

The background features several large, overlapping, rounded geometric shapes in various shades of orange and red, creating a dynamic and modern aesthetic.

Axcient

Replibit Management
Guide

axcient.com

Customer Support

At Axcient, we want to help you quickly resolve your technical issues. If you need assistance, please contact our Technical Support team.

- Call: 720-204-4500
- Submit a Ticket: [Axcient Support](#)
- Learn More: [Replibit Knowledgebase](#)

Table of Contents

Introduction	5
Managing your Appliances, Vaults, and Protected Systems with the Global Management Portal...6	
Accessing the Global Management Portal.....6	
Hosting the Global Management Portal in a Private Cloud Datacenter.....6	
Logging in to the Global Management Portal.....6	
Connecting Appliances and Vaults to the Global Management Portal.....7	
Option 1: Copy the Existing API Key	7
Option 2: Generate a New API Key.....7	
Accessing Reports with the Global Management Portal.....10	
Viewing the GMP Dashboard	10
Monitoring Appliances and Vaults using the Managed Systems Page.....11	
Monitoring Protected System Backups with the Backup Status Page.....14	
Monitoring Protected System Replication with the Replication Status Page.....16	
Identifying Problems with the Trouble Report.....17	
Verifying the Status of Devices with the Health Report.....20	
Managing Storage Usage with the Storage Report	21
Monitoring Your Protected Systems with the Boot VM Report	22
Managing Reports and Central Alerting.....24	
Configuring Global Management Portal Settings with the Settings Tab.....27	
Integrating with ConnectWise	32
Configuring ConnectWise for Third-Party Integration.....32	
Configuring ConnectWise Settings in Replibit.....32	
Managing Replibit Licenses.....35	
Adding Licenses.....35	
Removing Licenses.....37	
Managing Protected Systems.....39	
Viewing Protected Systems.....39	

Modifying the Configuration File40

Deleting a Protected System.....43

Managing Appliances45

 Monitoring Alerts in the Appliance Web Interface.....45

 Viewing Storage Settings for the Appliance48

 Managing Failed Disks51

 Expanding the Storage Pool.....52

 Managing iSCSI Storage53

 Viewing Appliance System Information54

Managing Vaults58

 Monitoring Alerts in the Vault Web Interface.....58

 Viewing Vault System Information61

Introduction

Axcient Replibit is a patented, Chain-Free™, end-to-end Backup and Disaster Recovery (BDR) platform. Replibit empowers MSPs to deliver profitable, globally managed business continuity services. As a Replibit partner, you will protect all 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.

After you complete the Replibit installation processes, you can manage and monitor your Appliances, Vaults, and Protected Systems. You will perform the majority of these Replibit management tasks within the Global Management Portal (or GMP). This guide outlines common management tasks, including:

- Managing with the Global Management Portal,
- Managing Protected Systems,
- Managing Appliances, and
- Managing Vaults.

Managing your Appliances, Vaults, and Protected Systems with the Global Management Portal

The Global Management Portal (GMP) is a stand-alone, multitenant portal that allows for centralized management of your Appliances and Vaults and provides a single-pane-of-glass view of device status and Protected System backups. The GMP allows you to:

- View dashboard and reporting details for all Customers you support,
- Remotely access all connected Appliances, Vaults, and their Protected Systems,
- Perform Health Checks, which provide a global overview of all Protected Systems in one single dashboard,
- Perform Trouble Checks, which display active issues associated with Vaults, Appliances, or Protected Systems in a single dashboard,
- Review detailed reports on active issues needing investigation and root-cause analysis,
- Access Storage Management, which provides a graphical representation of historical storage utilization, and
- Schedule and deliver reports through email.

Accessing the Global Management Portal

If you choose to replicate to the Axcient Storage Cloud, you will receive a GMP virtual machine in the Axcient cloud free of charge. Alternatively, if you are utilizing the GMP in a Private Cloud datacenter, you will be responsible for all hosting responsibilities.


Hosting the Global Management Portal in a Private Cloud Datacenter

Most Private Cloud partners run the GMP as a virtual machine for simple administration and management as it requires very few resources to monitor.

You can use the most current [Replibit.iso](#) file to install the GMP; you do *not* need to modify your firewall at the Customer location. For instructions on installing the Replibit Global Management Portal, please contact Axcient Support.

Logging in to the Global Management Portal

1. Open any web browser and navigate to the Global Management Portal.



<https://rb-edandt-mgmt.rb.sl.c.efscloud.net/login>

1. In the *Replibit Global Management Portal* page, enter your credentials:
 - In the *Username field*, enter the Username or the Partner Account Username that you received during your onboarding process.
 - In the *Password field*, enter the Password.
2. Click the **Login** button.



Connecting Appliances and Vaults to the Global Management Portal

Before you can begin utilizing the GMP to track and monitor Managed Devices, you will need to first connect each Appliance and Vault that you would like to manage in the Global Management Portal.

This integration process requires an API Key that is displayed on the *Users* page of the GMP. This API key will integrate each Appliance and Vault with the GMP.

You can generate API keys in one of two ways:

Option 1: Copy the Existing API Key

In most cases, you will simply copy the *admin API key* that is automatically generated for the GMP admin user during the provisioning process and is displayed in the *Users* page of the GMP.

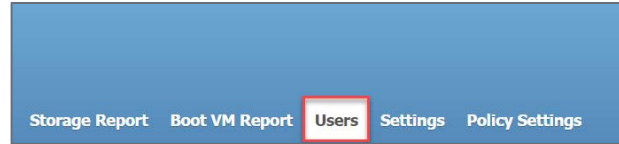
Note: This method is the most common option practiced by our partners.

Option 2: Generate a New API Key

For advanced management purposes, you can optionally generate a new API key for each Customer you support. This approach is useful if you plan to give your Customers login access to the GMP. When a Customer logs in to the GMP using his or her unique username and password, the GMP will display a filtered view of the Customer's Managed and Protected Systems.

To use a previously generated API key (Option 1):

1. In the Global Management Portal, click the **Users** tab. The *Users* page displays, showing a list of any previously generated API keys.



