

x360Recover Direct-to-Cloud Installation Guide

Last updated: October 2021

TABLE OF CONTENTS

x360Recover - Direct-to-Cloud (D2C)	3
x360Recover components.....	3
Install the x360Recover Direct-to-Cloud agent.....	4
Firewall considerations.....	4
Firewall ports.....	4
Create Direct-to-Cloud clients in the x360Recover vault	5
Create a client	5
Download and install the Direct-to-Cloud agent	7
Role of the Agent	7
Prerequisites	7
Install the Direct-to-Cloud Agent	7
Silent and RMM deployment of the agent	12
Update Direct-to-Cloud agent settings	13
Log in via Single Sign On (SSO)	15
Add Direct-to-Cloud clients from the vault	17
Create Direct-to-Cloud schedules	20
Backup Types	20
Creating schedules in the Vault Web Interface	20
Coming Soon: The Global Management Portal for Direct-to-Cloud customers	23
Accessing the Global Management Portal	24
Connecting vaults for D2C customers with the Portal	25
Recover Direct-to-Cloud protected systems with x360Recover	27
Troubleshoot Direct-to-Cloud agent errors	29
Firewall considerations.....	29

x360Recover - Direct-to-Cloud (D2C)

x360Recover is a patented, chain-free, end-to-end Backup and Disaster Recovery (BDR) platform, empowering MSPs to deliver profitable, globally-managed business continuity services. As an x360Recover partner, you will protect servers and critical workstations, recover data in minutes, take advantage of multiple recovery techniques, and safeguard all your backed up data with one comprehensive solution.

x360Recover components

x360Recover includes the following core components:

- **Agent** The agent software is installed on a protected system and performs image- based backups.
- **Appliance** The x360Recover appliance, which is deployed at a customer location, holds the backup data received from the agents.

NOTE With x360Recover Direct-to-Cloud, you do **not** need to deploy a local appliance.

- **Vault** The x360Recover vault receives incoming protected system data being replicated from a customer site. Vaults are designed to be multitenant. Vaults are typically deployed off-site.
- **Global Management Portal:** The Global Management Portal (GMP) allows for centralized management of your devices and provides a single-pane-of-glass view of each protected system.

Direct-to-Cloud backups

Axcient's x360Recover Direct-to-Cloud (D2C) provides MSPs with the same full-featured, image-based backups of traditional x360Recover, but without the expense of deploying or managing a local appliance. This user guide outlines installation steps to help you get started with the x360Recover Direct-to-Cloud agent.

Install the x360Recover Direct-to-Cloud agent

This guide outlines installation and configuration tasks, including:

- Creating clients,
- Installing the x360Recover Direct-to-Cloud agent,
- Creating schedules, and
- Recovery options.

Firewall considerations

Firewall ports

Direct-to-Cloud agents require several ports to be open for outbound internet connections between the protected system and the Cloud vault:

TCP 443 (Https/TLS)
TCP 9079 (Thrift/TLS - Endpoint Manager)
TCP 9082 (Thrift/TLS – Cloudserver)
TCP 9090 (Thrift/TLS – Backup Manager)

Note: On Axcient-hosted vaults with Scale-Out Cloud, the Cloudserver service is located directly on a storage node in our datacenter. Storage nodes are assigned dynamically, at the time of protected system registration.

If you must secure outbound traffic explicitly for protected systems, you can locate the assigned storage node URL in `aristos.log` for each protected endpoint.

Important: Storage node locations within our datacenter are subject to change without notification.

Create Direct-to-Cloud clients in the x360Recover vault

When you are ready, you can create a customer account within the x360Recover Vault.

Note: Create only one client account for each customer that you support.

Create a client

Please consider the following when creating clients:

- Each client account must be configured with a unique username. You cannot create two customer accounts with the same username within the x360Recover Vault.

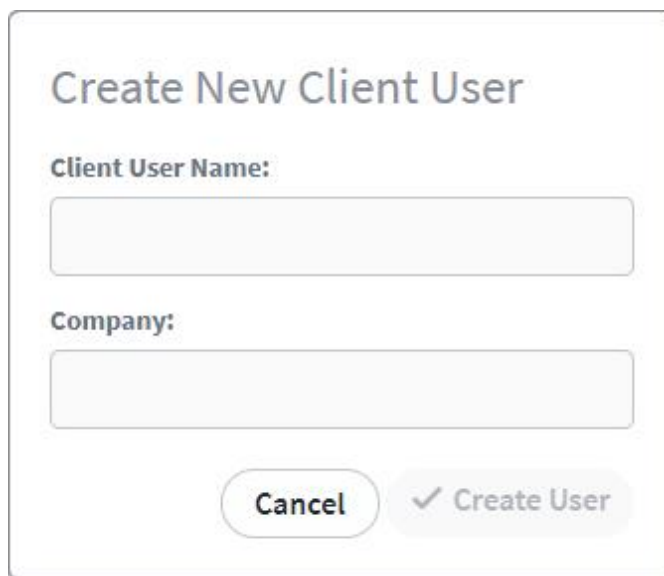
To create a new client:

1. From the x360Recover Vault left pane menu, click to expand *Clients*.

The screenshot displays the Axcient x360Recover Vault interface. On the left is a sidebar menu with options: Protected Systems, Backup Policies, Clients (highlighted), Jobs, Alerts, File Browser, Network Sharing, iSCSI, System Info, ConnectWise Settings, System Settings, and Downloads. The main area is titled 'Clients' and shows a list of client accounts. At the top right of the main area is a user profile 'admin'. Below the title bar are tabs for 'Clients' and 'Licenses', and an 'Add Client' button. A toolbar contains icons for Copy, CSV, Excel, PDF, and Print. The table lists clients with columns: CLIENT NAME, ROLE, DISK USAGE, and DOWNLOAD. The data rows are: khoffman (customer, 0.00B, Windows Agent), CSVTest (customer, 0.00B, Windows Agent), JCrystalMobile (customer, 0.00B, Windows Agent), YatesInc (customer, 0.00B, Windows Agent), and VICargo (customer, 0.00B, Windows Agent). At the bottom, it shows 'Showing 1 to 5 of 17 entries'.

CLIENT NAME	ROLE	DISK USAGE	DOWNLOAD
khoffman	customer	0.00B	Windows Agent
CSVTest	customer	0.00B	Windows Agent
JCrystalMobile	customer	0.00B	Windows Agent
YatesInc	customer	0.00B	Windows Agent
VICargo	customer	0.00B	Windows Agent

2. Click the **Add Client** button. The *Create New Client User* window displays.
3. In the *Create New Client User* window, populate the following fields:
 - a. In the *Client User Name* field, enter the **username** for the new customer. This field only accepts letters, numbers, and underscore characters. You cannot add spaces or other special characters.
 - b. In the *Company* field, enter the **name of the company**.
 - c. Click **Create User** at the bottom of the window to complete client user creation.



The image shows a 'Create New Client User' dialog box. It has a title bar at the top. Below the title, there are two text input fields. The first field is labeled 'Client User Name:' and the second is labeled 'Company:'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Create User'. The 'Create User' button has a checkmark icon next to the text.

Create New Client User

Client User Name:

Company:

Cancel ✓ Create User

Download and install the Direct-to-Cloud agent

After you log in to the x360Recover Vault and have created your Clients, you can download and install the Direct-to-Cloud agent software on protected systems.

Role of the Agent

The agent is software installed on a protected system. The agent performs the backup and sends the backup data to the vault. Consider the following important notes about the agent:

- The agent software must be installed on each system that needs to be protected.
- The Direct-to-Cloud agent cannot currently be installed over an existing agent. If an agent has been previously installed, it must be uninstalled. You must also delete the existing agent folder (typically located at *C:\Program Files (x86)\Replibit*). Failure to remove the previous agent files will prevent the Direct-to-Cloud agent from registering with the vault.
- Backups of protected systems are image-based.
- Supported platforms include most Windows workstation and server editions.
- You can install and uninstall agent software without the need to reboot the target device, reducing the impact to the customer environment.

Prerequisites

As an administrator, you will install the agent onto each protected device that you support. We recommend leaving third party backup solutions installed while the initial full backup is being completed and adjust scheduling so that the existing backups run during business hours and the x360 agent runs outside of business hours until completed, to avoid any gap in backup coverage.

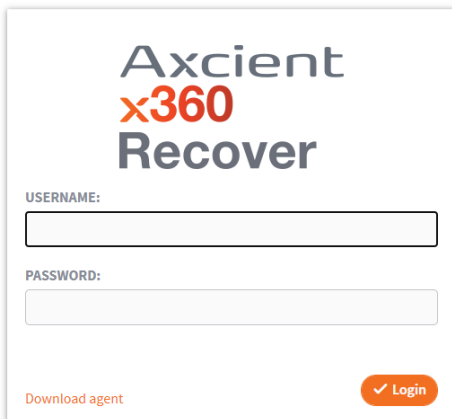
Install the Direct-to-Cloud Agent

You can download the agent from the *Clients* tab of the vault.

The installation file is valid for 14 days from the time of download. Installing from an expired agent installer file will fail and register invalid token errors within the log file.

