Axcient

Axcient Fusion Recovery Guide

Cloud Failover (Virtual Office)

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

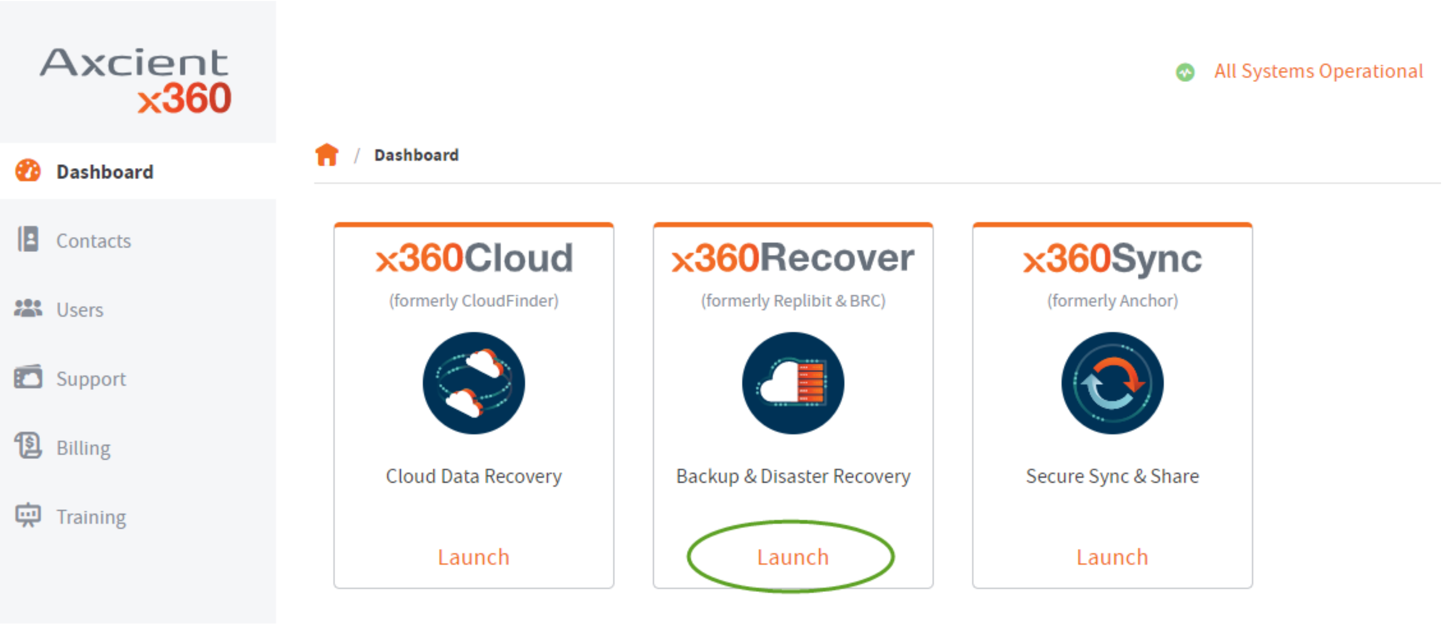
- Create a Virtual Office running in the Axcient data center that matches existing server configurations.
- Configure the network settings for the Virtual Office, including:
  - Provide secure access to the Virtual Office by configuring the VPN.
  - Configure multiple subnets for the Virtual Office.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

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

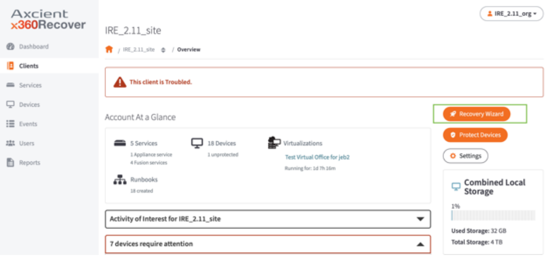
Get started: Access the RMC (Remote Management Console)

Log in to the x360 Portal at https://partner.axcient.com/login

Click **Launch** on the x360Recover tile.



The Remote Management Console (RMC) opens and displays the Dashboard.



This client is Troubled.

Running for: 1d 7h 16m

Used Storage: 32 GB

Total Storage: 4 TB

Activity of Interest for IRE_2.11_site

7 devices require attention

Start the Virtual Office

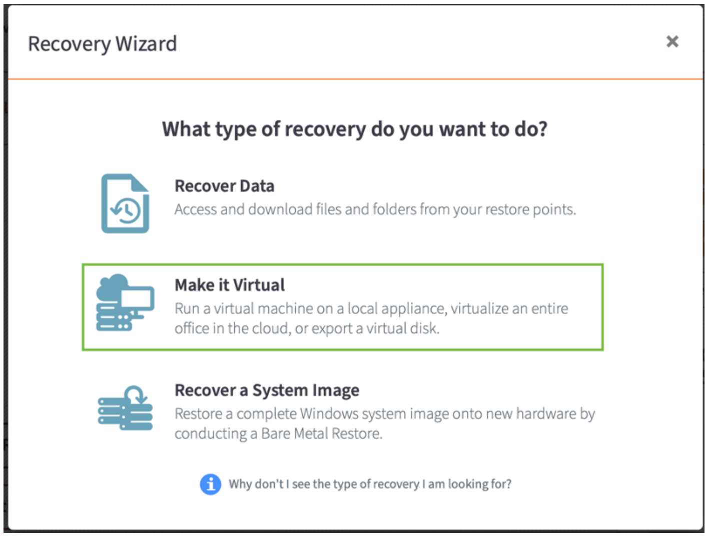
To start the Virtual Office:

STEP 1

From the Axcient Web Application, navigate to the *Client Details* page and click the Recovery Wizard button.

STEP 2

On the *Recovery Wizard* screen, click the Start Virtualization option.



Recovery Wizard

What type of recovery do you want to do?

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

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

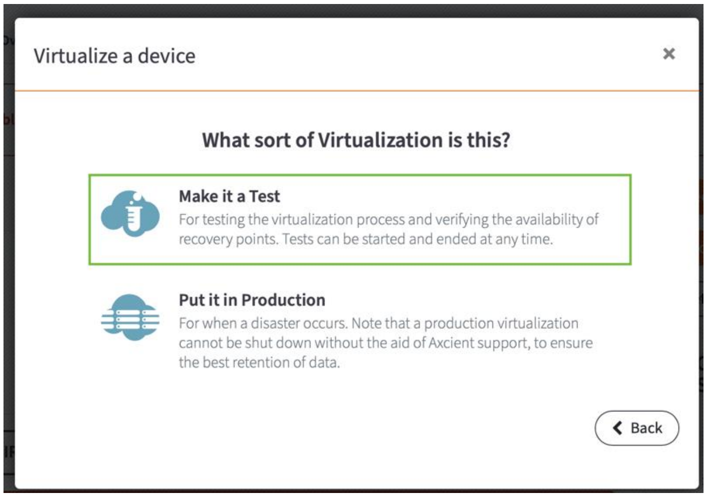
Recover a System Image
Restore a complete Windows system image onto new hardware by conducting a Bare Metal Restore.

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

STEP 3

Select the type of local virtualization to deploy:

- Select the Run as Test option to test the virtualization process and verify the availability of recovery points in case of an emergency.
- Select the Put it in Production option in the event ofa disaster. This local failover VM can be used to temporarily replace production devices until a permanent replacement is ready.



Virtualize a device

What sort of Virtualization is this?

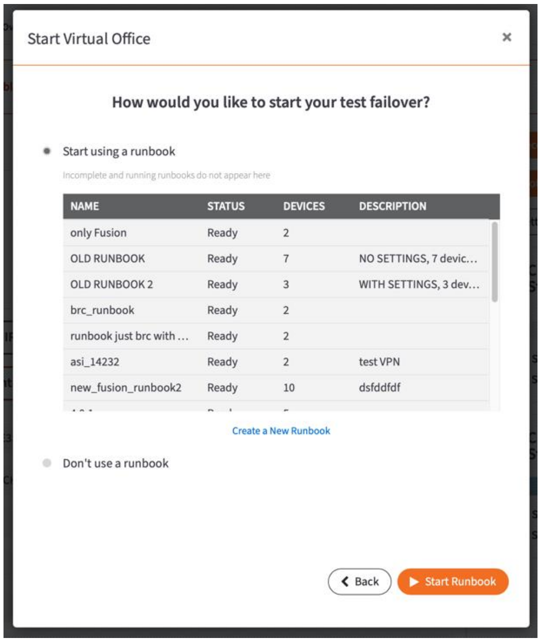
Make it a Test
For testing the virtualization process and verifying the availability of recovery points. Tests can be started and ended at any time.

Put it in Production
For when a disaster occurs. Note that a production virtualization cannot be shut down without the aid of Axcient support, to ensure the best retention of data.

STEP 4

Select how to start the Virtual Office:

- Select the Start using a Runbook radio button to select a pre-configured Runbook for deploying the Virtual Office. For more information, please reference the [Runbooks]() section of this guide.
- Select the Don't use a Runbook radio button to manually configure the Virtual Office, including network settings, device configurations, and more.



Start Virtual Office

How would you like to start your test failover?

● Start using a runbook

Incomplete and running runbooks do not appear here

NAME	STATUS	DEVICES	DESCRIPTION
only Fusion	Ready	2	
OLD RUNBOOK	Ready	7	NO SETTINGS, 7 devic...
OLD RUNBOOK 2	Ready	3	WITH SETTINGS, 3 dev...
brc_runbook	Ready	2	
runbook just brc with ...	Ready	2	
asi_14232	Ready	2	test VPN
new_fusion_runbook2	Ready	10	dsfddfdf

○ Don't use a runbook

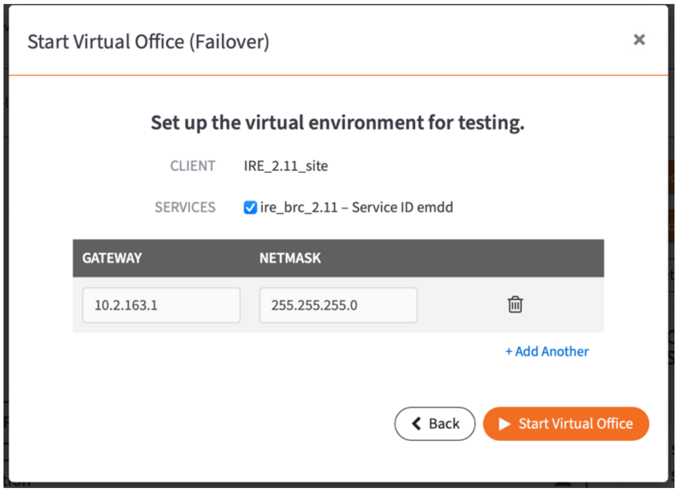
STEP 4

If you selected not to use a Runbook, configure settings for the Virtual Office:

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**.
- To add a new subnet for the Virtual Office, click **+ Add Another**. 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.