At a minimum, the *admin API key* will be listed, as it is automatically generated for the GMP admin during the provisioning process.

2. Copy the API key listed in the *API Key* column for the appropriate *User*.

Name	Role	API Key
admin	admin	[API Key]
customer2	customer	[API Key]

3. When you have recorded the appropriate API key, you can log in to each Appliance and Vault Web interface and paste the API key into the *API Key* field.

- Log in to the appropriate Web interface (Appliance or Vault).
- Click the **Settings** tab.
- In the *Settings* page, click to expand the **Management Portal** tab. The *Management Portal* section displays.



4. In the *Management Portal* section, enter API details:
 - In the *IP Address* field, enter FQDN of the Global Management Portal.
 - In the *Username* field, enter the *Username* associated with the API key.
 - In the *API Key* field, enter the *API key*.

IP Address:

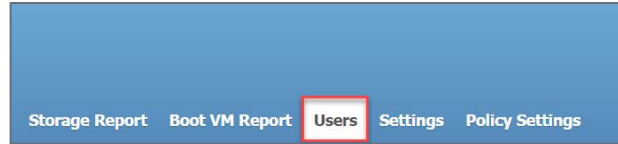
Username:

API Key:

5. Click the **Save** button to save your changes.

To generate a *new* API key (Option 2):

1. In the Global Management Portal, click the **Users** tab.



The *Users* page appears, showing a list of any previously generated API keys.

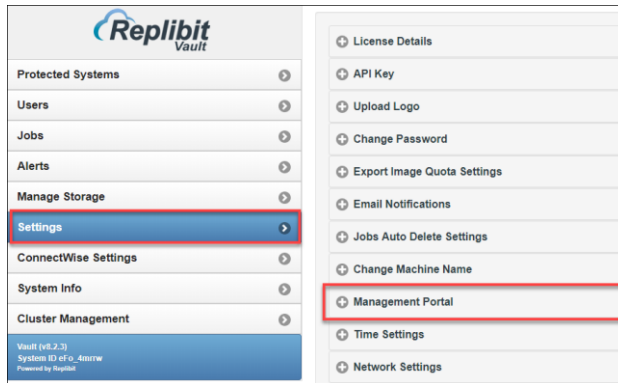
2. In the *Users* page, click the **Add** button and create a new user, which will be associated with a new API key:



- In the *Username* field, enter a **unique username** for this new user.
- In the *Password* field, enter a **complex password** for the user.
- In the *Role* field, select **Customer** to indicate that this is a Customer user.
- Click the **Submit** button to save your changes. The system will generate a new API key.

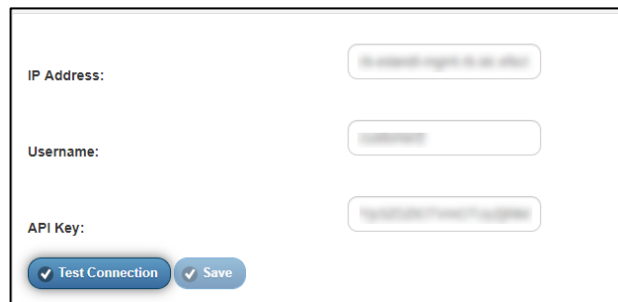
3. Copy the newly generated API key.
4. When you have recorded the appropriate API key, log in to each Appliance and Vault Web interface and paste the API key into the *API Key* field.

- In the Web interface, click the **Settings** tab.
- In the *Settings* page, click to expand the **Management Portal** tab.



5. In the *Management Portal* section, enter API details:

- In the *IP Address* field, enter the **FQDN** of the Global Management Portal.
- In the *Username* field, enter the **Username** associated with the API key generated in the steps above.



- In the *API Key* field, enter the **API key** generated in the steps above.
6. Click the **Save** button to save your changes.

Note: Managed Devices check in with the GMP once every hour. Each partner's sync time is offset by a random interval sometime within the hour. It may take up to two hours for new Managed Devices to completely sync their data with the GMP.

Accessing Reports with the Global Management Portal

When you have successfully integrated your Managed Devices (Appliances and Vaults) with the Global Management Portal, you can actively monitor, manage, and remotely access these devices.

After logging in to the GMP, you will be presented with a main navigation menu with a series of tabs. These tabs will allow you to navigate to all the reports and tools needed to monitor and manage your BDR processes effectively and efficiently.

Viewing the GMP Dashboard

You can reference the Global Management Portal *Dashboard* page for a quick count of your devices, organized by type.

Total Appliance 1	Total Vault 1	Total Managed Systems 2
Total Servers 0	Total Workstations 2	Total Protected Systems 2

To view the *Dashboard* page:

1. In the GMP, click the Dashboard tab.

The *Dashboard* page displays a listing of the number of Managed and Protected Systems connected to the GMP.



2. Use the Dashboard to view a count of Managed and Protected Systems, including:

- Total Appliances,
- Total Vaults,
- Total Managed Systems,
- Total servers,
- Total workstations, and
- Total Protected Systems.

Total Appliances	Total Vault	Total Managed Systems
1	1	2
Total Servers	Total Workstations	Total Protected Systems
0	2	2

Monitoring Appliances and Vaults using the Managed Systems Page

The *Managed Systems* page displays details of all connected Appliances and Vaults. You can use this page to track the details of each Appliance and Vault connected to the GMP.

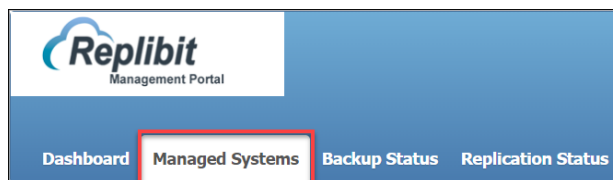
For example, you can use the *Version* column to ensure each Managed System is running the latest version of the Replibit software. You can also use the *Stats Time* column to verify that each Protected System is actively checking in with the GMP.

