**Appliance Deployment**

**Install the OS - x360Recover - BDR**

How to install the x360Recover OS

x360Recover runs on a custom Ubuntu 64-bit Linux operating system.

The x360Recover installation ISO will deploy the basic operating system along with all x360Recover application components.

* Download the latest x360Recover installation ISO [here.](https://axcient.helpjuice.com/software-downloads/downloads)

Once you have downloaded the ISO, you can make a bootable image of the installer on a USB flash drive.  For instructions on creating a bootable USB flash drive image of the installer, refer to this [KB article](https://axcient.helpjuice.com/01-install-faqs-/115006558547-x360Recover-How-to-download-the-x360Recover-software).

The following steps describe the installation of the underlying x360Recover operating system.

Prerequisites

* To ensure that the installation can be completed successfully, the system should be connected to a network with DHCP and open Internet access.
* After installation of the basic operating system, provisioning and configuring the x360Recover device requires Internet access to perform any necessary software updates and register the device to the License Portal.
* When booting from a USB device, it may be necessary to change the default boot order of the system.
  + Power on the system and press the appropriate key (Typically <Del>, <F1> or <F2> on most white-box systems, or <F9> on HP servers) to enter the BIOS setup menu.
  + Locate the boot order management page within the BIOS and configure the system to enable booting from USB Flash drive.
  + Ensure that the boot order places the USB device before internal Hard Drives.
* Systems booting from NVMe media must be configured to boot using UEFI mode in the system BIOS

**Note:** If the system is configured to boot via UEFI mode in the system BIOS, you must disable the **Secure Boot** option.  x360Recover uses dynamically generated kernel module drivers for Intel network adapters and ZFS that cannot be signed by a trusted certificate for every possible version of the Linux kernel that may be applied via updates

**Note:**x360Recover and the Linux operating system do not support booting from motherboard (fake) RAID controllers. (BIOS has an option to select RAID for the onboard SATA ports.)  This onboard ‘RAID’ functionality is really software-based RAID that requires Windows-only drivers that are not available on Linux.  If your motherboard has such an option, ensure that the SATA ports are configured in SATA or AHCI mode for compatibility with Linux.

Consult your system motherboard documentation for instructions on selecting between RAID and SATA/AHCI boot modes.

**Prepare to install**

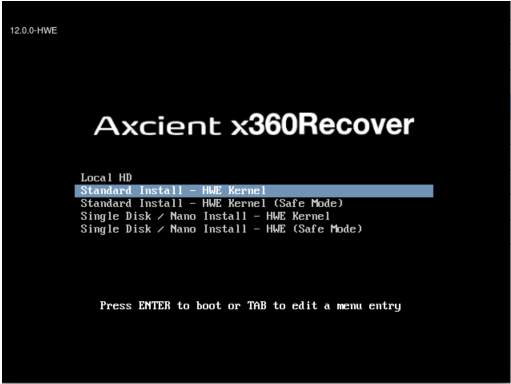
Once the BIOS configuration has been completed:

1. Ensure that the DVD or USB flash drive is inserted into the system.
2. Exit from the BIOS after saving any settings changes.
3. Reboot the machine.

The x360Recover installer should now load on the system.

Install x360Recover

**STEP 1**. Boot the x360Recover OS.



The initial Boot Menu defaults to the local hard drive.

Use the cursor keys to scroll up and down in order to select one of the available installation options:

|  |
| --- |
| **Standard Install - HWE Kernel** is the recommended option in most cases.  This installs x360Recover in standard mode (with dedicated OS disk and separate storage disks), using the Ubuntu 18.04 Hardware Enablement Linux Kernel.  **Standard Install - HWE Kernel (Safe Mode)** is recommended for systems that encounter video issues during the installation process.  Safe Mode uses a more conservative set of basic Linux video drivers during installation  **Single Disk / Nano Install \*\***is intended for  Axcient Nano devices but may also be used with BYOD hardware.  This special installation mode installs x360Recover onto systems that have only a single hard drive shared for both the operating system and data storage.  (In standard installation mode, x360Recover installs the operating system on a dedicated volume and then stores data on a separate set of multiple disks. This is allows for redundancy of your backup data in the event of a disk failure.) **IMPORTANT NOTE: We highly recommend using the standard installation method when building your own x360Recover BDR hardware.**The Nano installation provides no storage redundancy for your backup data. You cannot perform an OS recovery to repair Single Disk / Nano installations. |

After you select an option, the installer will boot to the Installation Wizard.

The x360Recover splash screen will be displayed while the installer loads.



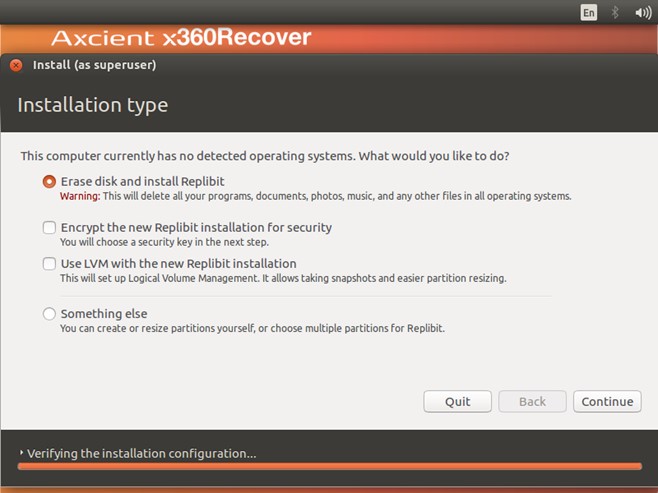
**STEP 2.**Select installation type.

The Axcient x360Recover installer menu appears.

Select **Erase Disk and Install Replibit.**

**Note**: Do **not**select encryption and do **not** select LVM partitioning.

**IMPORTANT NOTE: If any other operating system is installed on the system, it will be destroyed, and replaced with the x360Recover operating system.**



Click **Continue**

**STEP 3**. Select the drive to be used

Select the drive where you wish to install the x360Recover operating system.

Typically, this choice will be **(sda)**:

Graphical user interface, website

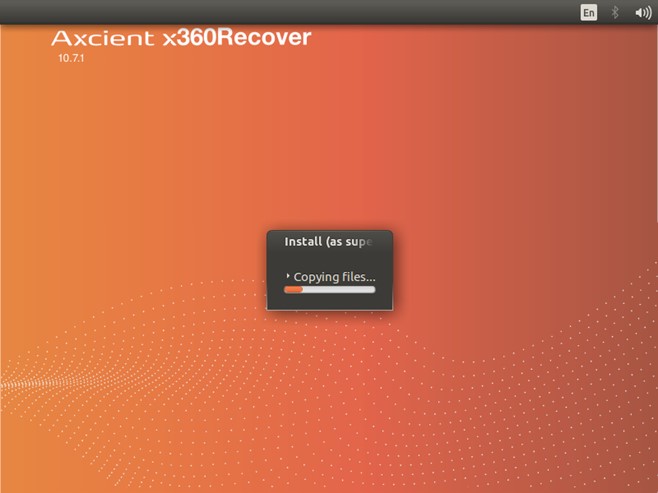
Description automatically generated

After you have selected the preferred drive, click **Install Now**.

