

# x360Recover Direct-to-Cloud Installation

Last updated: June 2021

## TABLE OF CONTENTS

x360Recover - Direct-to-Cloud .....	3
x360Recover Components.....	3
Direct-to-Cloud Backups .....	4
Install the x360Recover Direct-to-Cloud agent.....	4
Firewall Considerations .....	4
Firewall Ports .....	4
Log in to the x360Recover Licensing Portal .....	5
Create Direct-to-Cloud customers in the x360Recover Licensing Portal.....	7
Create a customer.....	7
Download and install the Direct-to-Cloud agent .....	10
Role of the Agent .....	10
Prerequisites .....	10
Install the Direct-to-Cloud Agent .....	10
Silent and RMM deployment of the agent .....	18
Update Direct-to-Cloud agent settings .....	18
Log in via Single Sign On (SSO) .....	20
Add Direct-to-Cloud clients from the vault .....	21
Create Direct-to-Cloud schedules .....	24
Backup Types .....	24
Creating schedules in the Vault Web Interface .....	24
Coming Soon: The Global Management Portal for Direct-to-Cloud customers .....	27
Role of the Global Management Portal .....	27
Accessing the Global Management Portal .....	28
Connecting Vaults with the Global Management Portal for Direct-to-Cloud customers.....	28
Recover Direct-to-Cloud protected systems with x360Recover .....	30
Troubleshoot Direct-to-Cloud agent errors .....	32

## x360Recover - Direct-to-Cloud

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:

- **Licensing Portal** The Licensing Portal is the central management point for customer and location management, and licensing and hardware orders.
- **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.



#### NOTE

The Beta release of x360Recover Direct-to-Cloud only supports Axcient Storage Cloud Vaults.

- **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:

- Accessing the x360Recover Licensing Portal,
- Creating customers,
- 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.

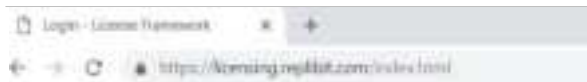
**Important:** Storage node locations within our datacenter are subject to change without notification.

## Log in to the x360Recover Licensing Portal

As a first step, you need to create customers in the x360 Licensing Portal. If you have already set up your customers, you can skip this step.

To log in to the x360Recover Licensing Portal:

1. Open any web browser and navigate to <https://licensing.replibit.com>.



2. In the *License Management window*, enter login credentials:
  - a. In the *Username field*, enter the **Partner Account username**.
  - b. In the *Password field*, enter the **password** that was assigned to you when you completed your initial x360Recover Onboarding training session. Your Partner username and password are case sensitive.



3. Click the **Login** button.
4. If you have forgotten your password, click the **Forgot Password** link. Your password will be sent to the email address specified when your Partner account was created.

## Logging In to the x360Recover Licensing Portal to Support Direct-to-Cloud Customers



The image shows the login page for the Replibit License Management portal. The page has a blue header with the text "License Management". Below the header is the Replibit logo, which consists of a blue cloud icon and the word "Replibit" in a stylized font. Under the logo are two input fields: "Username" with the text "partner" and "Password" with a masked password "\*\*\*\*\*". Below these fields is a blue "Login" button, which is highlighted with a red rectangular box. To the right of the "Login" button is a red "Forgot Password" button. Below the "Forgot Password" button is a green oval containing the text "Forgot Password". At the bottom of the page, there is a small link that says "© 2015 Replibit.com".

## Create Direct-to-Cloud customers in the x360Recover Licensing Portal

When you are ready, you can create a customer account within the Licensing Portal.



### NOTE

You should only create one customer account for each customer that you support.

## Create a customer

Please consider the following when creating customers:

- When you create a customer, you will be prompted to configure a username and password for the account. These credentials may be used when logging into the vault to recover data. We recommend recording the username and password. You can optionally share these credentials with the customer if they will be performing self-service restores from an off-site vault.
- Each customer account must be configured with a unique username. You cannot create two customer accounts with the same username within the x360Recover Licensing Portal.
- If you need to recover a lost password, click the **Change Password** button to reset the password.

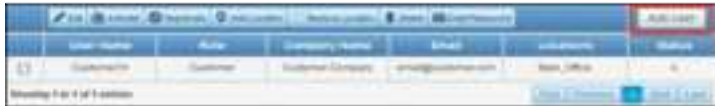
To create a customer:

1. From the x360Recover License Management left pane menu, click to expand *User Management* and then select **Users**.

## Creating Direct-to-Cloud Customers in the x360Recover Licensing Portal



2. Click the **Add User** button. The *customer Details* window displays.



3. In the *customer Details* window, update the following fields:
  - a. In the *customer Username* field, enter the **username** for the new customer. This field only accepts letters, numbers, and underscore characters. You can- not add spaces or other special characters.
  - b. In the *customer Company Name* field, enter the **name of the company**.
  - c. In the *customer Password* field, enter a complex **password**. You must confirm this password in the *customer Confirm Password* field.
  - d. In the *customer Email Address* field, enter an **email address** for the customer.
  - e. In the *Locations* field, enter one or more **Locations** for the customer. Separate each Location with a comma. This field only accepts letters, numbers, and underscore characters. You cannot add spaces or other special characters.



### NOTE

Do *not* assign additional licenses to the customer for Direct-to-Cloud protected systems. Direct-to-Cloud licensing is billed on a usage basis independent of the Licensing Portal. Assigning additional licenses here will result in double-billing for your Direct-to-Cloud endpoints.



## Creating Direct-to-Cloud Customers in the x360Recover Licensing Portal

The screenshot shows the 'Customer Details' form in the x360Recover Licensing Portal. The form is titled 'Customer Details' and has a blue header bar. On the right side of the header bar, there is a red box around the 'Add User' button. Below the header bar, there is a 'Status' dropdown menu. The form contains several input fields: 'User Role' (set to 'Customer'), 'Customer Username' (set to 'Customer'), 'Customer Company Name' (set to 'Customer Company'), 'Customer Password' (masked with asterisks), 'Customer Confirm Password' (masked with asterisks), 'Customer Email Address' (set to 'email@customer.com'), and 'Locations' (set to 'Main Office'). A note below the password fields states: 'Note: Customer password cannot be modified once it is entered.' At the bottom of the form, there is a green circle around the 'Submit' button. Below the 'Submit' button, there is a note: 'Note: Please enter multiple locations as comma separated, e.g. 'Main Office', 'New York'.