System ID	System Name	Version	IP Address	Management Port	Customer	Location	Stats Time	License						Actions
								Servers		Workstations		Storage		
								Used	Total	Used	Total	Used	Total	
dat_bdd7	ClassDemo	8.3.0+12	192.168.1.21	10000	ClassDemo	MyCity	Tue 06-18-19 01:00 PM	0	0	2	2	N/A	N/A	[P] [A] [M] [R] [E]
dat_7aa3	Vault1	8.3.0+12	10.2.68.35	10001	dataprotection	N/A	Tue 06-18-19 01:00 PM	N/A	N/A	N/A	N/A	N/A	N/A	[P] [A] [M] [R] [E]

To view the *Managed Systems* page:

1. In the GMP, click the Managed Systems tab.

The *Managed Systems* page displays, providing details of each Managed System connected to the GMP.



2. Use the *Managed Systems* columns to view system details about each Managed System. For example:
 - The *System ID* column displays the unique ID assigned to the device to help Technical Support connect via the Remote Assist feature.
 - The *System Name* column displays the name assigned to the system for identification purposes.
 - The *Version* column displays the version of Replibit software installed on a specific device. You should periodically verify that all devices have been updated to the latest software.
 - The *IP Address* column displays the local IP address allocated for your device.
 - The *Management Port* column shows the firewall port opened for the GMP. (HTTPS Connections to the GMP's URL are redirected to the Managed Device over a secure tunnel.)
 - The *Customer* column displays the Licensing Portal customer account to which the device is assigned.
 - The *Stats Time* column represents the current timeframe for the statistics shown for this device. The time should be less than two hours old (indicating that they are online and have recently reported in to the GMP).
3. Optionally, click a **column header** to sort by field. You can then click again to reverse the sort order.

The screenshot shows the Replibit Management Portal interface. The 'Managed Systems' tab is active. A table displays the following data:

System ID	System Name	Version	IP Address	Management Port	Customer	Location	Stats Time
04c_34607	ClassZero	9.2.3	192.168.1.21	10000	ClassZero	PH/Chy	Sun 05:45:14 01:00 PM
04c_71463	7x6E1	9.2.3	192.168.30	10001	detaportnet	N/A	Sun 05:45:14 01:00 PM

4. Use the *License* section of the page to view license information for each Managed System. For example, you can view a count of:

License					
Servers		Workstations		Storage	
Used	Total	Used	Total	Used	Total
0	0	2	2	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A

- Server licenses consumed,
- Workstation license consumed, and
- Storage consumed.

5. Use the *Actions* section of the page to actively control Managed Systems. For example:







- Click the **Remote** button to launch the Web interface of the Managed System within a new browser window.
- Click the **Terminal** button to launch the Managed System terminal within a new browser window.
- Click the **History** button to view historical information about the system, including *Stats Time* information and *License* usage over time.
- Click the **Systems** button to launch the *Backup Status* page, providing information about the Protected Systems connected to the selected Managed System. This page provides details of the latest backup and disk usage for each Protected System.
- Click the **Delete** button to delete the Managed System from the Global Management Portal.

Note: If you delete a Managed System currently connected to the Global Management Portal, settings will be cleared from the *Management Portal* page (accessible from the *Settings* tab) on the selected device. Deleting a Managed System will also delete all Protected Systems belonging to the device and their

associated metadata from the Global Management Portal database. If you do *not* have a means to connect directly to the Managed System Web interface (for example, through VPN or other remote access to the Customer network), you will no longer have access to the Managed System after deleting it from the Management Portal.

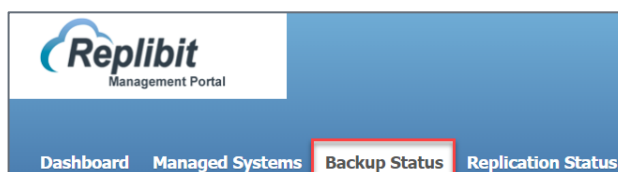
Monitoring Protected System Backups with the Backup Status Page





The *Backup Status* report provides a detailed list of Protected Systems. You can use this report to centrally monitor each Protected System in your environment. For example, you can track disk usage and backup status. Using the *Agent Version* column, you can confirm that the latest Replibit Agent is installed on the Protected System.

PS Name	OS Name	IP Address		Disk Usage			Agent Version	Agent Status	Last Backup Time	Actions
		Self	Appliance	Total	Used	Appliance				
efs-train-rklem	Microsoft Windows 10 (build 17134), 64-bit	192.168.253.137, 192.168.1.25, 192.168.56.1, 10.2.32.126	ClassDemo (192.168.1.21)	229.31G	197.09G	356.63G	2.23.191	✓	05/17/2019 07:00 AM	 
DemoVM	Microsoft Windows 10 (build 17134), 64-bit	192.168.1.26	ClassDemo (192.168.1.21)	34.00G	18.60G	31.71G	2.23.191	✓	05/16/2019 05:30 PM	 

To monitor Protected Systems using the *Backup Status* report:

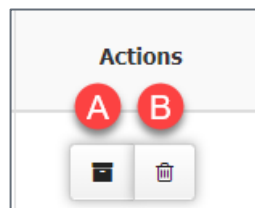
- In the GMP, click the **Backup Status** tab. The *Backup Status* report displays, providing details of each Protected System.
- Use the columns to view system details about each Protected System. For example:
 - The *PS Name* column identifies the name of the Protected System.
 - The *OS Name* column lists the Operating System name and version.
 - The *IP Address* section displays the IP address of both the Protected System and its Appliance.
 - The *Disk Usage* section displays the total and used disk usage for the



PS Name	OS Name	IP Address		Disk Usage			Agent Version	Agent Status	Last Backup Time	Actions
		Self	Appliance	Total	Used	Appliance				
efs-train-rklem	Microsoft Windows 10 (build 17134), 64-bit	192.168.253.137, 192.168.1.25, 192.168.56.1, 10.2.32.126	ClassDemo (192.168.1.21)	229.31G	197.09G	356.63G	2.23.191	✓	05/17/2019 07:00 AM	 
DemoVM	Microsoft Windows 10 (build 17134), 64-bit	192.168.1.26	ClassDemo (192.168.1.21)	34.00G	18.60G	31.71G	2.23.191	✓	05/16/2019 05:30 PM	 

Protected System. This section also displays disk usage of the Appliance.