**NOTE: This disk will be formatted and erased during the installation.**

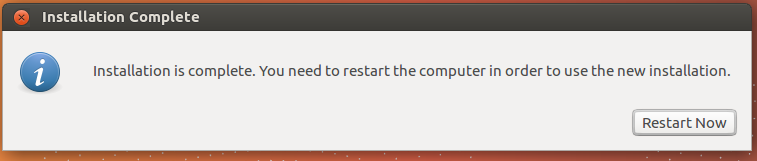
**STEP 4.** Complete the installation

Installation will now proceed. Please wait for this step to be fully complete. Loading the operating system may take several minutes, depending on the hardware and type of USB installation media being used.



 When the installation is complete, remove the DVD or USB flash drive from the system.

Then, click **Restart Now.**



 NOTE: Depending on your system BIOS, it may be necessary to press the <Space> bar once to continue (if the reboot appears to be stalled.)

Once the system has finished rebooting, the login screen will be presented.



Note the IP address presented and continue with [provisioning the setup and first-time login to the appliance.](https://axcient.helpjuice.com/001-install-agents/appliance-setup-and-first-time-login-x360recover)

# Appliance setup and first-time login - x360Recover

**Note: Before proceeding with deployment:** If this device is being deployed as an appliance at a client location, first verify (a) that a customer account in the Axcient x360Recover Licensing Portal has been created and that (b) the customer account has an unallocated location available.

If you need help setting up a customer account or identifying the locations available in the licensing portal, please review these instructions for using the  [Axcient x360Recover Licensing Portal.](https://axcient.helpjuice.com/001-install-agents/115006560127-x360Recover-How-to-set-up-initial-storage-pool-configuration" \t "_blank)

Device setup

Launch the Setup Wizard, apply updates and set passwords

**STEP 1.**To begin the device setup, open a web browser and navigate to the IP address of the new x360Recover device.

Locate the **IP address** of the device on the console above the login prompt.

**Note:** If there is no IP address displayed, wait one minute and press **<Enter>** to refresh the display.

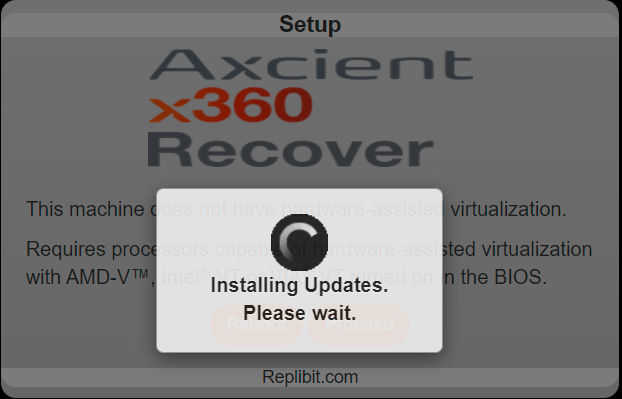
**STEP 2.**Launch the Setup Wizard, open a web browser and navigate to the IP address of the newly installed device.

Note: You must have internet access for the Setup Wizard to complete the setup and registration process.

If required software updates are available, you will see an **Applying Updates** popup window when you first access the device.

Applying updates may take as much as 20 minutes to complete.

After the completion of any needed updates, the device will reboot. Observe the device console and wait for the system to complete its reboot before proceeding.

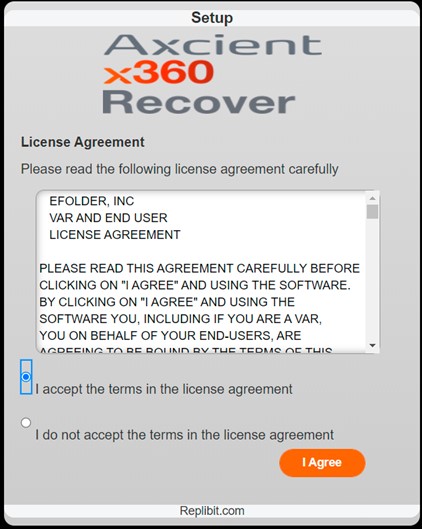
   

**STEP 3**. Once the system has applied any needed updates, the x360Recover License Agreement screen appears.

Read the agreement before continuing.

If you accept the terms of the agreement, select the radio button, **I accept the terms in the license agreement.**

Click on the**I Agree**button to continue the configuration process.

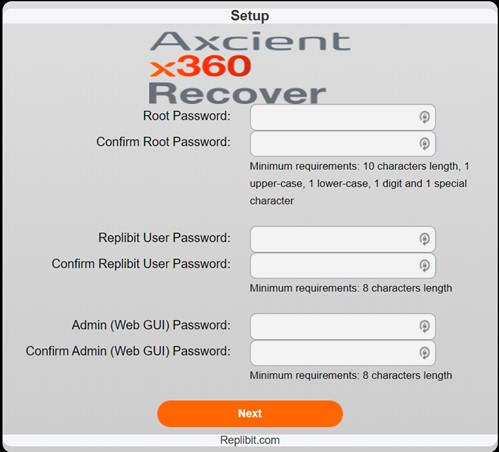


STEP 4. Select **First Machine in a Cluster** (Cluster deployments are deprecated.)



Click **Next**to proceed.

**STEP 5**. Enter **passwords.**



* **Root Password**is the Linux root user (the core operating system super-user) and requires a highly secure password.  Enter a root password at least 10 digits long containing upper case characters, lower case characters, numbers and special characters (for instance, #$%^&@!\*)
* **Replibit User Password** user is a limited access shell account whose password should be at least 8 characters long.
* **Admin (Web GUI) Password** is used to access the Web Interface and all x360Recover features. This password should be at least 8 characters long.

Click the **Next** button to proceed.

Select a role for the device

STEP 6. Select the intended role for the new device. These include:

* **Appliance**, which resides at the customer site, and receives backup data from agent software installed on the customer’s protected systems.
* **Vault,** which resides at the off-site recovery location or datacenter, and receives replication of recovery points created by one or more appliances.
* **Management Portal**, which collects statistics from connected appliance and vault devices, and provides secure remote access and management. Partners typically deploy only a single Management Portal for all managed devices.  (Management Portal has been deprecated by [x360Recover Manager.](https://axcient.helpjuice.com/x360Recover-Manager))
* **OS Recovery.**  Performing an OS recovery restores the previous role and settings of an existing system after the operating system has been lost and reloaded on a new boot disk.  For detailed instructions on performing an OS recovery for an appliance, see this [KB article.](https://axcient.helpjuice.com/005-backup/360020225494-x360Recover-What-is-RAID?from_search=69647248)



Click the **Next**button to proceed.

