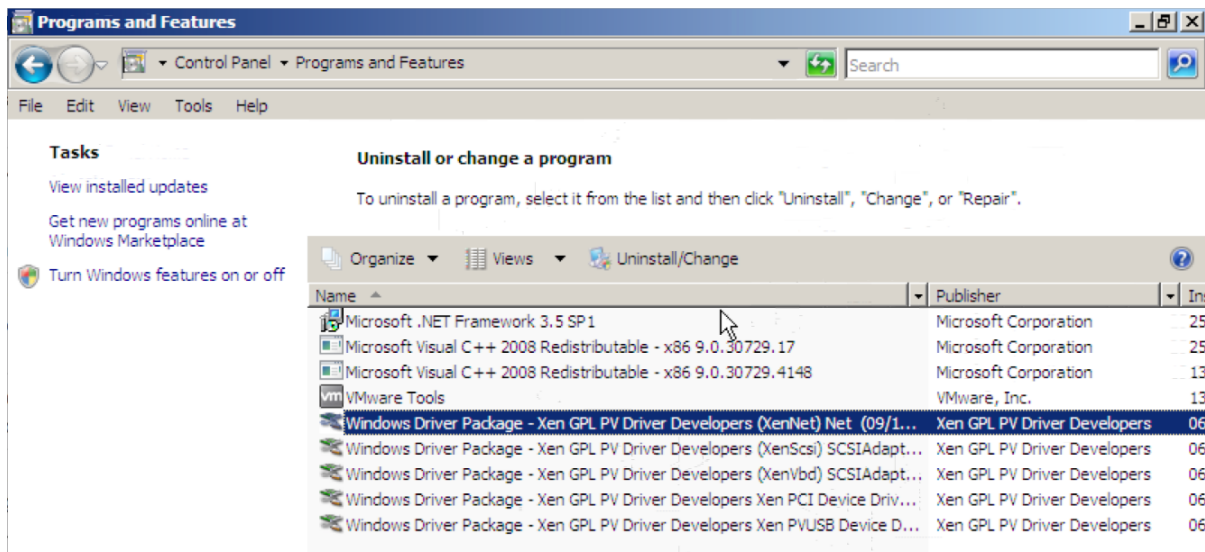
When protecting a device with the Windows Server 2008 SP1 operating system, you must confirm that *the 955430 package has been installed on the target device* before performing the recovery. Please refer to the [Microsoft KB955430](#) article for more information and to download the package.

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

Run Script to Correctly Apply Drive Letters

With the VM powered on and the GPLPV drivers installed, confirm that the GPLPV drivers have been successfully installed in the *Program and Features* window.

Figure 2 - Confirm GPLPV Drivers



When the GPLPV drivers have been successfully installed, run the following script, which is automatically copied over when deploying a Cloud Failover:

```
%SYSTEMDRIVE%/Windows/System32/fixdisks.js
```

