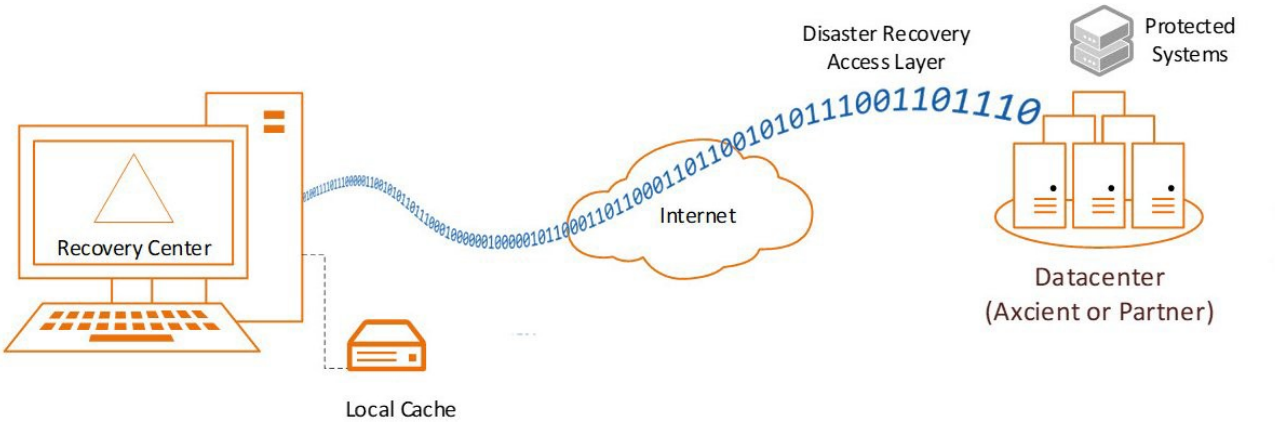


Recovery Center is a companion recovery platform for Direct-to-Cloud (D2C) protected systems.

Recovery Center is a stand-alone application that allows you to recover data directly from theAxcient Cloud or Private Cloud, with or without a local cache device.

With Recovery Center, you can directly mount a protected system's disk volumes from any recoverypoint hosted on a vault.

Recovery Center may be installed to any 64-bit Windows operating system.

Release 1.0.0 supports file and folder recovery and bare metal recovery (BMR)

Note: BMR from local cache is supported within the x360Recover Recovery Toolkit ISO. Later releases will add support for virtual disk image exports and direct virtualization of protected systemson a Hyper-V or ESXi host.

Rapid data recovery for offsite protected systems

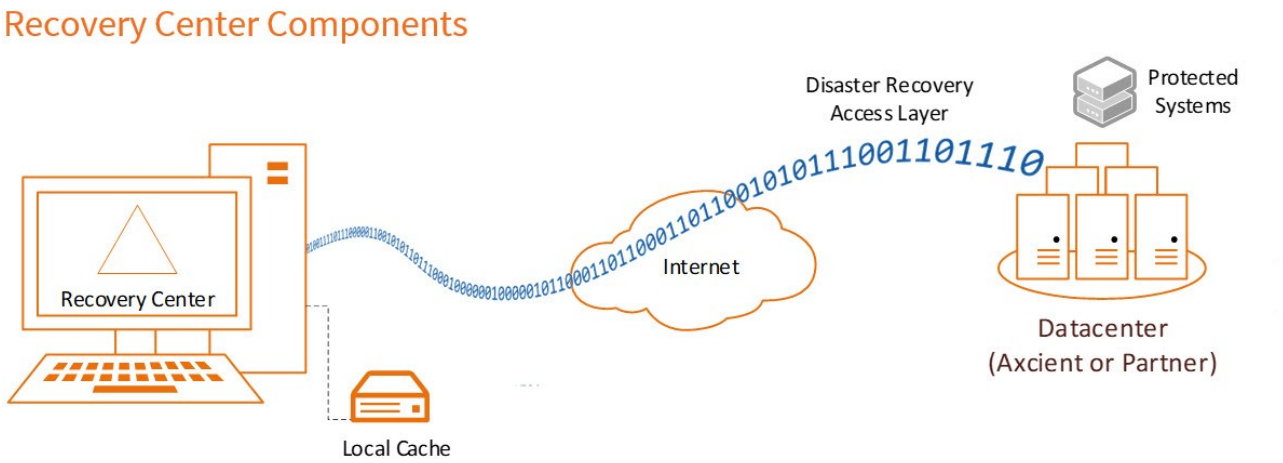
Recovery Center provides quick access to your offsite protected systems, whether they are locatedon an Axcient-hosted vault or a self-hosted private vault. Recovery Center is optimized to functionbest with D2C protected systems employing a local cache repository (which accelerates data recovery.) However, any system present on the vault may be recovered over the WAN.

Note: You may use Recovery Center to perform file and folder recovery for any protected system resident on a vault, with or without local cache, although performance without local cache will be subject to download bandwidth performance and, therefore, will potentially run much slower.

Recovery Center Components

Multiple components make it possible to recover data from the Cloud with Recovery Center:

- Two background services and a frontend UI application are installed on the target system. These communicate with the vault: performing authentication, browsing protected systemsand metadata, and retrieving data.
- An optional local cache repository, if available, can be used to greatly accelerate data recovery.For details on configuring your Direct-to-Cloud backup agent to generate a local cache, see this knowledgebase article.



Recovery Center component: Jobs Service

The ***xCloud Recovery Center Service*** runs in the background on the system to manage recovery jobs.

This service is responsible for creating, managing, and deleting recovery jobs constructed via the User Interface on demand, as well as providing for persistence of job states through reboots and system shutdowns.

A **recovery job** defines:

- type of recovery to be performed (currently limited to file and folder recovery)client
- protected system
- backup snapshot to recover data for
- authentication information
- how the selected protected system disk volumes will be presented to the local machine.

Recovery Center component: Virtual Disk Service

The ***xCloud Virtual Disk Service*** is the core of the recovery engine, providing the means to transform remote recovery points into locally mounted block storage devices for data retrieval.

Jobs defined in the User Interface and managed by the *xCloud Recovery Center Service* are executedby the *xCloud Virtual Disk Service*.