- The *Agent Version* column displays the version of the Replibit Agent installed on the Protected System. You can reference this column to ensure each device is protected with the latest version of the Replibit Agent.
 - The *Agent Status* column reports whether the Replibit Agent is active on the Protected System.
 - The *Last Backup Time* column displays the time and date of the latest backup on the Protected System.
3. Optionally, click a **column header** to sort by field. You can then click again to reverse the sort order.
 4. Use the *Actions* section of the page to actively control Protected Systems. For example:
 - A. Click the **History** button to view historical backup information for the Protected System, including the *Agent Status* and *Last Backup Time*.
 - B. Click the **Delete** button to delete the Protected System from the Global Management Portal.



Note: Deleted Protected Systems that still exist on the managed device will be re-registered within the GMP during the next sync cycle, but previous historical metadata will be lost.

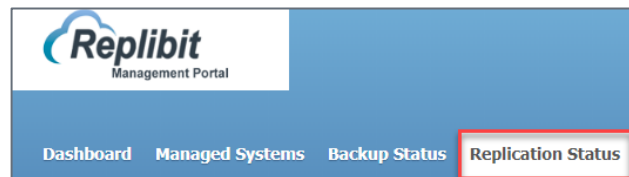
Monitoring Protected System Replication with the Replication Status Page

The *Replication Status* page lists the replication status of each Protected System, including off-site storage utilization, replication status, and last replication time.

PS Name	OS Name	IP Address			Disk Usage			Replication Status	Last Ingested Snapshot	Actions
		Self	Appliance	Vault	Total	Used	Vault			
efs-train-klam	Microsoft Windows 10 (build 17134), 64-bit	192.168.253.137, 192.168.1.25, 192.168.56.110, 2.32.126	ClassDemo (192.168.1.21)	N/A	229.31G	195.17G	N/A	✘	N/A	
DemoVM	Microsoft Windows 10 (build 17134), 64-bit	192.168.1.26	ClassDemo (192.168.1.21)	Vault1 (10.2.68.35)	34.00G	17.44G	29.97G	✔	05/21/2019 12:30 PM	

To monitor replication with the Replication Status Page:

1. In the GMP, click the Replication Status tab.



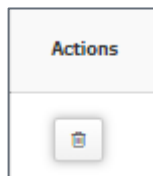
The *Replication Status* report displays, providing details of each Protected System being replicated to a Vault.

2. Use the columns in this report to view replication status details. For example:

- The *PS Name* column identifies the name of the Protected System.
- The *OS Name* column lists the Operating System name and version.
- The *IP Address* section displays the IP address of the Protected System, the Appliance, and the Vault, if applicable.
- The *Disk Usage* section displays the total and used disk usage for the Vault.
- The *Replication Status* column displays whether the Protected System is being replicated to a Vault. A green checkmark indicates that replication is configured, and a red x indicates that replication is *not* configured (local-only.)

PS Name	OS Name	IP Address			Disk Usage			Replication Status	Last Ingested Snapshot	Actions
		Self	Appliance	Vault	Total	Used	Vault			
efs-train-klam	Microsoft Windows 10 (build 17134), 64-bit	192.168.253.137, 192.168.1.25, 192.168.56.110, 2.32.126	ClassDemo (192.168.1.21)	N/A	229.31G	195.17G	N/A	✘	N/A	
DemoVM	Microsoft Windows 10 (build 17134), 64-bit	192.168.1.26	ClassDemo (192.168.1.21)	Vault1 (10.2.68.35)	34.00G	17.44G	29.97G	✔	05/21/2019 12:30 PM	

- The *Last Ingested Snapshot* column displays the time and date of the latest backup snapshot fully replicated and available on the Vault.
3. Optionally, click a **column header** to sort by field. You can then click again to reverse the sort order.
 4. In the *Actions* section of the page, click the **Delete** button to remove the Protected System and its history from the GMP.



Note: Managed Systems that have been retired and Protected Systems that no longer exist on their Appliance should be deleted from the Global Management Portal to ensure accurate reporting statistics. Deleting a Protected System from an Appliance does not automatically remove it from the GMP. Protected Systems that still exist on the Managed Device will be recreated within the GMP.

Identifying Problems with the Trouble Report

The *Trouble Report* page allows you to simplify the daily management and maintenance of your fleet of Replibit devices.

The *Trouble Report* page lists Appliances, Vaults, and Protected Systems being managed by the Global Management Portal filtered to only display items with a highlighted problem. This allows you to view an overall status of each problematic device, with statistics scored in **red**, **green**, or **yellow** (yellow) to indicate status.

Global Management Server Trouble Report												Last Updated on May 30, 2019 at 11:20:02 PM		
Appliance Machines With Reported Problems														
No Trouble Reported on Appliances														
Vault Machines With Reported Problems														
No Trouble Reported on Vaults														
Protected Systems With Reported Problems														
Customer Name: ClassDemo			Appliance Name: ClassDemo			IP Address: 192.168.1.21			Location: MyCity					
System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time	Last Replication Time	AutoVerify	Boot Check	Vlt Boot Check	Backup Statistics	Vols Retention	Disk Used	App Used	Vlt Used	
efs-train-rklem		Online	2.23.191	2019-05-30 10:00:00 PM	Replication Not Enabled		Disabled	N/A	Completed:29 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:0 M:0 Y:0	195.6GB	209.7GB	N/A	

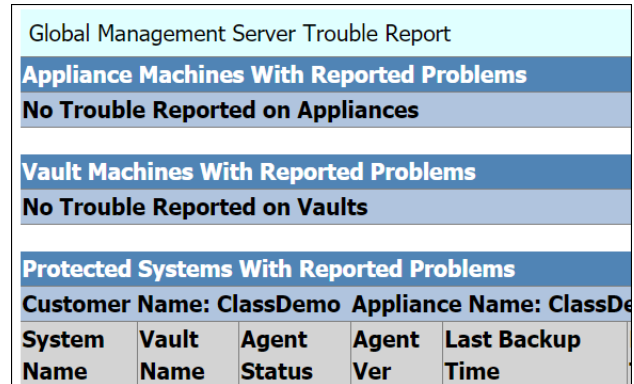
To monitor troubled devices:

1. In the GMP, click the Trouble Report tab.



The *Trouble Report* page displays, providing details of Managed and Protected System.