Axcient x360Recover Direct-to-Cloud (D2C) Installation Guide

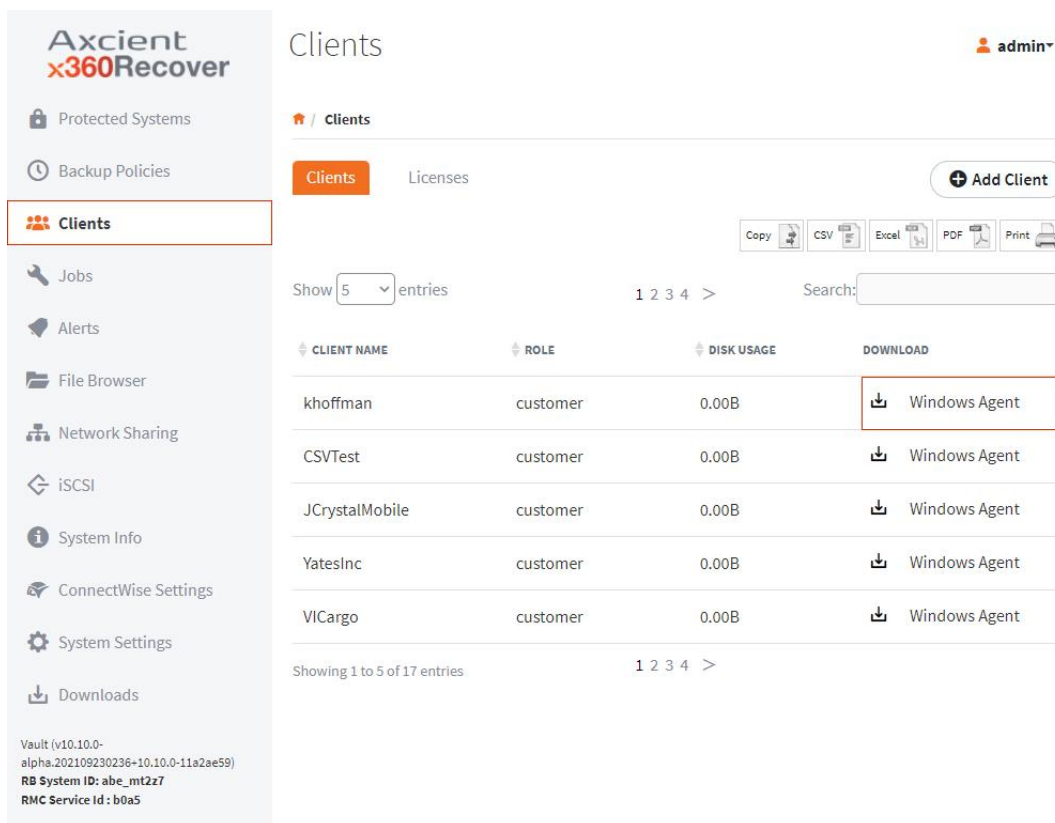
1. Open a Web browser, navigate to the Vault Web interface, and log in.



The login screen for Axcient x360Recover. It features the Axcient x360Recover logo at the top. Below the logo are two input fields: 'USERNAME:' and 'PASSWORD:'. At the bottom left is a link 'Download agent' and at the bottom right is a 'Login' button with a checkmark icon.

NOTE: Each Axcient Cloud vault has a unique URL that is provided during onboarding. If you do not have this URL, please contact Axcient Support.

2. In the vault web interface, click on the appropriate client's *Download Agent* link on the right hand side of the client table.



The screenshot shows the Axcient x360Recover web interface. On the left is a sidebar menu with options: Protected Systems, Backup Policies, Clients (highlighted), Jobs, Alerts, File Browser, Network Sharing, iSCSI, System Info, ConnectWise Settings, System Settings, and Downloads. The main area is titled 'Clients' and shows a table of clients. The table has columns: CLIENT NAME, ROLE, DISK USAGE, and DOWNLOAD. The first client, 'khoffman', has a 'Download Agent' link highlighted in a red box. Other clients listed are CSVTest, JCrystalMobile, YatesInc, and VICargo, all with 'Windows Agent' download links. At the bottom left of the main area, there is a 'Showing 1 to 5 of 17 entries' indicator and a pagination control showing '1 2 3 4 >'.

CLIENT NAME	ROLE	DISK USAGE	DOWNLOAD
khoffman	customer	0.00B	Download Agent
CSVTest	customer	0.00B	Download Agent
JCrystalMobile	customer	0.00B	Download Agent
YatesInc	customer	0.00B	Download Agent
VICargo	customer	0.00B	Download Agent

If your customers are not displaying in the Users tab, we recommend syncing the vault with the Licensing Portal. Do this by going to the Systems Settings left hand menu tab and navigating to the License Details section.

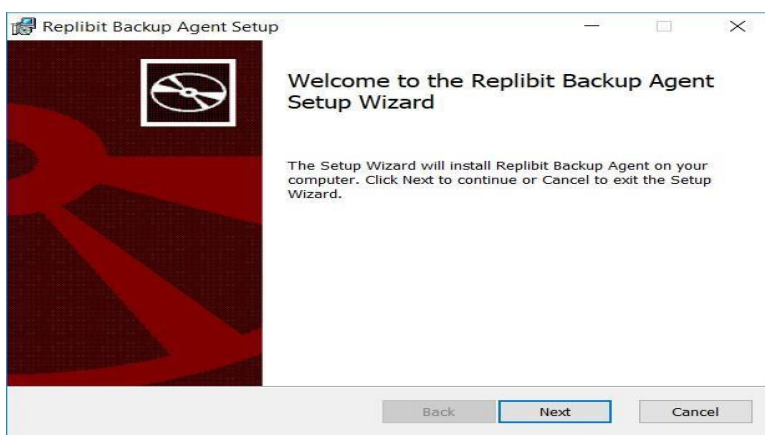
3. Locate the appropriate client and click the **Windows Agent** link.

Important note: Do not rename this file. The installation file downloaded from this page contains temporary token and identifying information embedded in the filename.

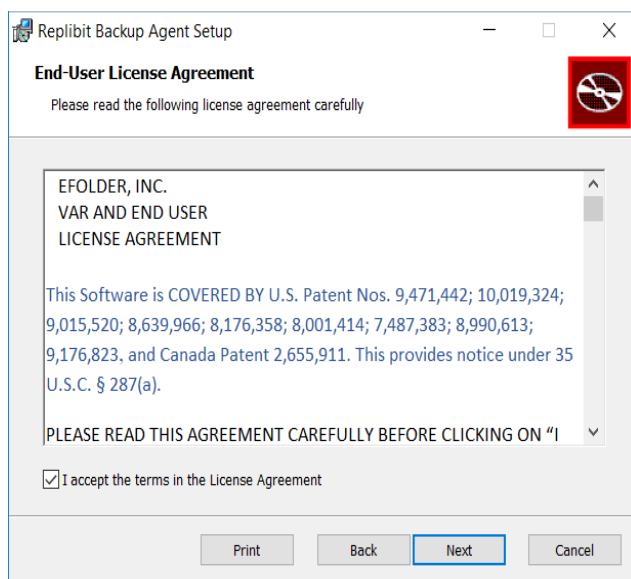
Note: The installation file is valid for 14 days from the time of download. Installing from an expired agent installer file will fail and register invalid token errors within the log file.

4. Click the **installation file** to initiate the installation process.

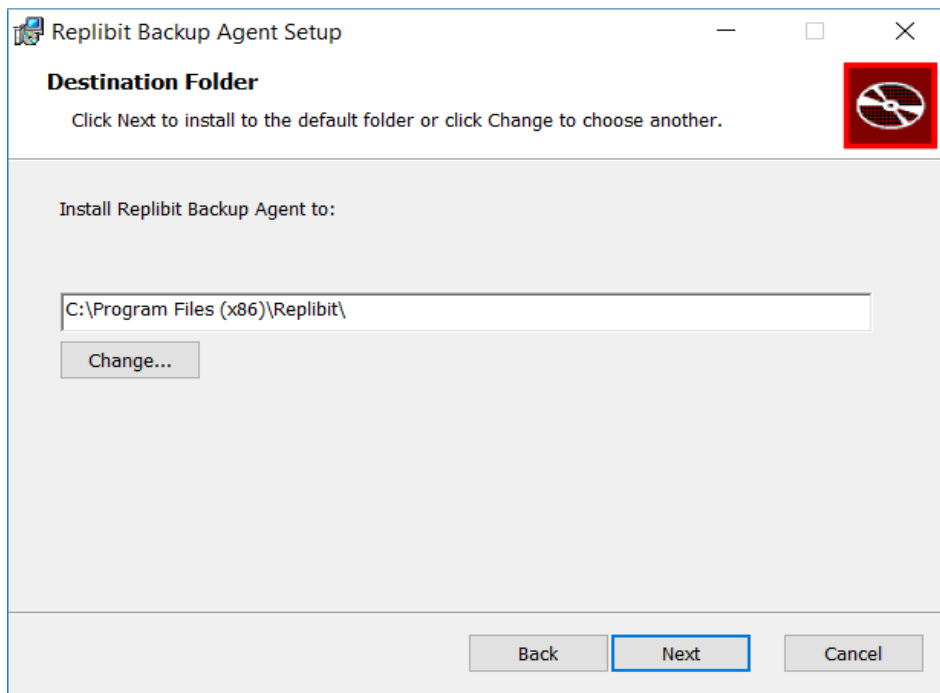
When the Setup Wizard opens, click **Next** to continue.