Cloud metadata is used to define the physical disks and volumes. Data is retrieved first from the local cache repository (if present) then over the WAN from the vault. The local machine is then presented with virtual block storage devices matching the selected protected system recovery point.The disk volumes from the selected protected system can be mounted to the local machine, either as new drive letters or as sub-folders within a selected folder.

Recovery Center component: DRAL

The **Disaster Recovery Access Layer (DRAL)** is a service running on the vault, providing a securedata transport layer, authentication system, and metadata retrieval service.

Recovery Center connects to DRAL in order to authenticate and browse protected systems and recovery points available on the vault. DRAL also transports any data not present within the optionallocal cache repository.

DRAL services are available on both Axcient-hosted vaults and self-hosted private vaults. Data forboth

appliance-based systems and D2C protected systems can be recovered with DRAL services.

Recovery Center component: (Optional) Local cache

An optional local cache repository, if available, can be used to greatly accelerate data recovery. Fordetails on configuring your Direct-to-Cloud backup agent to generate a local cache, see this knowledgebase article.

How does Recover Center work?

Metadata about the protected system is retrieved from the cloud (including available disk volumes,physical disks, and partition sizes.)

This metadata is used to build a locally attached block storage device, within which is presented the protected system disk volumes and data.

- If a local cache repository is available for the selected protected system, Recovery Centerretrieves any requested data blocks locally from the cache first, greatly accelerating data access.
- If a local cache is not available (or if select blocks of data are missing or not present within the cache), the blocks are instead read over the WAN from the vault. If the job is configured to leverage a local cache, any data forced to be retrieved from the cloud will then be stored inthe cache so that future requests for the retrieved block(s) will be found locally.

Please note: Although it is possible to perform general file and folder recovery for any protectedsystem present on a vault, Recovery Center has been **optimized primarily for use with a local cache repository** to accelerate data access.

How do I use Recovery Center?

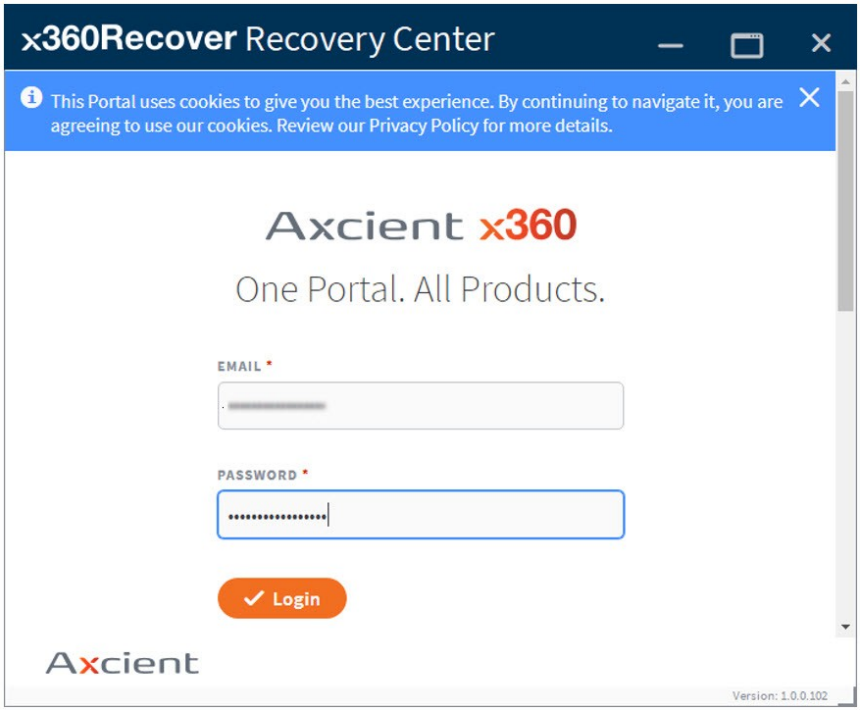
You can install Recovery Center onto any 64-bit Windows system where you wish to recover data.This may involve the original system where you are recovering data, or this may involve another location (such as an admin workstation from which to perform centralized recoveries.)

Recovery Center version 1.0.0 supports file and folder recovery. Later versions will provide virtual disk image export and full **no-hardware BDR recovery,** leveraging a Hyper-V or ESXi host to stageand natively manage virtual machines.

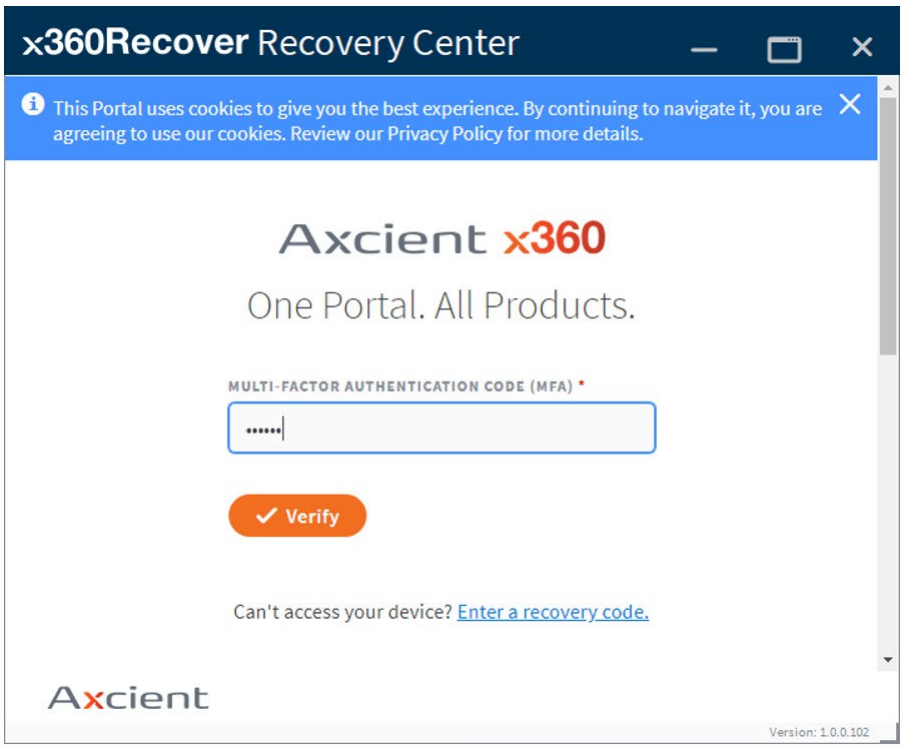
Launch Recovery Center

1. To launch Recovery Center, enter your Axcient x360Portal username and click **Continue.**
Note: Valid user accounts include x360Portal users or any Recover Manager (RMC) user account, including end client users.

