Axcient

Fusion Recovery Guide

axcient.com

NOTICE

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

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

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

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

Table of Contents

Introduction 3

Recovery of Encrypted Files 3
Foreign Character Support 3

File and Folder Restore 4

Cloud Failover (Virtual Office) 8

Start the Virtual Office 9
Virtual Office Page 13

Configure the Virtual Office 16

Network Settings 16
Virtual Private Network (VPN) 18
Port Forwarding 23
Public IP Settings 25
Site to Site VPN 27

Prepare Devices 30

How to Connect to a Device 32

Virtual Private Network (VPN) 32
Port Forwarding 34
Connecting to a Linux Device 36

Runbooks 37

Create a New Runbook 37
Start a Runbook 41
Edit a Runbook 43
Delete a Runbook 44

Failback 45

Introduction

You can leverage Axcient's Business Continuity tools in the event of data loss or disaster. Axcient Business Continuity tools allow you to replicate the entire protected environment in the Axcient Cloud with a click of a button.

Additionally, you can create Runbooks to automatically deploy virtualized devices in the Virtual Office. This automation minimizes downtime by virtualizing everything—from the protected devices to the network configuration settings.

The following tools are available:

- File and Folder Recovery
- Cloud Failover
- Cloud Failover with Orchestration and Automation

Recovery of Encrypted Files

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

Foreign Character Support

The Fusion solution supports protection and recovery of foreign characters that are UTF-8 encoded.

File and Folder Restore

In the event of data loss, you can restore a single file or folder, or multiple files and folders, from the Axcient Cloud.

When recovering the selected data, a URL will be generated that allows you to recover the selected file(s) and folder(s). This URL can be sent to a recipient or used to download the data locally.

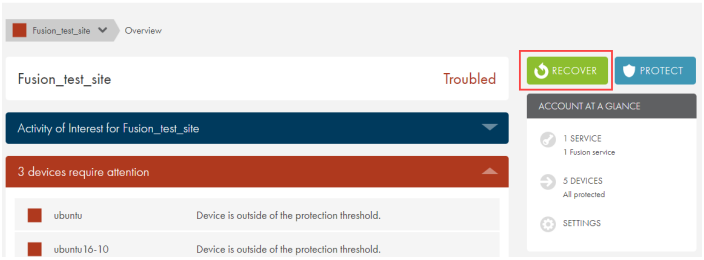
Warning!

You can recover a volume up to 4TB in size.

If the total size of the recovery job will exceed 4TB, you can recover multiple volumes at a time, as long as the size of each individual volume is less than 4TB.

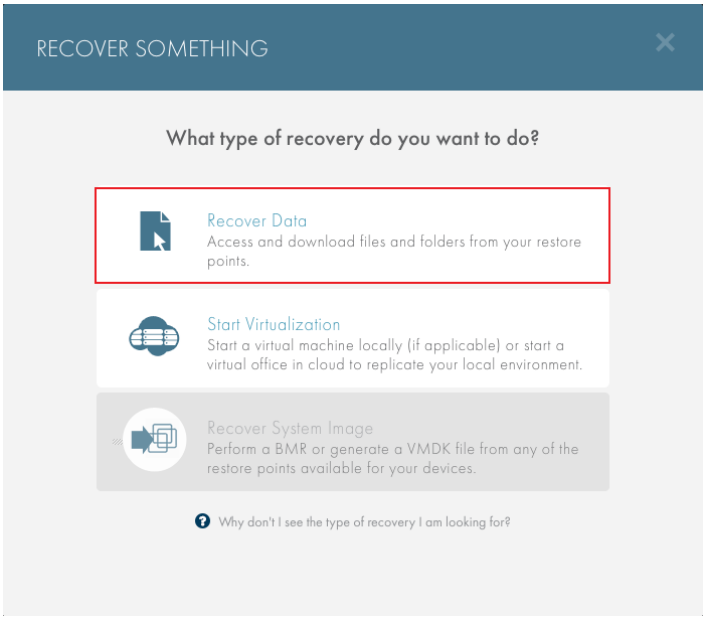
STEP 1

From the Axcient Web Application, navigate to the *Site Details* page and click the **Recover** button.



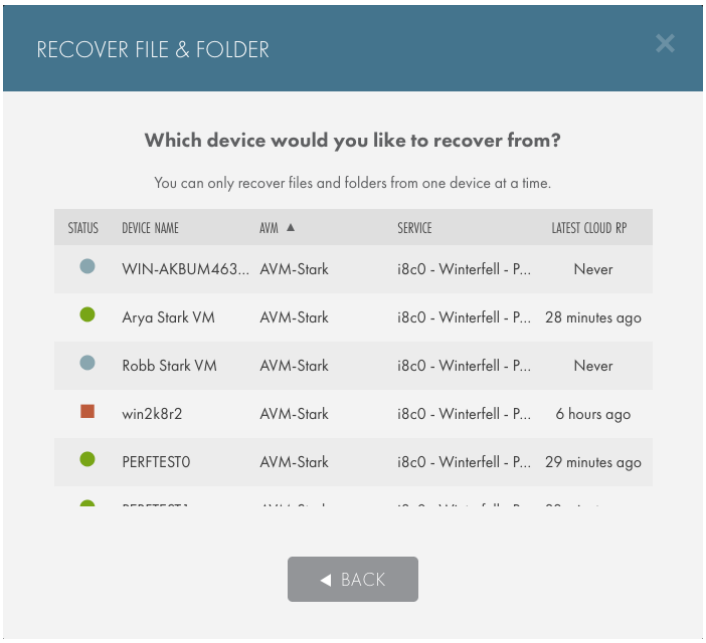
STEP 1

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



STEP 2

On the *Recover File & Folder* screen, select the device from which data needs to be recovered.



STEP 3

In the *Recover From* screen, use the *Calendar* field to select the appropriate **recovery point**.

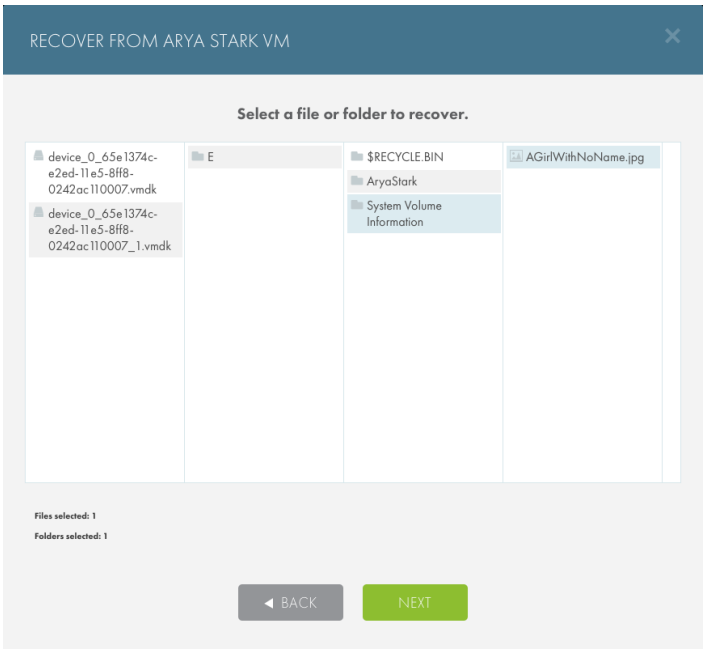
Click the **Recover** button when you are finished.

STEP 4

Browse and 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.

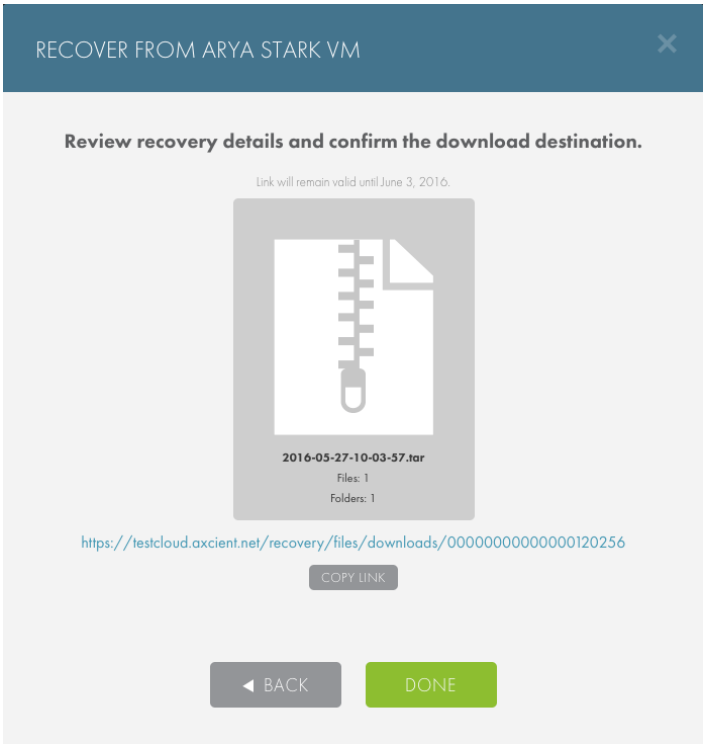


STEP 5

The generated URL can be used to retrieve the recovered data.