Customer Details

Add User

Status

User Role: Customer

Customer Username: Customer

Customer Company Name: Customer Company

Customer Password: \*\*\*\*\*

Note: Customer password cannot be modified once it is entered.

Customer Confirm Password: \*\*\*\*\*

Customer Email Address: email@customer.com

Locations: Main Office

Note: Please enter multiple locations as comma separated, e.g. 'Main Office', 'New York'

Submit Cancel

## Download and install the Direct-to-Cloud agent

After you log in to the vault, you can begin to 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 back- up 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 *Users* tab of the vault.



### 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.

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

The screenshot shows the Axcient x360 Recover login page. At the top, the logo 'Axcient x360 Recover' is displayed, with 'x360' in orange. Below the logo, there are two input fields: 'USERNAME:' and 'PASSWORD:'. At the bottom left, there is a link 'Download agent' in orange. At the bottom right, there is an orange button with a white checkmark and the text 'Login'.



### 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 the **Users** tab.



### NOTE

The *Users* tab reflects the list of customers created in the Licensing Portal. If your customers are not displaying in the *Users* tab, we recommend syncing the vault with the Licensing Portal.



3. Locate the appropriate client and click the **Download** link

## Downloading and Installing the Direct-to-Cloud Agent



### NOTE

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



### NOTE

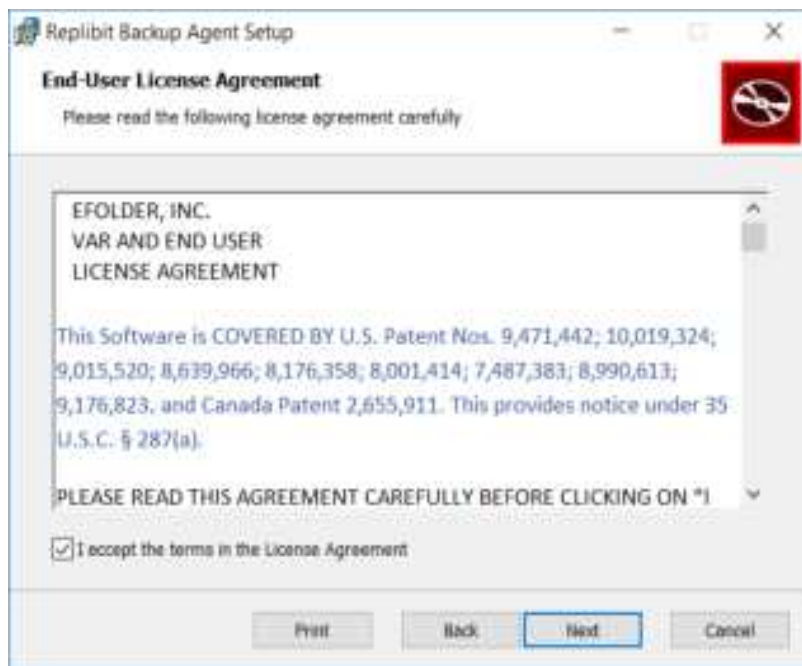
The installation file is valid for 14 days from the time of download. Installing from an expired agent installer file will fail and register invalid token errors within the log file.