5. After reading the agreement, select **I accept the agreement**. Click the **Next** button to continue.



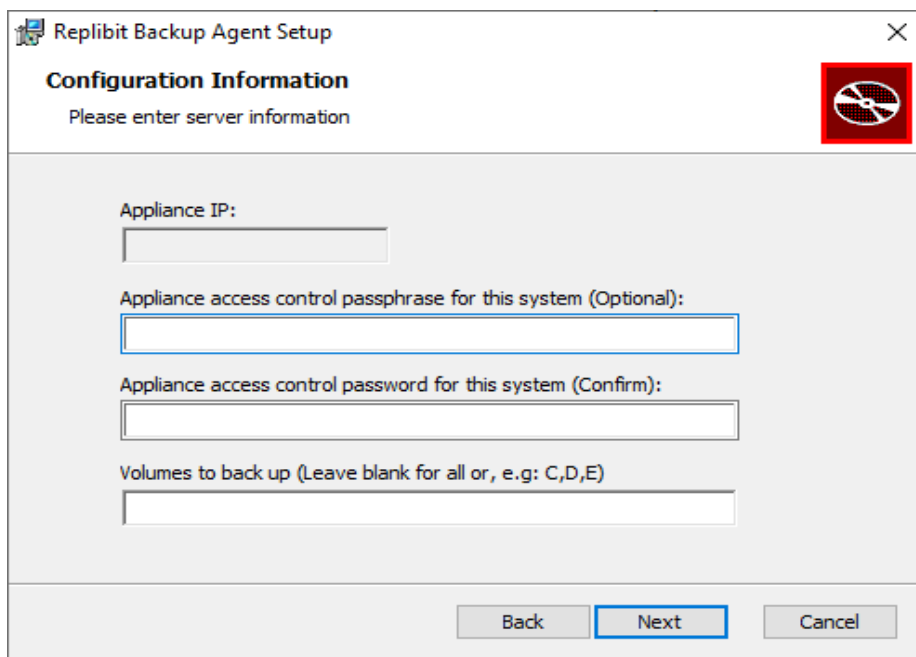
6. Accept the default installation folder. Click the **Next** button to continue.



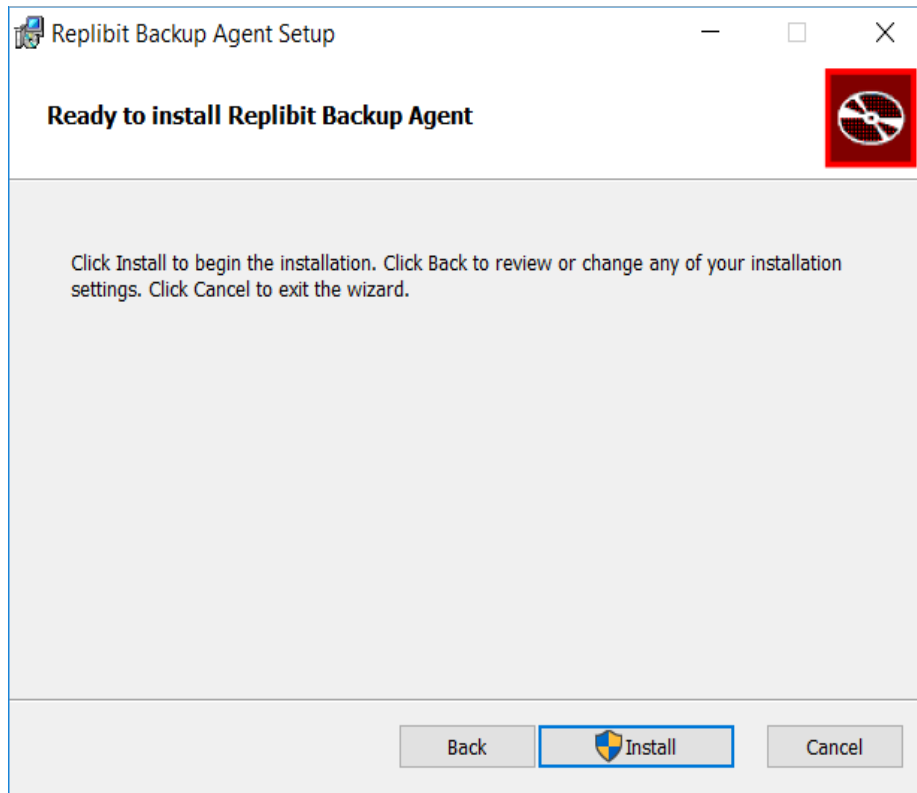
7. When prompted, enter the **Volumes to back up**. Click the **Next** button to continue.

Note: You do not need to enter an IP address.

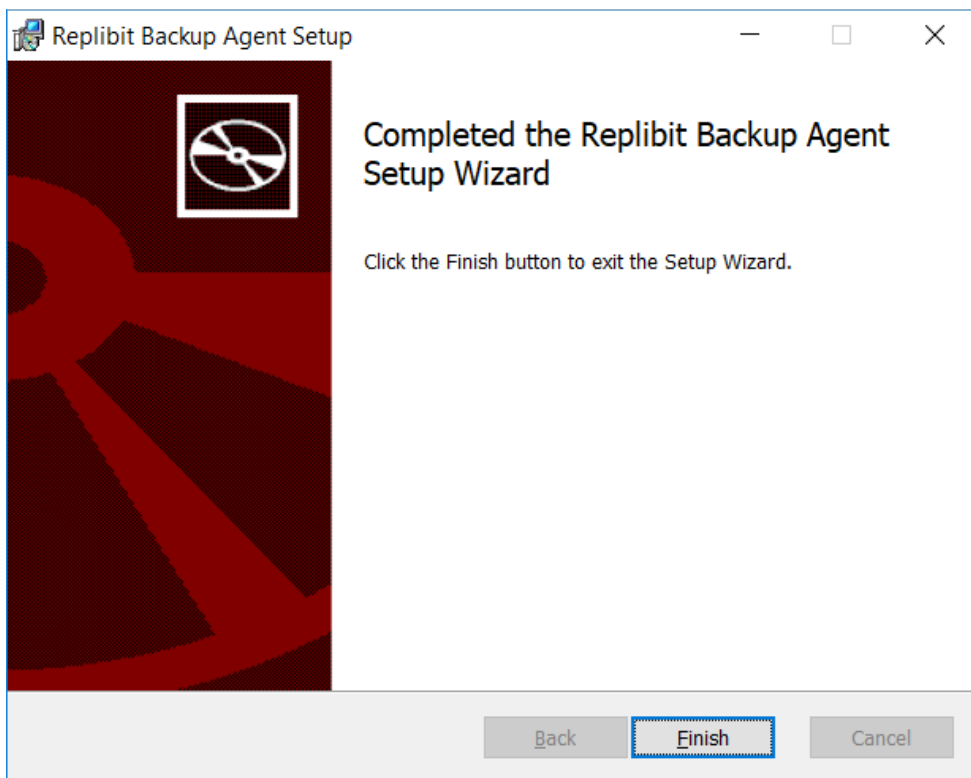
You can optionally enter an access control password. If you enter a password, the vault will prompt you for this password before you begin a system recovery. We recommend setting a unique password to enhance security.



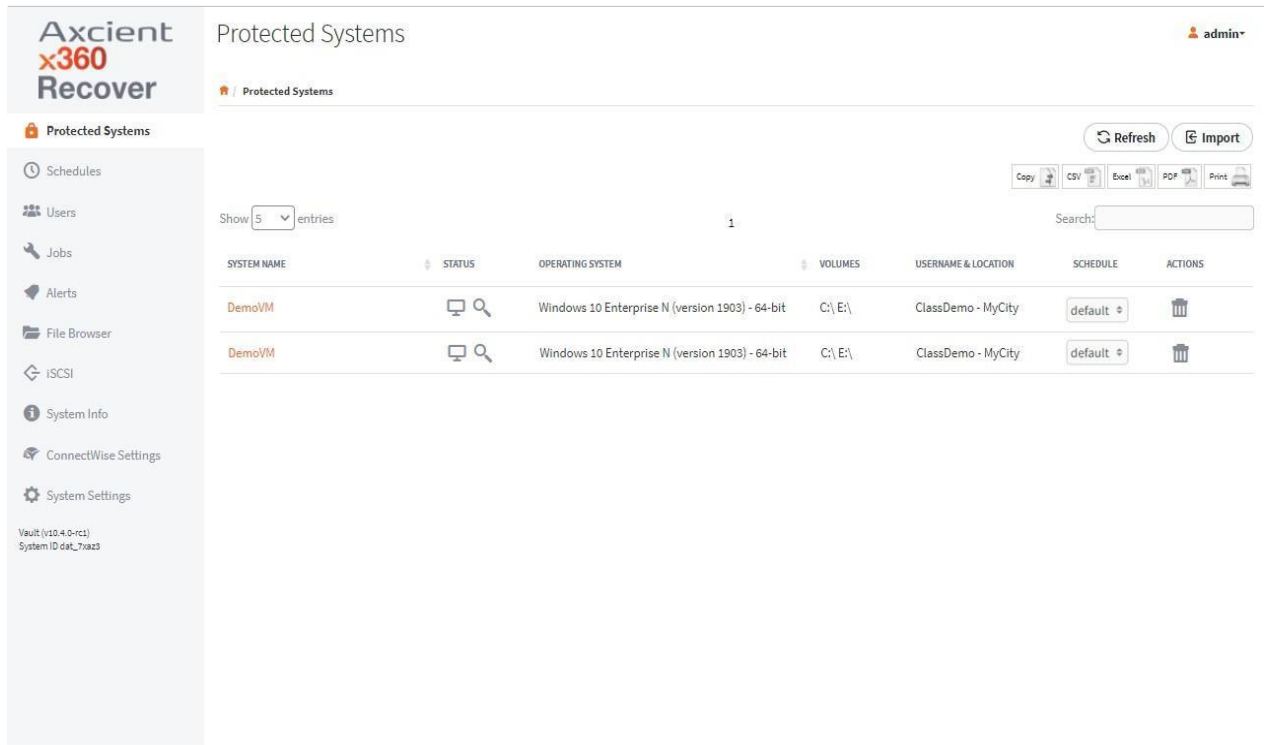
8. When you are ready, click the **Install** button to begin installation.



9. When installation completes, click **Finish** to exit.



10. After several minutes, the Vault Web interface will display the newly protected system in the *Protected Systems* tab. A full backup will automatically initiate based on your schedule settings.