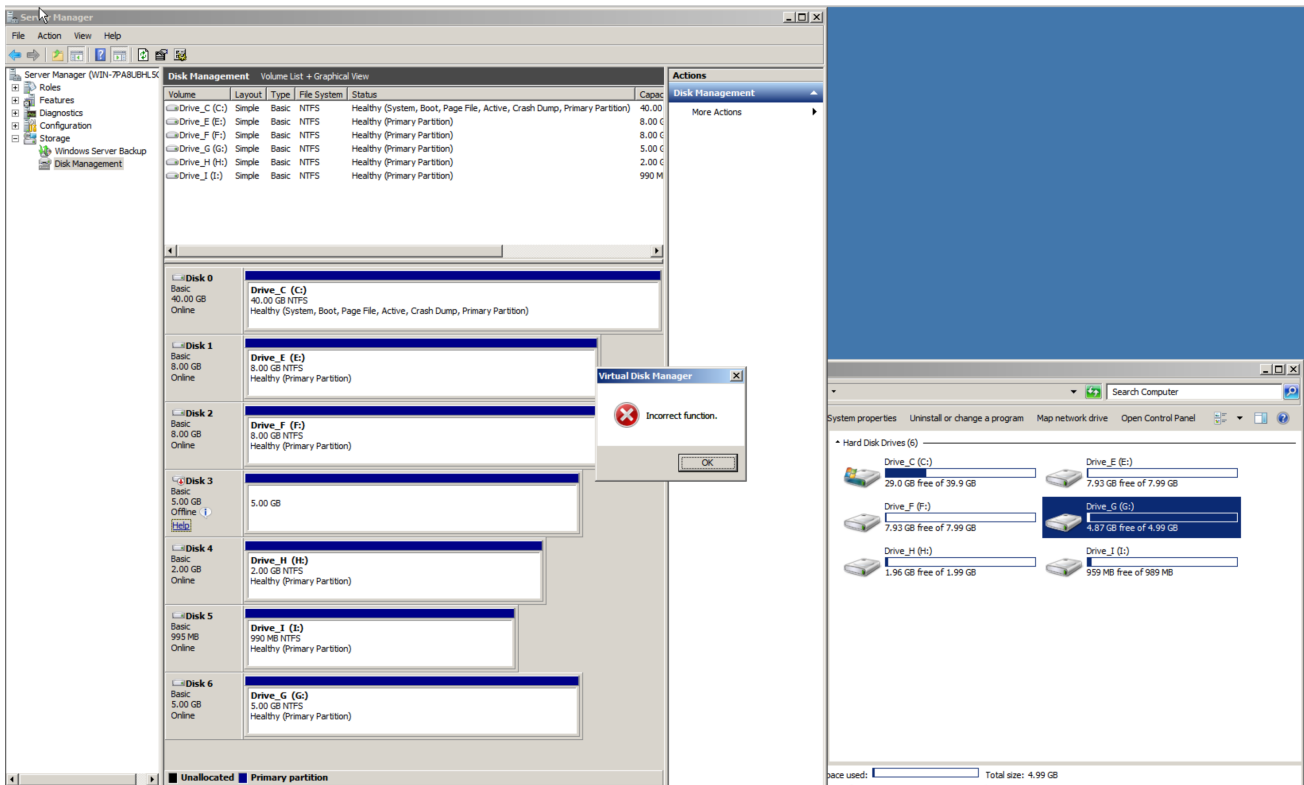
Reboot the VM when the script has finished successfully. The Failover VM of the Windows Server 2008 SP1 is now ready to be used.

Failing Over a Device with 5+ Drives

When failing over a device with 5 drives or more in either a test or production environment, you might see an extra disk displayed in the *Disk Management/Device Manager*. This extra disk will not show up in the *My Computer* screen, and you will receive an *Incorrect Function* error when attempting to bring the disk online.

This extra disk will not affect the failover or any other recovery-related process associated with the failover VM.

Figure 3 - 5+ Disk Error



Runbooks

Runbooks allow you to configure an automatic deployment plan for virtualized devices in the Virtual Office. You must first configure a subnet in the Network section that matches the subnet of the devices to be virtualized. By default, the subnet settings in the Network section are set by the network settings of the Appliance.

Runbooks can be leveraged for the following use cases:

- **Test Disaster Recovery** – Create a Runbook to test the user’s disaster recovery plan in the event of a real disaster situation. This will help address any potential issues that may arise so that if a disaster occurs, the user will experience no issues with deploying a production Virtual Office.
- **Production Disaster Recovery** – Create a Runbook to automatically deploy a production Virtual Office with all the desired devices and configurations. The user will require the help of Axcient Support to help shut down the Virtual Office when ready.

Runbooks are unique to each Virtual Office. After shutting down a Virtual Office, the Runbook changed state to *Ready*.