2. In the *Trouble Report* page, view a listing of each device by type, including *Appliance*, *Vault*, and *Protected System*.



3. Use the columns to view the details of each device. For example, to view the details of a troubled Protected System, reference the following columns:

- The *System Name* column identifies the name of the Protected System.
- The *Vault Name* column identifies the name of the Vault where Protected System Snapshots are being replicated.
- The *Agent Status* column lists the operational status of the Replibit Agent installed on the Protected System.
- The *Agent Version* section displays the current version of the Replibit Agent installed on the Protected System.
- The *Last Backup Time* column lists the time of the latest backup.
- The *Last Replication Time* column displays the time of the latest Snapshot replicated to the Vault.

System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time
ifs-train-blom	2.23.191	OK	2.23.191	2019-05-30 11:30:02 PM

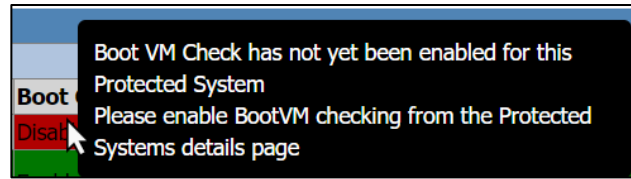
- The *AutoVerify* column displays the results of the *chkdsk* test and the *heartbeat* test.
- The *Boot Check* column indicates whether the Boot VM Check feature is turned on at the Appliance level.
- The *Vlt Boot Check* column indicates whether the Boot VM Check feature is turned on at the Vault level.
- The *Backup Statistics* column displays a count of *completed*, *failed*, and *missed* backups.
- The *Vols* column displays the Protected System volume(s) being backed up.
- The *Retention* column displays the Snapshot retention policies defined for all Snapshots, daily Snapshots, weekly Snapshots, monthly Snapshots, and Yearly Snapshots (for both the Appliance and Vault).
- The *Disk Used* column displays disk usage of the Protected System.
- The *App Used* column displays the disk usage within the Appliance.
- The *Vlt Used* column displays the disk usage within the Vault.

4. Reference highlighted cells for detailed status information:

Protected Systems With Reported Problems								
Customer Name: ClassDemo		Appliance Name: ClassDemo			IP Address: 192.168.1.21			
System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time	Last Replication Time	AutoVerify	Boot Check	Vlt Boot Check
efs-train-rklem		Online	2.23.191	2019-05-30 10:00:00 PM	Replication Not Enabled		Disabled	N/A

- A **green cell** indicates normal operations, such as an Agent being online, the date and time of a successfully completed backup, or a completed Backup with no failures.
- A **red** or **yellow** (yellow) cell indicates a potential issue, such as a Boot Check that is disabled.

- To view additional details, hover your mouse over a red or yellow (yellow) highlighted cell and review the pop-up bubble.



Verifying the Status of Devices with the Health Report

In the *Health Report* tab, you can view a listing and status of *all* Managed and Protected Systems visible in the GMP. The Health Status report allows you to view an overall health of each device, scored in red, green, or yellow (yellow) to indicate status.

Global Management Server Health Status Report										Last Updated on Jun 03, 2019 at 09:00:02 AM			
Appliance Hardware Status													
Customer Name	Appliance Name	Location	Site Licenses	Last Updated	Version	Protected System Count	Snapshot Usage	Storage Pool Status	Storage Pool Alerts				
ClassDemo	ClassDemo	MyCity	Servers: 0 / 0 Workstations: 2 / 0	2019-06-03 09:00:00 AM	8.2.3	2	None	Online	OK				
Vault Hardware Status													
Vault Name	Storage Pool Utilization	Incoming Snapshots	Exported Disks	Last Updated	Version	Protected System Count	Snapshot Usage	Storage Pool Status	Storage Pool Alerts				
Vault1	4.89GB of 152.78GB (18.10%)	0,00GB	0,00GB	2019-06-03 09:00:00 AM	8.2.3	1	None	Online	OK				
Protected Systems Status													
Customer Name: ClassDemo		Appliance Name: ClassDemo		IP Address: 192.168.1.21				Location: MyCity					
System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time	Last Replication Time	AutoVerify	Boot Check	Vit Boot Check	Backup Statistics	Vols Retention	Disk Used	App Used	Vit Used
efs-train-rklem		Online	2.23.191	2019-06-03 08:00:30 AM	Replication Not Enabled		Disabled	N/A	Completed:29 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:0 M:0 Y:0	196.1GB	202.9GB	N/A
DemoVM	Vault1	Online	2.23.191	2019-06-02 05:30:00 PM	2019-06-02 05:30:00 PM	chkdisk PASSED heartbeat PASSED	Enabled	Disabled	Completed:10 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:12 M:3 Y:0 E: Vault: A:3 D:30 W:0 M:3 Y:0	17.4GB	31.9GB	34.8GB

To view the health status of devices:

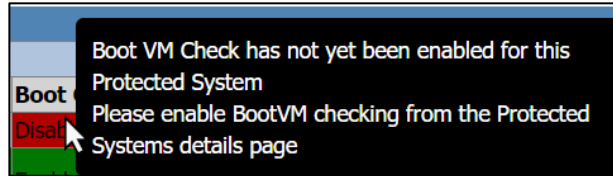
- In the GMP, click the Health Report tab. The *Health Report* page displays, listing details about each Managed Device.
- In the *Health Report* page, view a listing of each device by type, including:
 - Appliance,
 - Vault, and
 - Protected System (grouped by Appliance).
- Reference highlighted cells for detailed status information:
 - A green cell indicates normal operations, such as an Agent being online, the date and time of a successfully completed backup, or a completed Backup with no failures.