Silent and RMM deployment of the agent

The Direct-to-Cloud agent can be silently deployed through RMM or other tools as follows:

```
msiexec /i <agent file> /quiet
```

Optional parameters include:

- BACKUP_VOLUMES=<Drv>,<drv>...
- PASSWORD=<encryption passphrase>

For example:

```
msiexec /i <agent file> /quiet
```

```
BACKUP_VOLUMES=C,D,E PASSWORD=password123
```

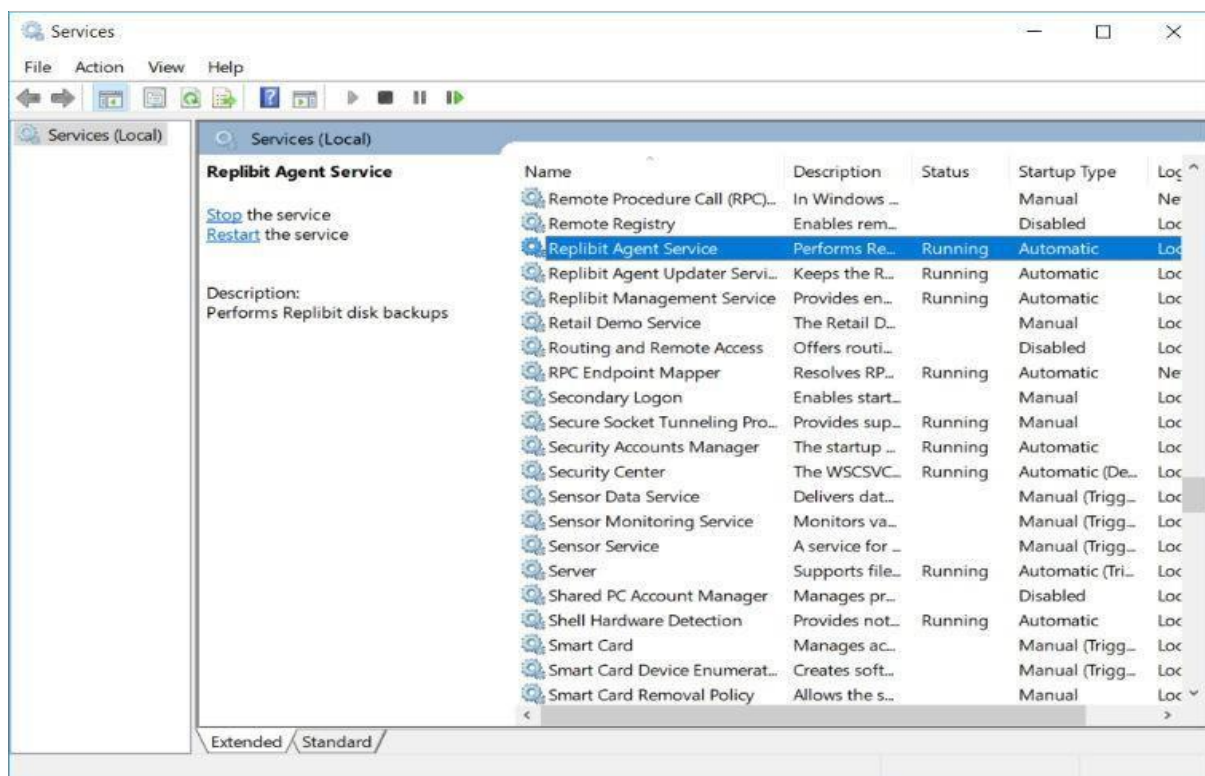
Update Direct-to-Cloud agent settings

In certain circumstances, you might need to update x360Recover agent settings after the installation process. For example, you can update the following details in the *aristos.cfg* file:

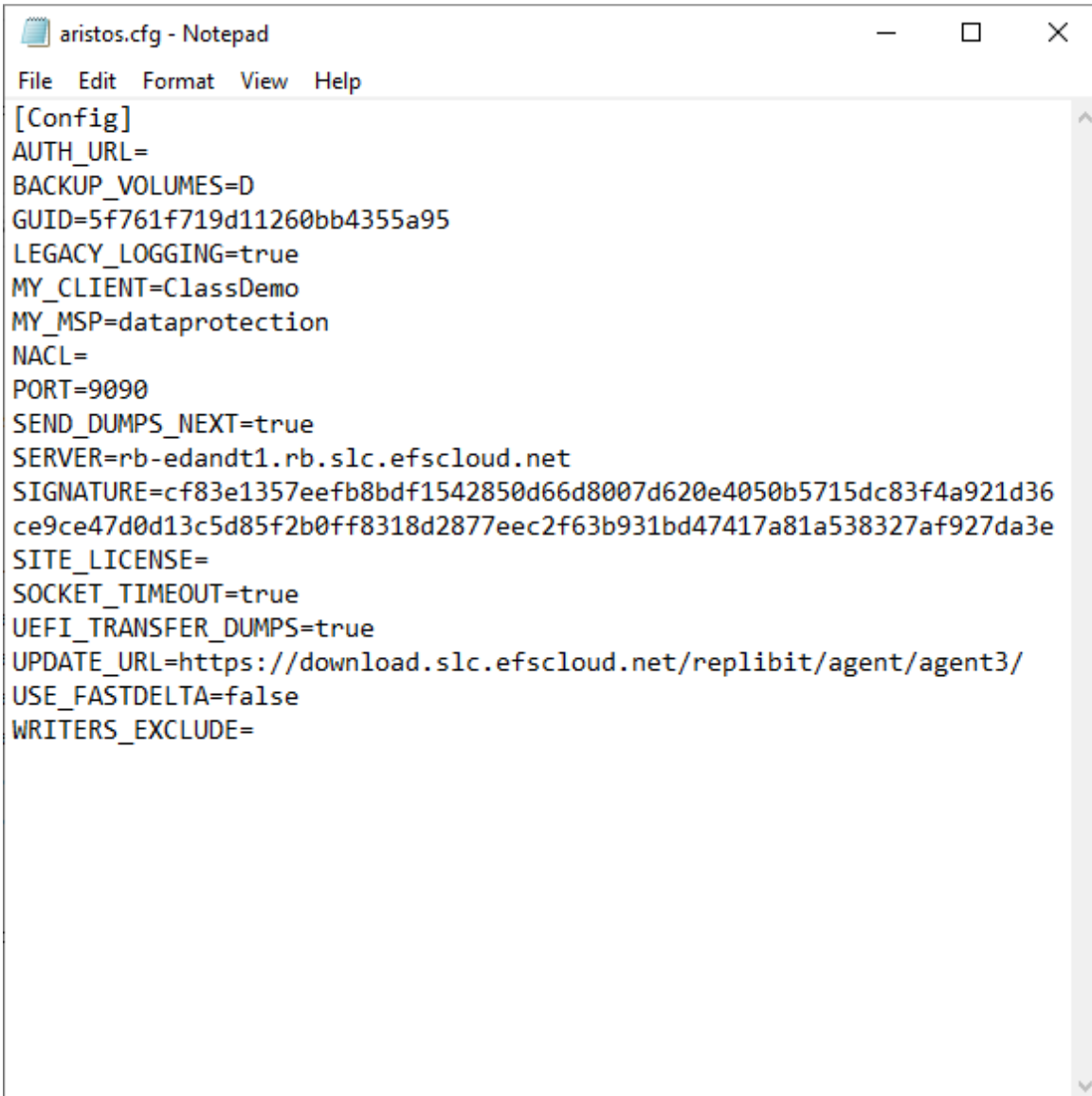
- A list of Backup Volumes.
- The IP address of the Vault.

To update x360Recover agent settings:

1. From the Services app on the target machine, *stop* and *disable* the agent service.



2. Navigate to the agent installation folder (typically *C:\Program Files (x86)*).
3. Open the *aristos.cfg* file with administrative privileges.



The screenshot shows a Notepad window titled "aristos.cfg - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text content of the file is as follows:

```
[Config]
AUTH_URL=
BACKUP_VOLUMES=D
GUID=5f761f719d11260bb4355a95
LEGACY_LOGGING=true
MY_CLIENT=ClassDemo
MY_MSP=dataprotection
NACL=
PORT=9090
SEND_DUMPS_NEXT=true
SERVER=rb-edandt1.rb.slc.efsccloud.net
SIGNATURE=cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36
ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
SITE_LICENSE=
SOCKET_TIMEOUT=true
UEFI_TRANSFER_DUMPS=true
UPDATE_URL=https://download.slc.efsccloud.net/replibit/agent/agent3/
USE_FASTDELTA=false
WRITERS_EXCLUDE=
```

4. Update settings in the *aristos.cfg* file. For example:
 - a. Edit the *Backup_Volumes* line to update the **list of volumes** to backup.
 - b. When you are finished, save the file and restart the agent service.