2. Enter your Password and click **Login.**



3. Enter your six-digit MFA (Multi-Factor Authentication) code (if required) and click **Verify** to complete the login process.



Create a recovery job

Once logged in, you can create a recovery job and begin retrieving data.Home

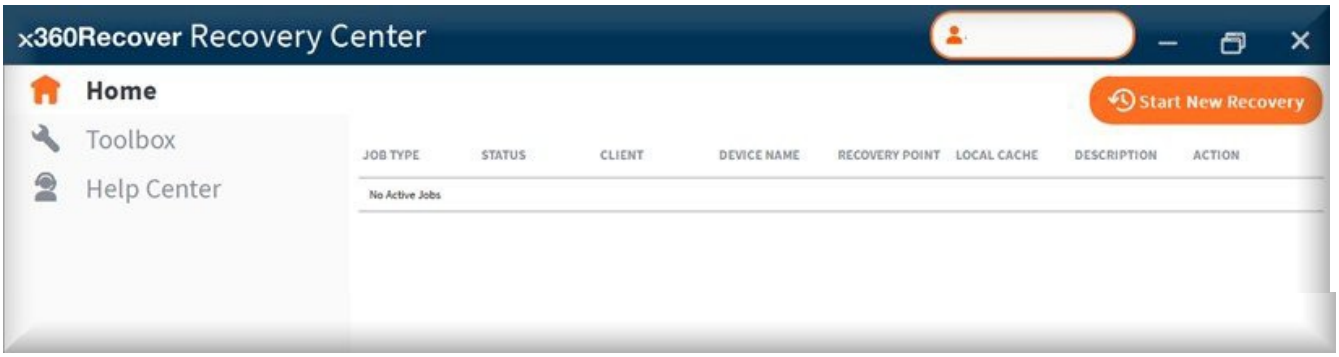
Page

The **Home** page view will load by default.

On this page, you may start new recovery jobs, monitor or manage existing jobs, or delete jobs thatyou are finished with.

- Recovery jobs run as a service and remain persistent in the background once created (whetherthe Recovery Center user interface is loaded or not.)
- Existing jobs will be restarted automatically after a system reboot.

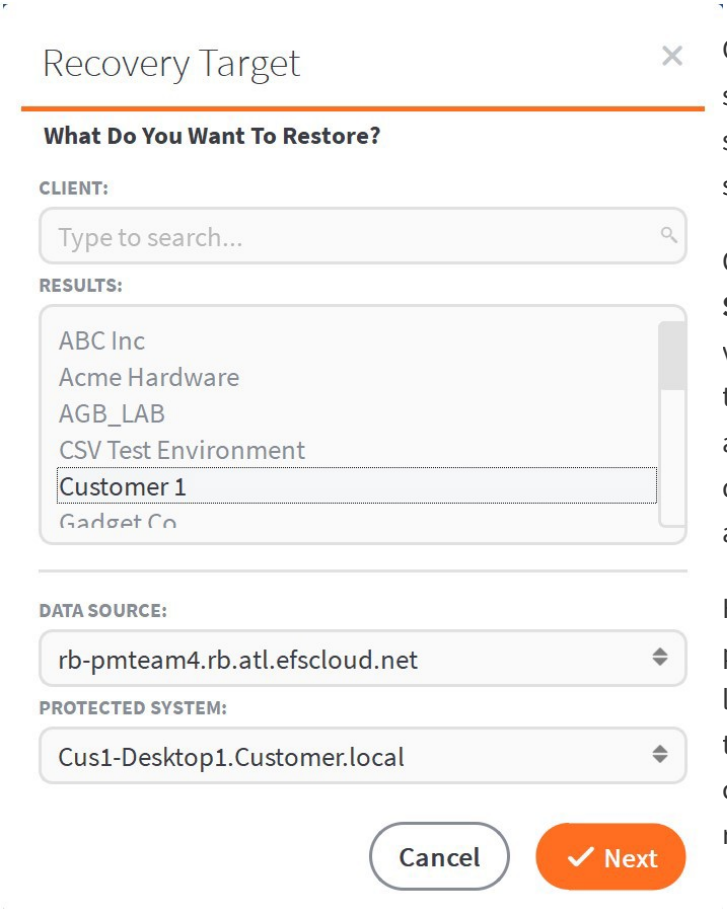
1. To create a new recovery job, click **Start New Recovery.**



2. The **Recovery Target** selection wizard will appear.

Wait for the list of available clients to complete downloading.

Then, select the desired client, data source (vault), and protected system you wish to recover.



Click inside the **Client** field and begin typingto search directly for a client. You can also simply scroll the list view. Click the desired client to select.

Once you have selected a client, the **Data Source** field will populate (with a list of all vaults containing protected systems belonging to that selected client.) The Data Source field automatically populates with thefirst discovered vault and protected system available on that vault.

Hint: You do not need to wait for all fields to populate before making selections. Once each level is populated, you may immediatelyclick or type to search for valid selections at that context level. The dependent selections will refresh.

