

# x360Recover Quick Start Deployment Guide

Last updated: November 2023

## Contents

Step 1: Create a customer and assign license(s)	4
Step 2: Provision the appliance	4
Firewall ports	4
Steps to provision the appliance	5
Step 3: Login and configure settings	5
Step 4: Configure other settings	5
Step 5: Deploy agents	6
Step 6: Add a vault	6
Step 7: Configure monitoring: PSA alerts	7
References	7
Support	7

Note: The first three steps below are for BYOD installations or for Axcient-built units that have not been preconfigured. If you have preconfigured your Axcient BDR, please skip to **Step 4. Configure Other Settings** below.

---

## Step 1: Create a customer and assign license(s)

Before you can deploy a new x360Recover BDR appliance at your customer site, you first need to create a customer account and then assign licenses by specifying the desired number of server and/or workstation endpoints to be protected. Note: If you are deploying an appliance to an *existing* customer account, simply add a new license to that customer.

- To create a customer account, refer to [Manage x360Recover users in x360Recover Manager](#)
- To assign licenses and specify the desired number of server and/or workstation endpoints to be protected, refer to [Manage licenses in x360Recover Manager](#)
- For detailed instructions on the licensing process launched in 2023, please see [Licensing in x360Recover Manager \(RMC\)](#)

## Step 2: Provision the appliance

Once you have created a customer account, complete the provisioning of the BDR device.

### Firewall ports

Firewall ports must be configured prior to provisioning the appliance or the storage will not be available for the appliance.

TCP/443/9080/9081 (The address for the vault for this appliance). Begins with rb-

TCP/443 [api.axcient.net](https://api.axcient.net)

TCP/2222 [rb-prd-slcflow.slc.efsccloud.net](https://rb-prd-slcflow.slc.efsccloud.net)

TCP/443 [licensing.replibit.com](https://licensing.replibit.com)

TCP/443 [appliances.efsccloud.net](https://appliances.efsccloud.net)

TCP/80 TCP/443 [pkgmgrrepo.replibit.net](https://pkgmgrrepo.replibit.net)

TCP/443 [download.slc.efsccloud.net](https://download.slc.efsccloud.net)

TCP/443 [rb-mirror.slc.efsccloud.net](https://rb-mirror.slc.efsccloud.net)

TCP/443 [pip.axcient.cloud](https://pip.axcient.cloud)

## Steps to provision the appliance

- Connect to a network with an internet connection
- Connect the BDR unit to the network.
- Attach keyboard, mouse, and monitor, and then power it on.
- Once booted, the login prompt will appear and display the currently assigned IP address.

Note: If the IP address is not displayed, wait one (1) minute, and press <Enter> to refresh the display.

- Connect to the BDR using a web browser on the assigned IP address.
- If updates are available, the updates will be installed, and the device will reboot. Please

follow Axcient's detailed instructions for setup and first-time login: <https://help.axcient.com/001-install-agents/appliance-setup-and-first-time-login-x360recover>

## Step 3: Login and configure settings

After provisioning, the device will reboot and display the login screen.

Note: It can take up to five (5) minutes for the storage pool to come online after a reboot.

- A message which says *Logins are unauthorized, wait a couple minutes and try again* indicates that the storage has not mounted yet.
- Log in to the device using the admin user, and the password you specified for the Web UI Admin during the provisioning process.
- On first login, you will be presented with the *Manage Storage* page. Create the storage pool using the available disks within the unit. For details, review [How to manage the storage pool](#).

## Step 4: Configure other settings

Once the storage pool has been created, select **Settings** from the left menu pane.

- Select **Change Machine Name** and assign a hostname to the device.

Use a naming convention that identifies both the customer name and function of the device. For example, if deploying an appliance to ABC Distributors, *ABCDist-BDR* might be an appropriate name. When deploying a new vault, either in the Axcient Cloud or at your own datacenter, you might name it *MyMSP-VLT1*, as an example.