CLIENT IRE_2.11_site

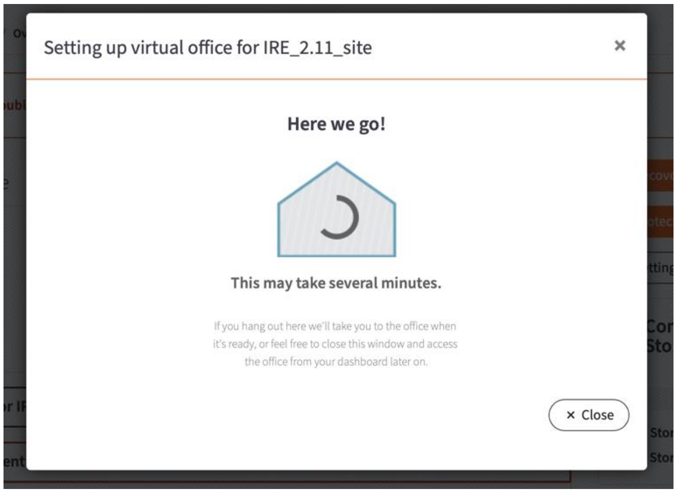
SERVICES ☑ ire_brc_2.11 – Service ID emdd

GATEWAY	NETMASK
10.2.163.1	255.255.255.0

STEP 5

The Virtual Office is being set up.

- You will taken to the Virtual Office when it is ready.
- If you opt to close this window, you can access the Virtual Office from the dashboard later



Setting up virtual office for IRE_2.11_site

Here we go!

This may take several minutes.

If you hang out here we'll take you to the office when it's ready, or feel free to close this window and access the office from your dashboard later on.

Virtual Office Page

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

The *Virtual Office* page includes the following sections:

❶ Virtual Office Summary

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

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

❷ Device List

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

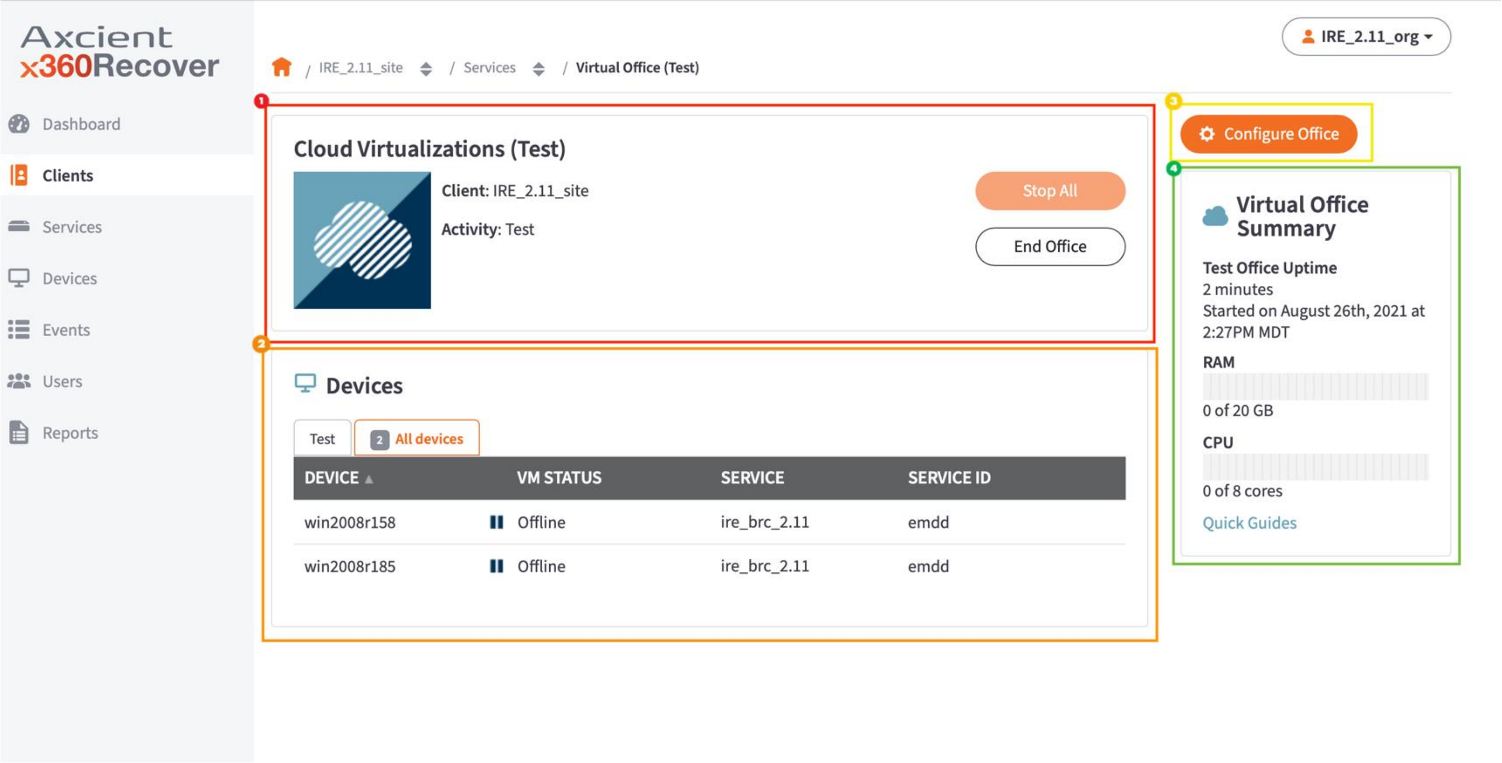
❸ Configure Office

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

❹ Resources

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

Figure 1 - Virtual Office Page



Cloud Virtualizations (Test)

Client: IRE_2.11_site

Activity: Test

Devices

DEVICE ▲	VM STATUS	SERVICE	SERVICE ID
win2008r158	Offline	ire_brc_2.11	emdd
win2008r185	Offline	ire_brc_2.11	emdd

Virtual Office Summary

Test Office Uptime
2 minutes
Started on August 26th, 2021 at 2:27PM MDT

RAM
0 of 20 GB

CPU
0 of 8 cores

Virtual Machine States

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

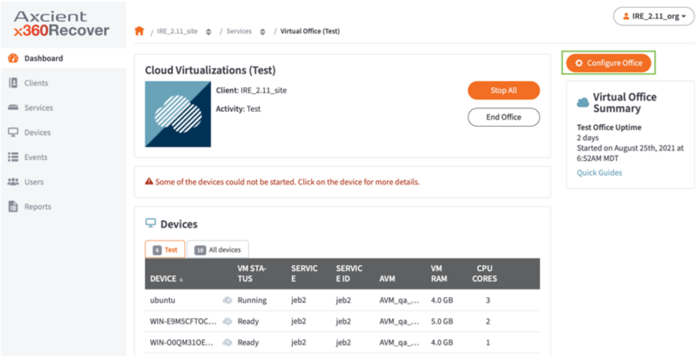
- Offline—VMs that have yet to be rendered. To render a device, click the Render button.
- Ready—VMs that have been rendered, but are not yet running. This means that you have allocated CPU cores and RAM to the VM. To start a device and make it accessible, click the Start button.
- Starting—VMs that are in the process of starting after clicking the Start button.
- Running—live VMs that are accessible through 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 to the device to an *Offline* state.
- Stopping—VMs that are shutting down after clicking the Stop button. These devices will revert back to the *Prepared* state.

Configure the Virtual Office

You can configure the cloud failover environment for various network options. To configure these options:

STEP 1

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



Cloud Virtualizations (Test)

Client: IRE_2.11_site

Activity: Test

Virtual Office Summary

Test Office Uptime
2 days
Started on August 25th, 2021 at 6:52AM MDT

Some of the devices could not be started. Click on the device for more details.

Devices

DEVICE	VM STATUS	SERVICE	SERVICE ID	AVM	VM RAM	CPU CORES
ubuntu	Running	jeb2	jeb2	AVM_qa_...	4.0 GB	3
WIN-E9M5CFTOC...	Ready	jeb2	jeb2	AVM_qa_...	5.0 GB	2
WIN-O0QM31OE...	Ready	jeb2	jeb2	AVM_qa_...	4.0 GB	1

Network Settings

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

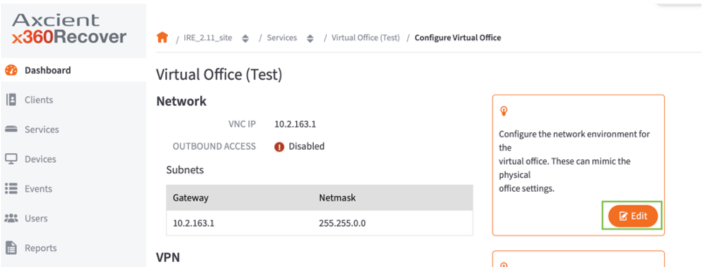
You must configure at least one subnet in the Virtual Office. This will be required when preparing a device.

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

To edit the network settings:

STEP 2

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


Axcient
x360Recover
/ IRE_2.11_site / Services / Virtual Office (Test) / Configure Virtual Office
Dashboard
Clients
Services
Devices
Events
Users
Reports
Edit

Virtual Office (Test)

Network

VNC IP 10.2.163.1

OUTBOUND ACCESS Disabled

Subnets

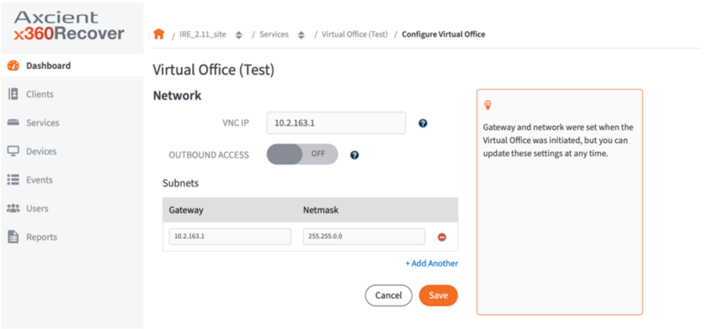
Gateway	Netmask
10.2.163.1	255.255.0.0

VPN

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:



Virtual Office (Test)

Network

VNC IP 10.2.163.1

OUTBOUND ACCESS OFF

Subnets

Gateway	Netmask
10.2.163.1	255.255.0.0

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

- 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.

Virtual Private Network (VPN)

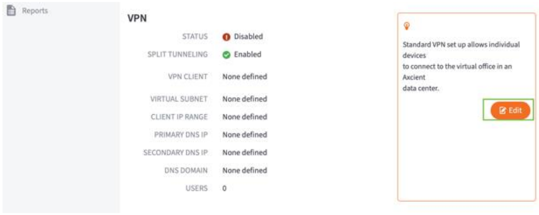
You can configure a VPN to create a secure connection over the public Internet so that outside devices can connect.