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

## Downloading and Installing the Direct-to-Cloud Agent

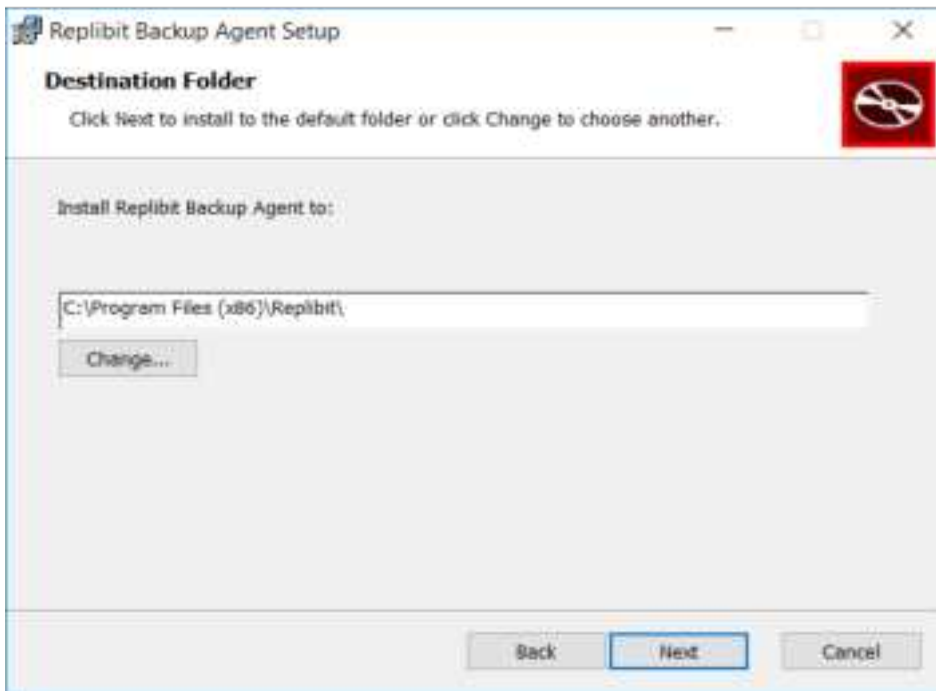


5. After reading the agreement, select **I accept the agreement**. Click the **Next** button to continue.



## Downloading and Installing the Direct-to-Cloud Agent

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

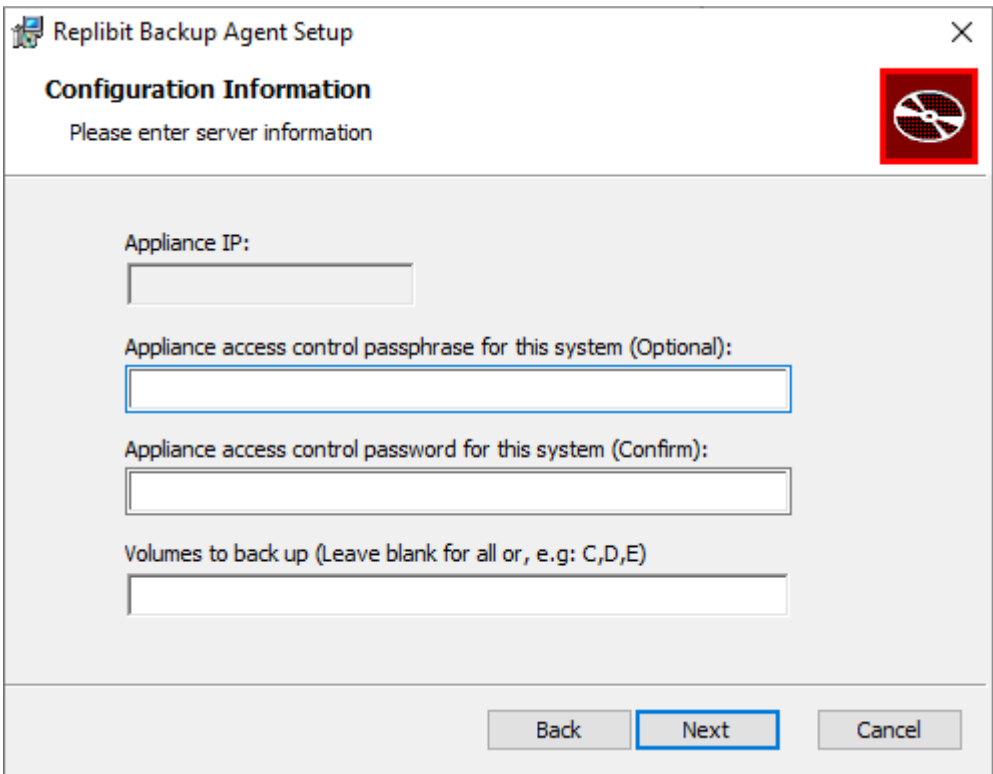
You do not need to enter an IP address.



### NOTE

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.

## Downloading and Installing the Direct-to-Cloud Agent



The screenshot shows the 'Replibit Backup Agent Setup' window at the 'Configuration Information' step. The window has a title bar with the application name and standard Windows window controls. Below the title bar, the text 'Configuration Information' is displayed in bold, followed by the instruction 'Please enter server information'. On the right side of the window, there is a red square icon containing a white CD-ROM symbol. The main area of the window contains four input fields: 'Appliance IP:', 'Appliance access control passphrase for this system (Optional):', 'Appliance access control password for this system (Confirm):', and 'Volumes to back up (Leave blank for all or, e.g: C,D,E)'. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

Replibit Backup Agent Setup

**Configuration Information**

Please enter server information

Appliance IP:

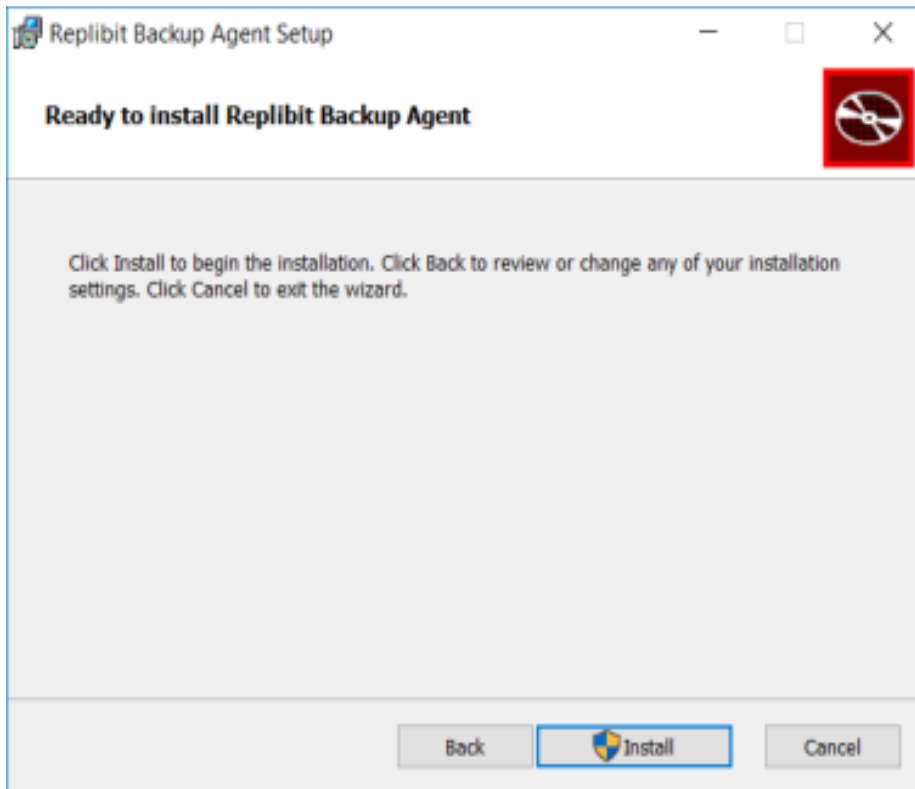
Appliance access control passphrase for this system (Optional):

Appliance access control password for this system (Confirm):

Volumes to back up (Leave blank for all or, e.g: C,D,E)

Back Next Cancel

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



The screenshot shows the 'Replibit Backup Agent Setup' window at the 'Ready to install' step. The window has a title bar with the application name and standard Windows window controls. Below the title bar, the text 'Ready to install Replibit Backup Agent' is displayed in bold. On the right side of the window, there is a red square icon containing a white CD-ROM symbol. The main area of the window contains the following text: 'Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.' At the bottom of the window, there are three buttons: 'Back', 'Install', and 'Cancel'. The 'Install' button is highlighted with a blue border.