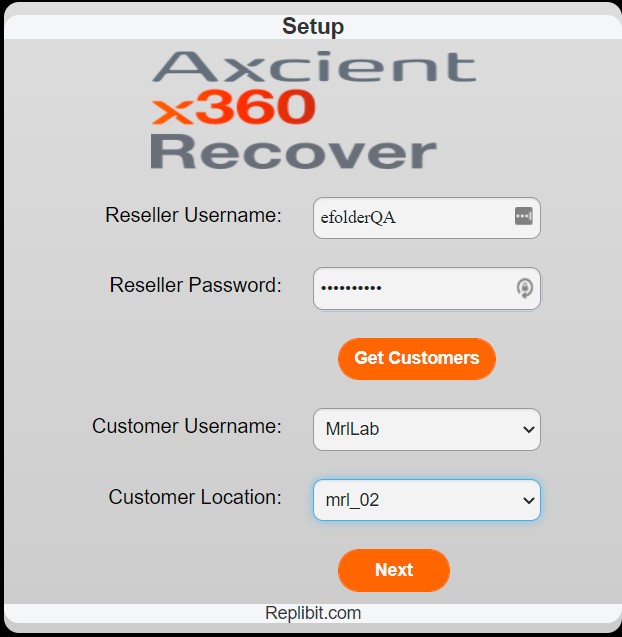
Fill in reseller credentials

STEP 7. In the **Reseller Username**field, enter the partner username (License Portal user) provided when you completed your Axcient x360Recover Partner Agreement and Licensing Portal training.

In the **Reseller Password** field, enter the Licensing Portal password provided when you completed your x360Recover Partner agreement and License Portal training.

If deploying a new appliance, click **Get Customers** to populate the list of customers with unallocated locations.

If deploying a vault, just click **Next** after entering the Reseller Username and Password.



Fill in customer credentials

STEP 8. From the **Customer Username** drop-down box, select the correct customer username.

From the **Customer Location** drop-down box, select from the desired customer location(s) available.

**Note**: As a reminder, you must first register in the Axcient x360Recover Licensing Portal to create customers and locations. If no customers or locations display, this means that no customer accounts within the Licensing Portal exist that have an unallocated location.

If you need help setting up a customer account or identifying the locations available in the licensing portal, please review these instructions for using the [Axcient x360Recover Licensing Portal.](https://axcient.helpjuice.com/001-install-agents/115006560127-x360Recover-How-to-set-up-initial-storage-pool-configuration" \t "_blank)

Click the **Next** button to proceed.

Complete the network setup

STEP 9. The network Setup screen appears.



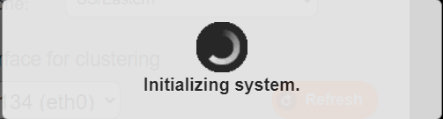
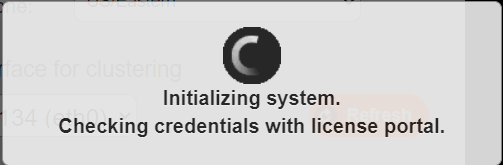
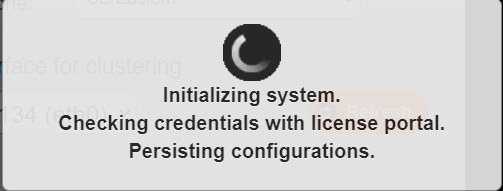
* Select the appropriate **Time Zone.**
* **Select a Network interface for clustering** with a valid DHCP IP address.

By default, Axcient x360Recover is configured for DHCP.

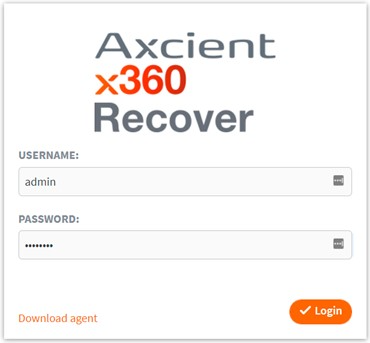
* Click **Setup** to continue.

STEP 10. Your device and role assignment selections will be saved, and the device setup will be completed.

* You will see the screens below, indicating that the system is being initialized.
* Once initialization has completed, the device will reboot automatically one last time.

* When reboot completes and the browser refreshes, the login page appears.
* You will now need to complete the steps for first-time login.



**Note**: The login page may appear before the device has rebooted, but you will not be able to log in until the reboot has been completed. This may take several minutes on some systems.

If you receive an error that the user is not authorized for login, wait two minutes, and try again.

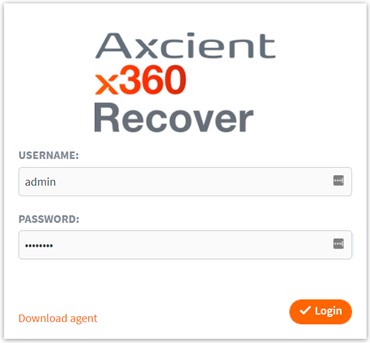
**First-time login**

Log in and complete configuration

STEP 1. Once the machine has rebooted, log in and complete configuring settings.

* In the **Username**field, enter the default username which is ‘admin.’
* In the **Password**field, enter the password you provided for the Admin (Web GUI) user during the setup and configuration process.

Click **Login** to continue.

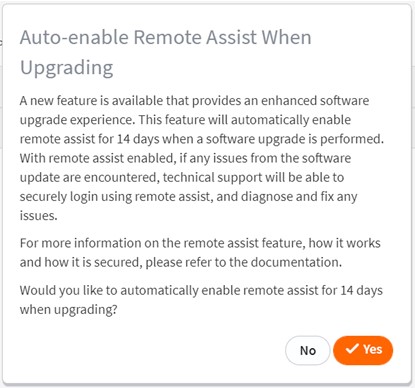


Enable Remote Assist

On the initial login, you will be presented with the option to automatically enable[**Remote Assist**](https://axcient.helpjuice.com/x360recover-duplicates/360015367054-x360Recover-System-ID-and-Remote-Assist-overview) after applying updates.

**Ancients recommend enabling this feature.**(See below for notes.)

Click **Yes** or **No**.



**Note:** When this option is enabled, the [**Remote Assist**feature](https://axcient.helpjuice.com/x360recover-duplicates/360015367054-x360Recover-System-ID-and-Remote-Assist-overview) will automatically be enabled for 14 days after an upgrade is deployed.

**Axcients recommend enabling this feature.**

If something goes wrong during an update, it may not be possible to access the UI to enable Remote Assist later.

Enabling Remote Assist now, during setup, will allow Axcient Support to proactively access failed devices after an upgrade and resolve problems.

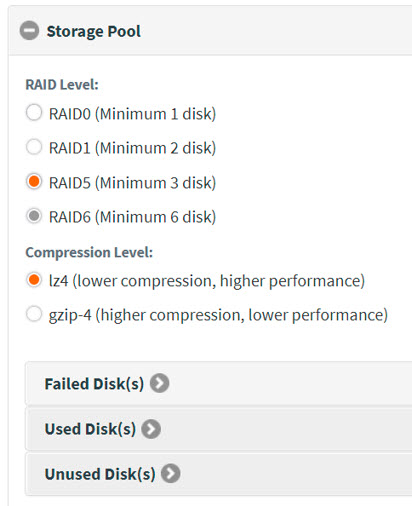
* **Configure the storage pool**

Once you have enabled **Remote Assist**, you must configure the storage pool.