Global Management Server Health Status Report										Last Updated on Jun 03, 2019 at 09:00:02 AM			
Appliance Hardware Status													
Customer Name	Appliance Name	Location	Site Licenses	Last Updated	Version	Protected System Count	Snapshot Usage	Storage Pool Status	Storage Pool Alerts				
ClassDemo	ClassDemo	MyCity	Servers: 0 / 0 Workstations: 2 / 0	2019-06-03 09:00:00 AM	8.2.3	2	None	Online	OK				
Vault Hardware Status													
Vault Name	Storage Pool Utilization	Incoming Snapshots	Exported Disks	Last Updated	Version	Protected System Count	Snapshot Usage	Storage Pool Status	Storage Pool Alerts				
Vault1	4.89GB of 152.78GB (18.10%)	0,00GB	0,00GB	2019-06-03 09:00:00 AM	8.2.3	1	None	Online	OK				
Protected Systems Status													
Customer Name: ClassDemo		Appliance Name: ClassDemo		IP Address: 192.168.1.21				Location: MyCity					
System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time	Last Replication Time	AutoVerify	Boot Check	Vit Boot Check	Backup Statistics	Vols Retention	Disk Used	App Used	Vit Used
efs-train-rklem		Online	2.23.191	2019-06-03 08:00:30 AM	Replication Not Enabled		Disabled	N/A	Completed:29 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:0 M:0 Y:0	196.1GB	202.9GB	N/A
DemoVM	Vault1	Online	2.23.191	2019-06-02 05:30:00 PM	2019-06-02 05:30:00 PM	chkdisk PASSED heartbeat PASSED	Enabled	Disabled	Completed:10 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:12 M:3 Y:0 E: Vault: A:3 D:30 W:0 M:3 Y:0	17.4GB	31.9GB	34.8GB

Protected Systems With Reported Problems													
Customer Name: ClassDemo		Appliance Name: ClassDemo		IP Address: 192.168.1.21				Location: MyCity					
System Name	Vault Name	Agent Status	Agent Ver	Last Backup Time	Last Replication Time	AutoVerify	Boot Check	Vit Boot Check	Backup Statistics	Vols Retention	Disk Used	App Used	Vit Used
efs-train-rklem		Online	2.23.191	2019-05-30 0:00:00 PM	Replication Not Enabled		Disabled	N/A	Completed:29 Failed:0 Missed:0	C: Appliance: A:7 D:7 W:0 M:0 Y:0	196.1GB	202.9GB	N/A

- A red or yellow (yellow) cell indicates a potential issue, such as a Boot Check that is disabled.
4. To view additional details, hover your mouse over a red or yellow (yellow) highlighted cell and review the pop-up bubble.



Note: All data and metrics reported by the *Health* and *Trouble* report pages is identical to the information available on the other pages of the Global Management Portal, but logical analysis has been performed in order to highlight potential trouble and overall health of each device in a more user-friendly format.

Managing Storage Usage with the Storage Report

You can use the Storage Report to manage your devices over time. The *Storage Report* page is broken into two sections of reporting that you can monitor:

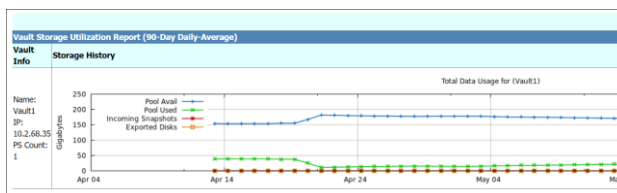
- The Vault Storage Utilization Report, and
- The Appliance Storage Utilization Report.

Protected Systems are sorted from largest to smallest and limited to only the largest 10 systems.



To view the Storage Report:

1. In the GMP, click the Storage Report tab. The *Storage Report* page displays.
2. Use the *Vault Storage Utilization* section to view storage history of data usage for each Vault.
3. Use the *Appliance Storage Utilization* section to view storage history of data usage for each Appliance. You can also use each sub-section to view a breakdown of usage by device type:
 - The *Protected System Usage* section shows the amount of storage utilization for each Protected System.
 - The *Appliance Usage* section shows the amount of storage utilization for each Appliance.
 - The *Vault Usage* section shows the amount of storage utilization for each Vault.



Monitoring Your Protected Systems with the Boot VM Report

The *Boot VM Report* provides a visual quick reference to the status of the latest Boot VM test for all Protected Systems managed by the Global Management Portal. With the details in this report, you can quickly verify that all Protected Systems are bootable.

Note: To properly utilize the Boot VM Report, the Boot VM Check feature must be enabled for each individual Managed System (Appliance and Vault). For instructions on enabling this feature, please reference the Replibit Installation Guide.

If the Boot VM Check feature is *not* enabled for a Managed System, the image column will display as *NA*.

Within the Boot VM Report, the *AutoVerify* column displays results of the AutoVerify check, which alerts you of possible issues with Protected Systems *before* they fail. With this advanced notification, you can ensure you have valid backups and the resources necessary to repair potentially bad data on the source system.

Customer	Location	PS Name	Device Type	IP Address	Snapshot Time	AutoVerify	Screenshot
ClassDemo	MyCity	efs-brain-r1em	appliance	ClassDemo (192.168.1.21)	Disabled		N/A
ClassDemo	MyCity	DemoVM	appliance	ClassDemo (192.168.1.21)	05/04/2019 09:30 PM	chkdsk PASSED heartbeat PASSED	
ClassDemo	MyCity	DemoVM	vault	Vault (b-edend1.rlb.ac.efscloud.net)	Disabled		N/A

To view the Boot VM Report:

- In the GMP, click the **Boot VM Report** tab. The *Boot VM page* displays.
- Use the columns to view the details of each Protected System boot process:
 - The *Customer* column identifies the Customer to whom the Protected System is registered.
 - The *Location* column identifies the geographic location of the Protected System.
 - The *PS Name* identifies the device name.
 - The *Device Type* section displays the type of device that is protecting the Protected System.
 - The *IP Address* column lists the IP address of the Protected System.
 - The *Snapshot Time* column displays the time of the latest Snapshot.
 - The *AutoVerify* column displays the results of the *chkdsk* test and the heartbeat test.



chkdsk confirms the integrity of the file

system. If `chkdsk` fails, a full backup of the Protected System might be triggered (if one has not already been performed recently) in an attempt to self-heal the failure.