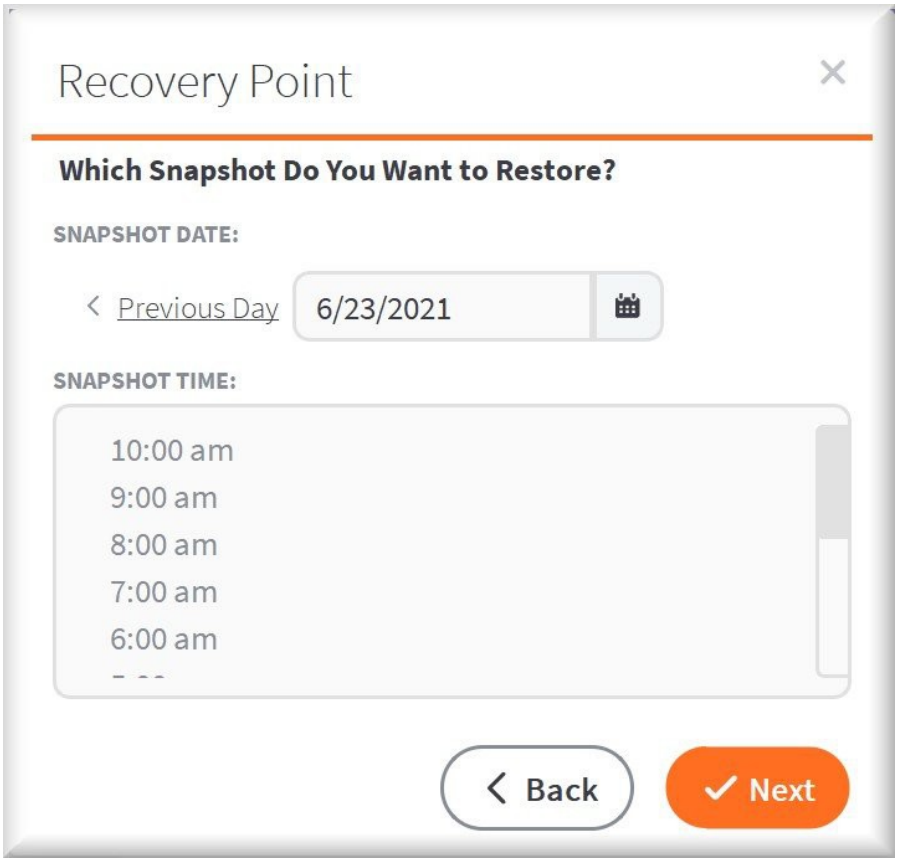
Click to select the desired vault and protected system, and then click **Next** to continue.

3. The **Recovery Point** selection page appears.

The initial date displayed will be the most recent date for which recovery points exist. (It may take a minute before the list populates with available recovery points from the selected vault.)

Click the calendar selector to choose a date or click the **Previous/Next Day** links to navigate toanother day if desired.

Click to select a snapshot from the desired time on the specified day:

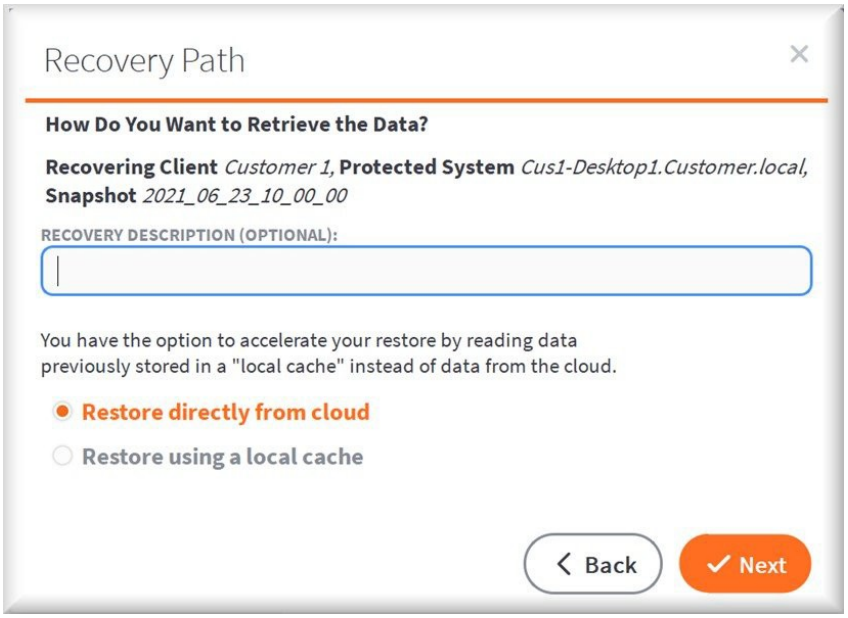


Click **Next** to continue.

4. The **Recovery Path** selection page appears. This is where you will specify how the recovery will be performed.

You may enter an optional description for this recovery job. This description will be displayed onthe *Home* page in the **Jobs** table.

You will then choose whether you wish to recover (a) directly from the cloud vault or (b) using a localcache.



- **Restore directly from cloud** means that all data is accessed remotely over the WAN using theDRAL (Disaster Recovery Access Layer.) **Note:** The process of recovering directly from the cloud has not yet been optimized. This means recovery performance is somewhat slow in this release. (You will NOT get your full internet download bandwidth using this mode.)
- **Restore using a local cache** means the local cache repository is first searched for requested data blocks. Only if a requested block is not available in the cache will it be retrieved over theWAN from the Disaster Recovery Access Layer.