Highlight the URL by using the mouse or by clicking the **Copy Link** button, and then copy the link.

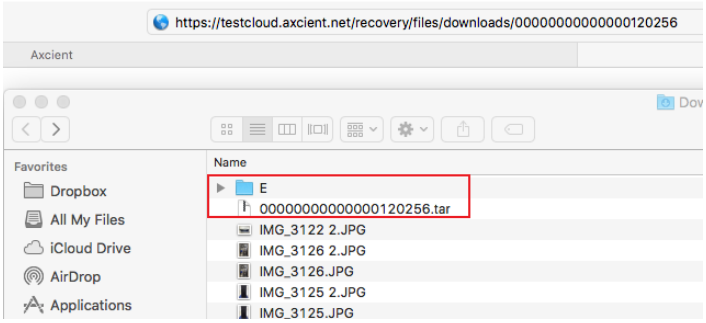
Click the **Done** button to close the screen.



STEP 6

Paste the URL in a web browser to download the `.tar` file that contains the recovered data.

After the file is downloaded, double click the `.tar` file to unzip the file and recover the data.



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.

Start the Virtual Office

Warning!

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

Note

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

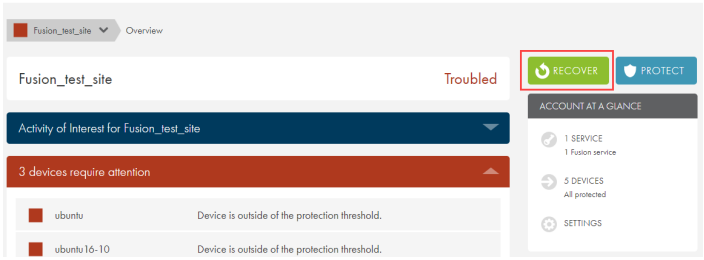
Fusion does not support a Virtual Office where devices belong to two different networks with Classless Inter-Domain Routing (CIDR) of /16.

Example: If Device A belongs to network 10.10.0.0/16, and Device B belongs to network 192.168.0.0/16, then the Virtual Office can be created with only a single type of CIDR; either 10.10.0.0/16 or 192.168.0.0/16. If the Virtual Office is created using the 10.10.0.0/16 network, then Device B will not be able to start in the Virtual Office.

To start the Virtual Office:

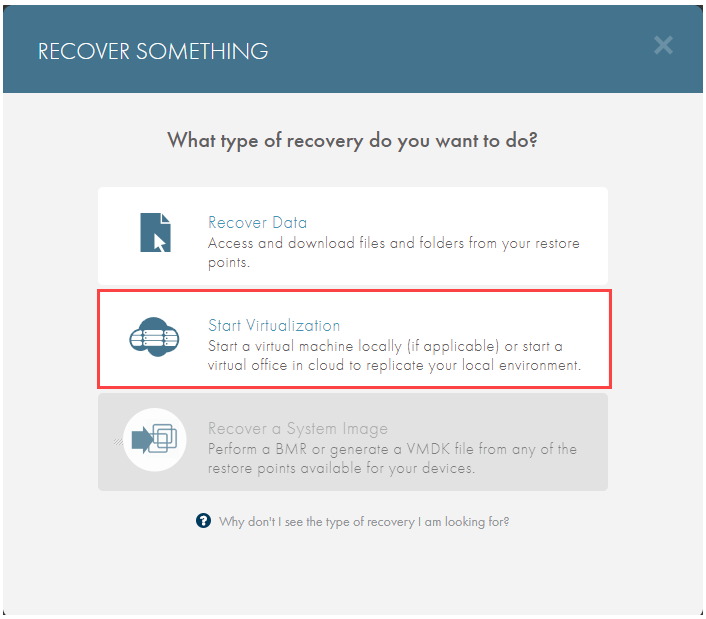
STEP 1

From the Axcient Web Application, navigate to the *Site Details* page and click the **Recover** button.



STEP 2

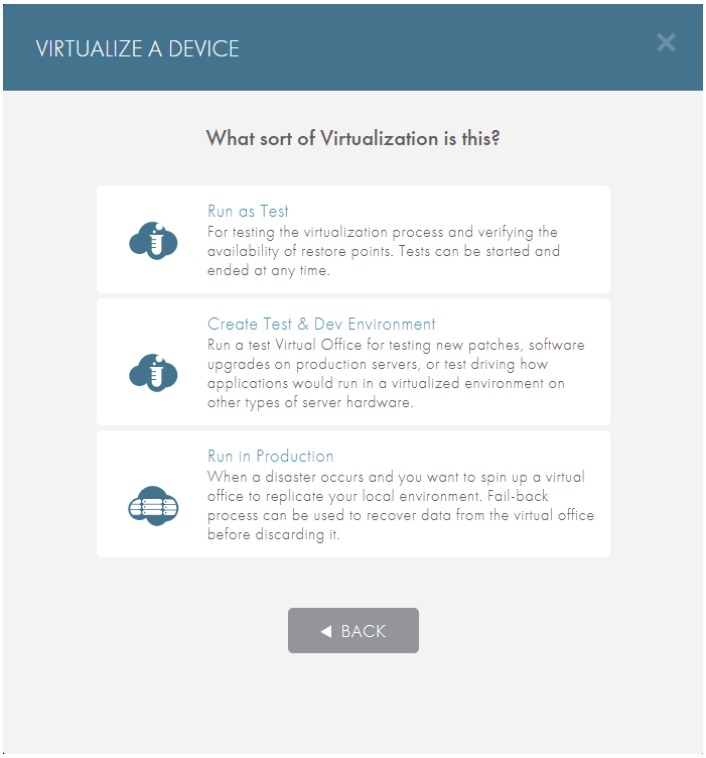
On the *Recover Something* screen, click the **Start Virtualization** option.



STEP 3

Select the type of local virtualization to deploy:

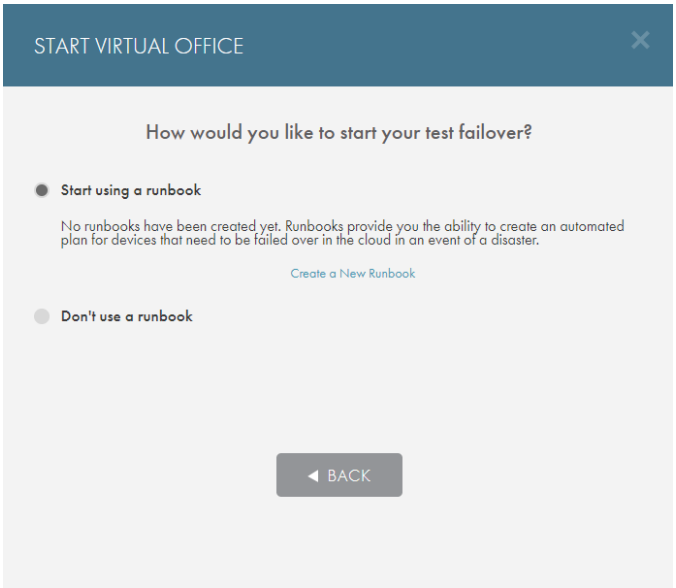
- Select the **Run as Test** option to test the virtualization process and verify the availability of recovery points in case of an emergency.
- Select the **Create Test & Dev Environment** option to test new patches, software, or other upgrades on a production server. These can be started and stopped at any time.
- Select the **Put 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 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.