[**[For first-time setup of the storage pool, refer to this KB article.]**](https://axcient.helpjuice.com/001-install-agents/115006560127-x360Recover-How-to-set-up-initial-storage-pool-configuration)

STEP 1. Expand the storage pool configuration section.

* Select the desired**RAID Level.**[(More about RAID here:)](https://axcient.helpjuice.com/005-backup/360020225494-x360Recover-What-is-RAID)
* Select the desired **Compression** **Level.**

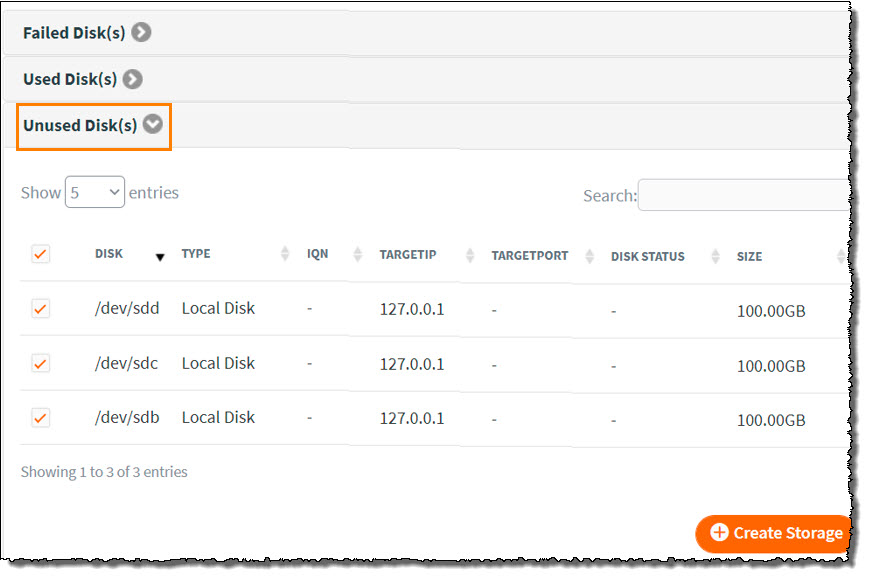


STEP 2. Expand the**Unused Disks**section.

Select the available drives.

Click **Create Storage** to create the storage pool.

For complete details on first-time setup of the storage pool, refer to this [KB article.](https://help.axcient.com/001-install-agents/115006560127-x360Recover-How-to-set-up-initial-storage-pool-configuration)



**Finishing up**

Once the storage pool is created, there are a few more items to configure before deploying x360Recover agents and beginning backups.

**A screenshot of a computer license

Description automatically generated with low confidence**

**Check licenses**

Click **System Settings** from the left menu pane

Expand **License Details:**

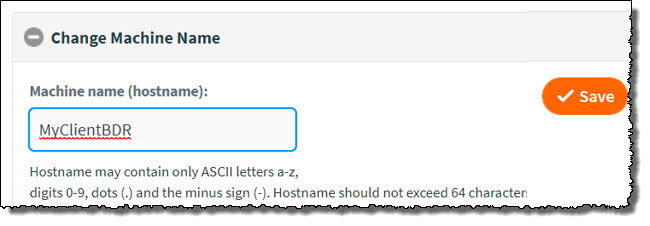
Verify that licenses have been correctly assigned.

If no licenses have been assigned to this appliance, visit the License Portal and assign the appropriate licensing to this customer account location.

After you assign the appropriate licensing to this customer account location, return to the appliance, and click **Sync** to immediately retrieve the License Portal changes.

Set machine name

* Create a friendly name for this backup server that will identify the device.
* Click **System Settings**from the left menu pane.
* Expand **Change Machine Name**
* Enter a friendly name in the **Machine Name** field and click **Save.**

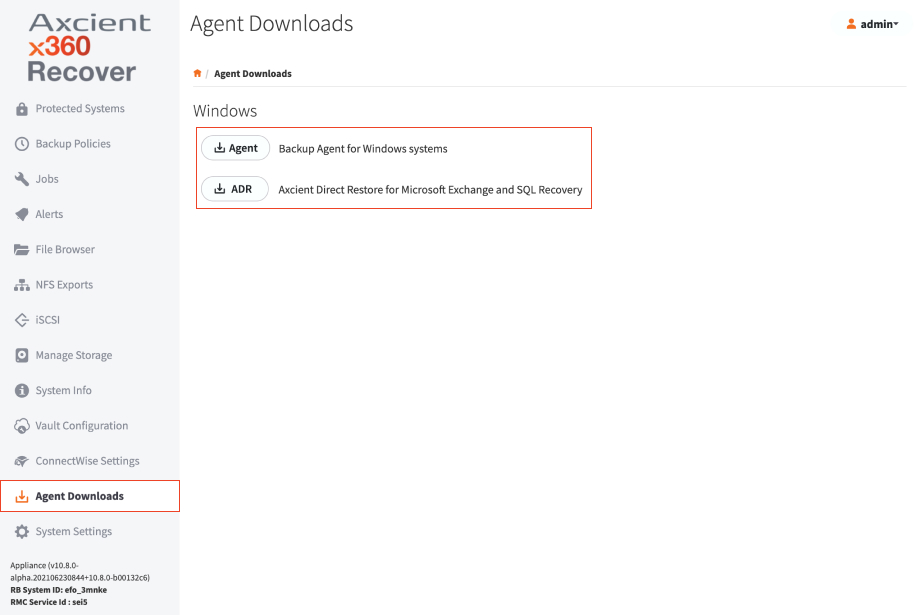
****

**Ready to deploy x360Recover agents**

You are now ready to begin deploying x360Recover agents and performing backups of your client protected systems.

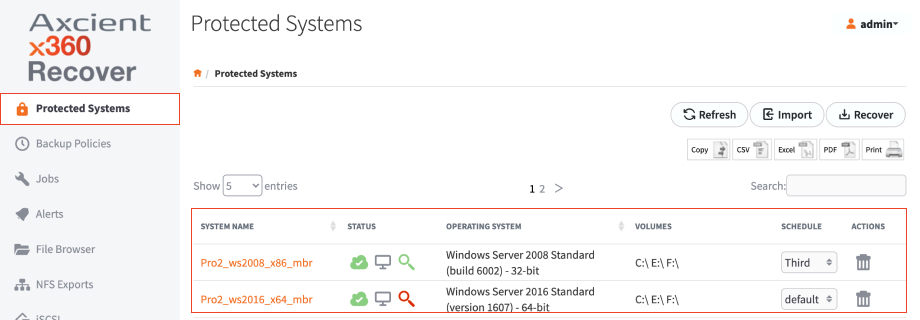
Step1: In the lefthand navigation, click**Agent Downloads**.