Configuring a Runbook will allow you to configure:

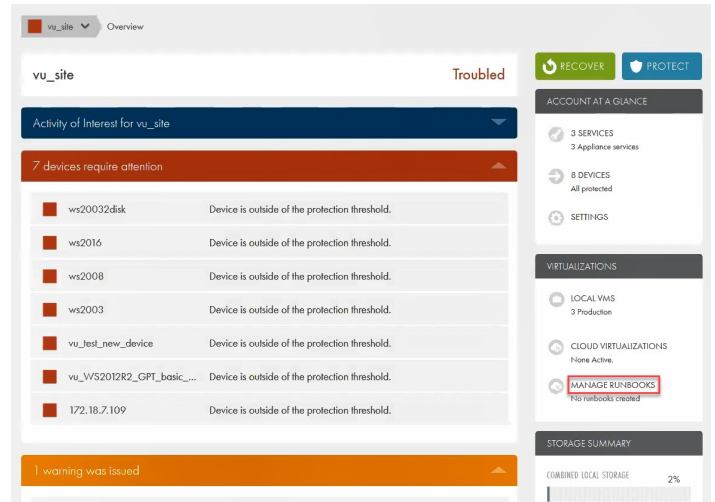
- Devices to be virtualized
- The order in which the devices should be virtualized
- Resources to allocate to each device
- Wait time between the deployment of each device

Create a New Runbook

To create a new Runbook:

STEP 1

On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.

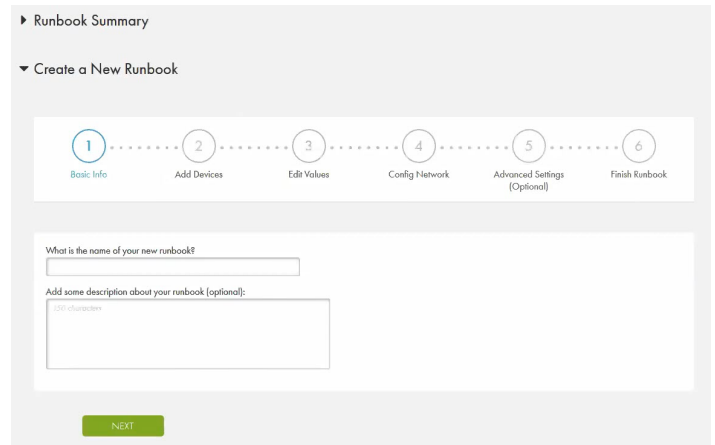


STEP 2

In the *Create a New Runbook* section of the page, enter the **name** of the new Runbook.

Optionally, enter a **description** for the Runbook.

Click the **Next** button to continue.



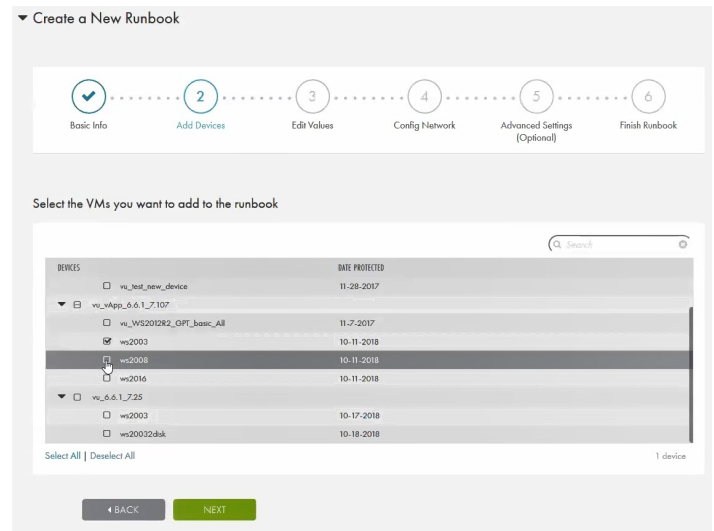
STEP 3

In the *Add Devices* screen, use the checkboxes to select the **devices** to include in the Runbook.