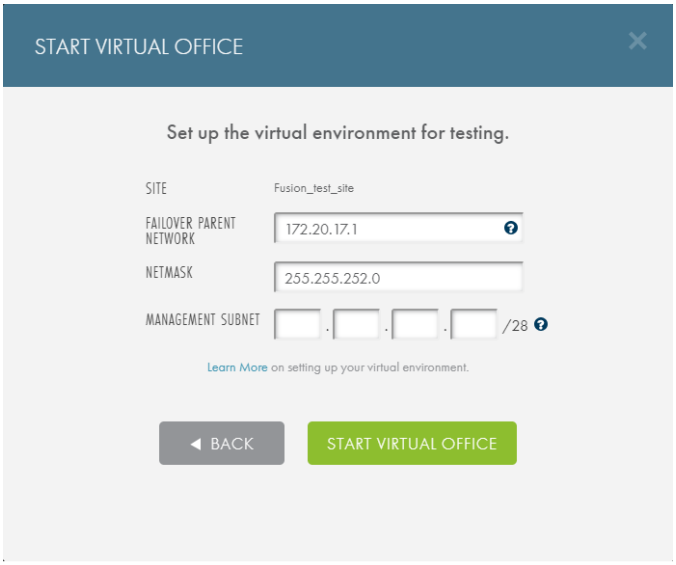


STEP 4

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

- In the *Failover Parent Network* field, configure the **IP** of the Virtual Office. This IP address must be on the same network as the devices that will be virtualized in the Virtual Office.
- In the *Netmask* field, configure the **netmask** of the Virtual Office. At most this is a 16-bit netmask. The smallest netmask is 255.255.0.0.
- In the *Management Subnet* field, configure the **management IP** of the Virtual Office. This IP address cannot be on the same network as the gateway IP or any subnets created in the Virtual Office. For example, if the Management IP address is 172.20.1.2, the gateway IP or the subnet cannot be on the 172.10.1.X network.

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



Virtual Office Page

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

The *Virtual Office* page includes the following sections:

1 Virtual Office Summary

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

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

2 Device List

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

3 Configure Office

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

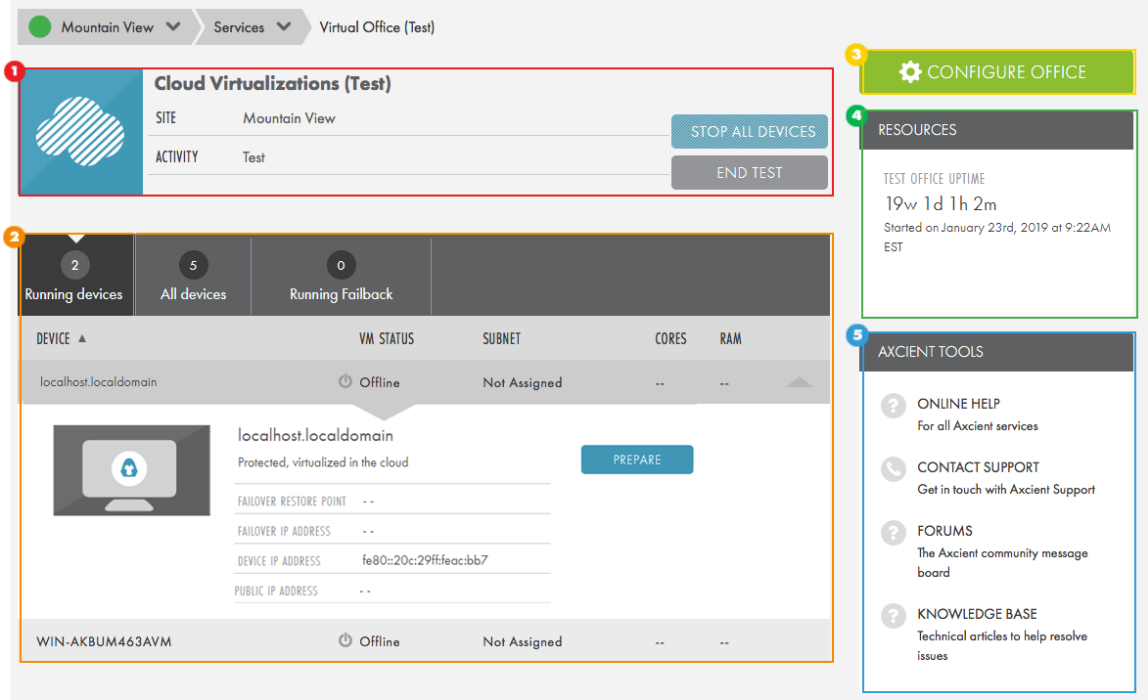
4 Resources

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

5 Axcient Tools

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

Figure 1 - Virtual Office Page



Virtual Machine States

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

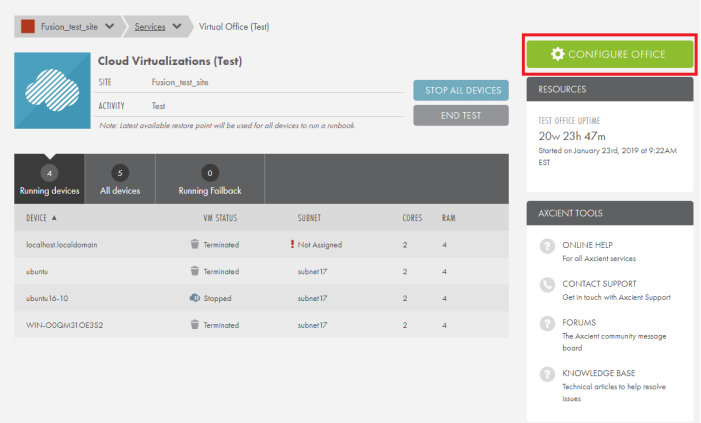
- **Offline**—VMs that have yet to be rendered. To render a device, click the **Prepare** button.
- **Preparing**—VMs that are currently being prepared. The Virtual Office is rendering them and allocating virtual resources for the VM.
- **Prepared**—VMs that have been prepared, but are not yet running.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

Configure the Virtual Office

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

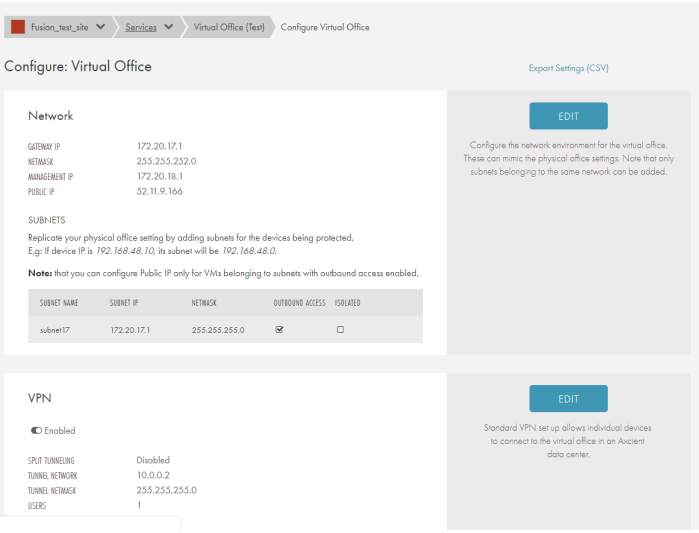
STEP 1

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



STEP 2

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



Network Settings

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

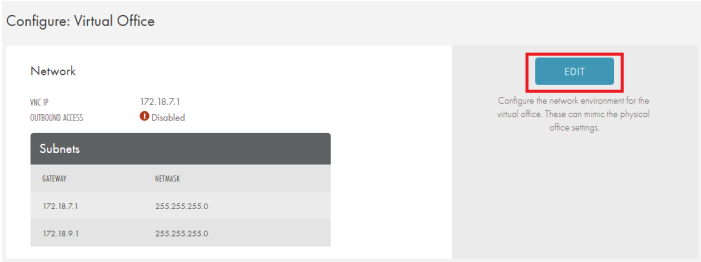
You must configure **at least one subnet** in the Virtual Office. This will be required when preparing a device.

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

To edit the network settings:

STEP 1

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

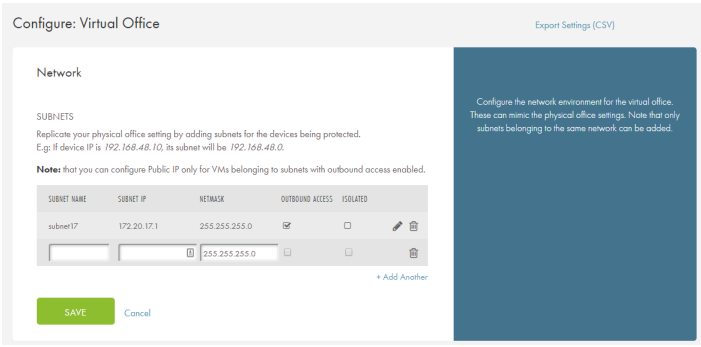


STEP 2

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

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

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



Note
You can only edit a subnet when the devices in the subnet are in an Offline, Prepared, or Stopped state. If one or more devices in a Subnet are in a Running state, the user will need to stop the running device(s) before editing the subnet.

Virtual Private Network (VPN)

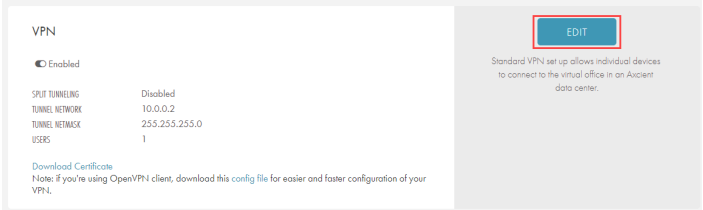
You can configure a VPN to create a secure connection over the public Internet so that outside devices can connect.