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

To edit VPN settings:

STEP 1

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



VPN

STATUS	Disabled
SPLIT TUNNELING	Enabled
VPN CLIENT	None defined
VIRTUAL SUBNET	None defined
CLIENT IP RANGE	None defined
PRIMARY DNS IP	None defined
SECONDARY DNS IP	None defined
DNS DOMAIN	None defined
USERS	0

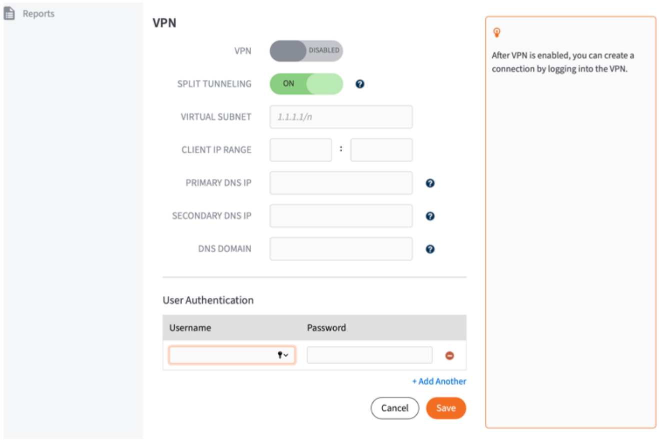
Standard VPN set up allows individual devices
to connect to the virtual office in an Axcient
data center.

STEP 2

On 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 *Virtual Subnet* 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, create login credentials for users to access the VPN. Click the Add Another button to create multiple user logins.

Click the Save button to save any new configurations.



VPN

VPN	DISABLED
SPLIT TUNNELING	ON
VIRTUAL SUBNET	1.1.1.1/n
CLIENT IP RANGE	:
PRIMARY DNS IP	
SECONDARY DNS IP	
DNS DOMAIN	

User Authentication

Username	Password

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

Connecting to VPN

When a VPN network has been configured in the Virtual Office, you will need to connect to the VPN network using OpenVPN agent.

To connect to the VPN network:

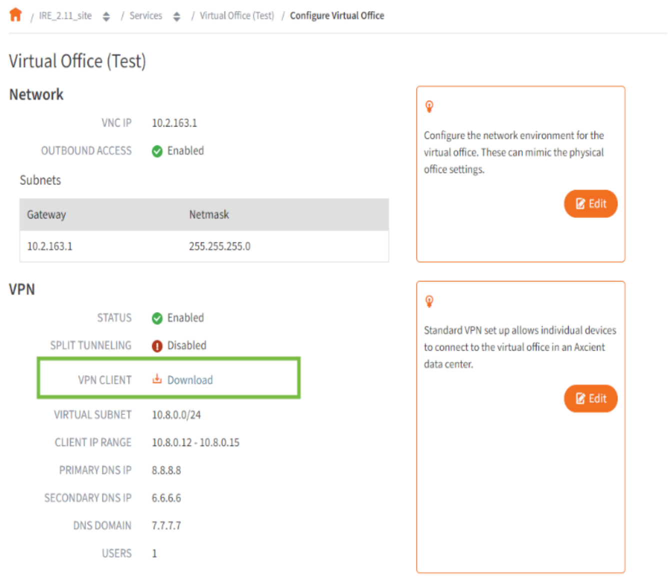
First install OpenVPN client on your laptop or desktop from where you will be connecting to virtual office VPN

OpenVPN Client can be downloaded from here

STEP 1

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

- One the VPN has beenconfigured successfully, click *Download* to download VPN client config files. These must be downloaded to the config folder of the OpenVPN agent.


IRE_2.11_site / Services / Virtual Office (Test) / Configure Virtual Office
Edit
Edit

Virtual Office (Test)

Network

VNC IP 10.2.163.1

OUTBOUND ACCESS ✓ Enabled

Subnets

Gateway	Netmask
10.2.163.1	255.255.255.0

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

VPN

STATUS ✓ Enabled

SPLIT TUNNELING ! Disabled

VPN CLIENT Download

VIRTUAL SUBNET 10.8.0.0/24

CLIENT IP RANGE 10.8.0.12 - 10.8.0.15

PRIMARY DNS IP 8.8.8.8

SECONDARY DNS IP 6.6.6.6

DNS DOMAIN 7.7.7.7

USERS 1

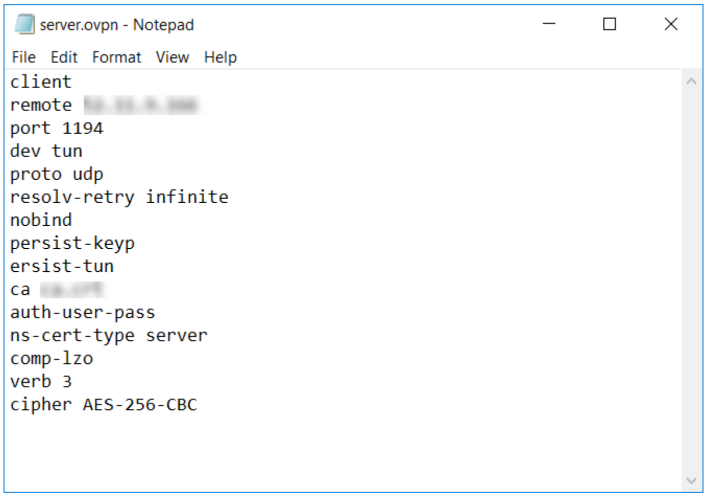
Standard VPN set up allows individual devices to connect to the virtual office in an Axcient data center.

STEP 2a

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

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

Confirm that the following text exists in the configuration file:

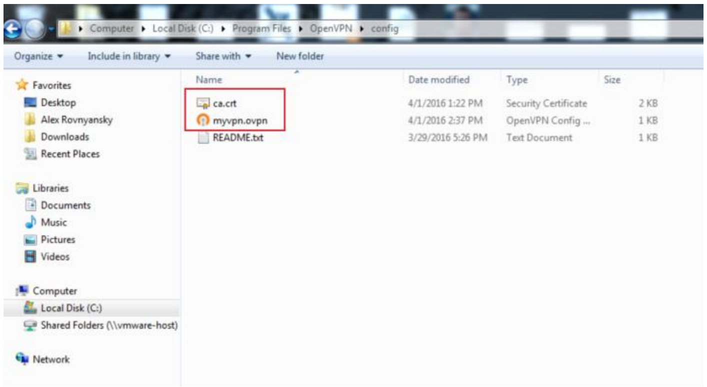


```
client
remote [redacted]
port 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-keyp
ersist-tun
ca [redacted]
auth-user-pass
ns-cert-type server
comp-lzo
verb 3
cipher AES-256-CBC
```

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

STEP 3

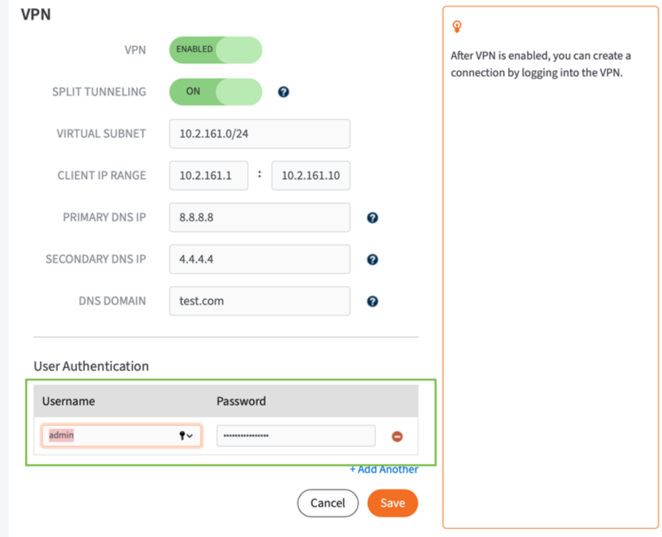
Save the changes to the configuration file. Make sure the `ca.crt` file and the configuration file are both saved in the config folder of the VPN agent.



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

STEP 4

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



VPN

VPN	ENABLED
SPLIT TUNNELING	ON
VIRTUAL SUBNET	10.2.161.0/24
CLIENT IP RANGE	10.2.161.1 : 10.2.161.10
PRIMARY DNS IP	8.8.8.8
SECONDARY DNS IP	4.4.4.4
DNS DOMAIN	test.com

User Authentication

Username	Password
admin	•••••••••••••••••

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

Port Forwarding

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

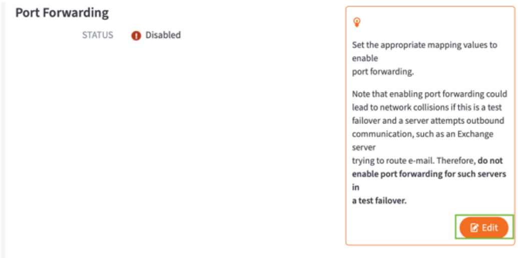
Enabling Port Forwarding could lead to a network collision if configured on a Test Virtual Office. Do not enable and configure Port Forwarding for a Test Virtual Office as productivity and data loss may occur.

Additionally, Port Forwarding must be enabled for Site to Site IPSec VPN to

function.To configure or edit the Port Forwarding settings:

STEP 1

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



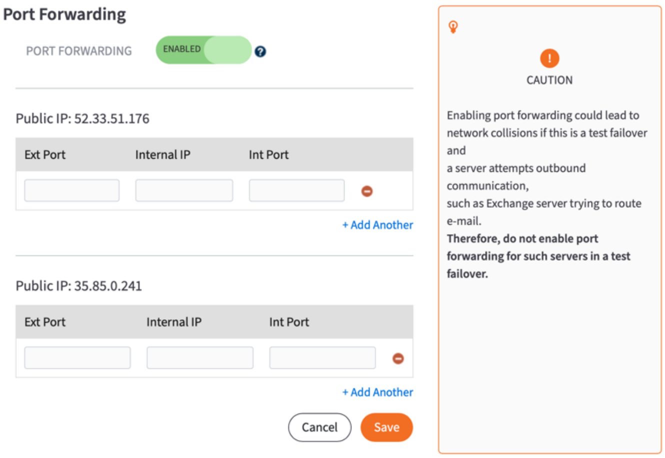
Port Forwarding

STATUS Disabled

Set the appropriate mapping values to enable
port forwarding.

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

STEP 2



Port Forwarding

PORT FORWARDING ENABLED

Public IP: 52.33.51.176

Ext Port	Internal IP	Int Port

Public IP: 35.85.0.241

Ext Port	Internal IP	Int Port

CAUTION

Enabling port forwarding could lead to network collisions if this is a test failover 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 failover.

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.

.

- Int Port—designate the internal port number of the target device being forwarded to.