Heartbeat confirms that the system was able to fully boot the operating system, start services, and accept commands to perform additional testing (for example, `chkdsk`.)

- The *Screenshot* column displays the captured image of the boot process to help you ensure the Protected System image was able to boot properly.

Note: Full scans generated by AutoVerify will occur no more than once every 30 day.

`chkdsk`s 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 and then a new full backup taken to fix this problem.)*

If `chkdsk` exits with error codes that indicate possible data consistency issues, the Appliance will attempt 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.

Managing Reports and Central Alerting

The GMP allows you to schedule recurring reports so that you can stay informed of important events that occur in the system. You can customize report delivery from within the GMP and select from a variety of administrative and customer-facing report types. You can choose to have these reports delivered to any email recipient(s) you define on a daily, weekly, or monthly schedule.

Additionally, you can turn on Central Alerting so that you are notified when devices are down. A single ticket is generated for each unique alert and is updated periodically if it has not been resolved. You can also use this feature in conjunction with the ConnectWise PSA platform. For more information, please review the Integrating with ConnectWise section of this guide.

For example, with Central Alerting, you can track the following alerts:

- Appliance offline
- Vault offline
- Replibit version out of date on device
- No recent backup of Protected System*
- No recent replication of Protected Systems to the Cloud

If you receive a report that highlights an issue, please reference the [Troubleshooting Guide](#) for support.

To schedule reports and enable ticketing:

1. In the GMP, click the **Settings** tab. The *Settings* page displays, showing all available GMP configuration options.
2. Click to expand the **Reporting Settings** section. The *Reporting Settings* section displays, allowing you to turn on and configure reports.
3. Click the **Email Delivery** checkbox to enable email.
4. Enter information about the email server, including:
 - The **From Email address**,
 - The **username and password** of a valid email account on the email server, and
 - The **hostname and port** of the server.



 A screenshot of the 'Reporting Settings' configuration page. At the top, there is a 'GMP URL' field with a dropdown menu. Below that, the 'Email Delivery' section is expanded and has a checked checkbox. It contains several input fields: 'SMTP Display Name' (filled with 'Gmail'), 'SMTP Email Address', 'SMTP Username', 'SMTP Password' (masked with dots), 'SMTP Server' (filled with 'smtp.gmail.com'), and 'SMTP Port' (filled with '465'). There is also a 'Connection security' dropdown menu set to 'SSL'. The 'Ticketing' section also has a checked checkbox and includes input fields for 'POP3 Server', 'POP3 Port', and 'To Email(s)' (with a placeholder 'Enter comma separated email(s)'). A 'Save' button is at the bottom left. A red error message at the bottom reads: 'Please make sure that all required fields are filled in correctly.'

5. Optionally, click the **Ticketing** checkbox to enable Central Alerting. This feature will alert you when devices are down.
6. Enter information about your mail server, including:
 - The POP3 server,
 - The POP3 port, and
 - The To Email address.
7. Click the **Save** button to save your settings.
8. After you configure the email server, you can select reports for delivery:
 - Click the **Add** button.
 - In the *Report Name* drop-down field, select the **type of report** you want delivered.
 - In the *Frequency* drop-down menu, select **how often** this report should be delivered.
 - In the *Hour* field, enter the **time of day** you want this report delivered.
 - If this is a Customer-specific report, use the *Customer* drop-down menu to select the name and email address of the **Customer** after you enter the required information in the *Recipients* field. Information displayed in this report will then be filtered for this Customer.
 - In the *Recipients* field, configure **recipients** who should receive this report.
 - Optionally, click the **Add** button to add additional recipients.
9. Click the **Submit** button to save your settings.

The Report Engine will process reporting schedules every 10 minutes.

If a delivery window was missed (for example, if the GMP was offline), any pending reports will be delivered in the next available 10-minute window. You can edit your settings at any time.

Configuring Global Management Portal Settings with the Settings Tab

The *Settings* page gives you access to a list of settings and configuration options to help you customize the GMP. For example, you can view or update the following key settings:

- The *API Key* tab allows you to retrieve your API Key.
- The *Change Machine Name* tab allows you to change your Machine or Host Name.
- The *Change Password* tab allows you to change and manage the Admin (Web UI) password.
- The *Date and Time Settings* tab allows you to manage the date, time, and time zone settings of the device.
- The *Multi-Factor Authentication* tab allows you to enable and configure the Multi-Factor Authentication (MFA) feature. Multi-Factor Authentication (MFA) adds a second verification step when a user accesses the Replibit platform. With MFA enabled, users will be prompted to enter a one-time password generated by an authentication app when logging in to the system.
- The *Reporting Settings* tab allows you to configure and customize the frequency and recipients of your reports.
- The *Update Manager* tab allows you to configure and manage updates to the Management Portal.
- The *Remote Assist* tab allows you to enable the Remote Assist feature, which gives Axcient Replibit Technical Support the ability to troubleshoot issues on your devices without requiring assistance from the Customer or the partner. For more information, please visit our Knowledgebase.
- The *Network Settings* tab allows you to manage the Network Settings on your device.
- The *Upload New Logo* tab allows you to customize your branding.
- The *Shutdown and Reboot* tab allows you to shut down or reboot your device.

To manage Global Management Portal settings:

1. In the GMP, click the **Settings** tab. The *Settings* page displays, showing all available GMP configuration options.



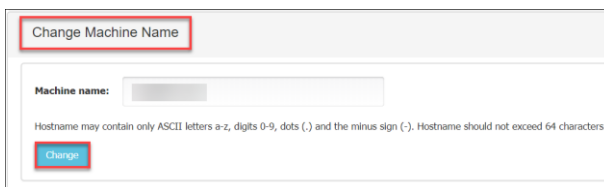
- Click to expand the API Key section to view your API Key.