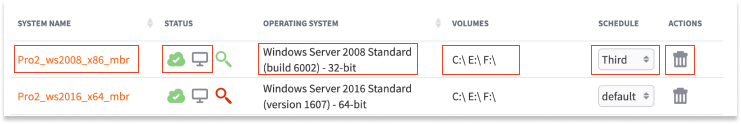
Step2: You will now be able to view and download agents and other components.



**To manage protected systems in the appliance**:

1. In the appliance left hand navigation, click on**Protected** **Systems.**You will see a list of the systems currently being backed up and protected by the appliance.



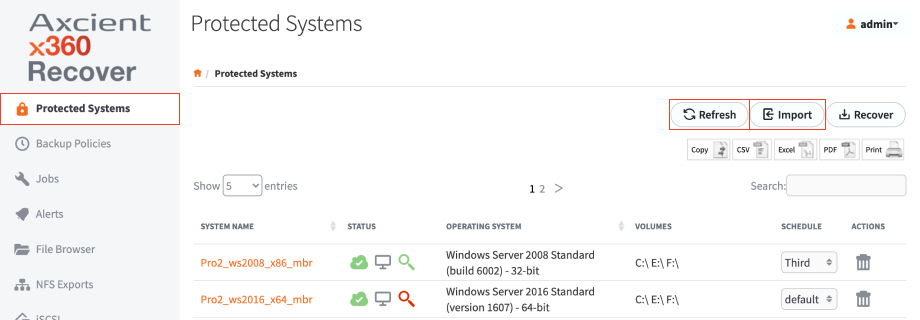
2. Use the controls to manage protected systems:

* The Status column displays icons that indicate whether the system is currently running as a virtual machine (the first icon will be green) and whether replication is enabled for the system. (The second icon will be blue).
* System Name (Hostname), Operating System, and Currently Protected Volumes (disk volumes), are listed for identification and information.
* The Schedule column contains a dropdown list of available backup schedules. The assigned schedule displays. To change schedules, click the **dropdown** and select the preferred schedule. For more information, please review the [Managing Schedules for Backup Jobs](https://help.axcient.com/001b-manage-appliances/115006586307-x360Recover-How-to-manage-schedules-for-backup-jobs-of-protected-systems) article
* The Actions column allows you to delete or view the details of a protected system.

**NOTE: Selecting Delete will prompt for the permanent deletion and removal of the protected system and all recovery points. Deleted systems are placed in a safety archive until removed via [AirGap](https://axcient.helpjuice.com/05-recover/airgap?from_search=71227229" \t "_blank) policy.**

Selecting the **Details** button will open the Protected System Details page, which contains many additional system specific configuration options

3. Click **Refresh** to update the display view with any newly discovered protected systems.



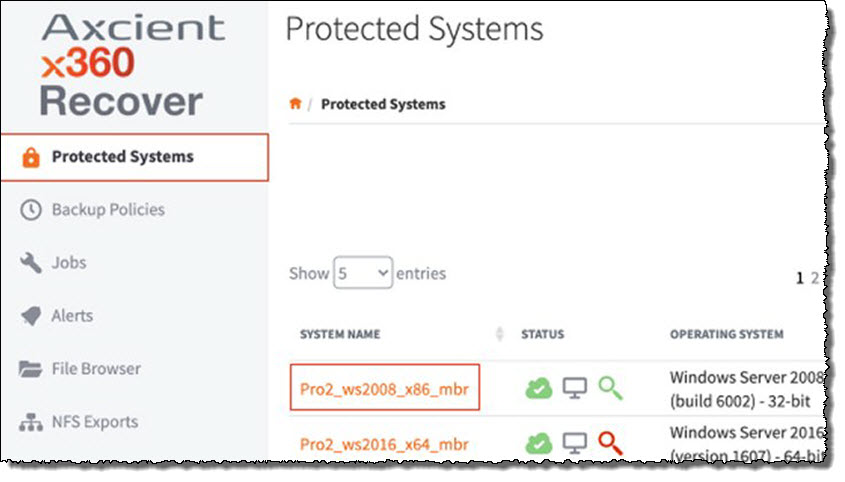
4. Click **Import** to retrieve protected systems being migrated or recovered via USB media and import the related data.

# Enable nightly boot checks of a protected system- x360Recover BDR

To enable nightly Boot VM checks of a protected system, follow these steps:

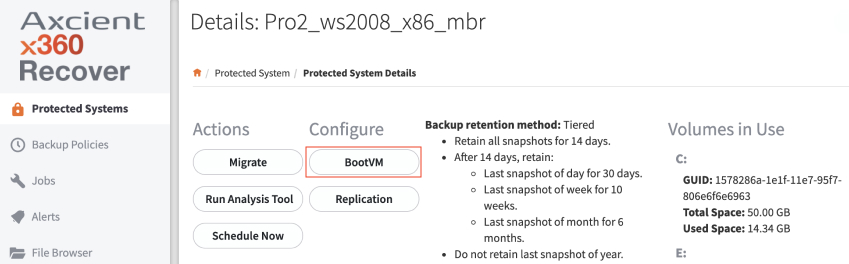
**STEP 1.** In the left navigation, select the **Protected Systems** tab.

You will see a list of the systems currently being backed up and protected by the appliance.

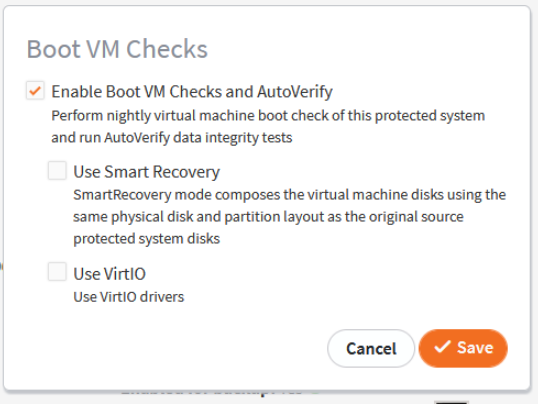


**STEP 2**. Click the appropriate **System Name** to launch the *Protected Systems Details* page.

**STEP 3**. In the *Protected Systems Details* page, click the **Boot VM** button.

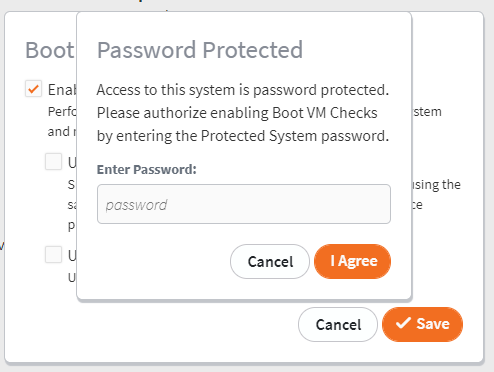


**STEP 4**. Check the box with the **Enable Boot VM Checks and Auto verify** option.

When the **Enable Boot VM Checks and Auto verify** option is enabled, the appliance will perform a nightly virtual boot of the protected system, using the most recent recovery point, and then take a screenshot of the running system.  