- Next, select **Network Settings**, and configure a static IP address. This static IP address will be used to configure the backup agent on the protected system(s). If you are bench-provisioning the appliance at your MSP office, leave as DHCP until finished with the setup. Once completed, change the appliance to a preset static address on the customer network.
- After assigning an IP address, select **Management Portal**, and configure the connection to your Management Portal.
- Enter the IP address or FQDN (URL) of the Management Portal.
  - You can locate user name and API key from the *Users* tab within the Management Portal.
  - For Management Portal settings, the user name is always admin (in lower case.)
- Test and save the settings. If an error occurs, ensure there is no hidden space before or after the address (backspace at the beginning or delete at the end). Test again and save.

## Step 5: Deploy agents

- Log in to each Windows system to be backed up with x360Recover.
- Open **services.msc** and disable the backup service for any existing Shadowprotect or Acronis agents currently installed.

Important Note: Do NOT disable the VSS (Volume Shadow Copy) services associated with third-party backup services.

- Open a web browser and connect to the IP address of the appliance.
- Download the agent from the link at the bottom of the login screen
- Install and configure the agent on each Windows system to be protected.
- To prevent possible future inclusion of any attached USB devices, specify which disk volumes should be backed up on each server when deploying the agent.
- Immediately stop the Replibit Agent Service and use the following list to make the required exclusions in the AV/firewall: <https://help.axcient.com/x360recover-faqs-agents/exclude-an-agent-from-anti-virus-scans-x360recover> Setting these exclusions ensures the agent is not blocked, quarantined or deleted.

Once the exclusions are completed restart the ReplibitAgentService:

- From the *Protected Systems Details* page, select **Schedule Now**, and run a full backup immediately to expedite the initial backup job.

## Step 6: Add a vault

- Configure a connection to a vault from the *Vault Settings* page.
- Enter a friendly name, IP address or FQDN, and click **Test Connection**.
- Create a bandwidth schedule by selecting the days of the week, and desired speed.
  - Set your internet connection speed at the maximum available value. (Zero (0) is full speed)
  - Set your firewall/router at the lowest possible priority (usually static IP).For details, review [Replication throttling between an appliance and a vault with QoS](#)
- From the *Protected Systems Details* page, select **Replication**, and configure a vault for each protected system you wish to replicate to the off-site vault.

Note: You cannot configure replication until at least one backup has completed for the protected system.

## Step 7: Configure monitoring: PSA alerts

Axcient supports ConnectWise and Autotask.

Alerts can be set up (a) on the appliance for individual alert settings or (b) on the Recover Manager (RMC) for individual customers or partner-wide universal settings.

- Instructions to set up individual **ConnectWise** alert settings on an appliance are here:  
<https://help.axcient.com/004-integrate-psa/115002405768-x360Recover-ConnectWise-Integration-Guide>
- Instructions to set up **ConnectWise** using the Recover Manager (RMC) are here:  
<https://help.axcient.com/004-integrate-psa/360059921654-ConnectWise-PSA-Integrate-x360Recover-RMC>
- Instructions to set up **Autotask** using the Recover Manager (RMC) are here:  
<https://help.axcient.com/004-integrate-psa/1500001508842-Autotask-PSA-Integrate-x360Recover-RMC>
- You can enable and configure the Email Alerting option within the *Settings* page.
  - You will need an authenticated email user account on an external mail server to use as the email sender. This can be any mail account that allows authenticated mail relay, including Gmail or an internal Exchange mailbox account.
  - Add the email address used by your PSA to receive tickets via email as the destination. Then select all alert classes for which you would like to receive tickets from this appliance

---

## References

- [x360Recover knowledgebase](#)
- [X360Recover Essential User Guide](#)

## Support

If you need assistance, please contact our Technical Support team.

- Call: 800-352-0248, Opt 2 (Toll Free)
- [Submit a Ticket: Axcient Support](#)
- Learn more: [x360Recover Knowledgebase](#)