Log in via Single Sign On (SSO)

1. In the vault web interface, click the **Vaults** tab.

Axcient x360Recover

Welcome! Here's what's happening:

Organization At A Glance

- 21 Clients (Last device added a week ago)
- 5 Services (No new services)
- 38 Devices
- 3 Vaults

1 Activity of Interest Across All Clients

- Cloud Virtualizations: 2 clients are running 2 test virtualizations. [More](#)

2. Click on a vault.

Axcient x360Recover

Vaults

Filter Vaults

Vault Search

Health

- ☐ Troubled
- ☐ Warned
- ☐ Healthy

Vault Type

- ☐ Private
- ☐ Axcient

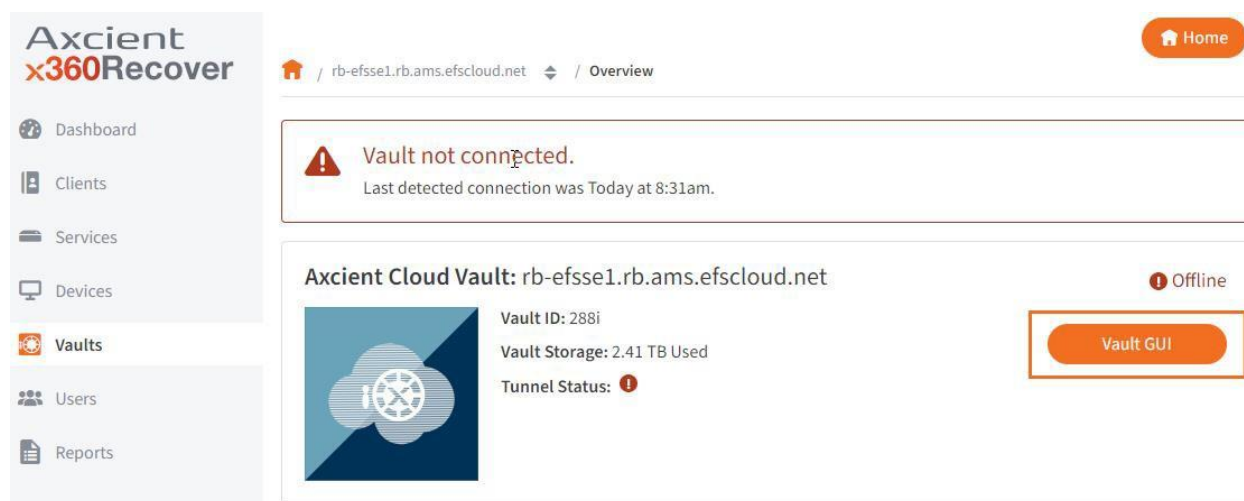
[Clear All Filters](#)

Filters

All 3 Vaults

Vault ID	Vault Type	Protected Servers	Protected Workstations	Clients
10.201.201.99	Private	2 total	0 total	1 total
rb-axcse1.rb.slc.efsccloud.net	Axcient	12 total	14 total	7 total
rb-efsse1.rb.ams.efsccloud.net	Axcient	4 total	11 total	3 total

3. Click the **Vault GUI** button.

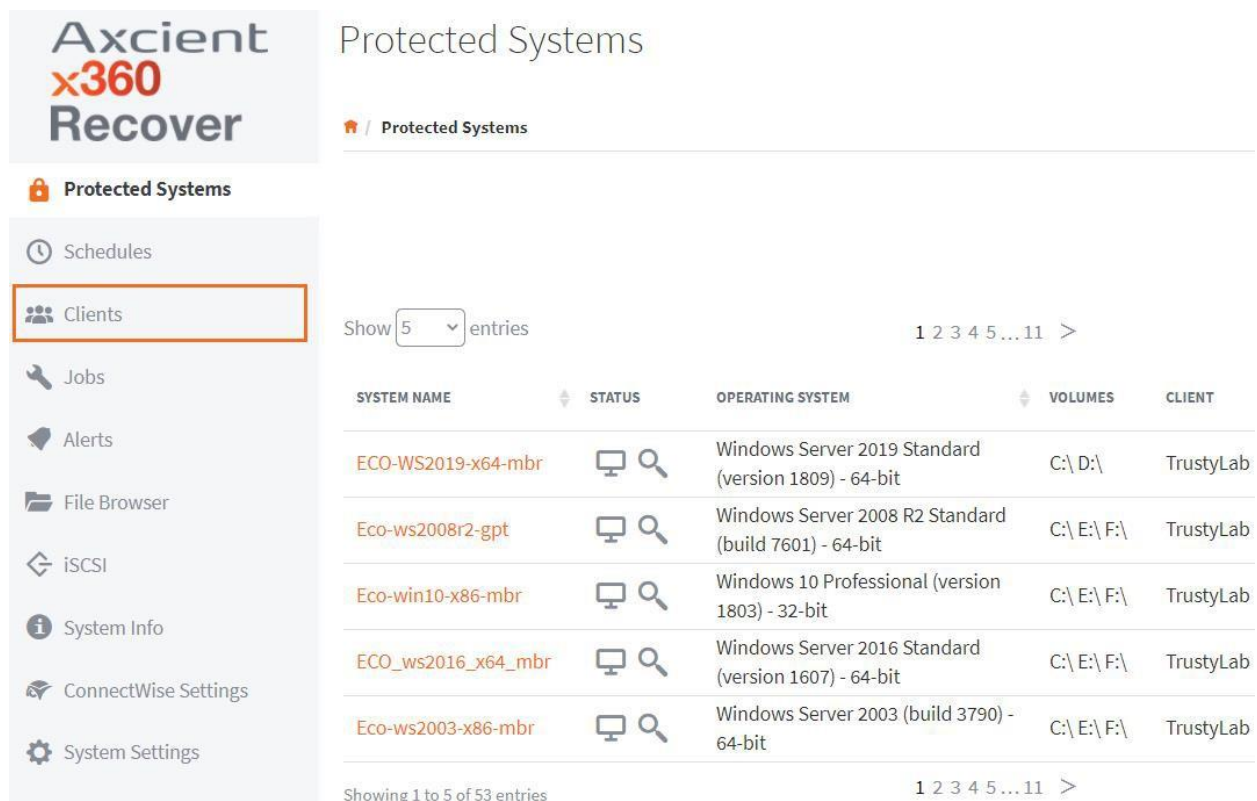


4. This will log you into the vault directly, without prompting you to enter a user name and password.

Add Direct-to-Cloud clients from the vault

To add a client:

1. In the Vault Web interface, click the **Clients** tab.



Axcient x360Recover

Protected Systems

Protected Systems

Schedules

Clients

Jobs

Alerts

File Browser

iSCSI

System Info

ConnectWise Settings

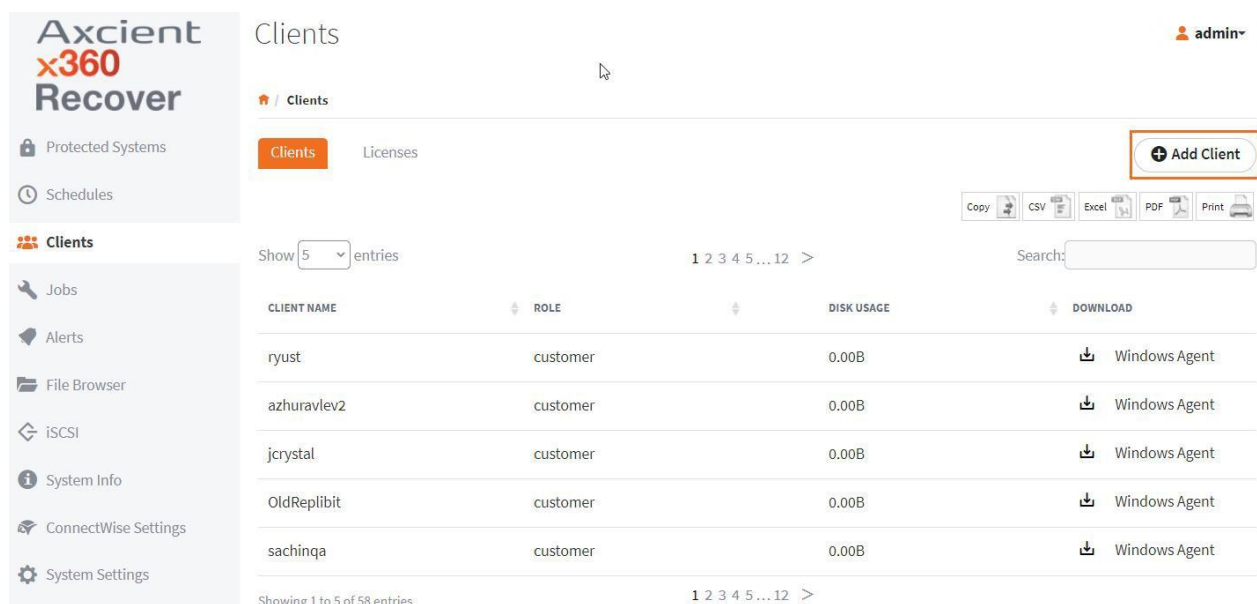
System Settings

Show 5 entries

SYSTEM NAME	STATUS	OPERATING SYSTEM	VOLUMES	CLIENT
ECO-WS2019-x64-mbr		Windows Server 2019 Standard (version 1809) - 64-bit	C:\ D:\	TrustyLab
Eco-ws2008r2-gpt		Windows Server 2008 R2 Standard (build 7601) - 64-bit	C:\ E:\ F:\	TrustyLab
Eco-win10-x86-mbr		Windows 10 Professional (version 1803) - 32-bit	C:\ E:\ F:\	TrustyLab
ECO_ws2016_x64_mbr		Windows Server 2016 Standard (version 1607) - 64-bit	C:\ E:\ F:\	TrustyLab
Eco-ws2003-x86-mbr		Windows Server 2003 (build 3790) - 64-bit	C:\ E:\ F:\	TrustyLab

Showing 1 to 5 of 53 entries

2. Click the **Add Client** button.



Axcient x360Recover

Clients

Clients

Licenses

Protected Systems

Schedules

Clients

Jobs

Alerts

File Browser

iSCSI

System Info

ConnectWise Settings

System Settings

Show 5 entries

CLIENT NAME	ROLE	DISK USAGE	DOWNLOAD
ryust	customer	0.00B	Windows Agent
azhuravlev2	customer	0.00B	Windows Agent
jcrystal	customer	0.00B	Windows Agent
OldReplbit	customer	0.00B	Windows Agent
sachinqa	customer	0.00B	Windows Agent