Click the Add Another button to add any additional entries.

Click the Save button to save any new configurations.

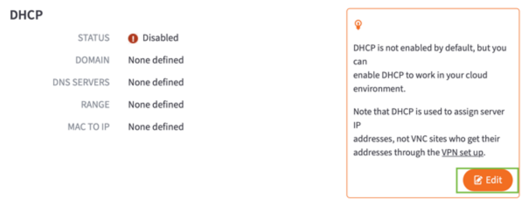
DHCP Settings

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.



DHCP

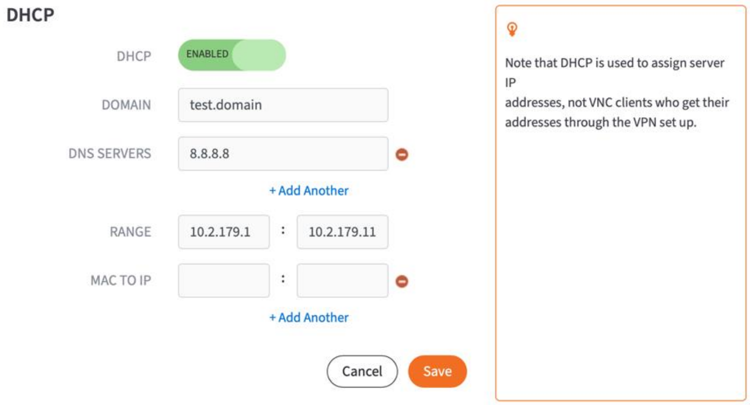
STATUS ❶ Disabled
DOMAIN None defined
DNS SERVERS None defined
RANGE None defined
MAC TO IP None defined

DHCP is not enabled by default, but you can
enable DHCP to work in your cloud environment.

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

STEP 2

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



DHCP

DHCP: ENABLED
DOMAIN: test.domain
DNS SERVERS: 8.8.8.8
RANGE: 10.2.179.1 : 10.2.179.11
MAC TO IP: :

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

- 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.

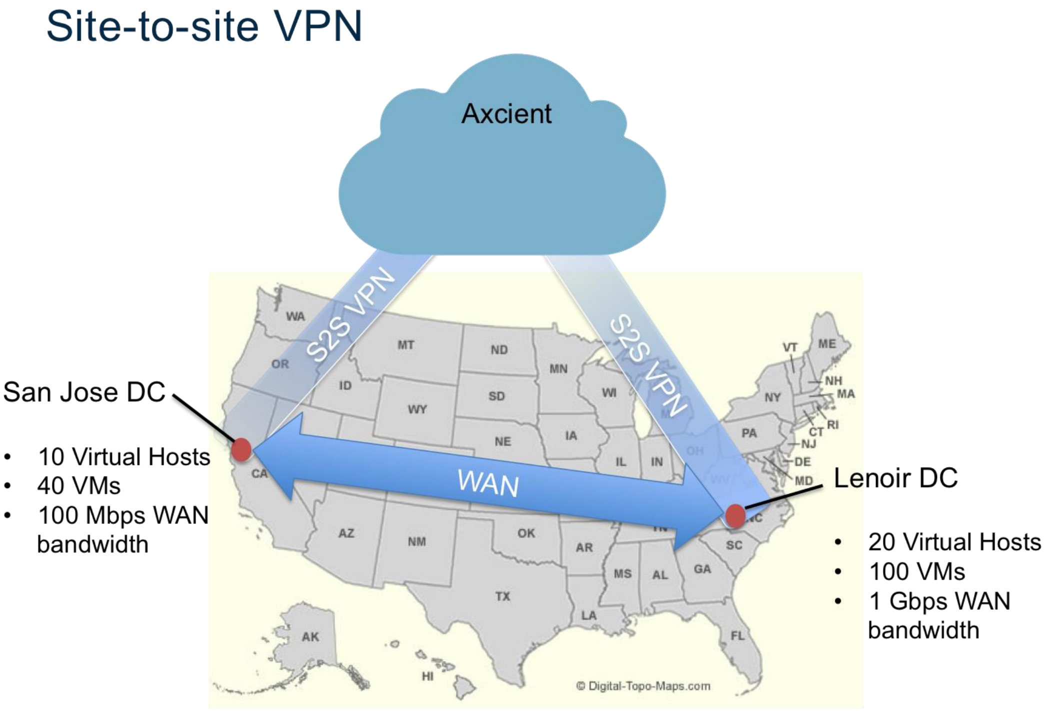
- Optionally, in the *MAC to IP* field, assign an IP address to a server by entering the MAC address and the desired IP address.
- Click the Add Another button to add more entries.

Click the Save button to save any new configurations.

Site to Site VPN

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

Figure 2 - Visualization of the Site-to-Site Endpoint Functionality



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

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

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

Note

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

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

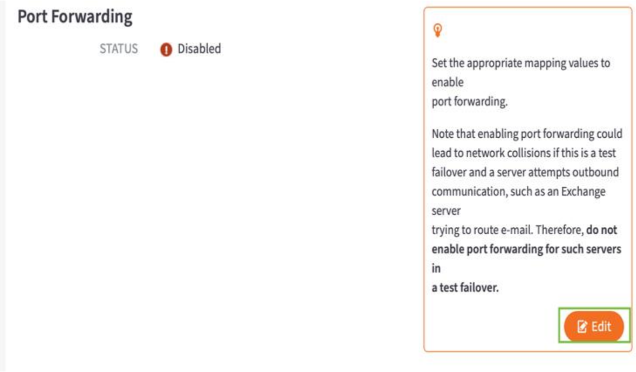
Note: IPSec Site-to-Site VPN is not recommended in a test environment.

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.

To set up a Site to Site IPSec VPN:

STEP 1

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



Set the appropriate mapping values to enable
port forwarding.

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

STEP 2

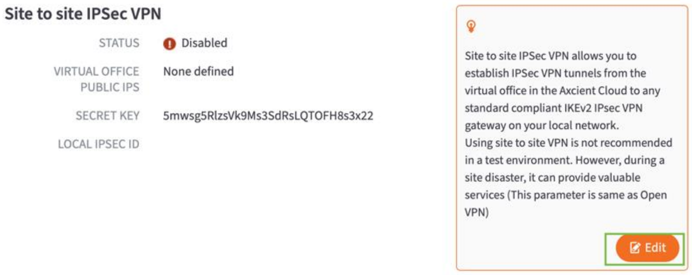
After Port Forwarding settings have been configured, navigate to the *Site to Site IPSec VPN* section and click the Edit button. You can configure the following options:

- Click the S2S IPSec option to enable Site to Site IPSec VPN settings.
- In the *Local IPSec ID* field, specify the IPSec identifier for the virtual office gateway. It can be an IP address (Virtual office public IP) or a distinguished name (FSDN or user FSDN or any unique string)

Configure Remote Sites:

- In Site Name Field, specify site name
- 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 Remote Subnets* section, enter the remote subnets in IPv4 format for sharing with the Virtual Office subnets. Please note that these subnets do not need to intersect with the Virtual Office subnets.
- In the *Remote IPSec ID* field, specify the IPSec identifier for the remote site gateway. It can be an IP address (Site public IP) or a distinguished name (FSDN or user FSDN or any unique string)

Click the Save button when you are finished.



Site to site IPSec VPN

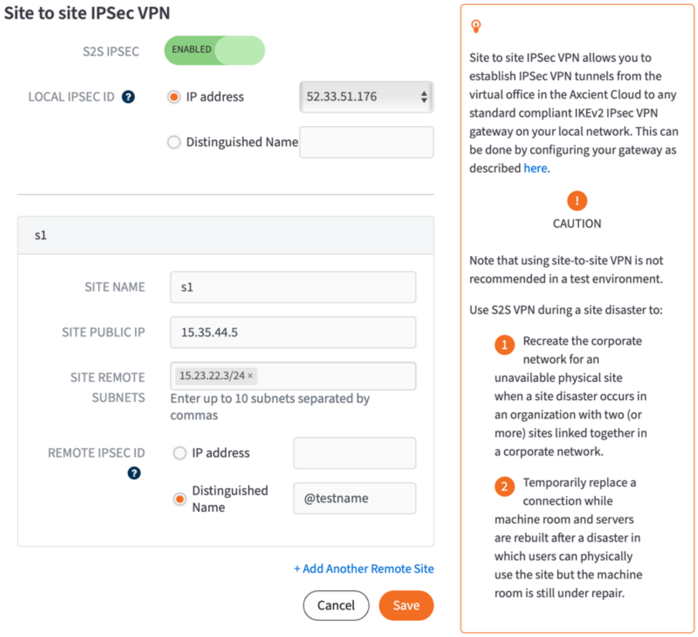
STATUS: Disabled

VIRTUAL OFFICE PUBLIC IPS: None defined

SECRET KEY: 5mwsg5RlzsVk9Ms3SdRsLQTOFH8s3x22

LOCAL IPSEC ID:

Site to site IPSec VPN 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.
Using site to site VPN is not recommended in a test environment. However, during a site disaster, it can provide valuable services (This parameter is same as Open VPN)



Site to site IPSec VPN

S2S IPSEC: ENABLED

LOCAL IPSEC ID: ● IP address 52.33.51.176 ○ Distinguished Name

s1

SITE NAME: s1

SITE PUBLIC IP: 15.35.44.5

SITE REMOTE SUBNETS: 15.23.22.3/24 ×
Enter up to 10 subnets separated by commas

REMOTE IPSEC ID: ○ IP address ● Distinguished Name @testname

Site to site IPSec VPN 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. This can be done by configuring your gateway as described here.

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.

Gateway Settings

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

Render and Start Devices

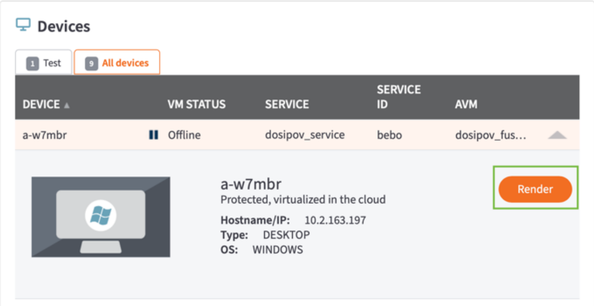
When the Virtual Office is configured, you *must* render devices within the Virtual Office. Rendering devices in the Virtual Offices includes the following steps:

- Select the desired restore point.
- Allocate resources.

To render a device:

STEP 1

On the *Virtual Office* page, expand a device and click the Render button.