Note: A device can only belong to one Runbook at a time.

Note: The Virtual Office will automatically select the most recent recovery point to use in deploying the Virtual Office.

Click the **Next** button to continue.

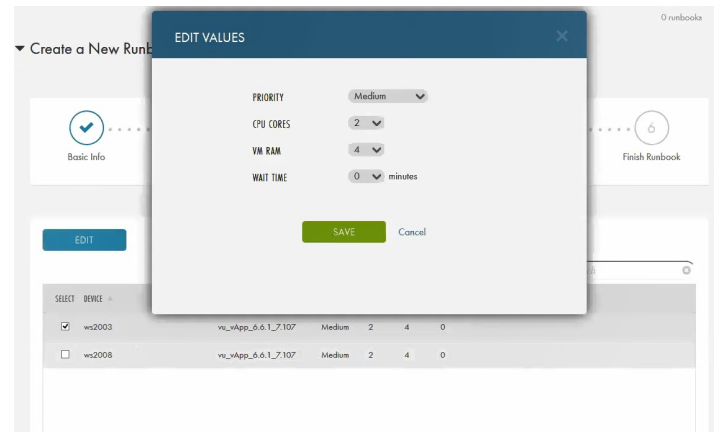


STEP 4

In the *Edit Values* section, review the selected devices. Click the **Edit** and **Delete** buttons to edit or delete any of the devices. You will be able to edit the following:

- In the *Priority* tab, specify the boot priority of the selected device(s). Devices with the same boot priority will be started at the same time.
- In the *CPU Cores* tab, specify the number of CPU cores to allocate to the selected device(s).
- In the *VM Ram* tab, edit the amount of virtual RAM to allocate to the selected device(s).
- In the *Wait Time* tab, edit the wait time between boot priority. For example, if you have a device with a Medium boot priority and a 15 minute wait time, and then a second device with a Low boot priority, the Runbook will wait 15 minutes before deploying the Low priority device. You can also configure different wait times between devices with the same priority.
- Click the **Save** button when you are finished.

Click the **Next** button to continue.



STEP 5

In the *Network* screen, you can configure the following:

- In the *Network* section, configure the **Gateway IP** and **Netmask** of the Virtual Office. Please refer to the [Configure Virtual Office](#) section for more information.
- In the *VNC IP* section, enter the **IP address** for the VNC clients, which can be any available (unused) IP address in the Virtual Office. This field is optional when you configure the network in the Runbook. If you leave this field blank, it will be filled in automatically after the Runbook is created from the first subnet. Please refer to the [Configure Virtual Office](#) section for more information.
- Optionally, enable the *Outbound Access* option to allow outbound access to the Internet. Please refer to the [Configure Virtual Office](#) section for more information.

Click the **Next** button to continue.

The screenshot displays the 'Network' configuration screen. At the top, a progress bar indicates the current step is '4 Config Network'. The main configuration area includes:

GATEWAY	NETMASK
172.18.8.1	255.255.255.0
172.18.7.1	255.255.255.0

Below the table is a 'VNC IP' field with a dropdown menu and a '+ Add Another' link. At the bottom of the configuration area is an 'OUTBOUND ACCESS' toggle switch, which is currently turned 'On'. Navigation buttons 'BACK' and 'NEXT' are located at the bottom of the screen.