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

To edit VPN settings:

STEP 1

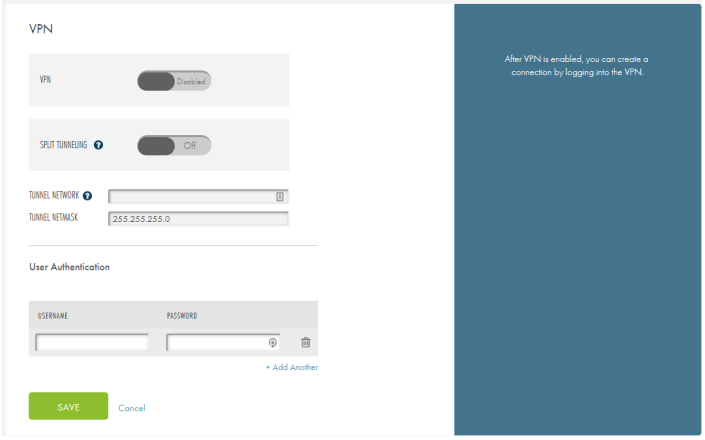
On the *Configure: Virtual Office* page, click the **Edit** button in the *VPN* section.



STEP 2

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

- **Split Tunneling**—enable split tunneling to route the VPN user's Internet access through their device. Disable to route all Internet traffic through the Virtual Office.
- **Tunnel Network**—create a network for the virtual office. The *Tunnel Network* address establishes a network tunnel between the user's device and the Virtual Office. It should meet the following guidelines:
    - Cannot be on the same network as the Virtual Office.
    - Cannot be on the same network as the device performing connecting to the Virtual Office.
    - Should be a private IP address, such as:
        - **Class A**—10.X.X.X
        - **Class B**—172.16.16.X - 172.16.31.X
        - **Class C**—192.168.X.X



- **Tunnel Netmask**—enter the primary Virtual Office netmask. Axcient recommends a small netmask, such as 255.255.255.X.
- **User Authentication**—create login credentials for users to access the VPN. Click the **Add Another** button to create multiple user logins.

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

Connecting to VPN

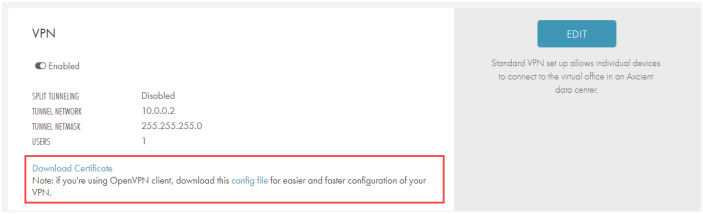
When a VPN network has been configured in the Virtual Office, you will need to connect to the VPN network using a preferred VPN agent. This procedure will use **OpenVPN** as the VPN agent for demonstration purposes. You can, however, use any preferred VPN agent.

To connect to the VPN network:

STEP 1

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

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

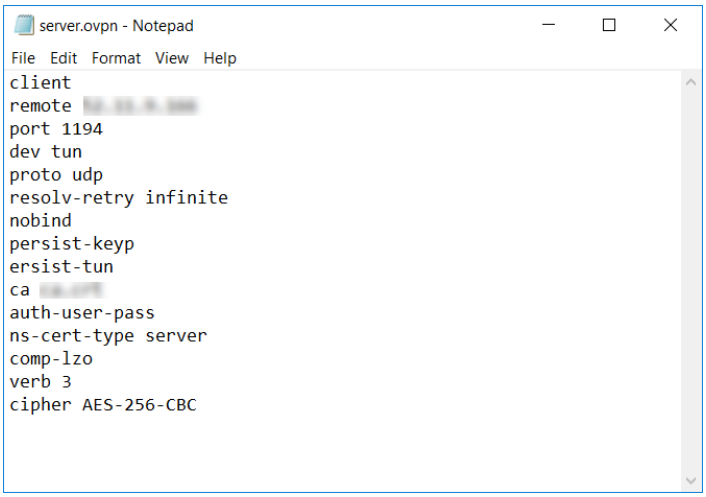


STEP 2a

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

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

Confirm that the following text exists in the configuration file:

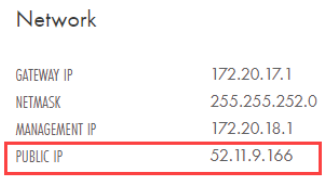


```
client
remote Public IP of Virtual Office
port 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
ca Certificate File filename
auth-user-pass
ns-cert-type server
comp-lzo
verb 3
cipher AES-256-CBC
```

STEP 2b

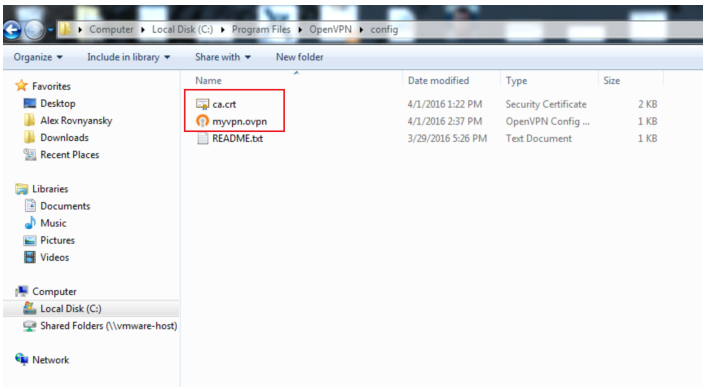
If you are using an alternative VPN option, locate the configuration file for the VPN agent. Configure the file using the correct information:

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



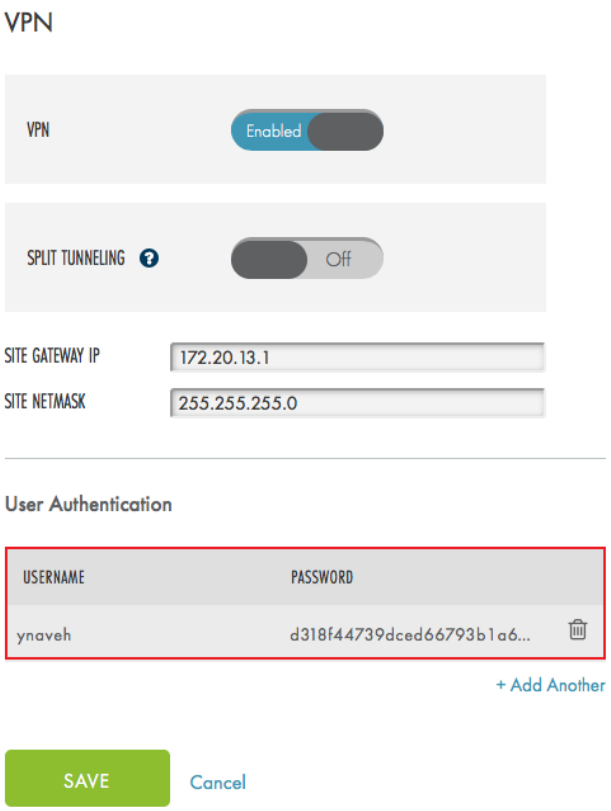
STEP 3

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.



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.



Port Forwarding

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

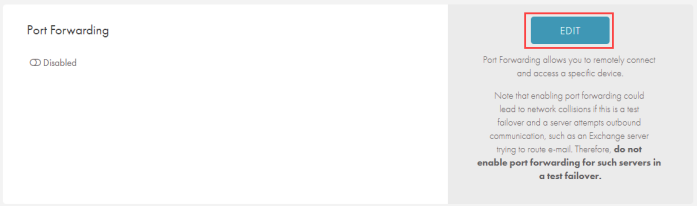
Enabling Port Forwarding could lead to a network collision if configured on a Test Virtual Office. Do not enable and configure Port Forwarding for a Test Virtual Office as productivity and data loss may occur.