Devices

DEVICE ▲	VM STATUS	SERVICE	SERVICE ID	AVM
a-w7mbr	Offline	dosipov_service	bebo	dosipov_fus…

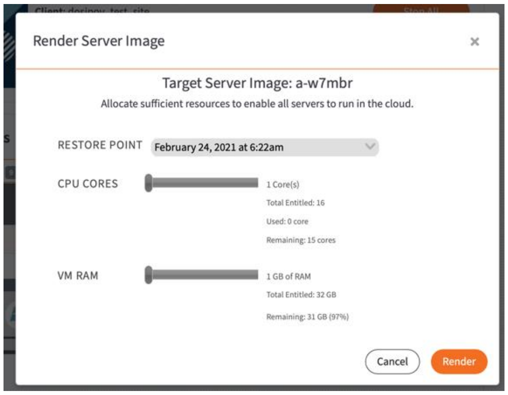
a-w7mbr
Protected, virtualized in the cloud
Hostname/IP: 10.2.163.197
Type: DESKTOP
OS: WINDOWS

STEP 2

In the *Render* screen, select the desired restore point and Allocate resources (*CPU CORES* and *VM RAM*)

Click the Start *Render* button when you are finished.

.



Render Server Image

Target Server Image: a-w7mbr

Allocate sufficient resources to enable all servers to run in the cloud.

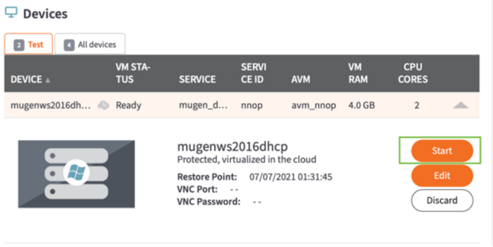
RESTORE POINT: February 24, 2021 at 6:22am

CPU CORES: 1 Core(s)
Total Entitled: 16
Used: 0 core
Remaining: 15 cores

VM RAM: 1 GB of RAM
Total Entitled: 32 GB
Remaining: 31 GB (97%)

STEP 3

On the *Virtual Office* page, expand a device and click the start button.



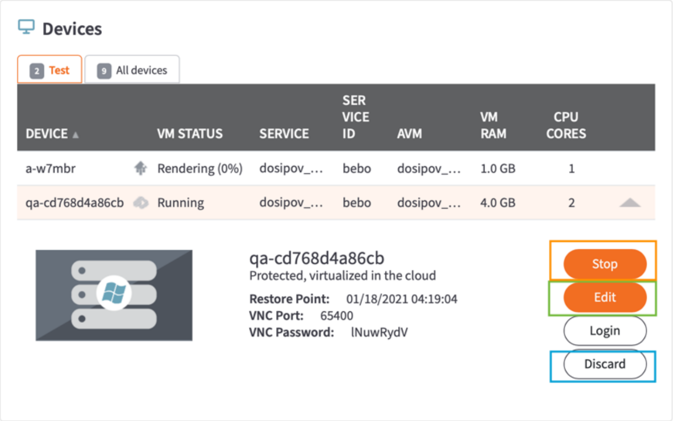
Devices

DEVICE ▲	VM STATUS	SERVICE	SERVICE ID	AVM	VM RAM	CPU CORES
mugenws2016dh…	Ready	mugen_d…	nnop	avm_nnop	4.0 GB	2

mugenws2016dhcp
Protected, virtualized in the cloud
Restore Point: 07/07/2021 01:31:45
VNC Port: - -
VNC Password: - -

You may:

- *Edit* a running device to allocate additional resources or
- *Stop* a running device or
- *Discard* a running device and re-render with a different Recovery point



DEVICE ▲	VM STATUS	SERVICE	SER VICE ID	AVM	VM RAM	CPU CORES
a-w7mbr	Rendering (0%)	dosipov_...	bebo	dosipov_...	1.0 GB	1
qa-cd768d4a86cb	Running	dosipov_...	bebo	dosipov_...	4.0 GB	2

qa-cd768d4a86cb
Protected, virtualized in the cloud

Restore Point: 01/18/2021 04:19:04
VNC Port: 65400
VNC Password: lNuwRydV

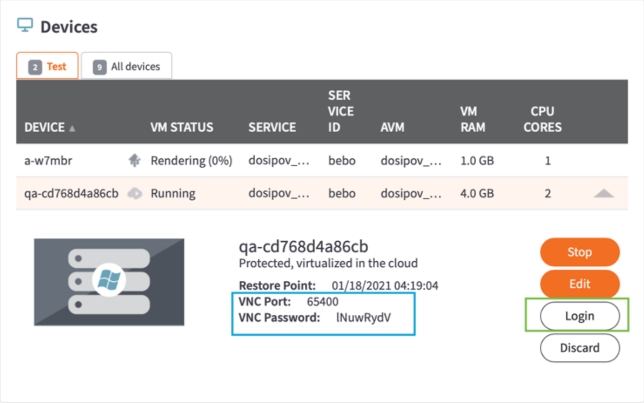
How to Connect to a Device

When the Virtual Office is configured and the devices have started, you might access a specific device by launching WebVNC application from x360Recover Manager (formerly known as RMC) or using RDP.

WebVNC

STEP 1

On the *Virtual Office* page, expand a device and click the Login button. It invokes a WebVNC session for your device



Devices

2 Test | 9 All devices

DEVICE ▲	VM STATUS	SERVICE	SER VICE ID	AVM	VM RAM	CPU CORES
a-w7mbr	Rendering (0%)	dosipov_...	bebo	dosipov_...	1.0 GB	1
qa-cd768d4a86cb	Running	dosipov_...	bebo	dosipov_...	4.0 GB	2

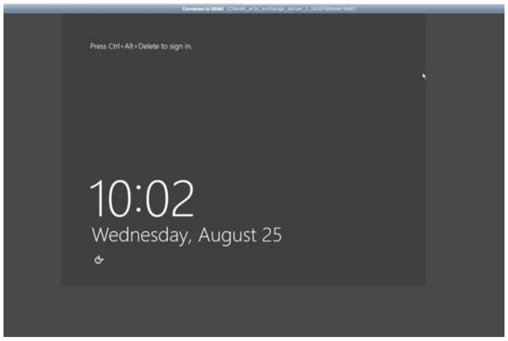
qa-cd768d4a86cb
Protected, virtualized in the cloud

Restore Point: 01/18/2021 04:19:04
VNC Port: 65400
VNC Password: lNuwRydV

STEP 2

In the *WebVNC* page, login to your device with VNC Credentials provided in the Virtual Office page

.



Connected to QEMU (ClientA_ar3c_exchange_server_1_local-failover-test)

Press Ctrl+Alt+Delete to sign in.

10:02
Wednesday, August 25

RDP

You can use a preferred third-party Remote Desktop Protocol (RDP) agent to interact directly with the device desktop.

Caution!

To RDP into a device, you must first enabled the *Allow users to connect remotely to your computer* option on the original device. The recovery point selected must have this option enabled; otherwise you will be unable to RDP into the device.

You can RDP into a device in one of three ways: through VPN, Site to Site IPsec VPN, or Port Forwarding. You can configure these settings in the Configure the Virtual Office page.

Virtual Private Network (VPN)

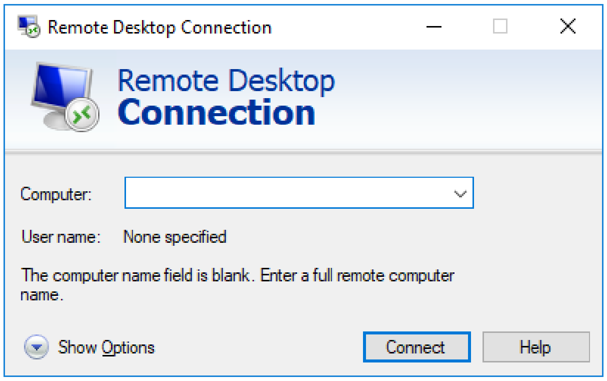
Before using the RDP agent to access a device over a VPN:

- Confirm the target device is in the *Running* system state.
- Configure a VPN network in the VPN settings section.
- Connect to the VPN when it has been successfully configured.

After you configure and connect to the VPN network:

STEP 1

Open the preferred RDP agent. In this example, we will use the Microsoft Remote Desktop RDP agent.

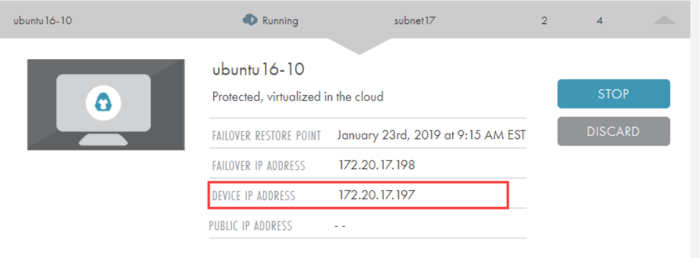


The computer name field is blank. Enter a full remote computer name.

STEP 2

To complete the connection process, find the IP address and credentials for the device.

To obtain the IP address, open the *Virtual Office* page and expand the target device. Use the IP address listed in this section.



ubuntu 16-10 Running subnet17 2 4

ubuntu 16-10

Protected, virtualized in the cloud

FAILOVER RESTORE POINT January 23rd, 2019 at 9:15 AM EST

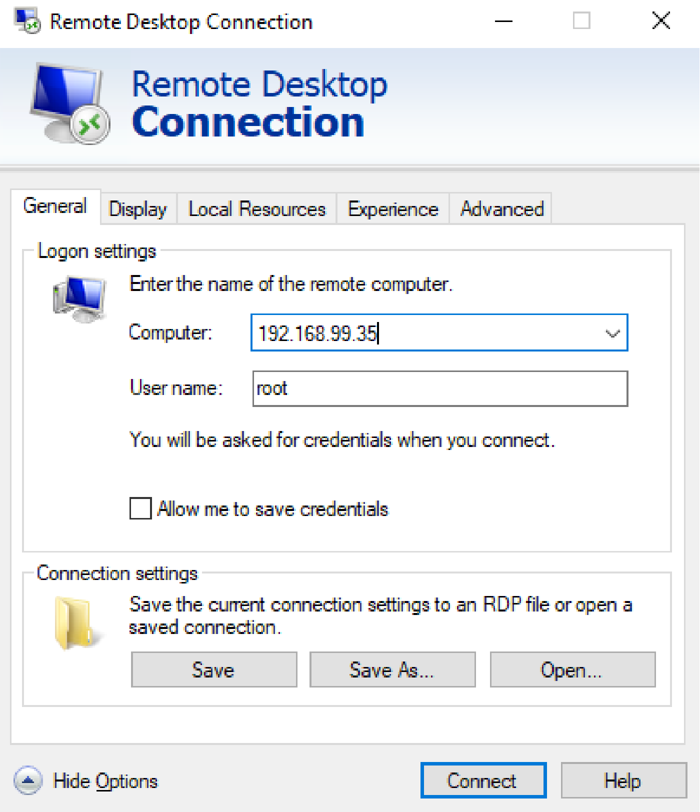
FAILOVER IP ADDRESS 172.20.17.198

DEVICE IP ADDRESS 172.20.17.197

PUBLIC IP ADDRESS - -

STEP 3

Save the new connection. You can now RDP into the target device.