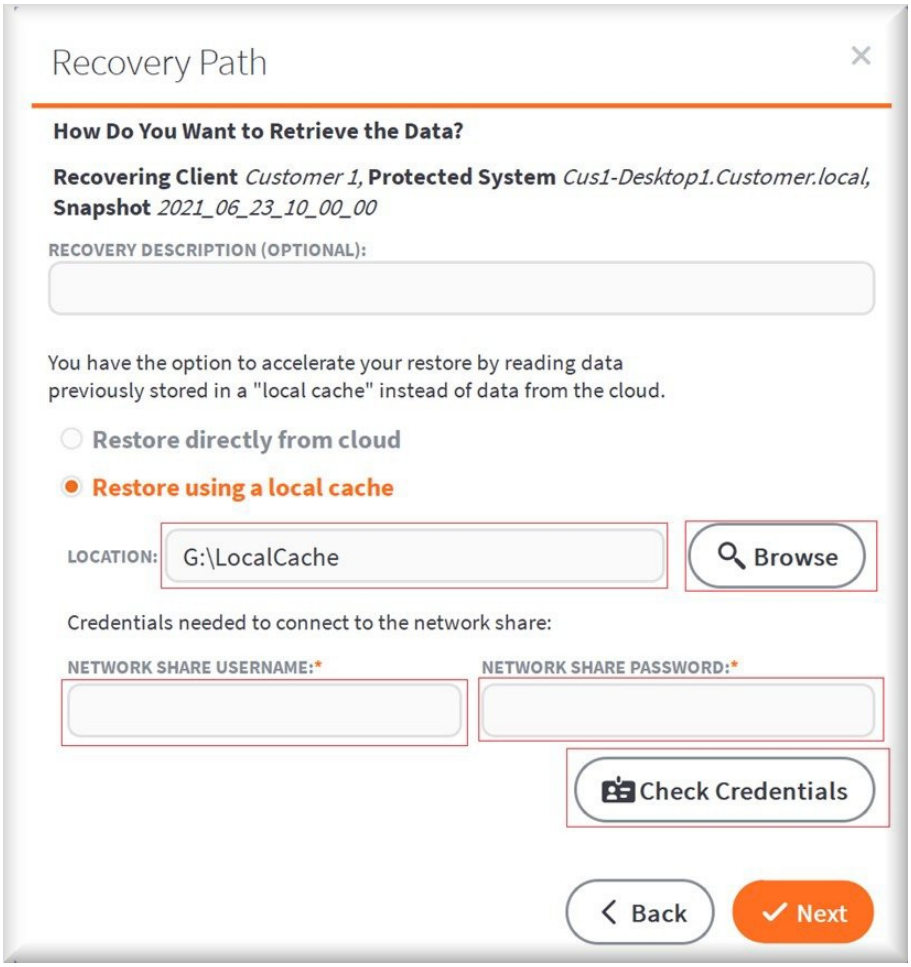
Restore using a local cache

4a. If you have a local cache repository available for the protected system, browse or type the pathto the cache files in the **Location** field.

Note: See this article for more details on enabling and configuring local cache settings within the x360Recover agent.

4b. Browse to the root level of the folder containing the local cache data. Local cache data may be located either on a directly-attached device (such as a USB hard drive) or on a network share location.

- For local devices, leave the credentials fields blank and click **Next** to continue



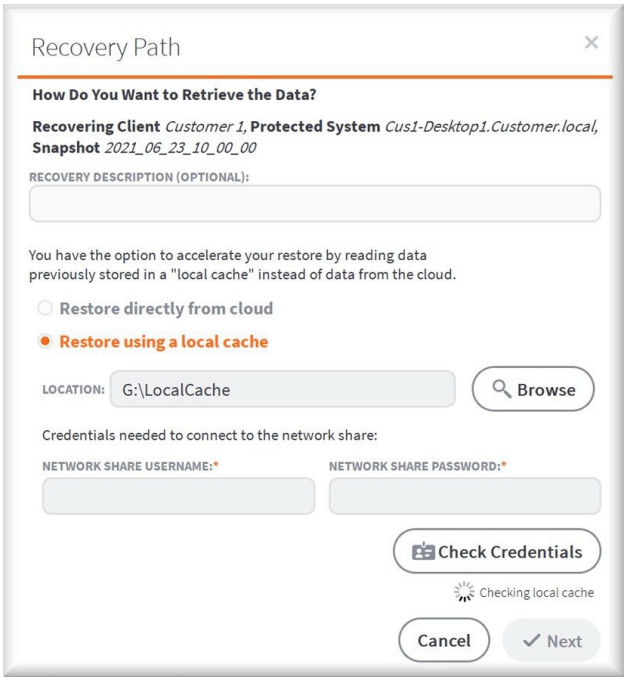
- For local cache data located on a network share, you must enter the path in UNC format. Forexample:

\\<server>\<share>\<folder

- You cannot use a mapped drive letter in the path to a network shared local cache. Enter a
- username and password that has authorization to access the network share.
- If the shared folder is accessible via anonymous access (This is not recommended!) you mayleave the credentials fields blank.
- Click **Check Credentials** to validate access, then click **Next** to continue.

4c. If local cache mode is selected, the wizard will first attempt to open the local cache.

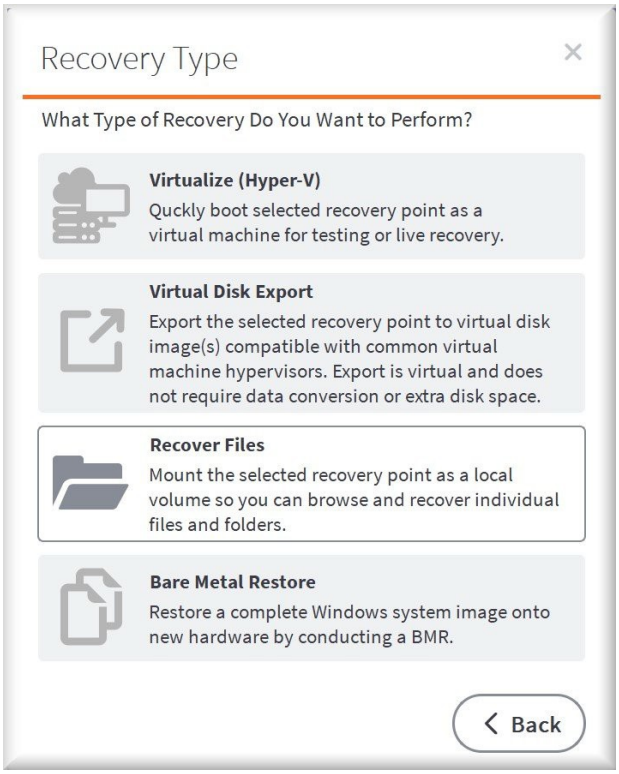
The wizard will then try to verify that the local cache is accessible. The wizard will also confirm thatthe local cache belongs to this client account, and that the local cache has data pertaining to the selected protected system.



4d. Once the credentials and local cache data have been validated, you can select the type ofrecovery on the *Recovery Type* window.

Currently, **Recover Files** is the only available option in the Recovery Center wizard. Additionaloptions will become available in future releases.

4e. Select **Recover Files** to continue.



5. The **Recovery Settings** page view will load by default.

Choose how you wish to mount the protected system disk volumes for recovery.

- You may choose to have **each volume mounted to individual drive letters**, starting with thefirst letter selected.

For example, if your protected system has C, E, and F drives, you may mount them beginning withdrive G. This would provide G, H, and I drives for the three volumes.