Replibit Backup Agent Setup

**Ready to install Replibit Backup Agent**

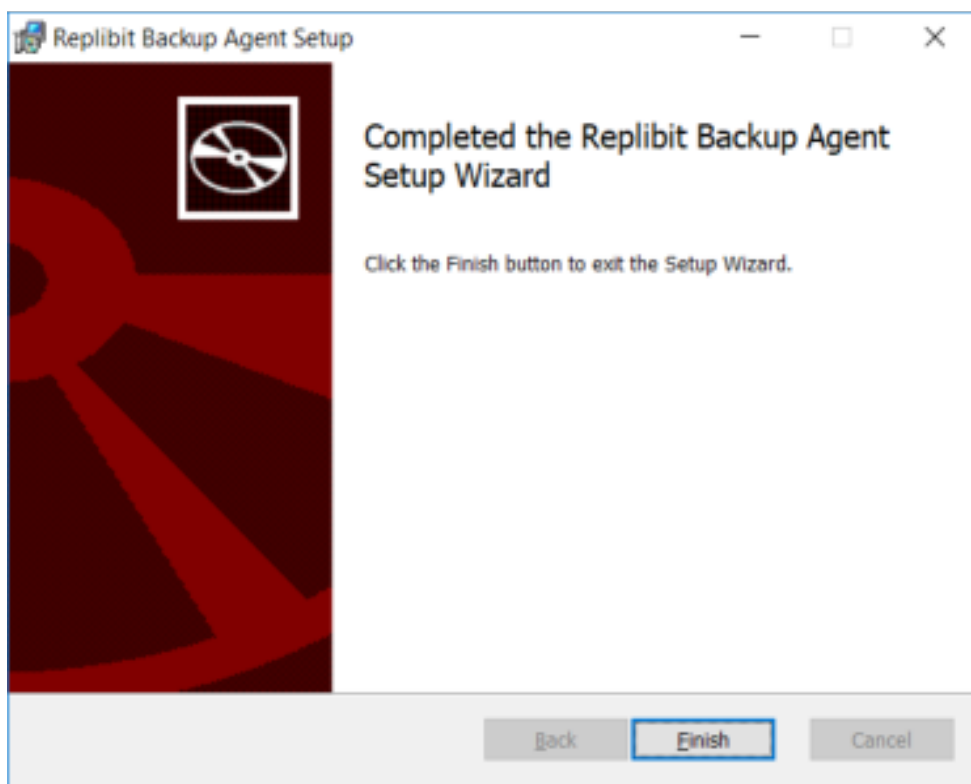
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Back Install Cancel

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



## Downloading and Installing the Direct-to-Cloud Agent



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

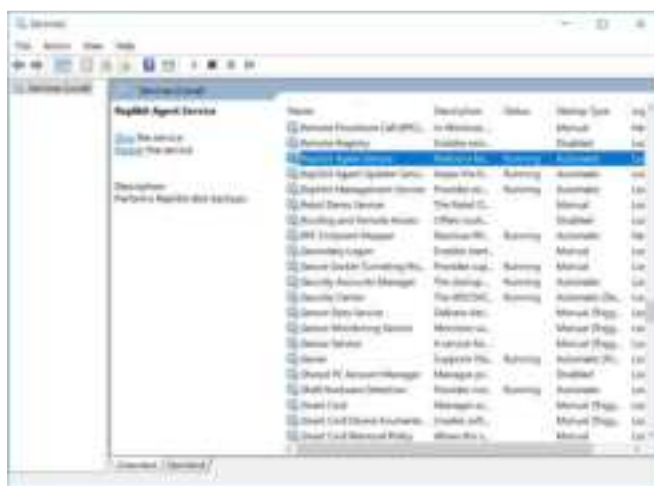
### Update Direct-to-Cloud agent settings

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.

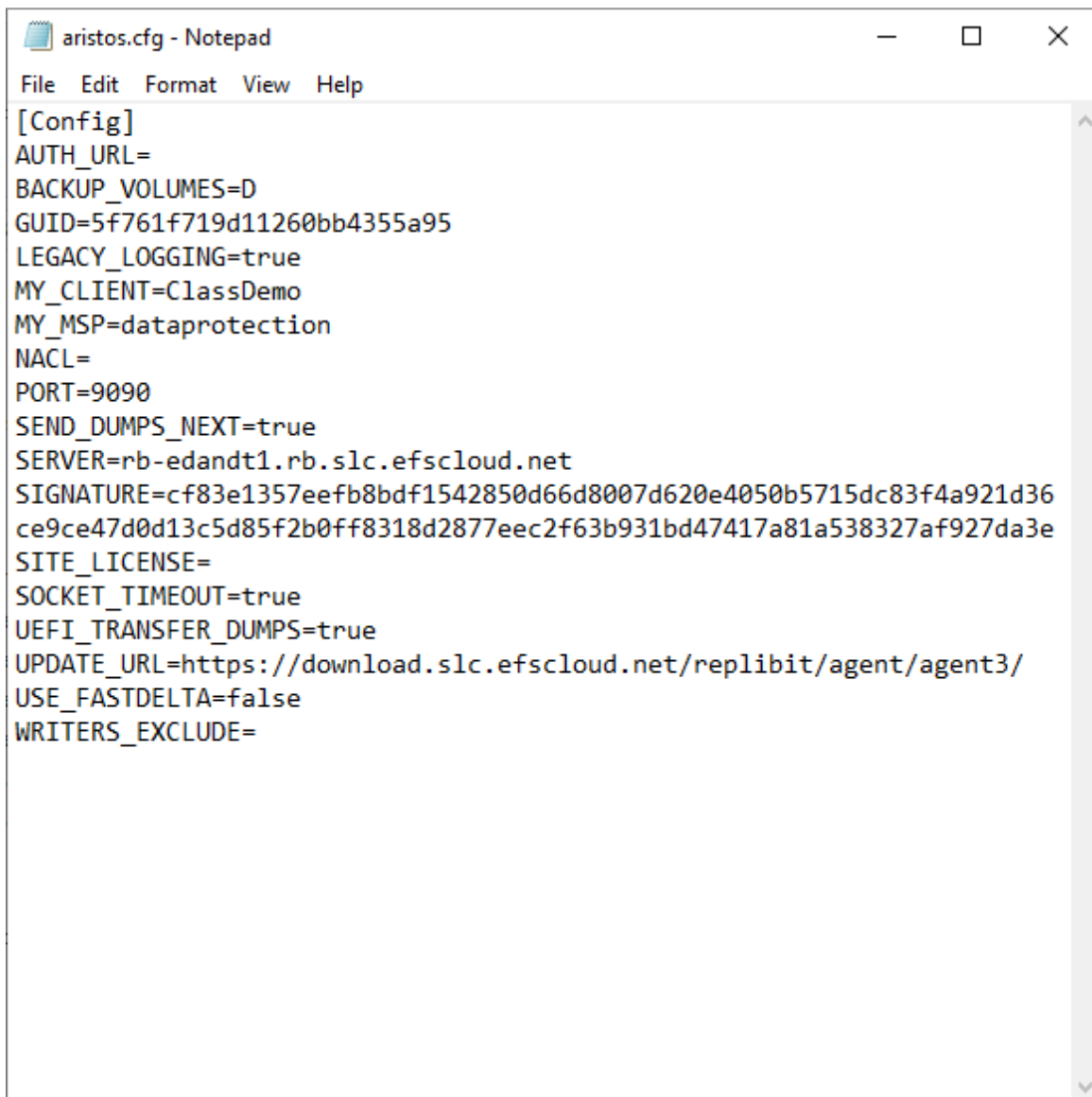
To update x360Recover agent settings:

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.

## Downloading and Installing the Direct-to-Cloud Agent

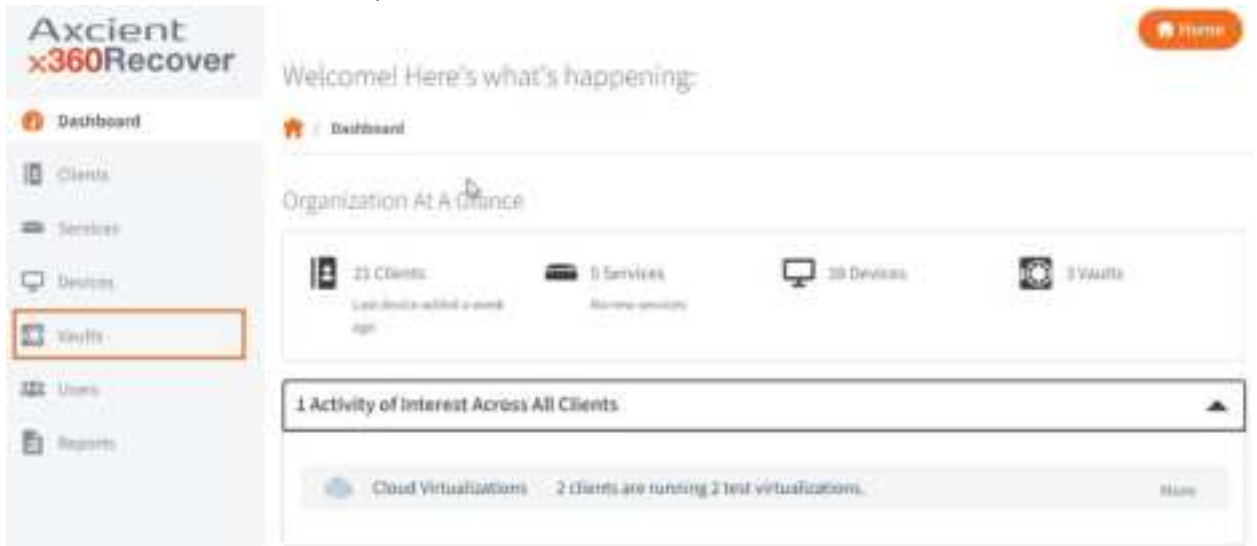
A screenshot of a Notepad window titled 'aristos.cfg - Notepad'. The window has a standard menu bar with 'File', 'Edit', 'Format', 'View', and 'Help'. The text content is as follows:

```
[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=cfc83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36
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=
```

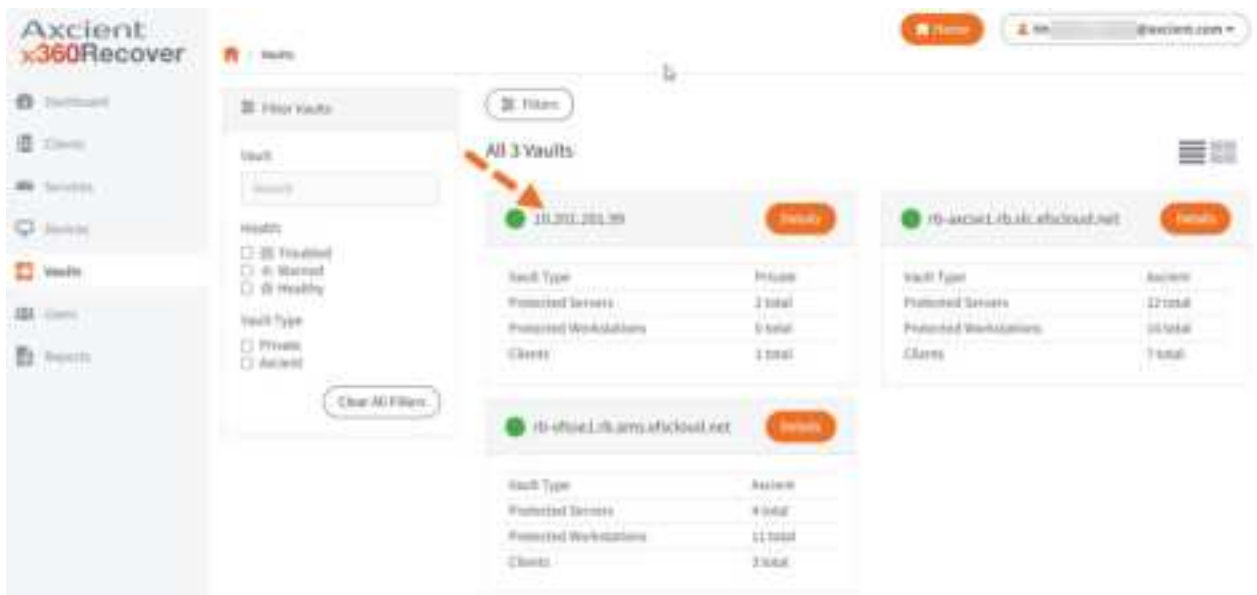
4. Update settings in the *aristos.cfg* file. For example:
  - a. Edit the *Backup\_Volumes* line to update the **list of volumes** that you want to back up.
  - b. When you are finished, save the file and restart the agent service.