Remote Desktop Connection

Remote Desktop **Connection**

Logon settings

Enter the name of the remote computer.

Computer: 192.168.99.35

User name: root

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Port Forwarding

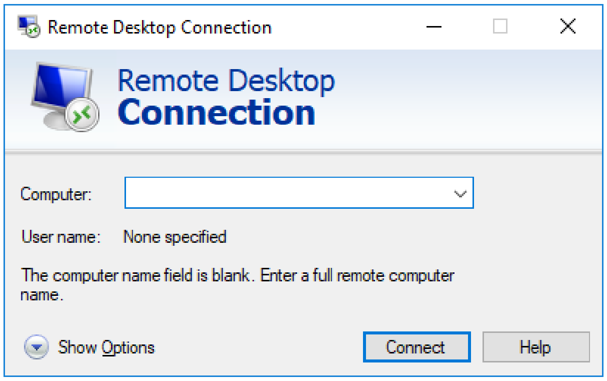
Before using the RDP agent to access a device using Port Forwarding:

- Confirm the target device is in a *Running* system state.
- Successfully configure one or more Port Forwarding rules.

After have successfully configured one or more Port Forwarding rules:

STEP 1

Open the preferred RDP agent. In this example, we will use the Microsoft Remote Desktop RDP agent.



Computer:

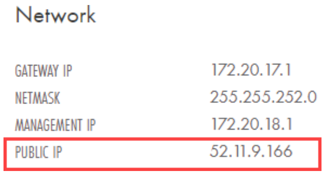
User name: None specified

The computer name field is blank. Enter a full remote computer name.

STEP 2

To complete the connection process, find the following information:

- The automatically assigned public IP address for the Virtual Office. This can be found in the Network section of the *Configure Virtual Office* page.
- The external port number (Ext Port Number) configured for the Port Forwarding rule.
- The device login credentials.



Network

GATEWAY IP	172.20.17.1
NETMASK	255.255.252.0
MANAGEMENT IP	172.20.18.1
PUBLIC IP	52.11.9.166

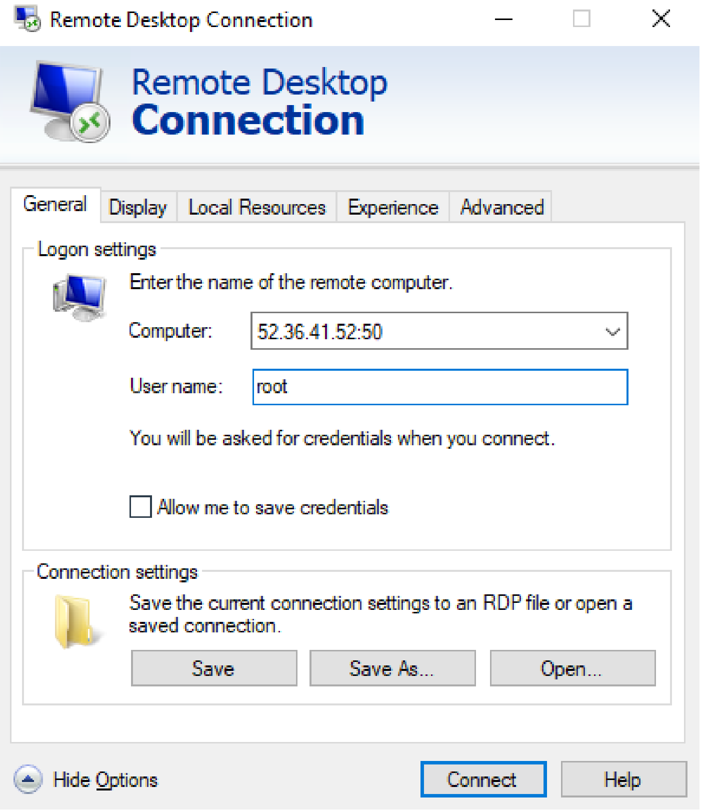
STEP 3

Enter the information collected in the steps above to create the new connection.

When entering the IP address of the device, you will need to be entered as follows:

`<Virtual Office Public IP Address>:<External Port Number>`

You can now RDP into the target device.



Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: 52.36.41.52:50

User name: root

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Connecting to a Linux Device

Unless a 3rd party application has been installed on the Linux device that allows the user to access a GUI of the device's desktop, you will be unable to RDP into a Linux device deployed in the Virtual Office. To access the virtualized Linux device in the Virtual Office, you will need to SSH into the device.

As a first step, you will need to configure one of the following:

- Create and connect to a VPN.
- Create and connect to a Site-to-Site VPN.
- Configure a Port-Forwarding rule.

When the above connection options has been successfully configured, you can use the command line to SSH or use a preferred SSH client to access the device in the Virtual Office.

If using the command line, SSH in to the virtualized device using the following command:

```
ssh <Username>@<IP Address>
```

You will then be prompted to enter the password for the specified Username. The credentials (Username, IP Address, and Password) entered in the SSH command will be that of the original device. If accessing the device using Port-Forwarding, a public IP address will be generated, which you can use to issue the SSH command.

After an SSH connection has been successfully established to the device, you can begin issuing commands via the command line.

Runbooks

Runbooks, sometimes called Orchestration, 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. The devices cannot be virtualized unless an appropriate subnet is first created before starting the Runbook.

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.

Configuring a Runbook will allow you to configure:

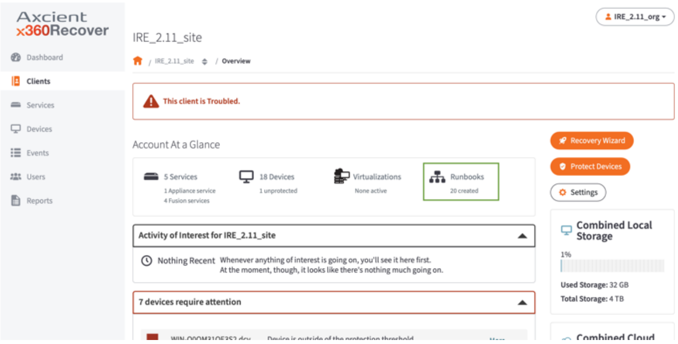
- Devices to be virtualized,
- The order in which the devices should be virtualized,
- Resources to allocate to each device,
- Wait time between the deployment of each device,
- Network settings, and
- Other advanced options, like VPN settings, Port Forwarding, and Site-to-Site VPN.

Create a New Runbook

To create a new Runbook:

STEP 1

On the *client Details* page, click the Runbooks link found in the Account At a Glance section of the page.



IRE_2.11_site

This client is Troubled.

Account At a Glance

5 Services: 1 Appliance service, 4 Fusion services

18 Devices: 1 unprotected

Virtualizations: None active

Runbooks: 20 created

Activity of Interest for IRE_2.11_site

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

7 devices require attention

Combined Local Storage: 1%

Used Storage: 32 GB

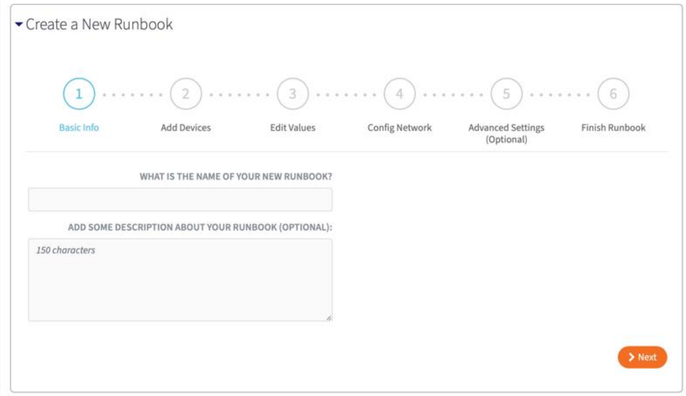
Total Storage: 4 TB

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.



Create a New Runbook

1 Basic Info · 2 Add Devices · 3 Edit Values · 4 Config Network · 5 Advanced Settings (Optional) · 6 Finish Runbook

WHAT IS THE NAME OF YOUR NEW RUNBOOK?

ADD SOME DESCRIPTION ABOUT YOUR RUNBOOK (OPTIONAL):

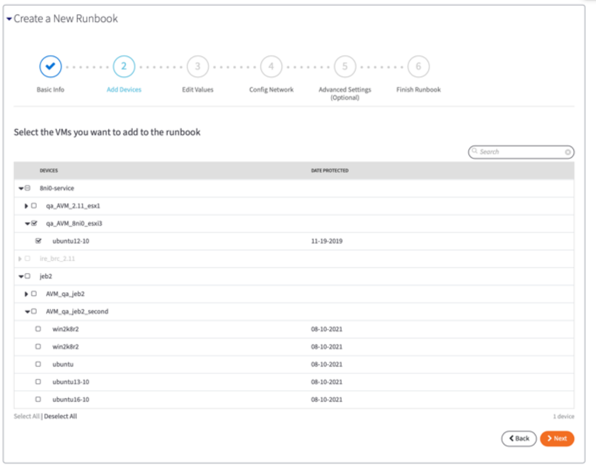
150 characters

STEP 3

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

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

Click the Next button to continue.



Create a New Runbook

✓ Basic Info · 2 Add Devices · 3 Edit Values · 4 Config Network · 5 Advanced Settings (Optional) · 6 Finish Runbook

Select the VMs you want to add to the runbook

DEVICES	DATE PROTECTED
⊟ 8ni0-service	
□ qa_AVM_2.11_esx1	
☑ qa_AVM_8ni0_esxi3	
☑ ubuntu12-10	11-19-2019
□ ire_brc_2.11	
□ jeb2	
□ AVM_qa_jeb2	
□ AVM_qa_jeb2_second	
□ win2k8r2	08-10-2021
□ win2k8r2	08-10-2021
□ ubuntu	08-10-2021
□ ubuntu13-10	08-10-2021
□ ubuntu16-10	08-10-2021

Select All | Deselect All

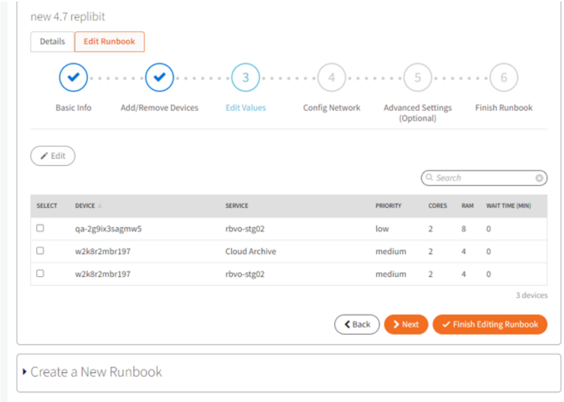
1 device

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 can edit the following:

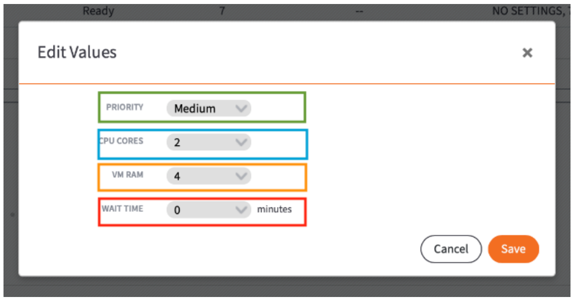
- Device boot PRIORITY,
- Number of virtual CPU CORES allocated to the device(s),
- Amount of virtual RAM allocated to the device(s),
- WAIT TIME in between the booting of virtual devices inthe Virtual Office

Click the Next button to continue.