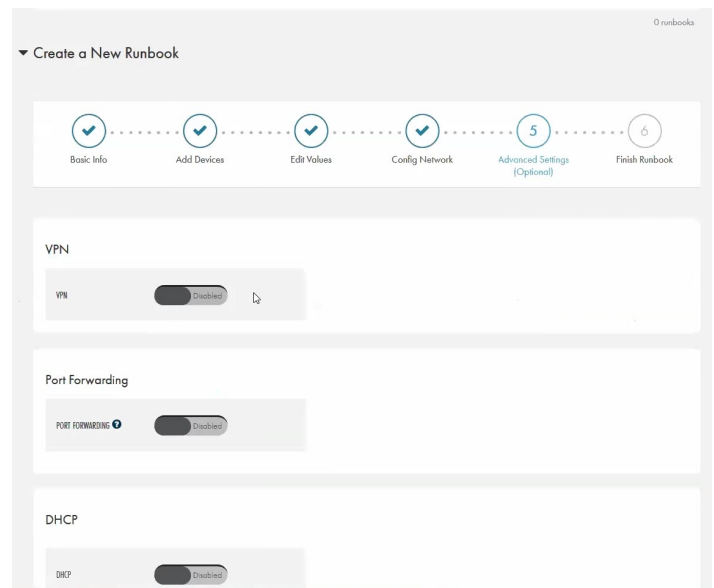
STEP 6

In the *Advanced Settings* section, you can enable and configure the following methods for accessing devices in the Virtual Office:

- VPN
- User Authentication
- Port Forwarding
- DHCP
- Site-to-Site VPN
- Site-to-Site IPSec VPN

You can also update these settings after the Runbook has started from the *Configure Office* page. Please refer to the [Configure Virtual Office](#) section for more information.

Click the **Next** button to continue

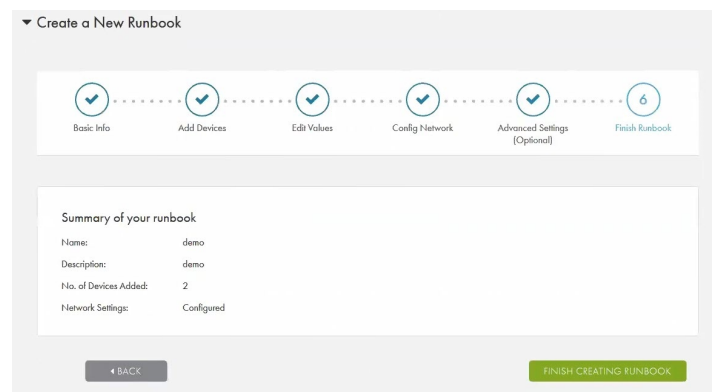


STEP 7

In the *Finish Runbook* screen, review summary information to confirm that the Runbook settings are correct.

Click the **Finish Creating Runbook** button to create the Runbook.

The Runbook will now be listed under the Runbook Summary section where you can edit or delete the Runbook as needed.



Start a Runbook

You can start a Runbook in one of the following ways:

- On the *Site* or *Service* page, click the **Recover** button and then select a **Runbook**.
- On the *Runbook* page, select a **Runbook** and then click the **Run Runbook** button.

A Runbook cannot be started under the following circumstances:

- *A Virtual Office or Runbook is already running under the Site*
Runbooks are Site-specific, and only a single Runbook may be running at a time for any given Site. If a Runbook is already running under a Site, the user will be unable to deploy a second Runbook.
- *No Subnet is configured in the Runbook for at least one device*
A subnet must be configured for at least one of the devices in the Runbook in order to start the Runbook. If no subnet is configured for any devices in the Runbook, the Runbook will not start.

If a subnet is configured for only one or some of the devices, you will need to create the additional subnets in the *Virtual Office Configuration* page in order to virtualize the remaining devices when the Runbook is in a Running state.

Additionally, you can edit the Runbook to create any additional subnets. The devices with subnets created after the Runbook has been deployed will not adhere to the device boot order configured in the Runbook.

This example will start on the *Runbook* page.

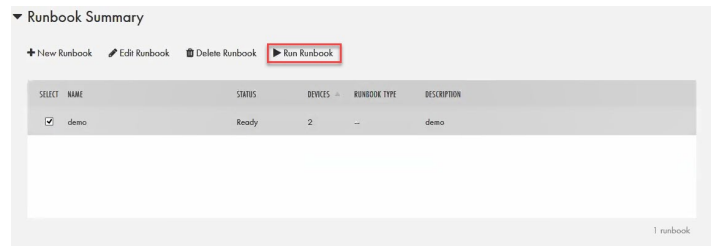
STEP 1

On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.