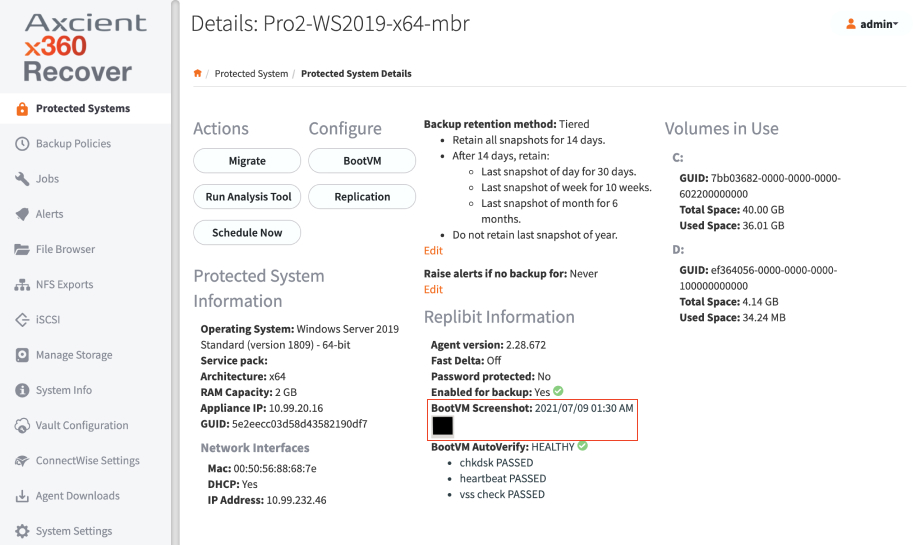
Click **Save** to continue.

If an encryption passphrase was specified when deploying the agent to the protected system, the **Password Protected** prompt displays:



Enter the **Encryption Password** and click the **I Agree** button to continue.

Back in the *Protected System Details* page, the most recent screenshot image can be viewed by clicking the **BootVM Screenshot** button.



**AutoVerify operations**

As of x360Recover v8.3.0, BootVM AutoVerify performs the following operations to validate each protected system snapshot status:

**Heartbeat**

The appliance verifies basic communications with the running virtual machine, and if not established, fails the check. This operation confirms that the system was able to fully boot the operating system, start services, and complete plug-n-play device discovery

**Check Disk** ([chkdsk)](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/chkdsk)

A Windows ‘chkdsk’ operation (using a Windows utility that checks the integrity of a file system) is performed on each volume within the protected system.

* ‘chkdsk’ may fail due to the following conditions:

Corrupted or incomplete backup snapshot on the BDR appliance.  
(A new full backup will likely resolve the issue)

File system corruption on the source protected system disk(s).  
(‘chkdsk’ should be run on the protected system to fix the disk problem)

* If chkdsk exits with specific errors codes that indicate possible data consistency issues, the appliance attempts to resolve the issue by performing a new full scan of the protected system and an alert is generated on the appliance. Alerts generated by AutoVerify are automatically closed after the full scan completes.
* Note: Full scans generated by AutoVerify will occur no more than once every 30 day

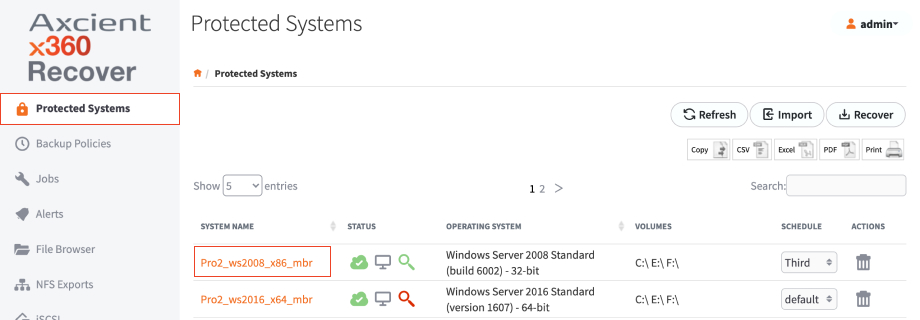
Note: ‘Self-heal’ full backups are disabled in the initial release

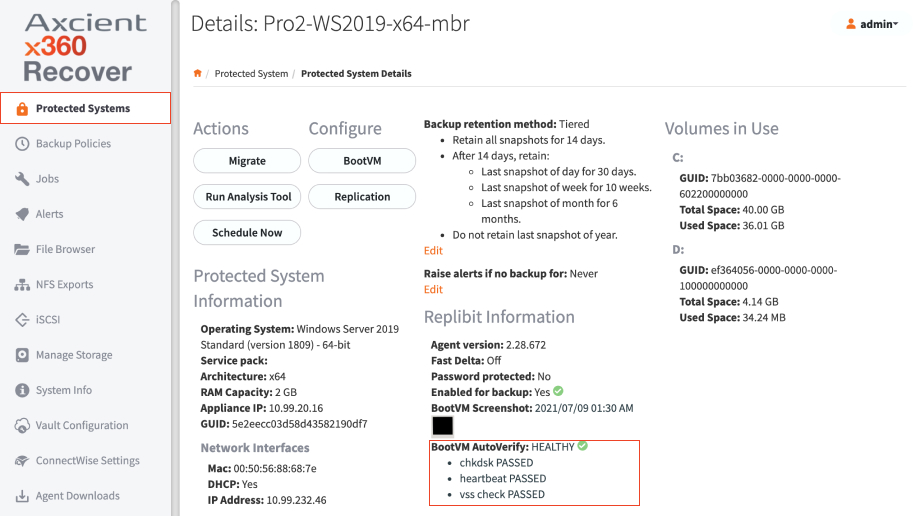
BootVM checks automatically allocate RAM dynamically to the virtual machine during testing. One quarter of available RAM is allocated to the VM, with a minimum of 2GB and a maximum of 12GB, to ensure sufficient resources to complete the AutoVerify operations.

Boot VM checks end automatically. The appliance monitors the status of the AutoVerify operations and the virtual machine will be shut down as soon as all checks are complete. Note: Maximum virtual machine run time is 90 minutes (about 1 and a half hours), and the AutoVerify operation will fail if not completed by then.