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

To configure or edit the Port Forwarding settings:

STEP 1

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

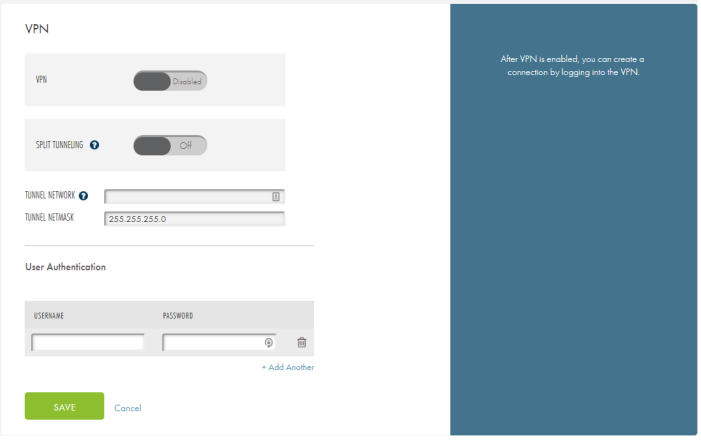


STEP 2

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

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

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



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

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

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

Public IP Settings

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

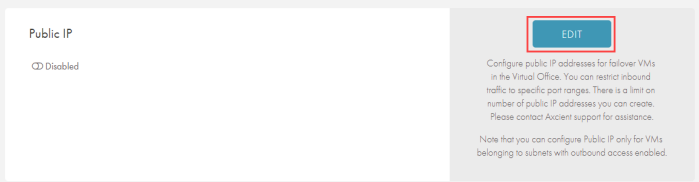
Note

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

To configure a public IP address:

STEP 1

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



STEP 2

On the Port Forwarding page, update the following fields:

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

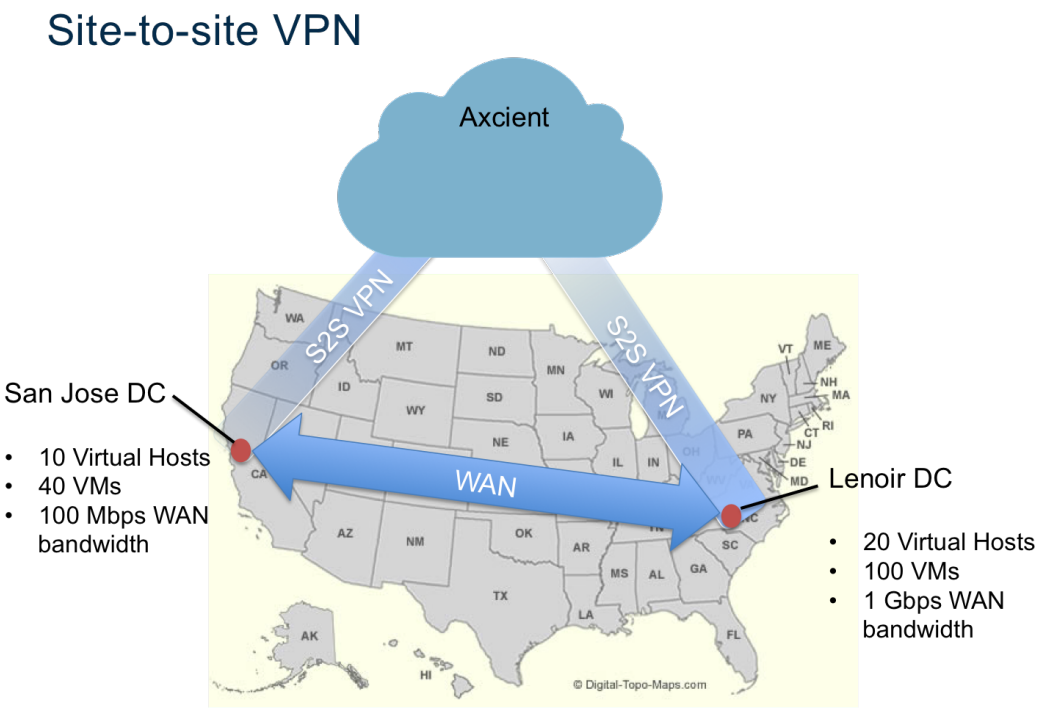
- Click the **Add Another** button to add additional entries.

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

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.

To set up a Site to Site VPN:

STEP 1

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

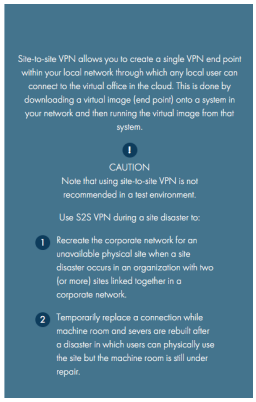
STEP 2

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

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

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

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



How to Deploy the Site to Site VPN Endpoint

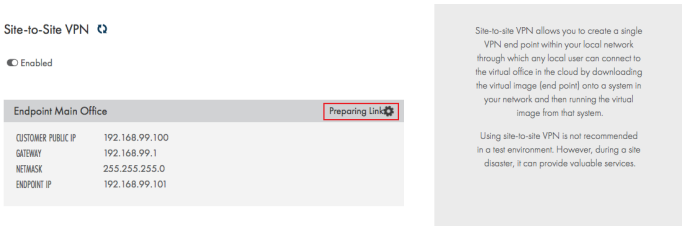
When Site to Site VPN is configured for the Virtual Office, you can then download the image of the Endpoint. This image should be deployed at the desired location using any VMware virtual machine software.

To deploy the Site to Site VPN Endpoint:

STEP 1

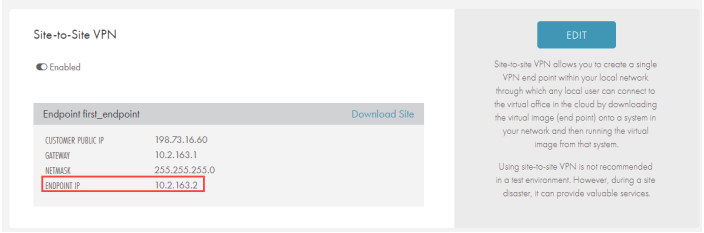
On the *Configure: Virtual Office* page, find the *Network* section.

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



STEP 2

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



Prepare Devices

When the Virtual Office is configured, you *must* prepare devices within the Virtual Office.

Preparing devices in the Virtual Offices includes the following steps:

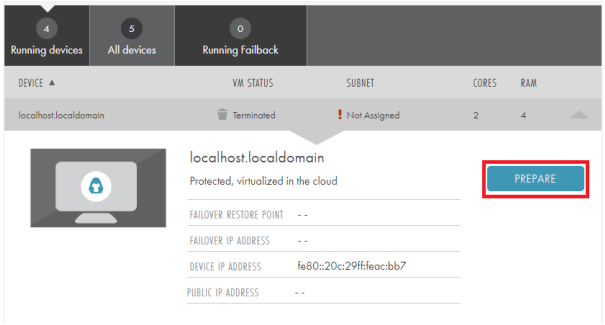
- Select the desired restore point.
- Configure the device's subnet and the device's virtual resources.

Preparing devices is a required step in the Virtual Office deployment process. All devices operating within the Virtual Office must be prepared.

To prepare a device:

STEP 1

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



STEP 2

In the *Prepare* screen, select the desired **restore point**.

The *Cached Restore Points* display in **blue**. These are restore points that have already been prepared in the Axcient Cloud. You will spend less time preparing the device when selecting a cached restore point.

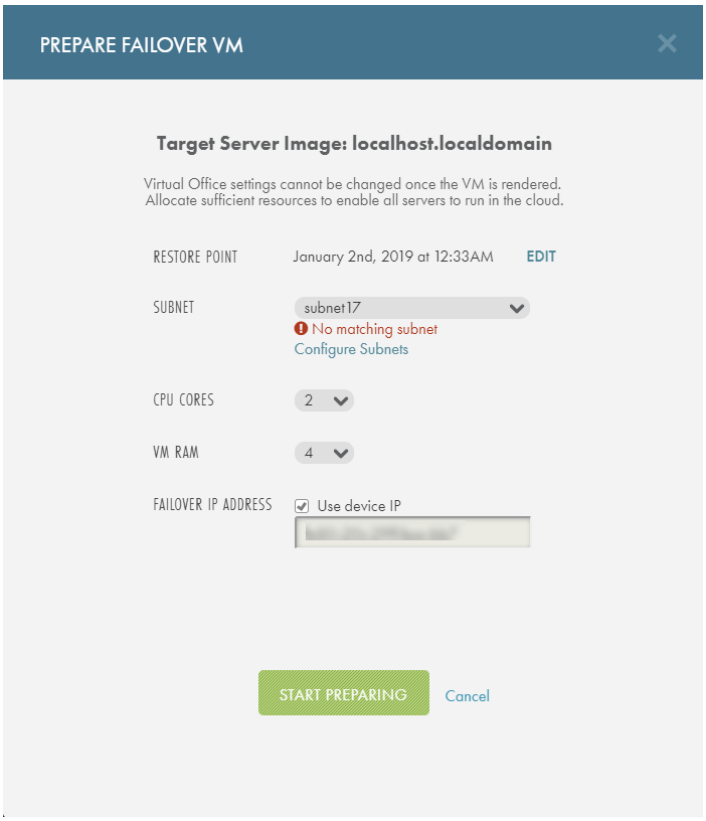
The *Uncached Restore Points* display in Green. These are restore points that have *not* already been prepared in the Axcient Cloud. You will spend more time preparing the device when selecting these restore points.