SELECT	DEVICE	SERVICE	PRIORITY	CORES	RAM	WAIT TIME (MIN)
□	qa-2g9ix3sagmw5	rbvo-stg02	low	2	8	0
□	w2k8r2mbr197	Cloud Archive	medium	2	4	0
□	w2k8r2mbr197	rbvo-stg02	medium	2	4	0

3 devices



PRIORITY: Medium

CPU CORES: 2

VM RAM: 4

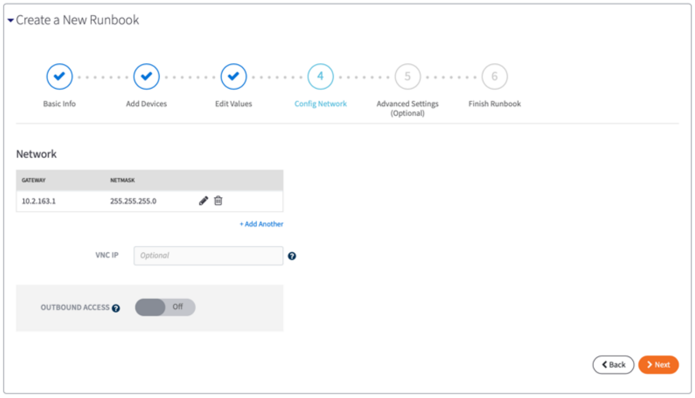
WAIT TIME: 0 minutes

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 the 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 the Virtual Office section for more information.
- Optionally, enable the *Outbound Access* option to allow outbound access to the Internet. Please refer to the Configure the Virtual Office section for more information.

Click the Next button to continue



Network

GATEWAY	NETMASK
10.2.163.1	255.255.255.0

VNC IP: Optional

OUTBOUND ACCESS: Off

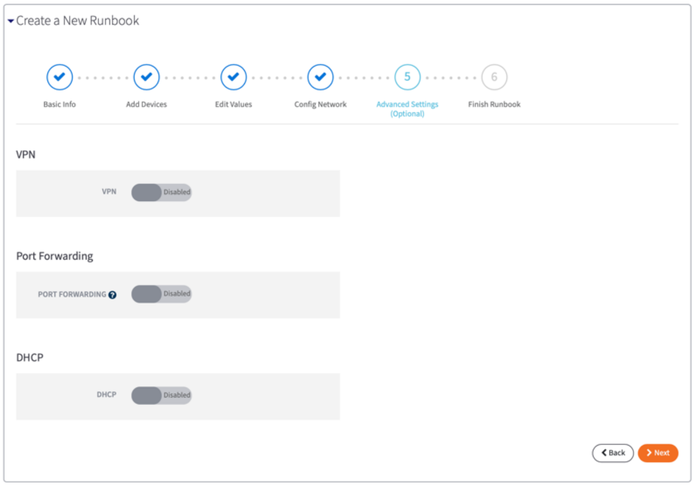
STEP 5

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

- VPN
- Port Forwarding
- DHCP

You can also update these settings after the Runbook has started from the *Configure Office* page.

Click the Next button to continue.



VPN

VPN: Disabled

Port Forwarding

PORT FORWARDING: Disabled

DHCP

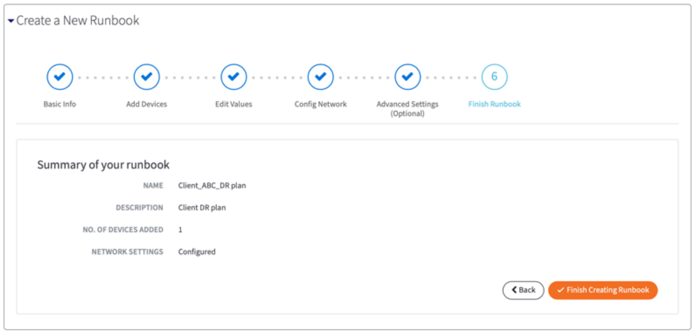
DHCP: Disabled

STEP 5

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.



Summary of your runbook

NAME: Client_ABC_DR plan

DESCRIPTION: Client DR plan

NO. OF DEVICES ADDED: 1

NETWORK SETTINGS: Configured

Start a Runbook

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

- On the *Virtual Office* 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 Client-specific, and only a single Runbook may be running at a time for any given Client. If a Runbook is already running under a client, 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.

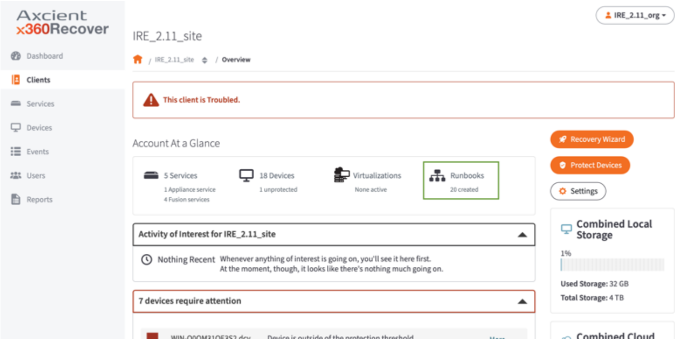
If a subnet is configured for only one or some of the devices, you will need to create the additional subnets in the *Virtual Office Configuration* page in order to virtualize the remaining devices when the Runbook is in a Running state.

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 *client Details* page, click the Runbooks link found in the Account At a Glance section of the page.



IRE_2.11_site

IRE_2.11_site / Overview

This client is Troubled.

Account At a Glance

5 Services — 1 Appliance service, 4 Fusion services
18 Devices — 1 unprotected
Virtualizations — None active
Runbooks — 20 created

Activity of Interest for IRE_2.11_site

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

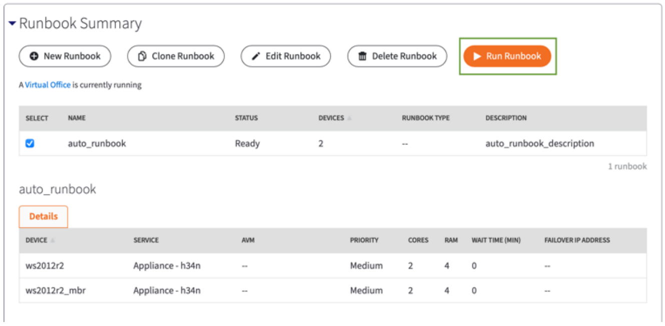
7 devices require attention

Combined Local Storage
1%
Used Storage: 32 GB
Total Storage: 4 TB

Combined Cloud

STEP 2

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



Runbook Summary

A Virtual Office is currently running

SELECT	NAME	STATUS	DEVICES	RUNBOOK TYPE	DESCRIPTION
☑	auto_runbook	Ready	2	--	auto_runbook_description

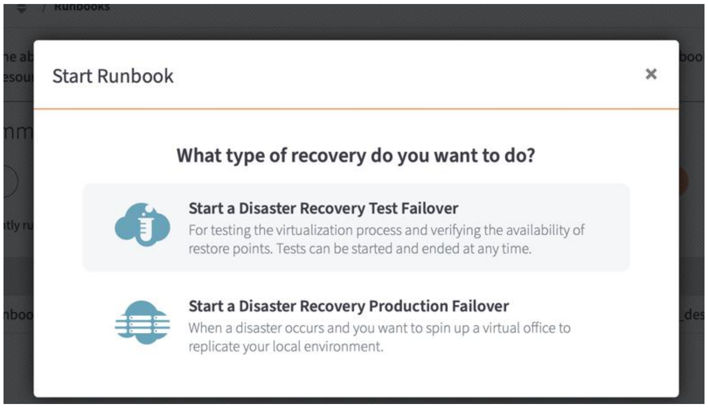
1 runbook

auto_runbook

DEVICE	SERVICE	AVM	PRIORITY	CORES	RAM	WAIT TIME (MIN)	FAILOVER IP ADDRESS
ws2012r2	Appliance - h34n	--	Medium	2	4	0	--
ws2012r2_mbr	Appliance - h34n	--	Medium	2	4	0	--

STEP 3

On the *Start Runbook* screen, select the type of Virtual Office to deploy.



Start Runbook ×

What type of recovery do you want to do?

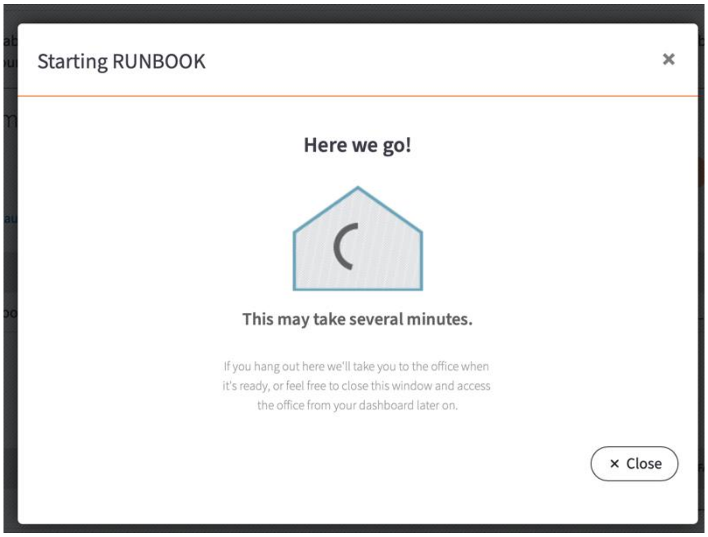
Start a Disaster Recovery Test Failover
For testing the virtualization process and verifying the availability of restore points. Tests can be started and ended at any time.

Start a Disaster Recovery Production Failover
When a disaster occurs and you want to spin up a virtual office to replicate your local environment.

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.



Starting RUNBOOK ×

Here we go!

This may take several minutes.

If you hang out here we'll take you to the office when it's ready, or feel free to close this window and access the office from your dashboard later on.