- Alternatively, you may choose to **mount all volumes to a single folder path**. Subfolders willbe created where each protected system volume will be mounted

For example: if you select C:\Recovery for the mount location, subfolders for Drive0, Drive1, andDrive2 will be created and each volume will be mounted to the designated folder.

6. Click **Start File Recovery** to complete this job and launch it..

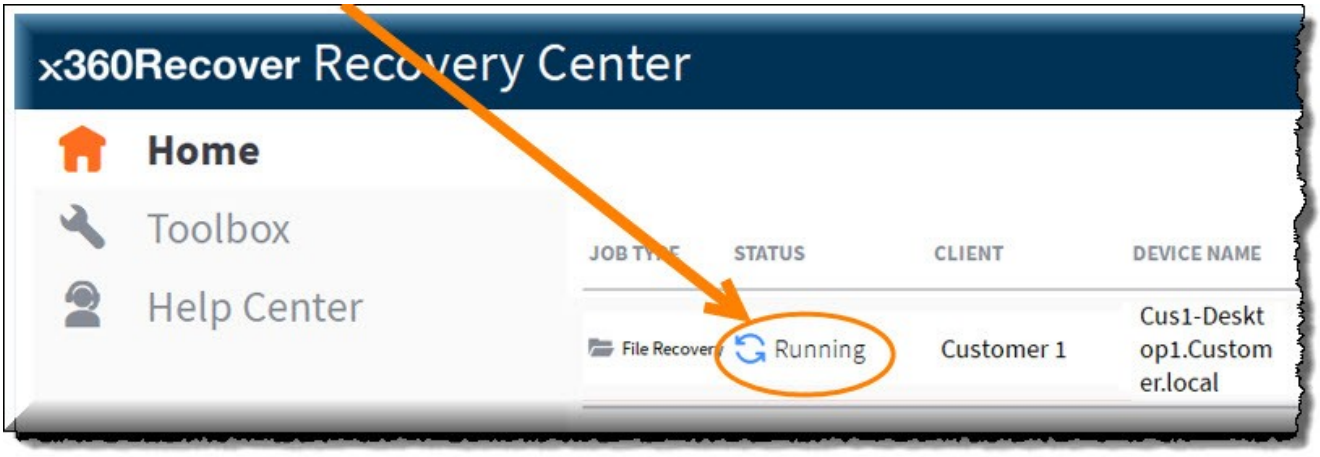
7. File recovery will begin building and mounting block devices for the selected protected system volumes. Staging the recovery may take some time for large volumes.

Note: Hash data for each volume must first be downloaded from the cloud, and this can take sometime for larger disk volumes.

You may close the **File Recovery Started** dialog if you wish and the recovery job will continue to runas a background service. (You may also close the entire Recovery Center user interface.) Active jobs will be restarted automatically on a reboot of the system.

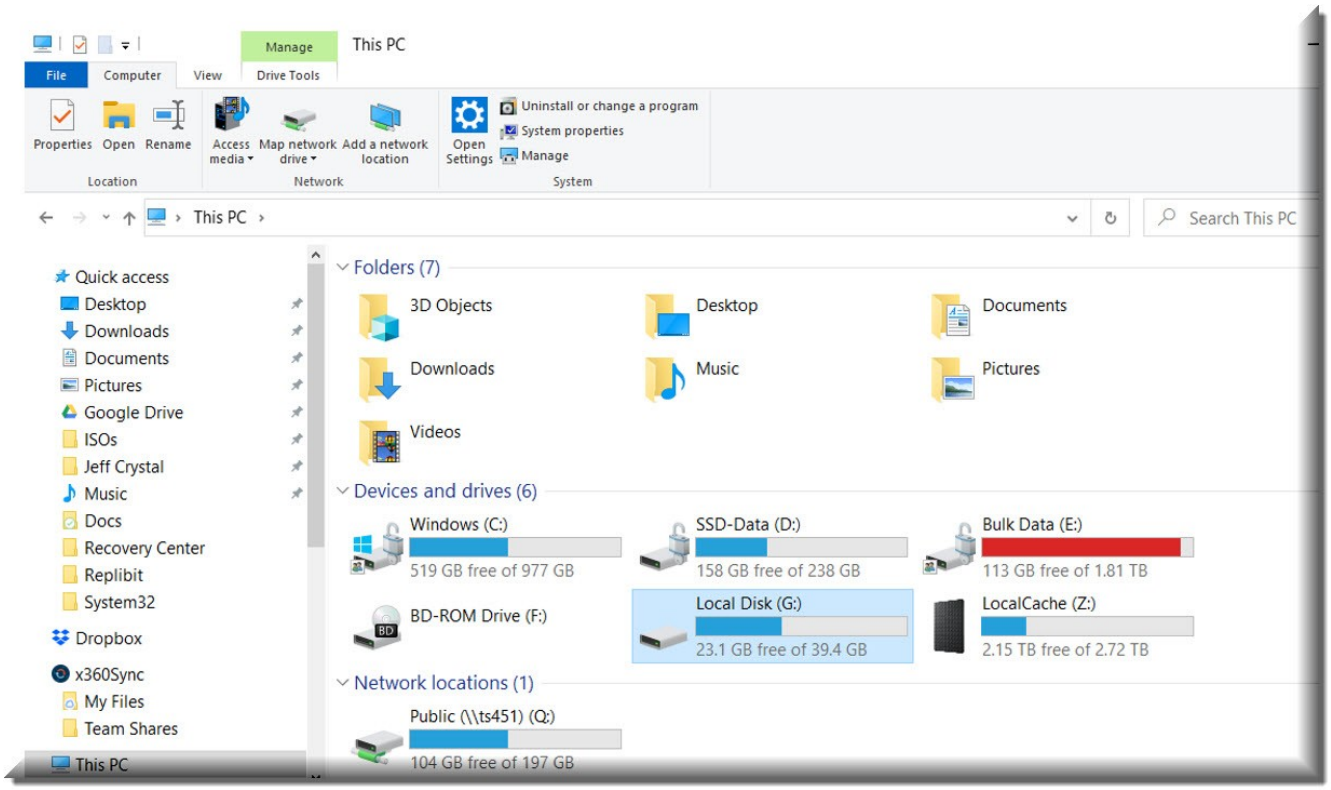
Monitor jobs in progress

Once the **Status** on the *Home* page indicates this job is **Running,** all disk volumes should be mounted and present on the local machine.