STEP 3

Configure the following fields:

- Optionally, click the **Edit** link to update the restore point selected in the steps above.
- In the *Subnet* field, select the appropriate **subnet device**. If a subnet device has not yet been created, please refer to the Network section of this guide.
- In the *CPU Cores* drop-down menu, select the **number of virtual CPU cores** for the device.
- In the *VM RAM* drop-down menu, select the **amount of RAM** for the device.
- In the *Failover IP Address* section, click the **Use Device IP** checkbox to use the selected device's IP address for failover purposes. Alternatively, you can uncheck this option and configure a new failover IP address.

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



How to Connect to a Device

When the Virtual Office is configured and the devices have started, you might need to directly access a specific device. 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 VPN, or Port Forwarding. You can configure these settings in the Configure the Virtual Office page.

Virtual Private Network (VPN)

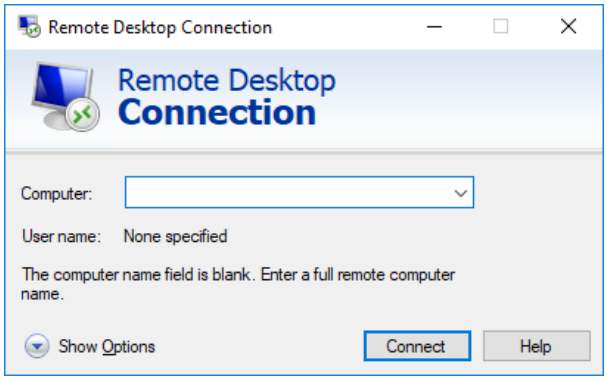
Before using the RDP agent to access a device over a VPN:

- 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

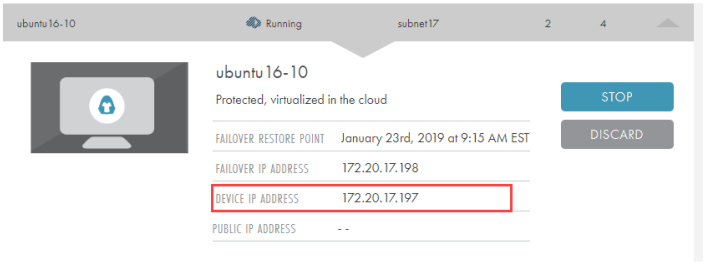
Open the preferred RDP agent. In this example, we will use the Microsoft Remote Desktop RDP agent.



STEP 2

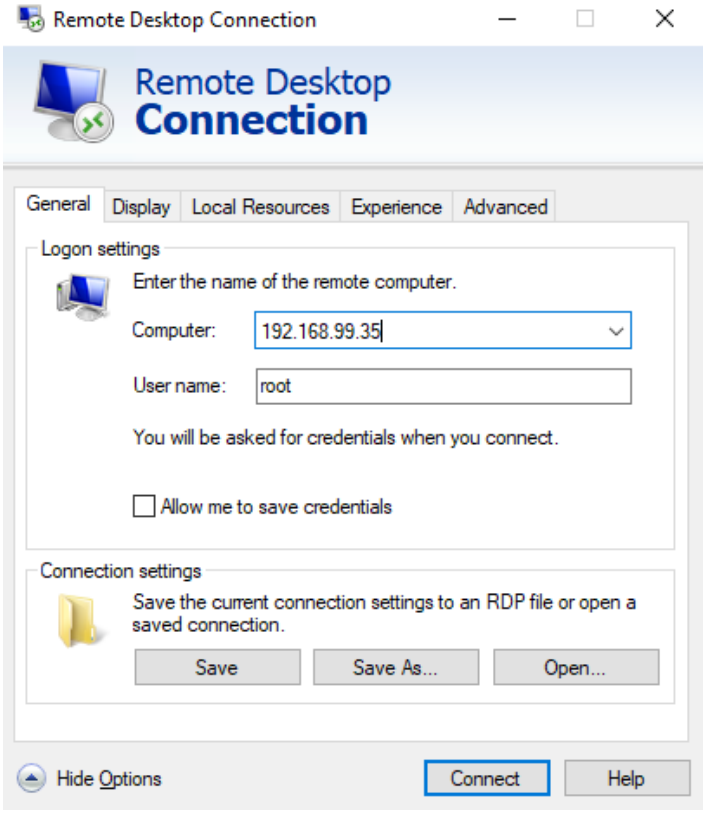
To complete the connection process, find the IP address and credentials for the device.

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



STEP 3

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



Port Forwarding

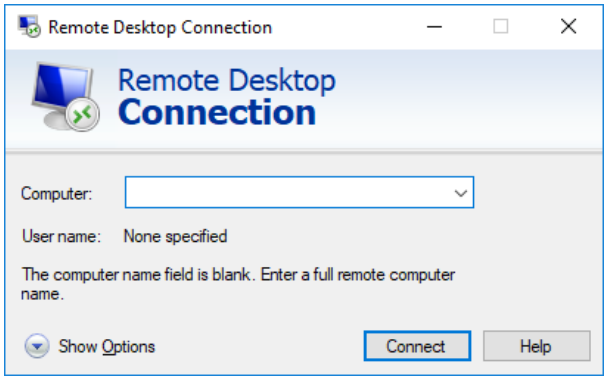
Before using the RDP agent to access a device using Port Forwarding:

- 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

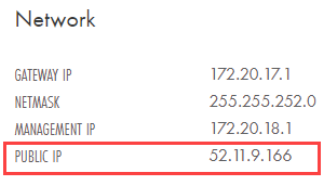
Open the preferred RDP agent. In this example, we will use the Microsoft Remote Desktop RDP agent.



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.



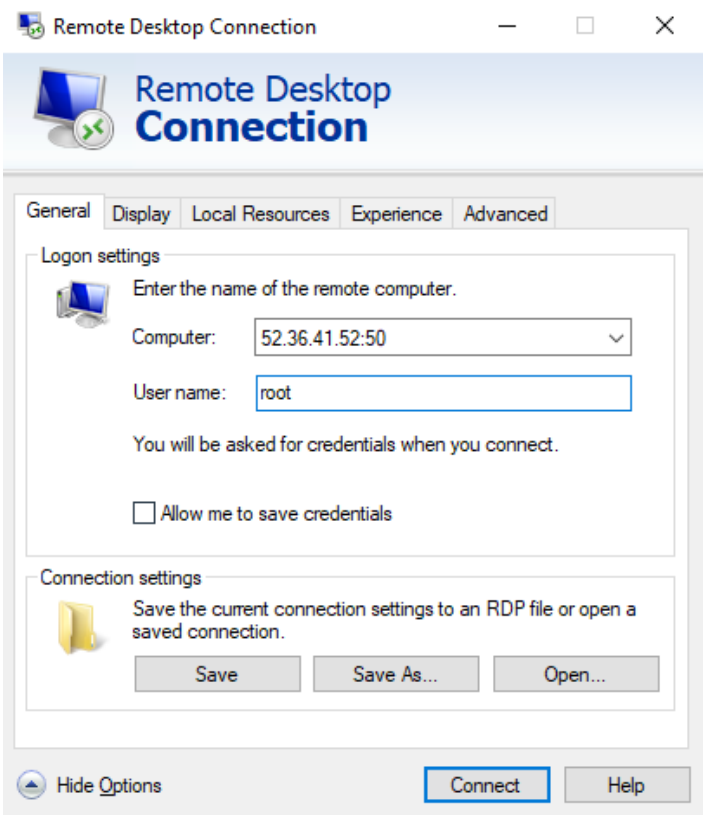
STEP 3

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.



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 & Dev** – Create Runbooks to automatically deploy an environment on which the user can test patches and software updates to see how they would affect the production environment.
- **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:

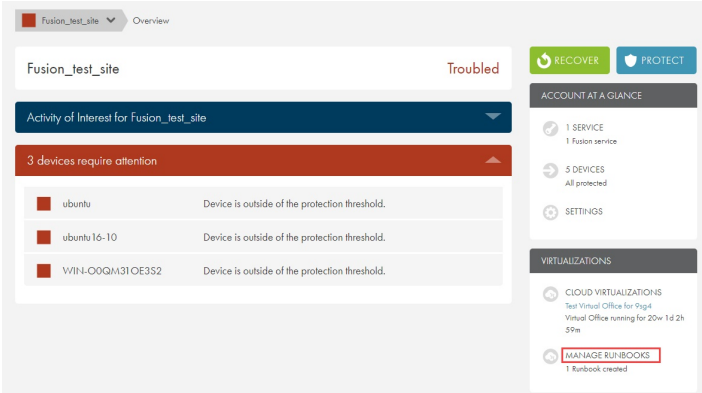
- Devices to be virtualized,
- The order in which the devices should be virtualized,
- Resources to allocate to each device,
- Wait time between the deployment of each device,
- Network settings, and
- Other advanced options, like VPN settings, Port Forwarding, and Site-to-Site VPN.