× Close

Edit a Runbook

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

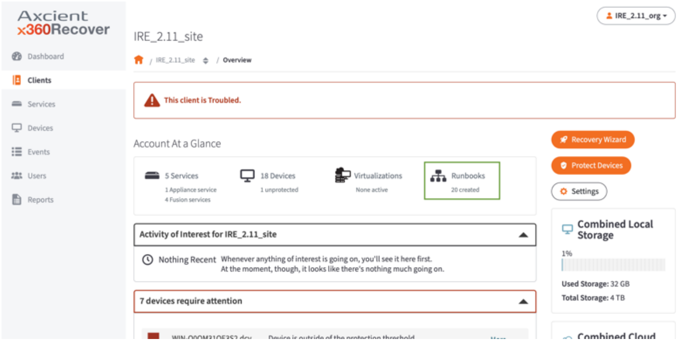
While a Runbook is inactive, all aspects of the Runbook and Virtual Office can be edited; however, not all aspects of the Runbook can be edited while the Runbook is running. For example, you *cannot* edit included devices when the Runbook is running, but you *can* edit network information.

After edits have been made, changes are immediately saved and applied. When the Runbook is running, the user can click the Configure Office button to make any changes. These changes will be automatically applied to the running Virtual Office, and will be applied and saved to the Runbook as well.

To edit a Runbook:

STEP 1

On the *client Details* page, click the Runbooks link found in the Account At a Glance section of the page.



This client is Troubled.

Activity of Interest for IRE_2.11_site

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

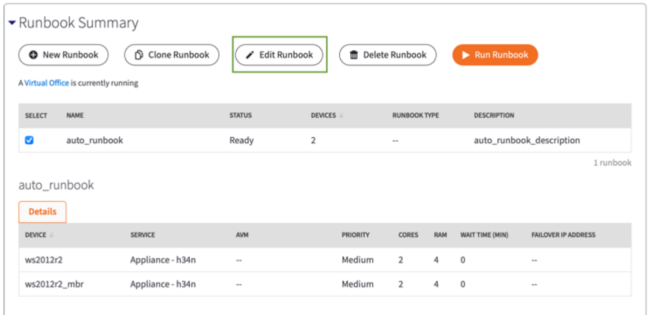
7 devices require attention

Used Storage: 32 GB
Total Storage: 4 TB

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.



A Virtual Office is currently running

SELECT	NAME	STATUS	DEVICES	RUNBOOK TYPE	DESCRIPTION
☑	auto_runbook	Ready	2	--	auto_runbook_description

1 runbook

auto_runbook

DEVICE	SERVICE	AVM	PRIORITY	CORES	RAM	WAIT TIME (MIN)	FAILOVER IP ADDRESS
ws2012r2	Appliance - h34n	--	Medium	2	4	0	--
ws2012r2_mbr	Appliance - h34n	--	Medium	2	4	0	--

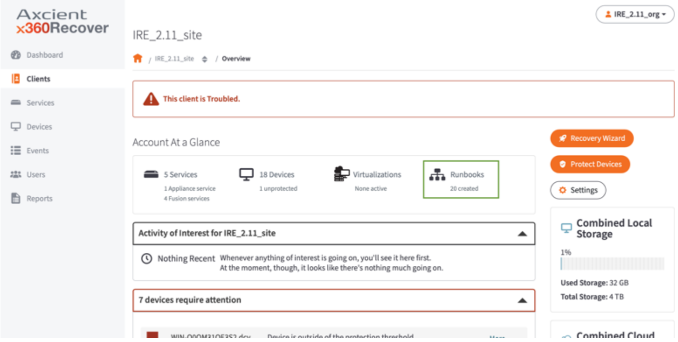
Clone a Runbook

You can optionally clone a Runbook, which allows you to create a new Runbook from an existing Runbook and make changes where needed. Cloning a Runbook is a quick and easy way to create a new Runbook with slightly different settings.

To clone a Runbook:

STEP 1

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



IRE_2.11_site

IRE_2.11_site / Overview

This client is Troubled.

Account At a Glance

5 Services
1 Appliance service
4 Fusion services

18 Devices
1 unprotected

Virtualizations
None active

Runbooks
20 created

Activity of Interest for IRE_2.11_site

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

7 devices require attention

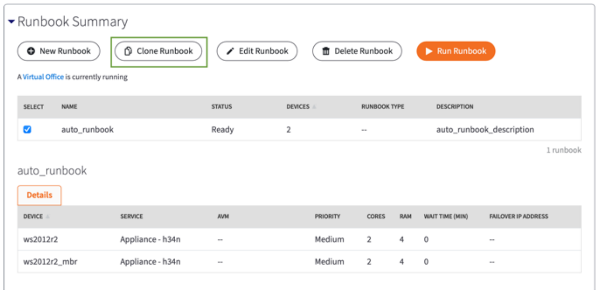
WIN-O0QM31OF3S2.dcv Device is outside of the protection threshold

Combined Local Storage
1%
Used Storage: 32 GB
Total Storage: 4 TB

Combined Cloud

STEP 2

In the Runbook Summary section of the page, use the checkboxes to select the Runbook you want to clone and then click the Clone Runbook button.



A Virtual Office is currently running

SELECT	NAME	STATUS	DEVICES	RUNBOOK TYPE	DESCRIPTION
☑	auto_runbook	Ready	2	--	auto_runbook_description

1 runbook

auto_runbook

DEVICE	SERVICE	AVM	PRIORITY	CORES	RAM	WAIT TIME (MIN)	FAILOVER IP ADDRESS
ws2012r2	Appliance - h34n	--	Medium	2	4	0	--
ws2012r2_mbr	Appliance - h34n	--	Medium	2	4	0	--

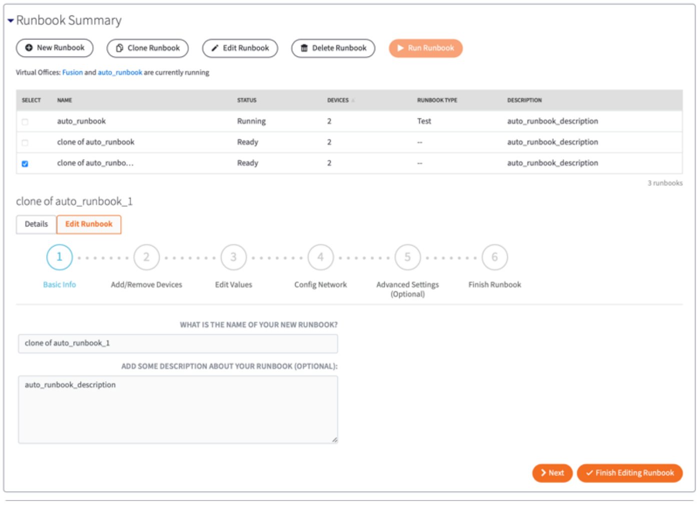
STEP 3

In the *Edit Runbook* tab, you can optionally edit the settings inherited from the original Runbook.

For example, you can add or remove devices, change values, update network settings, and more.

Click the Next button to move through each step of the editing process.

When you are finished making changes, click the Finish Creating Runbook button.



Virtual Offices: Fusion and auto_runbook are currently running

SELECT	NAME	STATUS	DEVICES	RUNBOOK TYPE	DESCRIPTION
□	auto_runbook	Running	2	Test	auto_runbook_description
□	clone of auto_runbook	Ready	2	--	auto_runbook_description
☑	clone of auto_runbo…	Ready	2	--	auto_runbook_description

3 runbooks

clone of auto_runbook_1

WHAT IS THE NAME OF YOUR NEW RUNBOOK?
clone of auto_runbook_1

ADD SOME DESCRIPTION ABOUT YOUR RUNBOOK (OPTIONAL):
auto_runbook_description

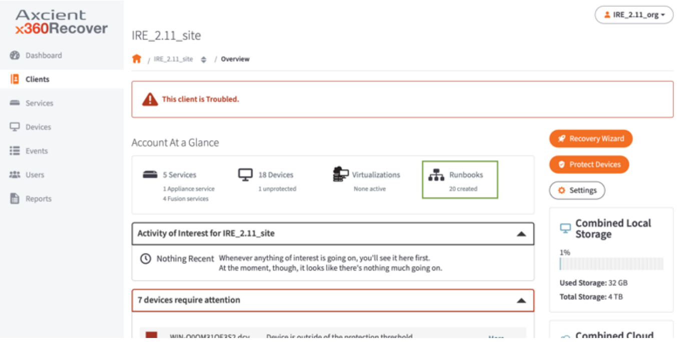
Delete a Runbook

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

To delete a Runbook:

STEP 1

On the *client Details* page, click the Runbooks link found in the Account At a Glance section of the page.



IRE_2.11_site

This client is Troubled.

Account At a Glance

5 Services	18 Devices	Virtualizations	Runbooks
1 Appliance service 4 Fusion services	1 unprotected	None active	20 created

Activity of Interest for IRE_2.11_site

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

7 devices require attention

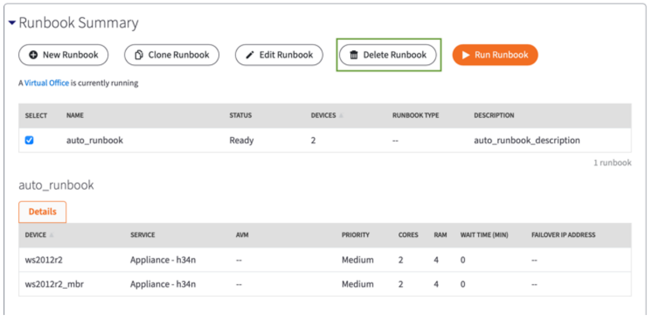
Combined Local Storage
1%
Used Storage: 32 GB
Total Storage: 4 TB

Combined Cloud

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.



Runbook Summary

A Virtual Office is currently running

SELECT	NAME	STATUS	DEVICES	RUNBOOK TYPE	DESCRIPTION
☑	auto_runbook	Ready	2	--	auto_runbook_description

1 runbook

auto_runbook

DEVICE	SERVICE	AVM	PRIORITY	CORES	RAM	WAIT TIME (MIN)	FAILOVER IP ADDRESS
ws2012r2	Appliance - h34n	--	Medium	2	4	0	--
ws2012r2_mbr	Appliance - h34n	--	Medium	2	4	0	--

Failback

Failback is the process of restoring a production Virtual Office data back to the production devices and/or data centers. This is accomplished by exporting data in the from of virtual servers from the Axcient Cloud as system images and loading them back on to the production hardware.

Axcient provides 30 days of free cloud usage for a production Virtual Office disaster recovery scenario*. Beyond 30 days, Axcient will start incurring a minimal overage per server per hour for devices in the production Virtual Office in the Axcient Cloud. While Axcient will run the Virtual Office for as long as required, Axcient strongly recommends to start preparing for failback to hardware on the user's on-premise data center within those 30 days.

Once the on-premise hardware is ready, contact Axcient Support to create and execute the failback schedule.

**Please check with your sales representative for more details on pricing and benefits included in the service.*