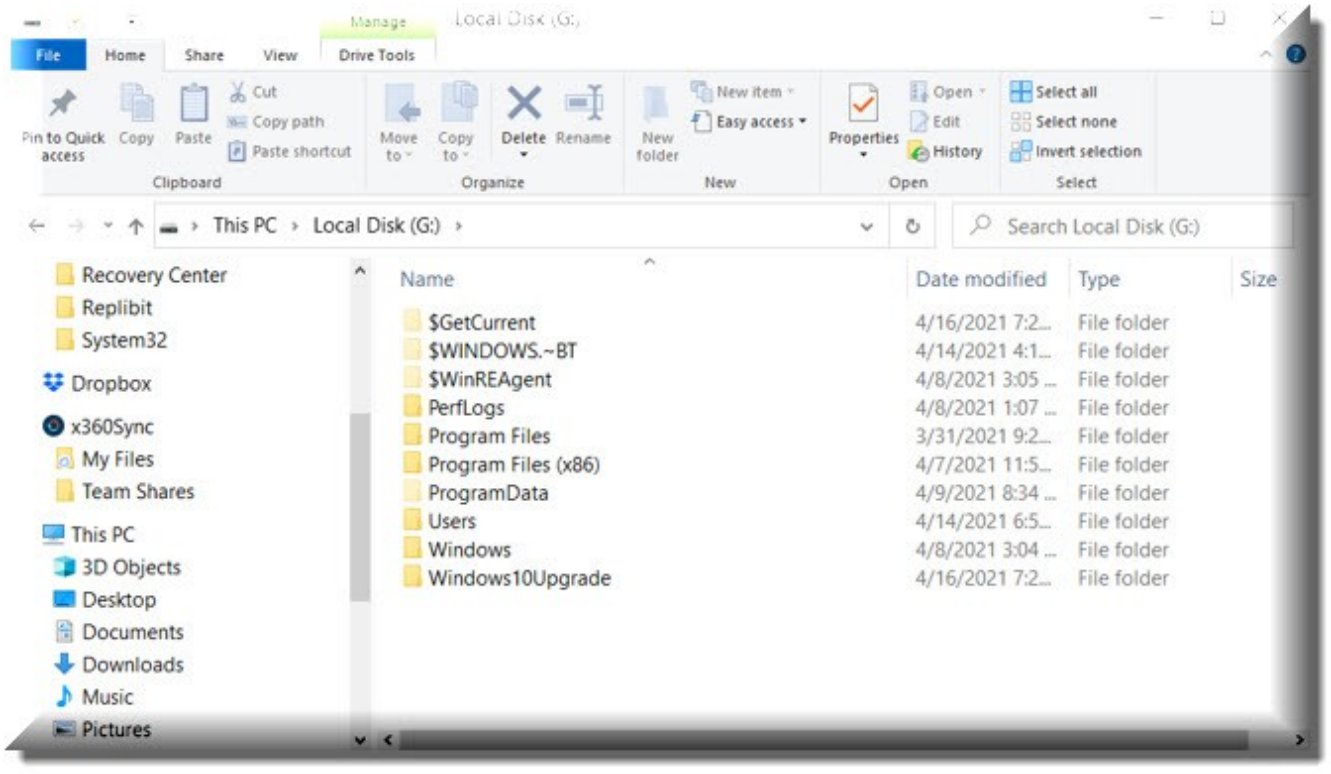


Use Windows File Explorer to browse, search, copy, and paste files and folder you wish to recover.

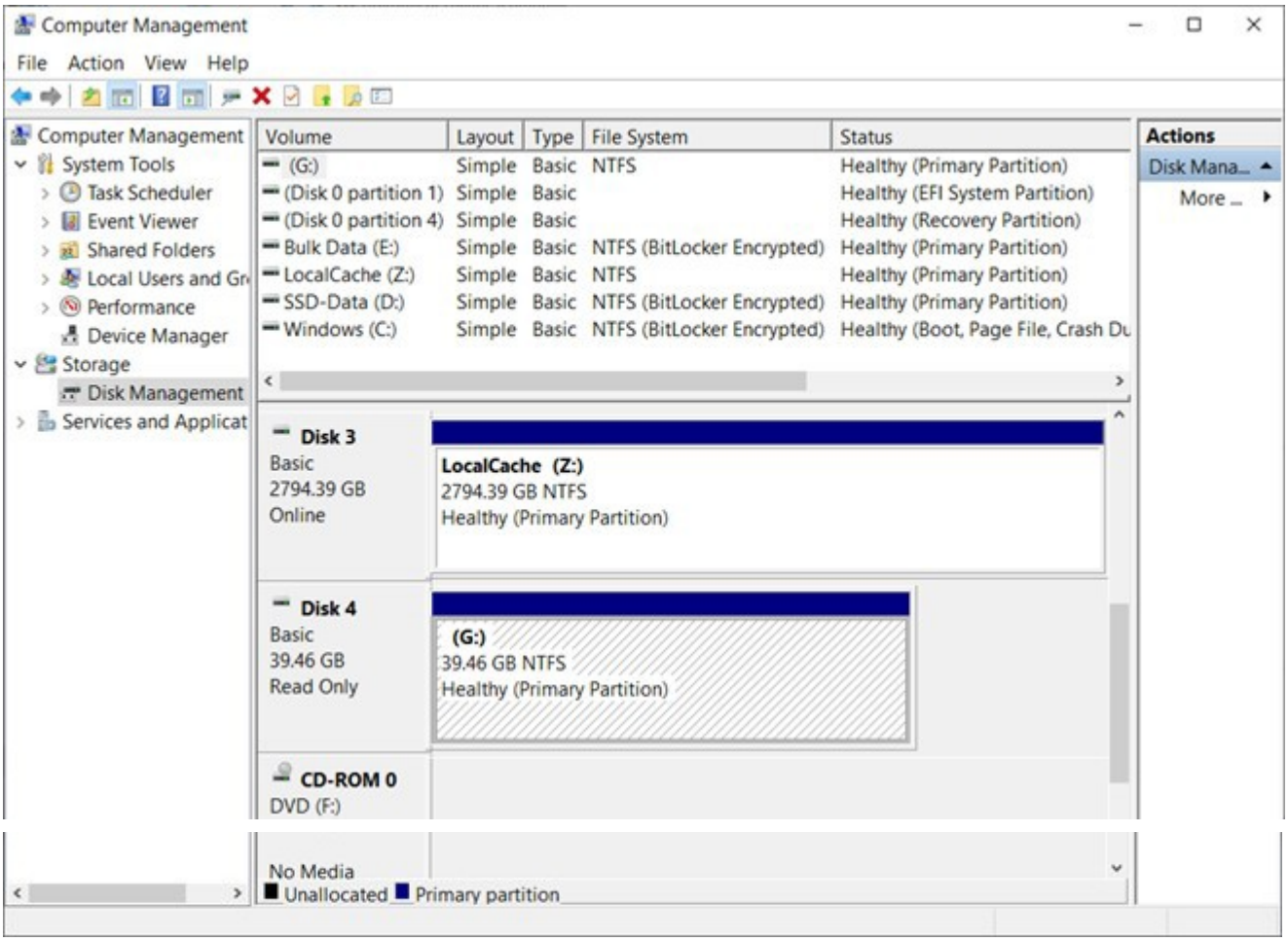
Depending on your mount point selections, the volumes should either be listed as individualmounted drive letters or mounted within the folder path you specified during job creation.