Create a New Runbook

To create a new Runbook:

STEP 1

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

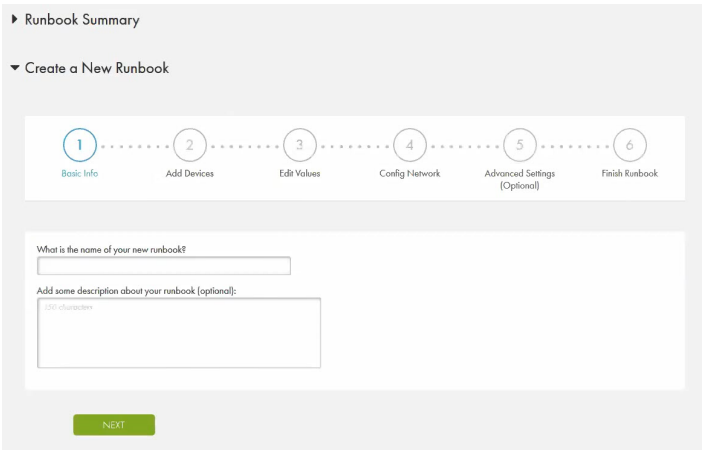


STEP 2

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.

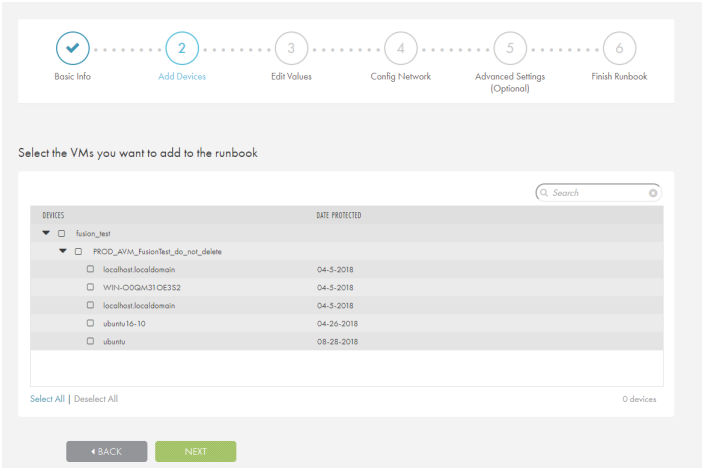


STEP 3

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

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

Click the **Next** button to continue.

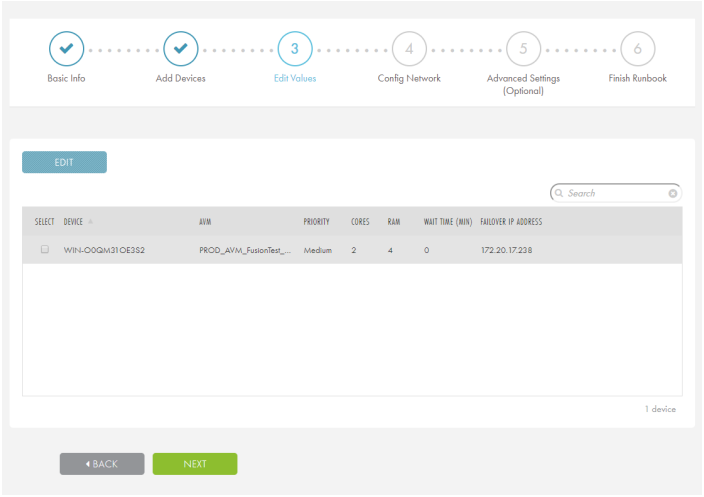


STEP 4

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

- Device boot priority,
- Number of virtual cores allocated to the device(s),
- Amount of virtual RAM allocated to the device(s) ,
- Wait time in between the booting of virtual devices in the Virtual Office, and
- Failover IP address.

Click the **Next** button to continue.

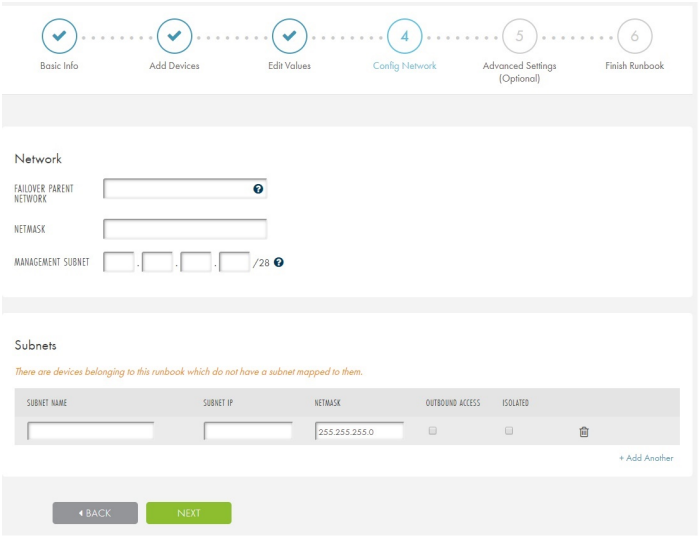


STEP 5

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

- In the *Network* section, configure the Failover Parent Network, Netmask, and Management Submit of the Virtual Office. Please refer to the **Configure the Virtual Office** section for more information.
- In the *Subnets* section, create one or more subnets for the devices in the Runbook. Failure to create a subnet, or creating an incorrect subnet, will prohibit the devices from being deployed in the Virtual Office. Please refer to the **Configure the Virtual Office** section for more information.

Click the **Next** button to continue.



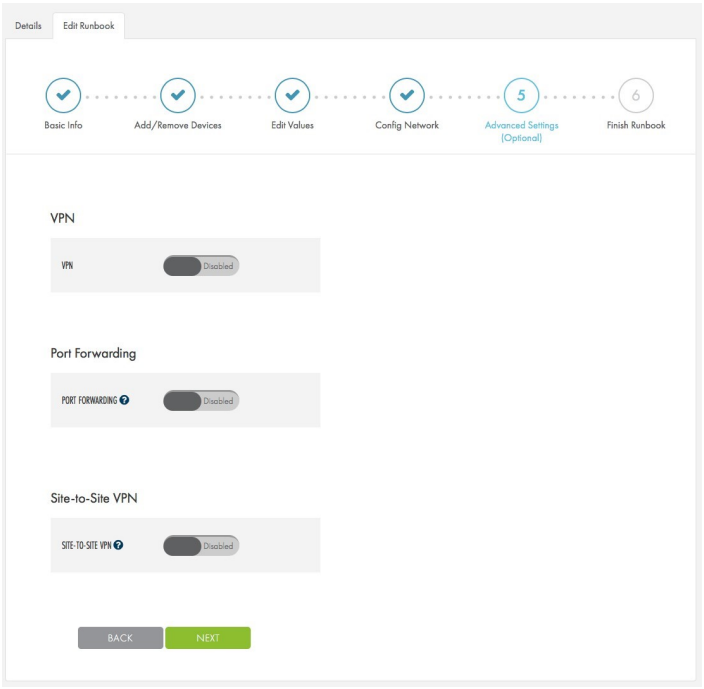
STEP 5

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

- VPN
- Port Forwarding
- Site-to-Site VPN

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

Click the **Next** button to continue.

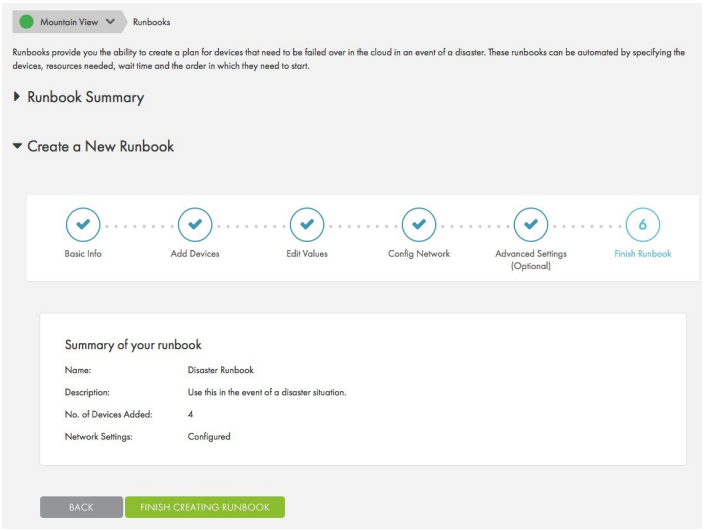


STEP 5

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.



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 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.