## Log in via Single Sign On (SSO)

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

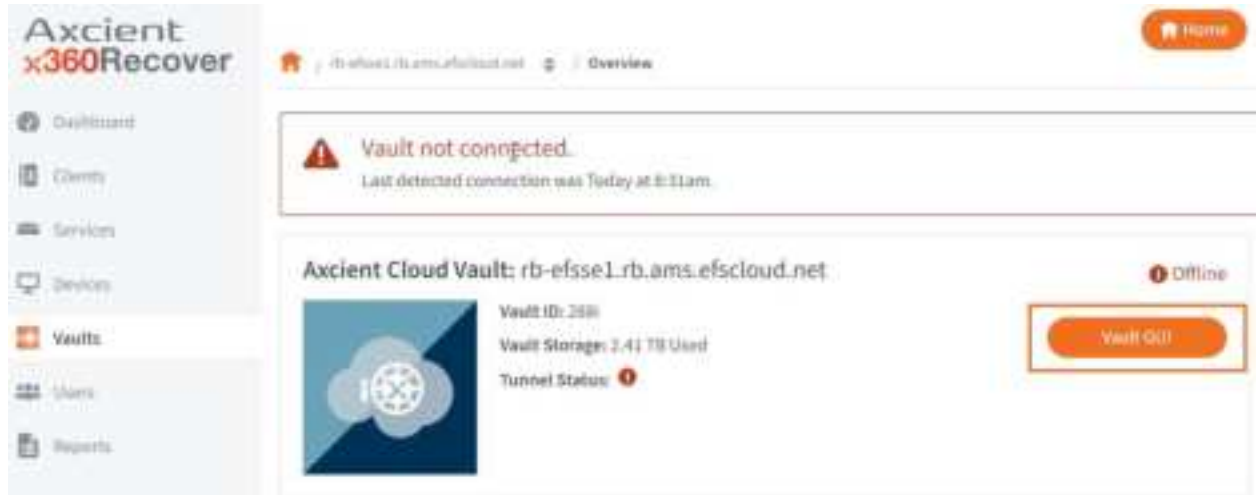


2. Click on a vault.



## Creating Direct-to-Cloud Schedules

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

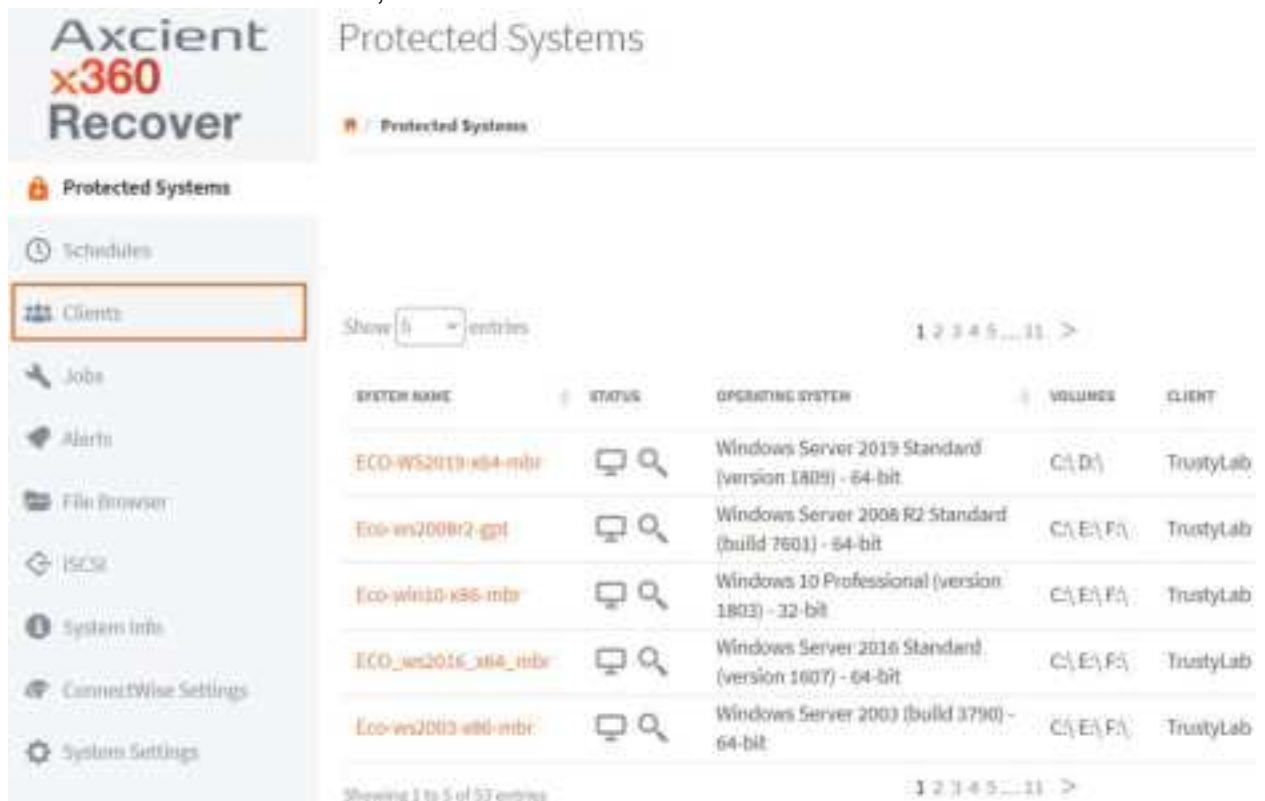


4. This will log you into the vault directly, without prompting you to enter a username and password.

## Add Direct-to-Cloud clients from the vault

To add a client:

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

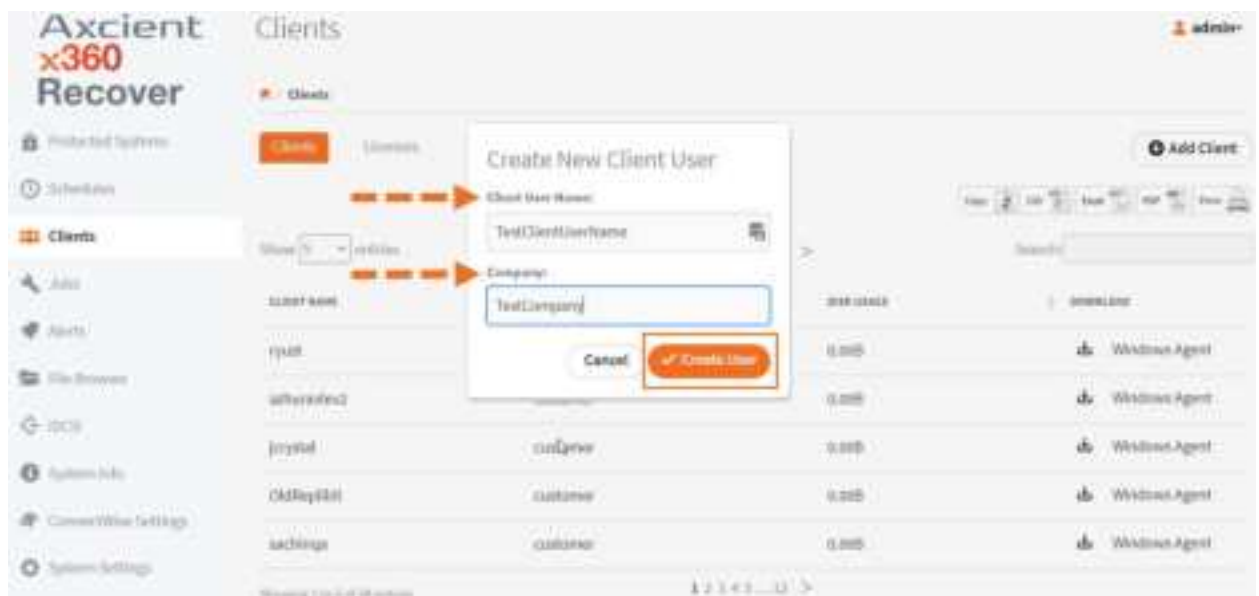


## Creating Direct-to-Cloud Schedules

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

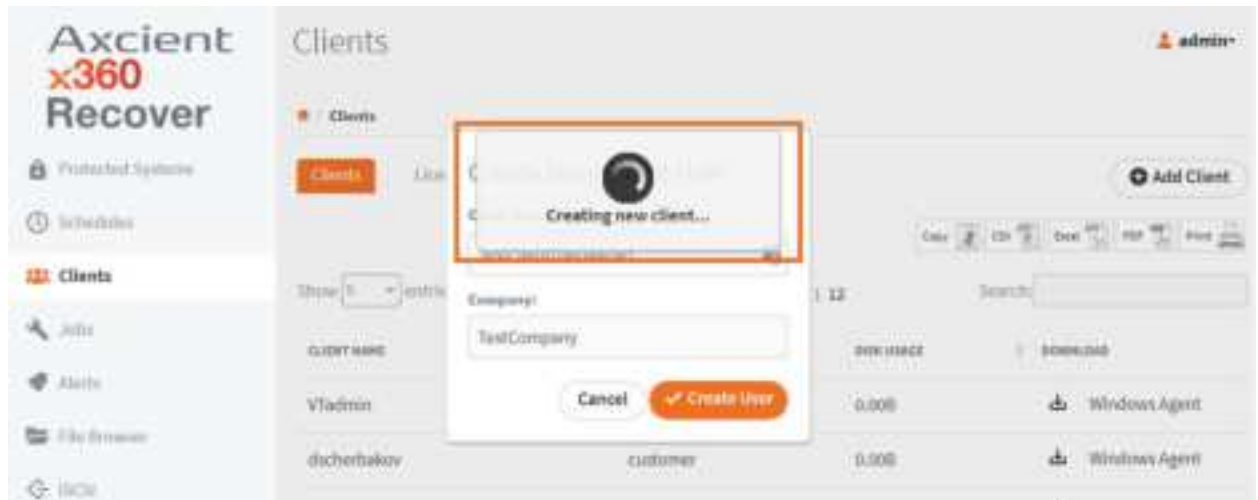


3. The Create New Client User popup will appear.
4. Fill in the **Client User Name** and **Company** field, and then click the **Create User** button to continue.



## Creating Direct-to-Cloud Schedules

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



6. 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.



## 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

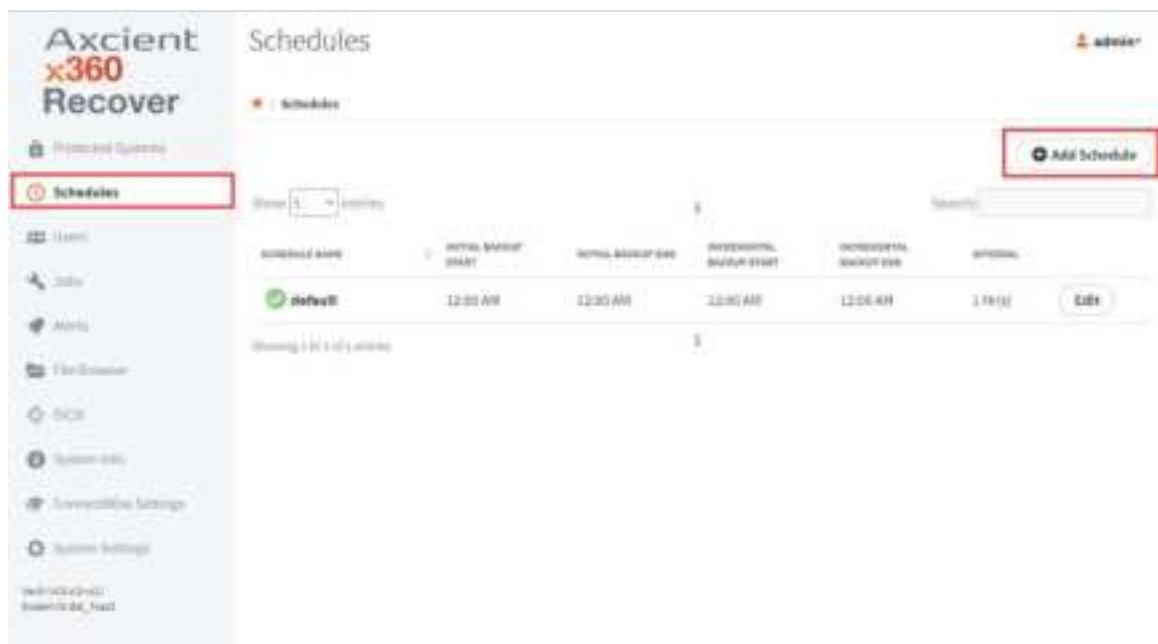
Within the Vault Web interface, you can use the *Schedules* page to define initial back-up schedules and ongoing incremental snapshot schedules. You can create an unlimited number of schedules and assign them to different machines according to special requirements or technical limitations. You can also 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.