Showing 1 to 5 of 58 entries

admin

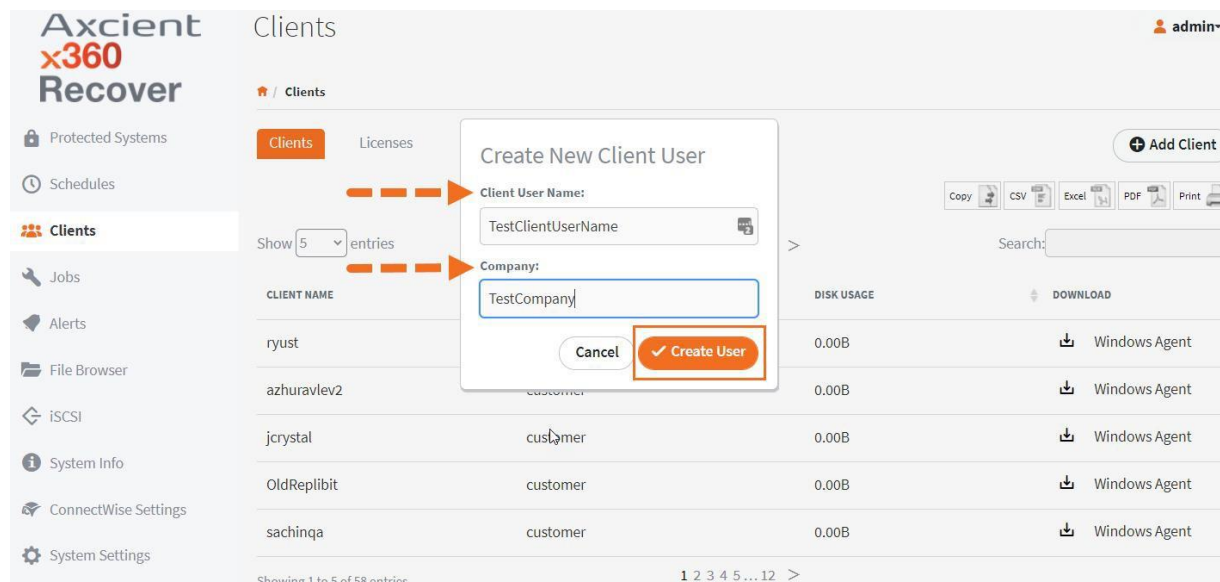
Add Client

Copy CSV Excel PDF Print

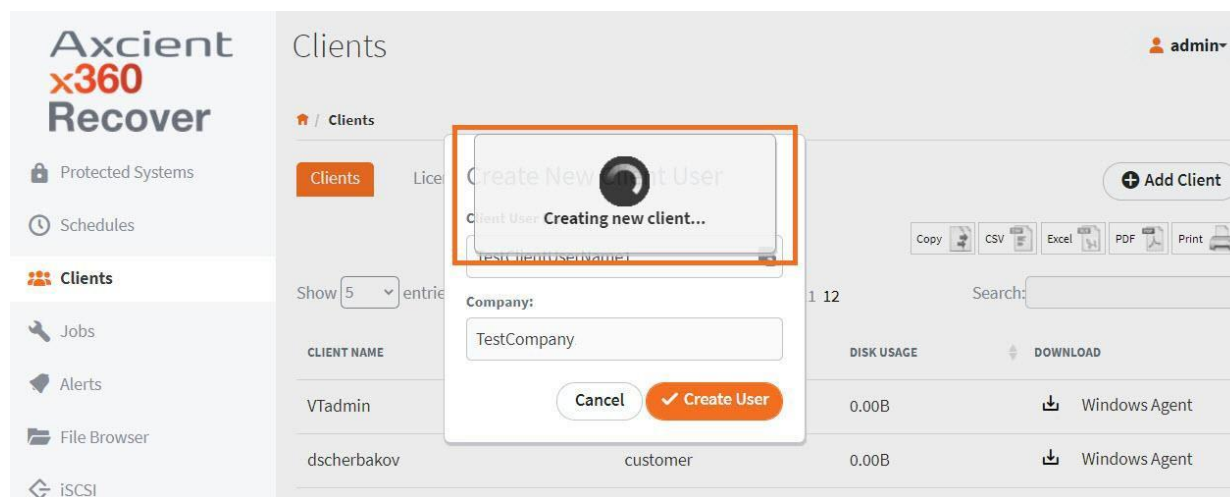
Search:

3. The Create New Client User popup will appear.

Fill in the **Client User Name** and **Company** field, and then click the **Create User** button to continue.



4. You will then see a processing popup. This displays as the new account is created.



5. The new client will appear in the list of clients. Click the download symbol to the left of *Windows Agent* to retrieve the installer for the new client.

Axcient
x360
Recover

Protected Systems

Schedules

Clients

Jobs

Alerts

File Browser

iSCSI

System Info

ConnectWise Settings

Clients

admin

Clients / Clients

ClientsLenses

CopyCSVExcelPDFPrint

Show 5 entries

< 1 ... 8 9 10 11 12

Search:

CLIENT NAME	ROLE	DISK USAGE	DOWNLOAD
ann_logvaneva	customer	0.00B	Windows Agent
DellQACustomer	customer	0.00B	Windows Agent
PXE	customer	0.00B	Windows Agent
TestClientUserName	customer	0.00B	Windows Agent

Create Direct-to-Cloud schedules

When the agent is installed on a protected system, you can create schedules and apply these schedules to protected systems. All schedules are created and maintained within the vault.

Schedules allow for full flexibility when defining your Recovery Point Objectives for each customer and protected system. x360Recover supports a Recovery Point Objective (RPO) of 15 minutes for systems that require industry-leading RPOs.

All schedules are created and maintained within the vault. You can create schedules for the Initial Backup and Incremental Backups.

Backup Types

When you create a schedule, you define two types of backups:

The initial backup (also called a full backup) copies all sectors of the image.

Incremental backups (also called snapshots) back up changes only, saving time and disk space. You cannot schedule an incremental backup unless you have completed the Initial backup (full backup). Because x360Recover is chain-free, snapshots are not dependent on previous snapshots.

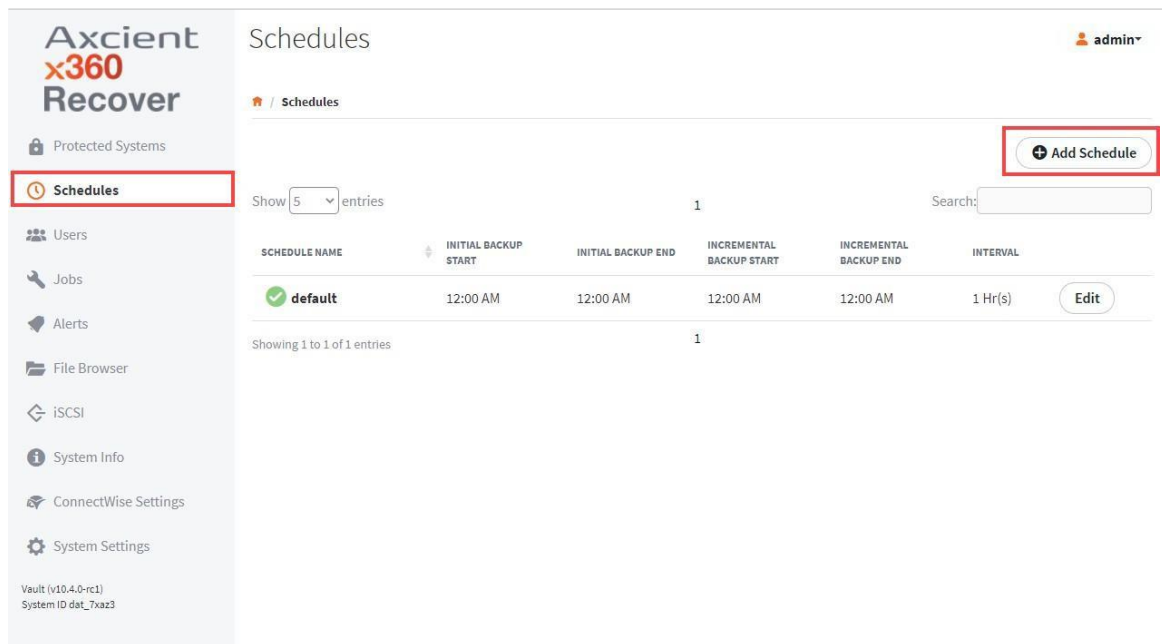
Creating schedules in the Vault Web Interface

Within the Vault Web interface, you can use the *Schedules* page to define initial back-up schedules and ongoing incremental snapshot schedules. You can create an unlimited number of schedules and assign them to different machines according to special requirements or technical limitations. You can also adjust the initial backup schedule to run during certain hours of the day and pause at other hours of the day to limit user impact during office hours.

After a schedule is created, you must assign the schedule to a protected system from the *protected systems* page.

To create a schedule:

1. Log in to the Vault Web interface.
2. In the left-hand navigation menu, click the **Schedules** tab.
3. In the *Schedules* page, click the **Add Schedule** button.