Note: Since the recovery volumes are mounted as locally attached block devices, the original file andfolder permissions from the protected system will be maintained.



In **Recovery Center** release 1.0, all disk volumes are combined into a single virtual disk and mounted as a local block device on the recovery system. This disk is read-only and can be seen inWindows Disk Manager for reference.

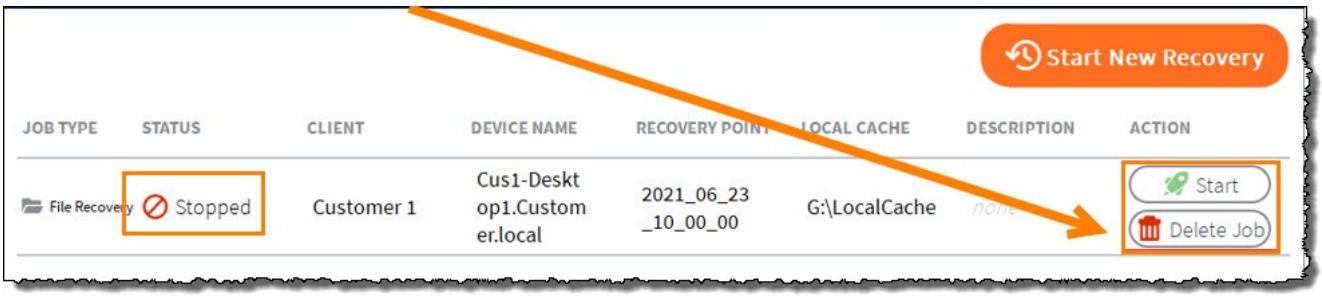


Details of all configured jobs can be seen within the Recovery Center user interface.

- Jobs remain active until stopped or deleted.
- Active jobs will remain persistent and will be automatically restarted after a reboot of the local machine.
- One or more jobs may be configured and running simultaneously.

Delete recovery jobs upon completion

When you have finished performing a recovery, you should stop and then delete the configured jobsto remove them from the backend jobs service.



Toolbox options

The Toolbox contains links to other related Axcient recovery tools.

Direct Restore

Direct Restore is a granular recovery utility for Microsoft SQL and Exchange databases. With Direct Restore, you can open and browse Exchange and SQL databases and select individual objects, tables,folders, or emails to be recovered. Export recovered items to a file or directly back into a live Exchange or SQL system.

Click the **Direct Restore** tile in the *Toolbox* to download the latest Axcient Direct Restore installation package.

Bare Metal Restore

Bare Metal Restore (BMR) is the process by which a protected system image may be written directlyback to a new hardware system from an offline recovery utility. The x360Recover Recovery

Toolkit ISO comes loaded with general troubleshooting and diagnostics utilities in a Linux Live ISO. Included in the Toolkit is the x360Recover Bare Metal Restore utility and the offline Driver Injector tool (used for recovering to dissimilar hardware when the original protected system image does notsupply a driver.)

Click the **Bare Metal Retore** tile in the *Toolbox* to download the latest version of the x360Recover Recovery Toolkit.

Help Center

Click the **Help Center** tile to access tools for troubleshooting in the event you have issues usingRecovery Center.

Analysis Tool

The Axcient Analysis Tool is a helpful utility for our Support team. Running the Analysis Tool gathers troubleshooting, diagnostic, configuration, and logs data from the running system and optionally uploads the to an open Support Ticket to assist in resolving any issues you might be having. Learn more about the Analysis Tool.

Other recovery alternatives

In addition to Recovery Center, Axcient offers other options for recovering your backup dataincluding:

Virtual Office
Virtual Office can be used to virtualize one or many protected systems in the Axcient Cloud. Virtual Office is fully self-managed and can be used by MSPs for true disaster recoveries or disaster recovery testing / client validation.

Bare Metal Recovery
Our x360Recover Recovery Toolkit hosts our Bare Metal Recovery wizard.With Bare Metal Recovery, simply boot a new-deployed or recently repaired system from ISO image and recover complete system images directly to the hardware. Bare Metal Recovery can operate directly from the appliance or vault, leverage previously downloaded Virtual Disk images, or perform recovery directly from the vault, with or without a local cache repository – just like Recovery Center.

File Browser
Mount a snapshot on any appliance or vault and use the web-based File Browser to quickly download individual files for recovery.

FTPS

For larger file and folder recovery operations, use our FTPS service to quickly download your bulk file and folder items using any standard FTPS client. FTPS offers faster, multi-threaded downloads, automatic retries, and resuming interrupted large file downloads.

Instant Disk Export

Perform an instant disk export from any appliance or vault. Then download a virtual disk image in any standard Hypervisor format, including VHD, VHDX, VMDK, VDI, and RAW