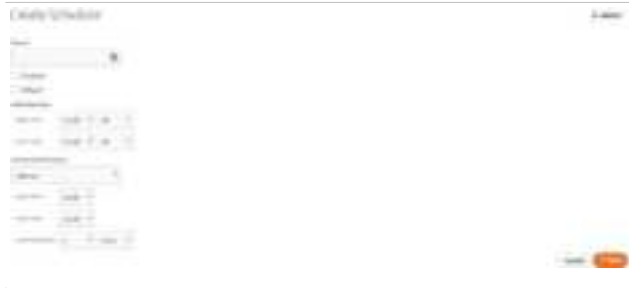




4. In the *Add Schedule* page, enter information about the new Schedule:
  - a. In the *Name* field, enter a **descriptive name** for the schedule. For example, you might create a scheduled titled, *Critical*, for servers that require 15-minute incremental backups; and *Non-Critical* for servers that 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.

## Creating Direct-to-Cloud Schedules

- 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.



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



### NOTE

Coming Soon: 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 total time 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 the following:

- 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**.



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



## Connecting Vaults with the Global Management Portal for Direct-to-Cloud customers

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.



### NOTE

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.

2. **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.



3. **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.



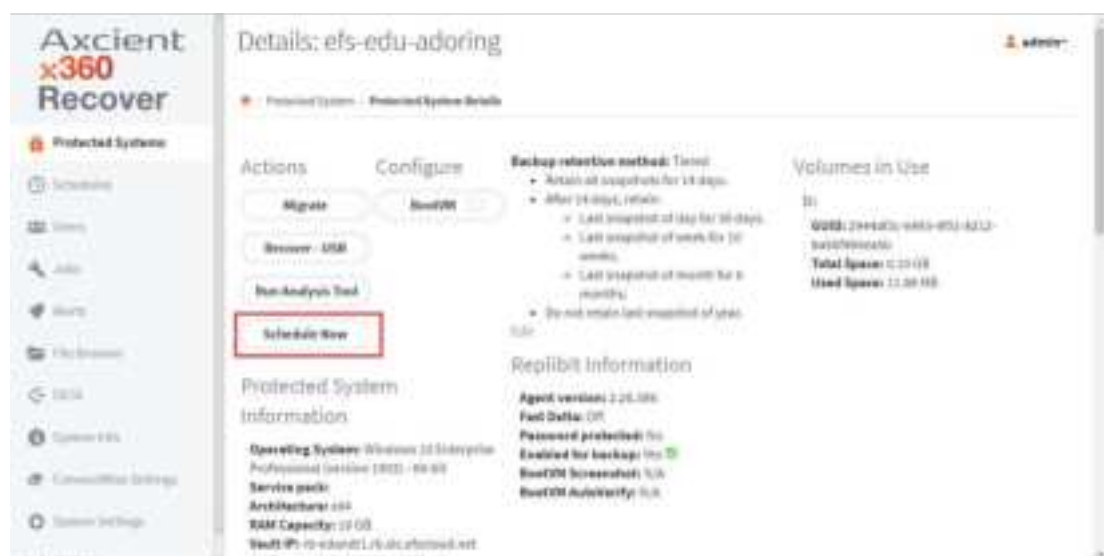
## Recover Direct-to-Cloud protected systems with x360Recover

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.

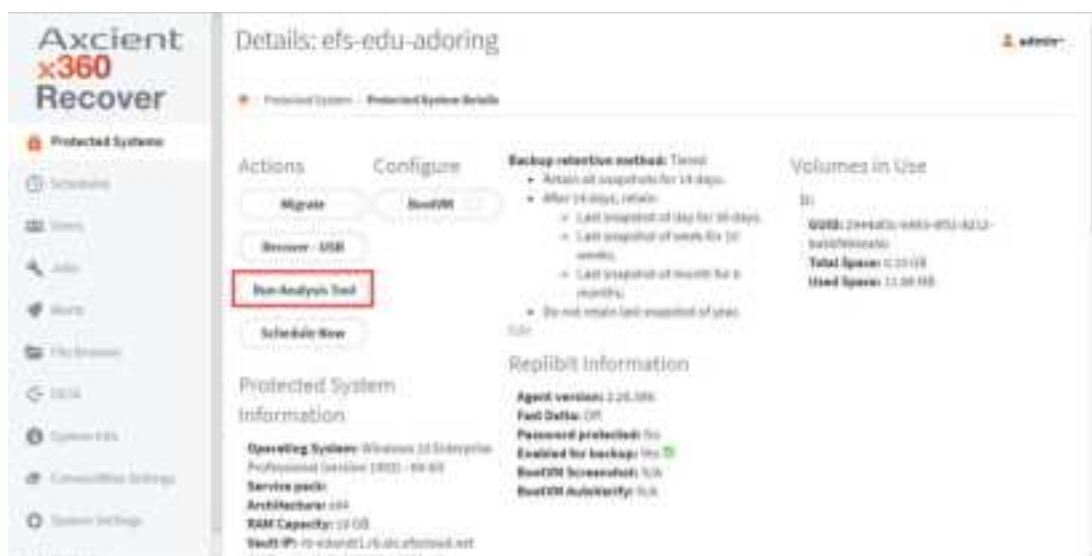
To access recovery options:

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 Protected System 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.

## Recovering Direct-to-Cloud Protected Systems with x360Recover



- 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.



## 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.