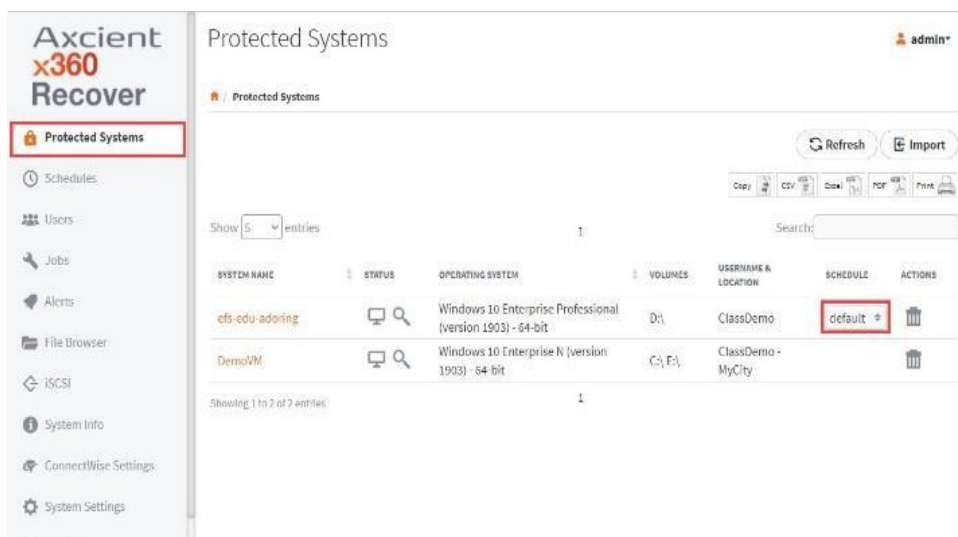


4. In the *Add Schedule* page, enter information about the new schedule:
 - a. In the *Name* field, enter a **descriptive name** for the schedule. For example, you might create a scheduled titled, *Critical*, for servers that require 15-minute incremental backups; and *Non-Critical* for servers that only require incremental backups every hour.
 - b. Ensure the *Enabled* checkbox is selected to activate this new schedule. If the schedule is not enabled but later assigned to a protected system, backups for the protected system will be disabled.
 - c. Optionally, click the **Default** checkbox to assign this schedule as the default schedule for all protected systems.
 - d. In the *Initial Backup* section, define a **Start Time** and **End Time** for the first, full initial backup. This timeframe allows you to limit the impact of the initial backup on the user experience.
 - e. In the *Incremental Backup* section, you can optionally use the drop-down menu to change the Incremental Backup type from *Internal* to *Manual*. The *Manual* setting allows you to create snapshots at specific times instead of intervals.
 - f. If you selected **Interval** in the drop-down menu, define a **Start Time**, **End Time**, and **Interval** for all future incremental backups.

- g. Click the **Save** button when you are finished. The schedule is now created and will be listed in the *Schedules* page. You can manage and edit schedules in the *Schedules* page.

The screenshot shows the 'Create Schedule' form. It includes fields for Name, Enabled checkbox, Default checkbox, Initial Backup (Start Time: 12 AM, End Time: 12 AM), Incremental Backup (Interval: 1 Hr(s), Start Time: 12 AM, End Time: 12 AM), and buttons for Cancel and Save.

5. After the schedule is created, you can assign the schedule to a protected system.
 - a. In the left-hand navigation menu, click the **Protected Systems** tab.
 - b. Find the protected system and use the *Schedule* drop-down menu to select the appropriate **Schedule**. The schedule is now assigned to the protected system.



Coming Soon: The Global Management Portal for Direct-to-Cloud customers

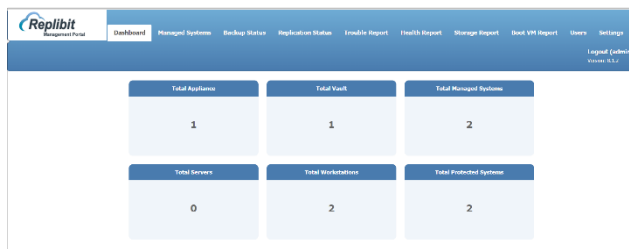
Direct-to-Cloud support within the Global Management Portal is scheduled to be part of a future release. You can also access the RMC to manage Direct-to-Cloud Customers.

The x360Recover Global Management Portal (GMP) is a multitenant, centralized portal that delivers secure, remote access to your Vaults and protected systems. With its single pane of glass architecture, the GMP streamlines administrative tasks, significantly reducing the totaltime required to manage your devices and reports.

Role of the Global Management Portal

The GMP is the central management point, providing a single-pane-of-glass view of each of your Vaults, as well as the protected systems they protect. With the GMP, you can perform thefollowing:

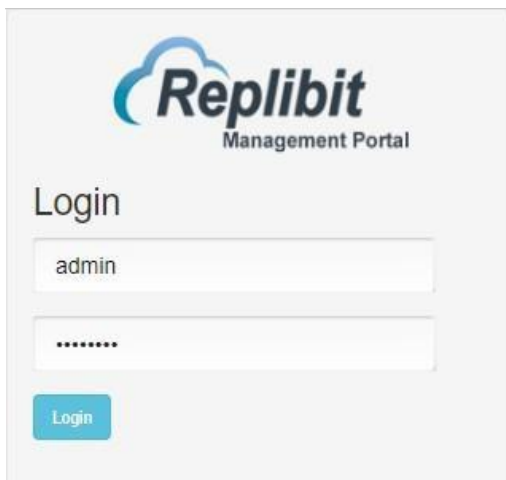
- Remotely access all connected vaults.
- View dashboard and reporting details.
- Review health checks.
- Review trouble checks.
- View historical storage utilization.



Accessing the Global Management Portal

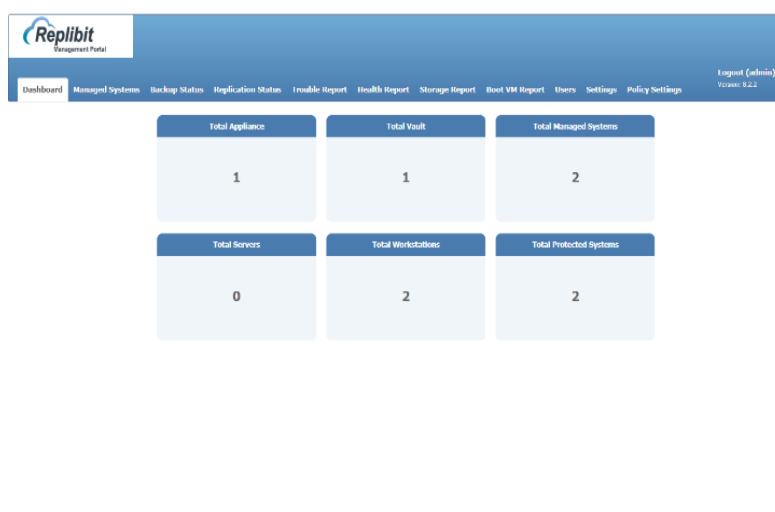
When you replicate to the Axcient Cloud, you will be given a GMP virtual machine in the cloud free of charge. You will receive login credentials when you onboard as a new Partner.

1. Navigate to the URL provided to you. If you are a Private Cloud partner, navigate to the URL configured when you installed the GMP.
2. When prompted, type your **Username** and your **Password** and then click the **Login** button. If Multi-Factor Authentication (MFA) has been enabled for your environment, you will also be prompted to enter an **MFA Token**.



The image shows the login interface of the Replibit Management Portal. At the top is the Replibit logo with the text 'Management Portal' below it. Underneath is the heading 'Login'. There are two input fields: the first contains the text 'admin' and the second contains a series of dots representing a password. Below the password field is a blue button labeled 'Login'.

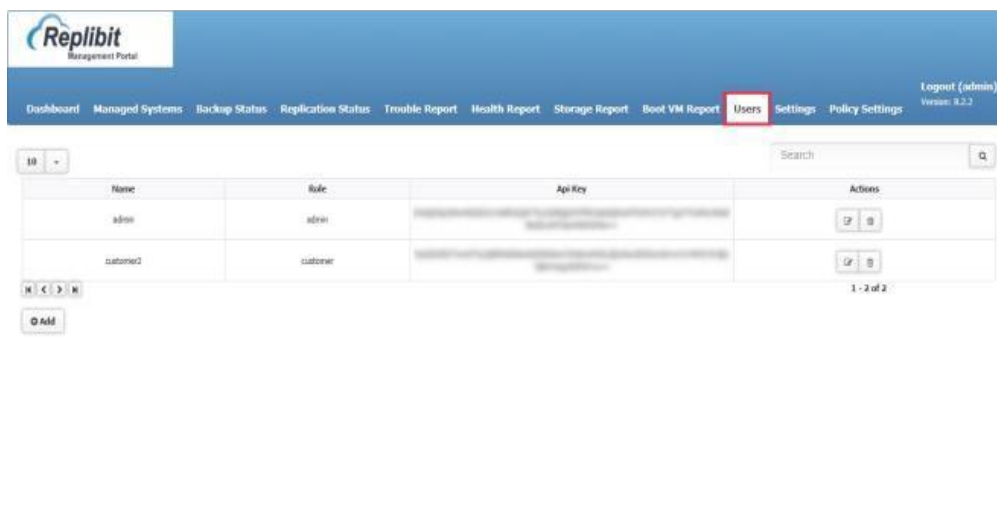
3. In the GMP Web interface, you can now browse and manage settings.



Connecting vaults for D2C customers with the Portal

In the GMP, the *Users* page allows you to create an API key so that you can integrate each vault with the GMP. When you create a user in the *Users* page, the GMP automatically generates an API key that you can use for integration purposes.

1. In the GMP, click the **Users** tab. The *Users* page displays, showing a list of all previously generated API keys.



You can optionally share Customer-specific user credentials to allow the Customer to log in and view their Managed Devices. Most partners, however, choose not to share these credentials. If you are interested in sharing user credentials with a customer, please contact Axcient Support for advice and best practices.

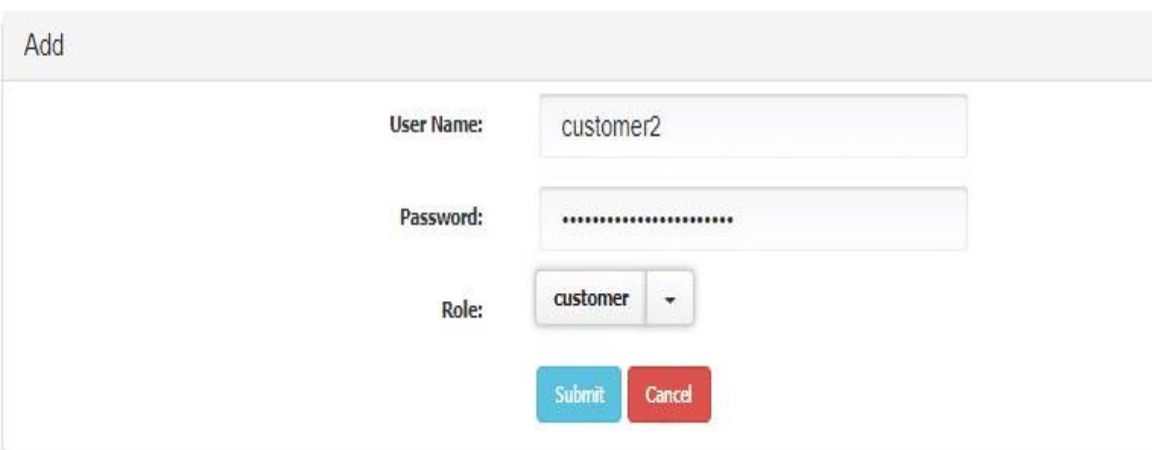
Option 1: In most cases, simply record the **admin API key** that is automatically generated for the GMP admin user during the provisioning process.