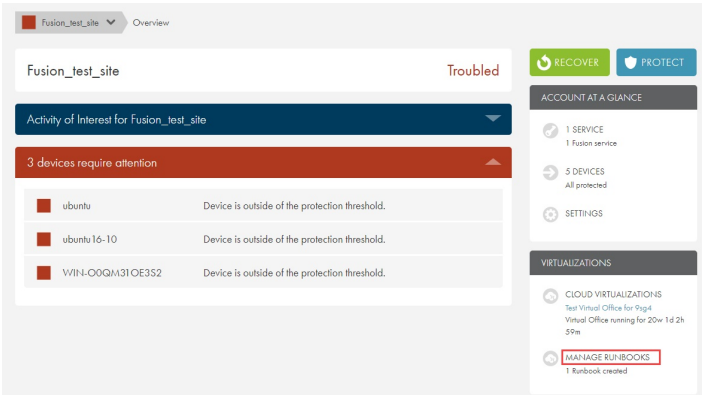
If a subnet is configured for only one or some of the devices, you will need to create the additional subnets in the *Virtual Office Configuration* page in order to virtualize the remaining devices when the Runbook is in a Running state.

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.

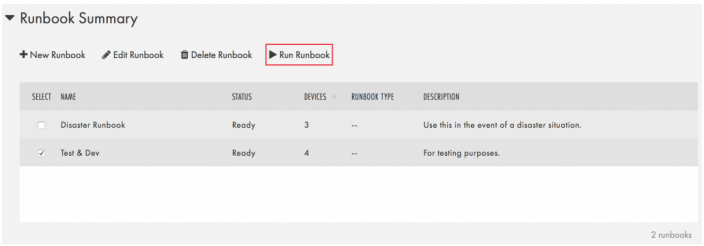
STEP 1

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



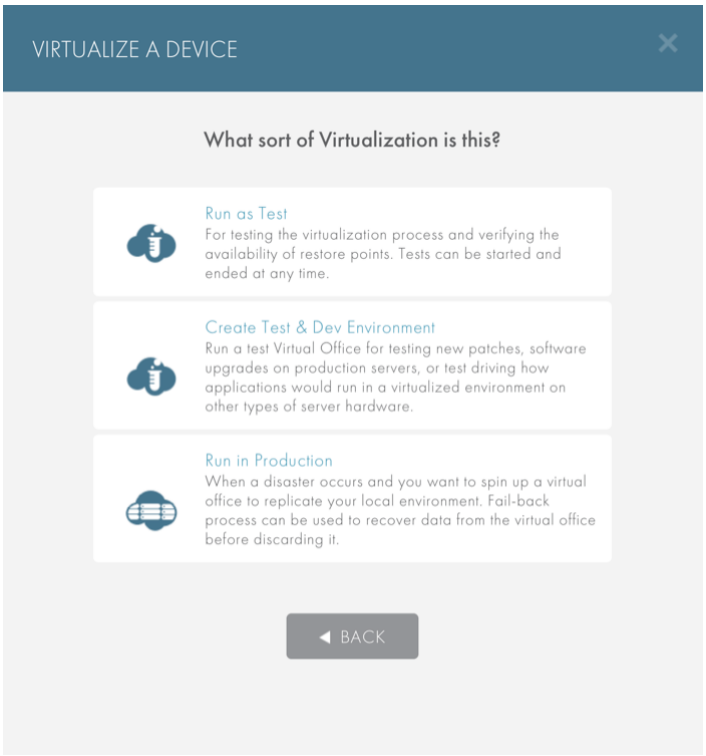
STEP 2

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



STEP 3

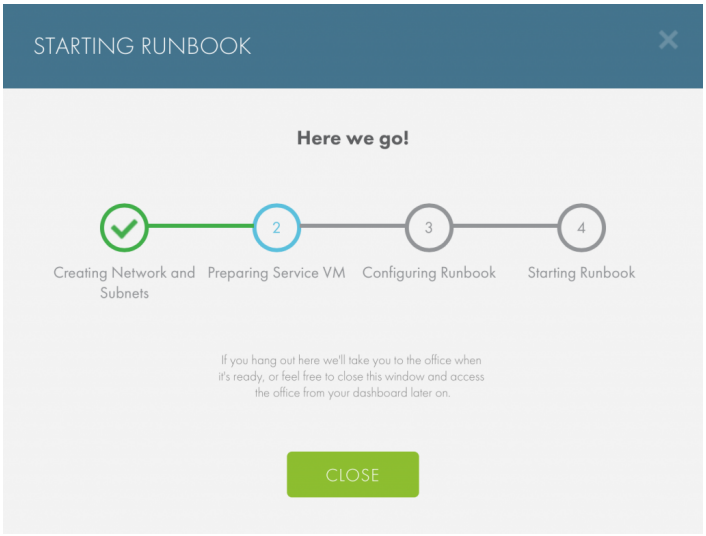
On the *Start Runbook* screen, select the type of Virtual Office to deploy.



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.

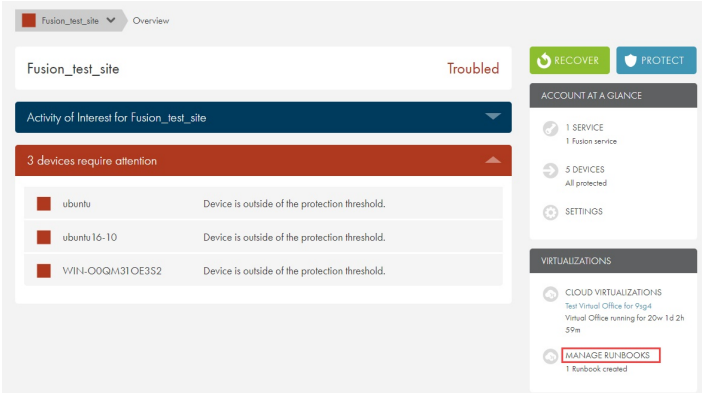
While a Runbook is inactive, all aspects of the Runbook and Virtual Office can be edited; however, not all aspects of the Runbook can be edited while the Runbook is running. For example, you *cannot* edit included devices when the Runbook is running, but you *can* edit network information.

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

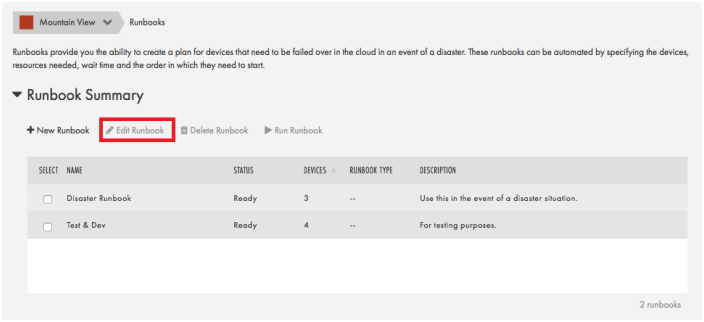
On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.



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.



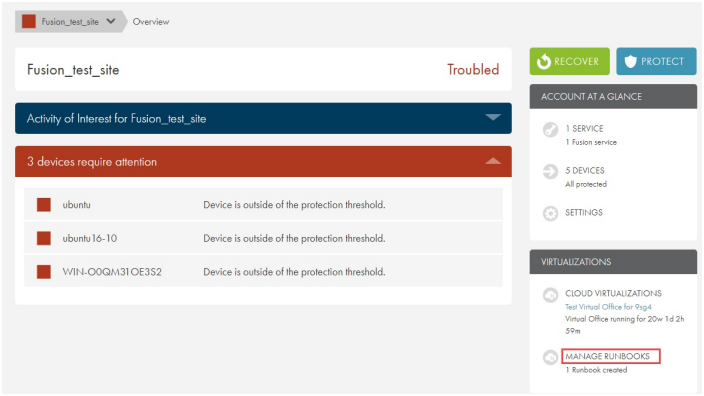
Delete a Runbook

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

To delete a Runbook:

STEP 1

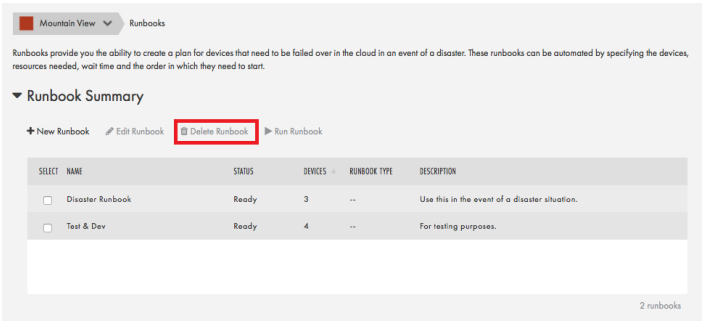
On the *Site Details* page, click the **Manage Runbooks** link found in the Virtualization section of the page.



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.



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.*