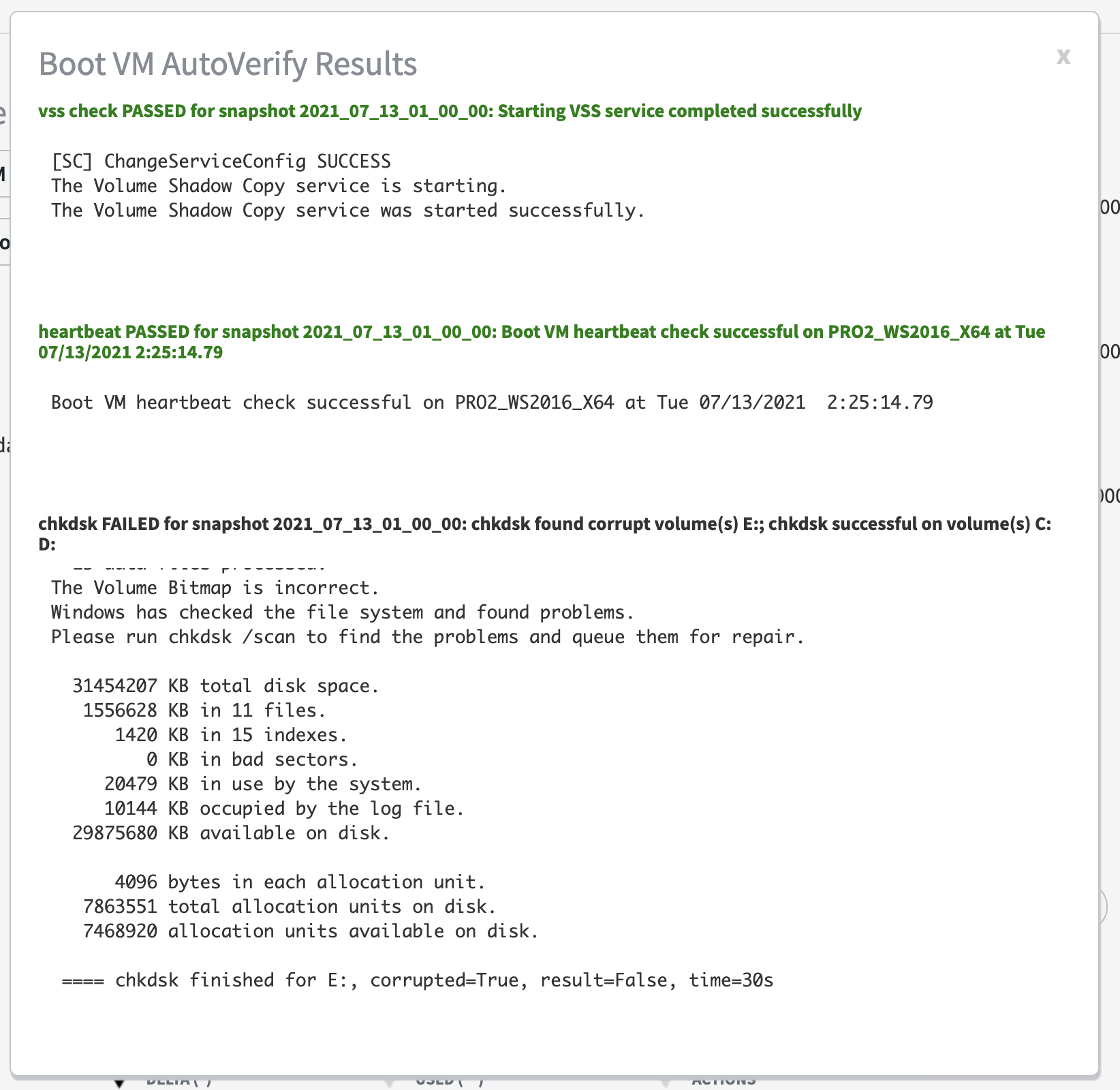
**AutoVerify results**

AutoVerify results, including complete heartbeat and ‘chkdsk’ details, are available on the protected systems *Details* page within the appliance.





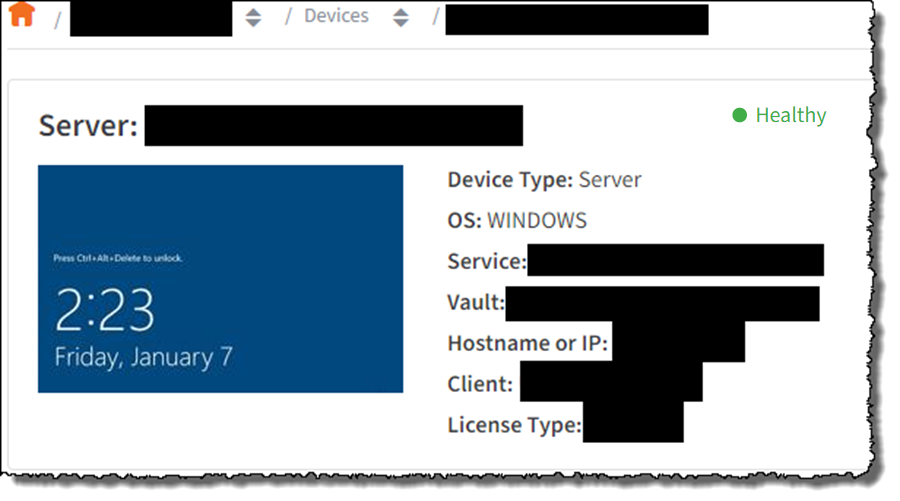
Clicking on the AutoVerify results provides BootVM AutoVerify complete details on all operations:



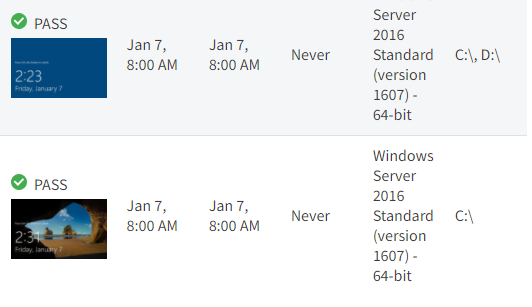
AutoVerify Global Monitoring

In addition to appliance-level alerting, AutoVerify has been integrated into x360 Recover Manager reporting. This means you can easily see AutoVerify operations across all of your appliances and protected systems.  
   
A summary of AutoVerify operations exists in two places:

1. On the *Devices* page:



2. On the Backup summary report:



# Backup policies (schedules)

How will you use an x360Recover backup policy?

First, you'll create backup policies (schedules) and apply these for each customer. Backup policies should be in place before the agent performs a backup and sends that backup to the local appliance.

Then, you'll install the x360Recover agent software on a protected system.

**Backup policy types**

When you create a backup policy, you define two types of backups: ·

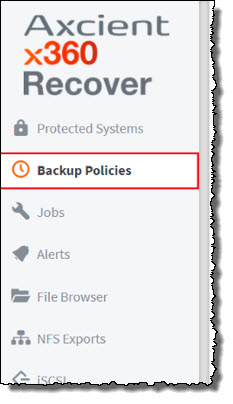
The **initial backup** (full backup) which copies *all* sectors of the image.

The **incremental backups** (snapshots) which *only* copy anything that has changed, saving time and disk space.

Note: You can't schedule an incremental backup unless you have completed the initial (full) backup. Because x360Recover is chain-free, snapshots are not dependent on previous snapshots.

**Where do you find the backup policy settings?**

The **Backup Policies** tab in the left menu pane is where you set up these policies.



When creating a policy-based backup schedule, you first designate which days of the week and hours of the day are considered business hours.

Then, you define the backup parameters. For each time frame, you'll select an incremental backup frequency and decide whether full backups will run during this window.