You can optionally use this admin API key to integrate each vault that you support.

Option 2: Alternatively, for management purposes, you can generate a new API key for each customer that you support. This approach is especially useful if you plan to give your customer login access to the GMP. Please contact Axcient Support for more information regarding this process. To create an API key:

- a. Click the **Add** button. The *Add* page displays, prompting you to create a new username and password for the user.
- b. In the *Username* field, enter a unique **username** for the customer.
- c. In the *Password* field, enter a **complex password** for the customer.
- d. In the *Role* field, select **customer** to indicate this is a customer user.
- e. Click the **Submit** button when you are finished. The system will automatically generate a new API key for this customer. Record this API key.



The screenshot shows a web form titled "Add" in a light gray header. The form contains three input fields: "User Name:" with the text "customer2", "Password:" with masked characters ".....", and "Role:" with a dropdown menu showing "customer". Below these fields are two buttons: a blue "Submit" button and a red "Cancel" button.

Recover Direct-to-Cloud protected systems with x360Recover

As an MSP, you have a lot riding on service level agreements (SLAs) for the clients you support. x360Recover helps you meet these SLAs, with multiple recovery options, helping you restore client data and applications faster than traditional file-based back-up and restore tools.

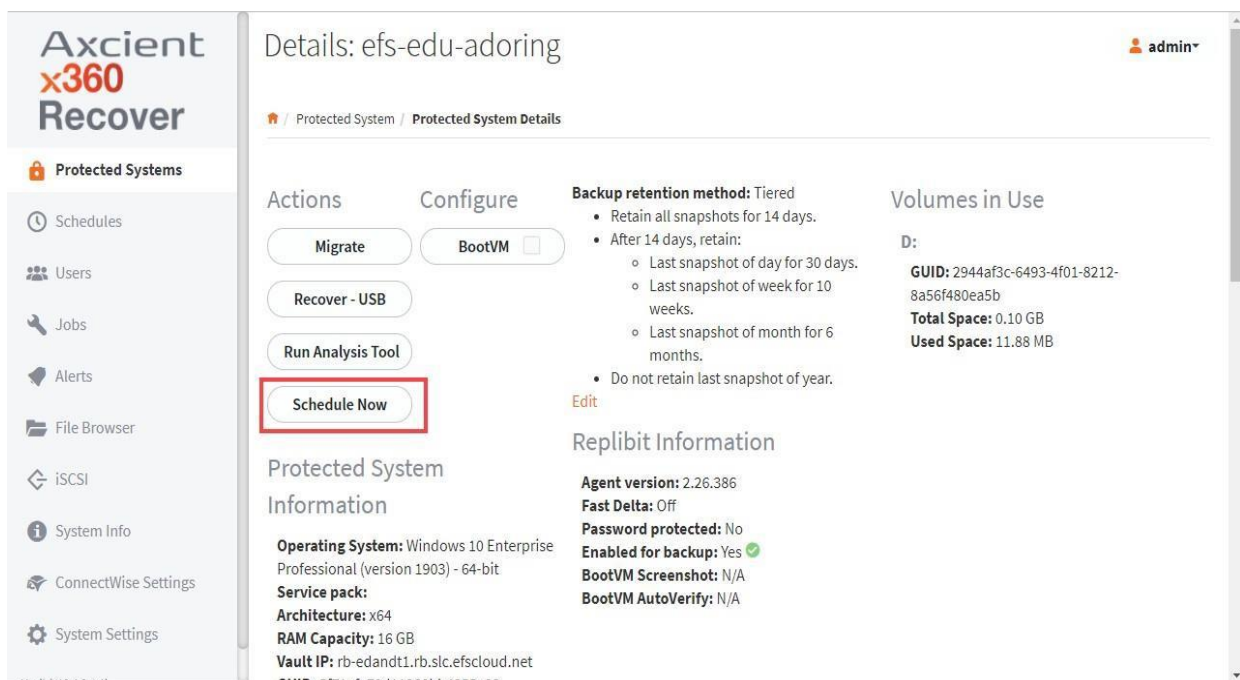
x360Recover gives you multiple options to restore lost or corrupted files, temporarily run critical workstations or servers, or permanently recover from a site-wide disaster.

To access recovery options:

1. Log in to the vault.
2. Click the **Protected Systems** menu item.
3. To access recovery options, click the **protected system name**.

In the ProtectedSystem Details page, you can:

- a. Click the **Schedule** button schedule a full or incremental backup.



- b. Click the **Run Analysis Tool** button to collect event-related information and submit to Axcient Support.

Axcient x360Recover Direct-to-Cloud (D2C) Installation Guide

The screenshot shows the 'Protected System Details' page for a system named 'efs-edu-adoring'. The left sidebar contains navigation links: Protected Systems, Schedules, Users, Jobs, Alerts, File Browser, iSCSI, System Info, ConnectWise Settings, and System Settings. The main content area is divided into several sections:

- Actions:** Includes buttons for 'Migrate', 'BootVM', 'Recover - USB', 'Run Analysis Tool' (highlighted with a red box), and 'Schedule Now'.
- Configure:** Includes a 'BootVM' checkbox.
- Backup retention method:** Tiered. Retain all snapshots for 14 days. After 14 days, retain:
 - Last snapshot of day for 30 days.
 - Last snapshot of week for 10 weeks.
 - Last snapshot of month for 6 months.
 - Do not retain last snapshot of year.
- Volumes in Use:** Shows details for volume 'D:' including GUID, Total Space (0.10 GB), and Used Space (11.88 MB).
- Replibit Information:** Includes Agent version (2.26.386), Fast Delta (Off), Password protected (No), Enabled for backup (Yes), BootVM Screenshot (N/A), and BootVM AutoVerify (N/A).
- Protected System Information:** Includes Operating System (Windows 10 Enterprise Professional), Service pack, Architecture (x64), RAM Capacity (16 GB), Vault IP, and GUID.

- Find a snapshot and click the **Mount** button to browse and recover files from the snapshot.
- Click the **Export** button to create a virtual disk export for download and for failback from the cloud.
- Click the **iSCSI** button to virtualize a protected system in the Axcient Continuity Cloud for cloud failover.

The screenshot shows the 'Snapshots' page for the same system 'efs-edu-adoring'. It displays a table of snapshots with columns for Snapshot Name, Delta, Used, and Actions. The table shows 5 snapshots, with the first 4 having a 'Mount' button and the last one having a 'Dismount' button. The 'Actions' column includes buttons for 'Start VM', 'Mount', 'Export', and 'iSCSI Start'. The page also includes a search bar and a legend for the Delta and Used columns.

SNAPSHOT NAME	DELTA (*)	USED (**)	ACTIONS
Mon 09-28-20 11:00 AM	232.50K	720.75K	Start VM Mount Export iSCSI Start
Mon 09-28-20 10:00 AM	232.50K	232.50K	Start VM Mount Export iSCSI Start
Mon 09-28-20 09:00 AM	249.94K	232.50K	Start VM Mount Export iSCSI Start
Mon 09-28-20 08:18 AM	232.50K	232.50K	Start VM Mount Export iSCSI Start
Mon 09-28-20 08:15 AM	720.75K	232.50K	Start VM Dismount Export iSCSI Start

Showing 1 to 5 of 5 entries

(*) Represents how much data changed vs the prior snapshot (indicates how much additional storage is needed to maintain this snapshot).
(**) For the latest snapshot, this represents the total data used. For all other snapshots, this represents the amount of data that would be freed if the snapshot was deleted (because multiple snapshots can share data, this is often smaller than the delta size).

Troubleshoot Direct-to-Cloud agent errors

If you are experiencing registration issues, please check the following:

- Network connectivity—The agent must be able to communicate with the vault. If networking errors or other issues interfere with this communication process, the agent will not successfully register with the vault.
- Previous Installations—The Direct-to-Cloud agent cannot currently be installed over an existing agent. If an agent has been previously installed, it must be uninstalled. You must also delete the existing agent folder (typically located at *C:\Program Files (x86)\Replibit*). Failure to remove the previous agent files will prevent the Direct-to-Cloud agent from registering with the vault.
- Firewall considerations—The agent needs to communicate outbound on the internet to the vault on the following ports: 443, 9079, 9082, and 9090.

Firewall considerations

Firewall Ports

Direct-to-Cloud agents require several ports to be open for outbound internet connections between the protected system and the Cloud vault:

TCP 443 (Https/TLS)
TCP 9079 (Thrift/TLS - Endpoint Manager)
TCP 9082 (Thrift/TLS – Cloudserver)
TCP 9090 (Thrift/TLS – Backup Manager)

Note: On Axcient-hosted vaults with Scale-Out Cloud, the Cloudserver service is located directly on a storage node in our datacenter. Storage nodes are assigned dynamically, at the time of protected system registration.

If you must secure outbound traffic explicitly for protected systems, you can locate the assigned storage node URL in *aristos.log* for each protected endpoint.

Important: Storage node locations within our datacenter are subject to change without notification.