The screenshot displays the 'vu_site' Overview page in a 'Troubled' state. The main content area shows a list of 7 devices that require attention, all of which are outside of the protection threshold. The devices listed are: ws20032disk, ws2016, ws2008, ws2003, vu_test_new_device, vu_VS2012R2_GPT_basic..., and 172.18.7.109. Below this list, a warning is issued for the device vu_vApp_6.6.1_7.107, stating 'Appliance lost network connectivity.' The right-hand sidebar provides a summary of the site's status, including 3 services (3 appliance services), 8 devices (all protected), and 1 runbook created. The storage summary indicates that 2% of the combined local storage is used, with a total of 98 GB of 4 TB local storage available.

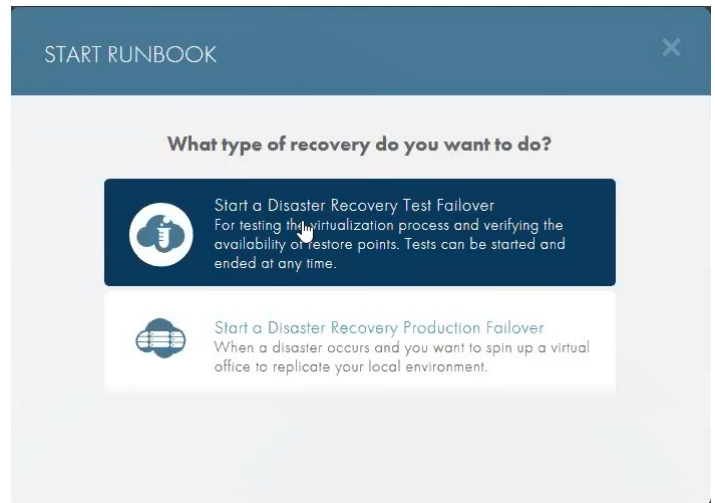
STEP 2

In the *Runbook Summary* section of the page, use the checkboxes to select the **Runbook** and then click the **Run Runbook** button.



STEP 3

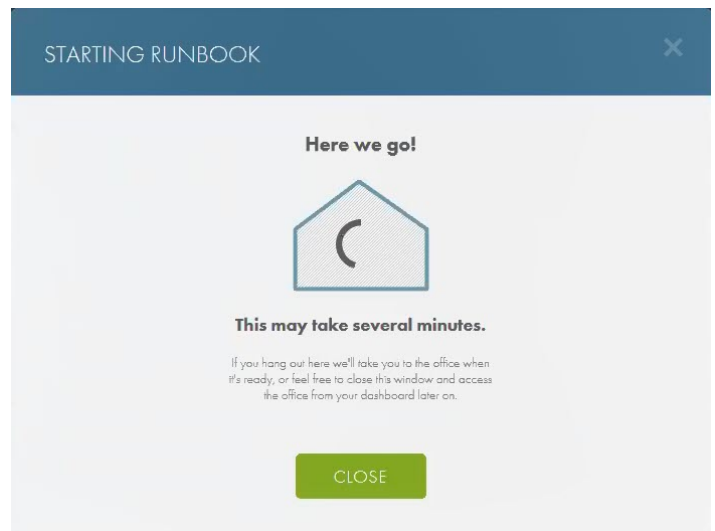
On the *Start Runbook* screen, select the type of Virtual Office to deploy (Test or Production).



STEP 4

The Runbook will start and the *Starting Runbook* screen will display the progress.

You can click the **Close** button to leave the screen while the Runbook starts.



Edit a Runbook

You can edit a Runbook whenever needed, including when the Runbook is inactive and when it is running.