**Steps to create a backup policy**

**How to create a policy-based schedule**

1. Log in to the appliance or vault

2. Navigate to the *Backup Policies* page.

3. Click **Add Policy** to create a new backup schedule. Optionally, click **Edit** to edit an existing schedule.

Note: Existing classic backup schedules may be edited and converted to new, advanced policy-based schedules.

4, Enter a name for the new schedule and select **Policy-Based Schedule** to choose the new advanced schedule type.

5. Check the **Enabled** check box to enable the policy. Optionally, you may set this schedule to be the system default and enter a description for the schedule.

6. Expand the **Business Hours** dropdown menu and select the desired days of the week and the hours of each day. These choices are now considered the designated business hours. Note that any remaining times *outside* this time window will be considered **non-business hours**.

7. Expand the **Backup Schedule** dropdown menu and set the desired backup parameters for both business and non-business hour timeframes:

The **Interval** parameter (frequency of incremental backups) may be set to **None.**

The **Allow Full Backups** parameter may be enabled or disabled for either timeframe

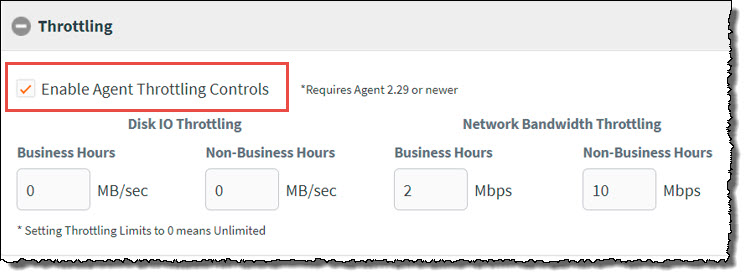
Note: You cannot (a) set *BOTH* timeframes to **None** and/or (b) disable all full backups. This is because the incremental and full backups MUST be allowed to run sometime during the week.

**Agent throttling**

## **Specify agent throttling**

Throttling allows you to control the maximum disk I/O and network bandwidth consumed by the agent during a backup within each time frame.

To set up the agent throttling settings, expand the **Throttling** dropdown menu and click the **Enable Agent Throttling Controls** checkbox.



Note that the throttling control requires agent 2.29 or newer to be effective.

**Disk I/O** is expressed in MB/sec (Megabytes per second). This is the maximum rate at which data will be read from each disk volume in the protected system. Note that the limit is applied to each volume separately: This is *not* a limit on total disk I/O overall, but each volume separately.

Setting a disk I/O limit can be useful if your protected system is a virtual machine or has otherwise slow storage drives which impact users during backup operations.

**Network bandwidth** is expressed in Mb/sec (Mega*bits* per second). This is the total maximum network transmit speed allowed to the agent when transferring data to the server. Unlike Disk I/O throttling, network bandwidth throttling is applied as an *overall* total, regardless of how many disk volumes are in the system.

Network bandwidth throttling is effective in reducing user impact on internet access performance due to Direct-to-Cloud (D2C) Cloud backup operations.

You can specify different limits to be applied during each timeframe, based on whether this falls within business or non-business hours.

Setting a throttling value of 0 (zero) sets the limit to *unlimited*.

Once all settings have been configured, click **Save** to complete the changes to the backup schedule.

## **Update existing schedules**

Traditional Classic schedules, including manual schedules, are still supported.

|  |
| --- |
| Note: Existing classic backup schedules are not affected by the change to the new engine. It is still possible to create and manage your existing classic schedules.  To take advantage of the new policy features available with business hour scheduling login, you must create a new policy-based schedule and assign it to your protected systems. |

1. Log in to the appliance or vault

To apply a new **Business Hours** backup schedule to existing protected systems:

Navigate to the *Protected Systems* page and select the desired schedule from the **Schedule** column:

To create or edit a traditional Classic schedule for your protected systems, select **Classic Schedule** in the *Edit Schedule* page of the **Backup Policies** tab:

As an alternative to creating and applying a new schedule to each protected system, you can simply convert the currently applied classic schedule to a policy-based schedule, by editing the **Backup Schedule Type.**

**To create a backup policy:**

1. Log in to the vault web interface.

2. In the left-hand navigation menu, click the *Backup Policies* tab.

3. In the *Schedules* page, click the **Add Policy** button.

4. In the *Create Schedule* page, enter information about the new backup policy:

In the *Name* field, enter a **descriptive name** for the backup policy. For example, you might create a backup policy titled *Critical* for servers requiring 15-minute incremental backups; and *non-Critical* for servers that only require incremental backups every hour.

Ensure the *Enabled* checkbox is selected to activate this new backup policy. If the backup policy is not enabled but later assigned to a protected system, backups for the protected system will be disabled.

Optionally, click the **Default** checkbox to assign this backup policy as the default backup policy for all protected systems.

Choose a backup schedule type: either Classic or Policy-based.

If a **description** of this backup schedule type is needed, enter that information here.

Open the *Backup Schedule* dropdown menu.

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.

In the *Incremental Backup* section, you can optionally use the drop-down menu to change the incremental backup type from *Interval* to *Manual*. The *Manual* setting allows you to create snapshots at specific times instead of intervals.

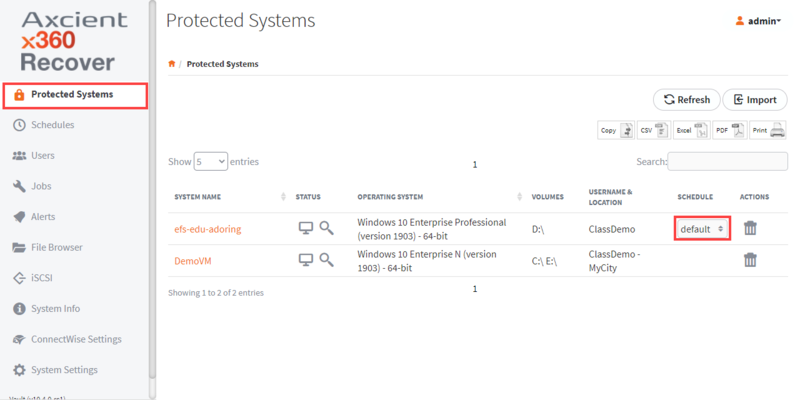
If you selected **Interval** in the drop-down menu, define a **Start Time**, **End Time**, and **Interval** for all future incremental backups.

Click the **Save** button when you are finished. The backup policy is now created and will be listed in the *Schedules* page. You can manage and edit backup policies in the *Schedules* page.

5. After the backup policy is created, you can assign the backup policy to a protected system.

a. In the left-hand navigation menu, click the **Protected Systems** tab.

b. Find the desired protected system and use the *Schedule* drop-down menu to select the appropriate **Schedule**. The schedule is now assigned to the protected system.



**Here the KB Articles for more details:**

**Agent Appliance Setup:**

<https://help.axcient.com/001-install-agents/appliance-setup-and-first-time-login-x360recover>

**Set up initial storage pool configuration - x360Recover – BDR:**

<https://help.axcient.com/001-install-agents/115006560127-x360Recover-How-to-set-up-initial-storage-pool-configuration>