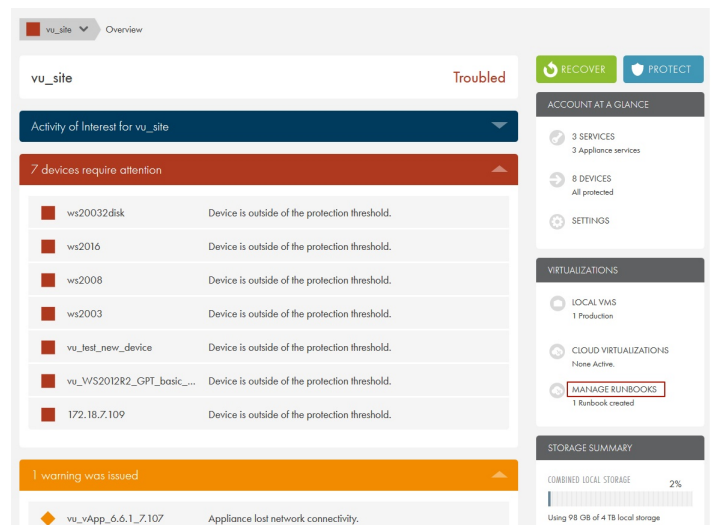
While a Runbook is inactive, all aspects of the Runbook and Virtual Office can be edited; however, not all aspects of the Runbook can be edited while the Runbook is running. For example, you *cannot* edit included devices when the Runbook is running, but you *can* edit network information.

If the Runbook is running, you can incorporate changes on the *Advanced Settings* page. However, these changes will not apply until you restart the Runbook. Additionally, if you update Virtual Office settings from the Runbook, the settings will not change for the running Runbook.

To edit a Runbook:

STEP 1

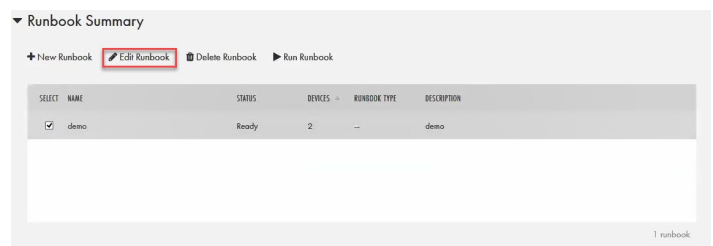
On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.



STEP 2

In the *Runbook Summary* section of the page, use the checkboxes to select the **Runbook** and then click the **Edit Runbook** button.

Update the Runbook as appropriate.



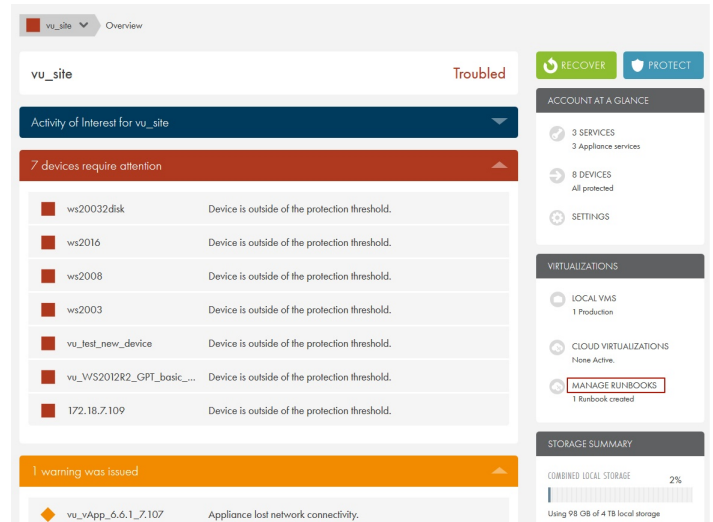
Delete a Runbook

When a Runbook is deleted, *it will not be recoverable*.

To delete a Runbook:

STEP 1

On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.



STEP 2

In the *Runbook Summary* section of the page, use the checkboxes to select the **Runbook** and then click the **Delete Runbook** button.

The Runbook is now permanently deleted.