For instructions on working with the API Key, please reference the [Connecting Appliances and Vaults to the Global Management Portal](#) section of this guide.



- Click to expand the Change Machine Name section to view or update the name of the GMP machine.

- In the *Machine name* field, enter a descriptive name for the machine.
- Click the **Change** button to save your changes.

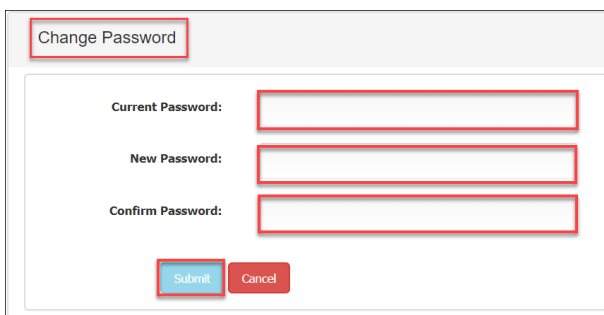


- Click to expand the Change Password section to update your password to the GMP.

- In the *Current Password* field, enter your Current Password.
- In the *New Password* field, enter your New Password.
- In the *Confirm Password* field, re-enter your New Password.

Note: Minimum password length is 8 characters.

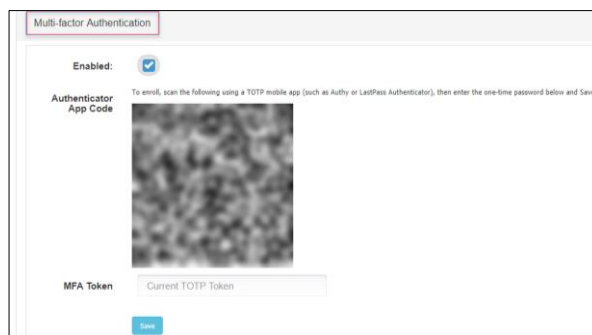
- Click the **Submit** button to save your changes.



- Click to expand the Multi-Factor Authentication tab.

- Click the **Enabled** checkbox to turn on MFA. A QR code image will display for configuring your preferred authenticator app.

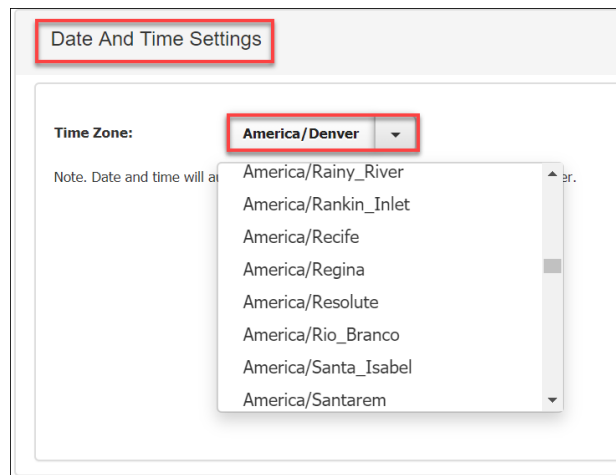
Note: You must keep the generated QR code image secure. Any user with access to this image can generate MFA Tokens. Do not digitally share or



otherwise expose this image online.

- Open an authenticator app on your smartphone and scan the QR code to configure the MFA token.
 - When your authenticator app is configured, return to the GMP and enter the generated MFA Token in the *MFA Token* field.
 - Click the **Save** button to save your settings.
6. Click to expand the **Date and Time Settings** section to view your time settings.
- In the *Time Zone* drop-down menu, select your **Time Zone**.
 - Click the **Save** button to save your settings.
7. Click to expand the **Reporting Settings** section to configure email delivery sections for reports.

For complete instructions, please reference the [Scheduling and Managing Reports](#) section of this guide.



8. Click to expand the **Update Manager** section to turn on or off the *Enable Auto Update* feature, which will automatically update the GMP to the latest available Replibit version. You can enable this feature by clicking on the **Enable Auto Update** checkbox.

Note: As a best practice, we suggest that you check the *Auto-Enable Remote Assist When Upgrading* checkbox. This tool allows Axcient Technical Support to remotely assist and diagnose issues if they arise during the upgrade process.

9. Click to expand the **Remote Assist** section to turn on the Remote Assist tool. You can enable this service by clicking on the **Enable** checkbox. Please note that Remote Assist automatically expires and is disabled after the selected expiration date.

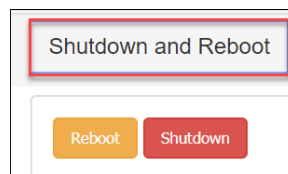
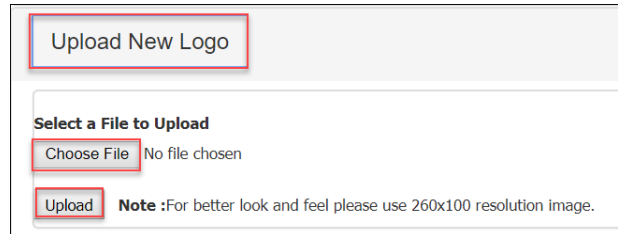
Note: As a best practice, we recommend that you turn on this feature and select an expiration date at least 7 days in the future when you submit a ticket to Axcient Support.

10. Click to expand the **Network Settings** section to manage Network Settings on the device.
 - From the *Method* drop-down menu, select either DHCP or Static.
 - In the *IP Address* field, enter the **IP address** of the device.
 - In the *Subnet Mast* field, enter the **subnet mask** of the device.
 - In the *Network Gateway* field, enter the **network gateway** address of the device.

- In the *DNS* field, enter the **DNS address**. Multiple DNS Server entries can be entered by separating each entry with a comma.
 - Click the **Submit** button to save your changes.
11. Click to expand the **Upload New Logo** section to upload your logo and brand the GMP according to your company branding standards.
- Click the **Update New Logo** section to add your organization's uniquely branded logo to the GMP.

Note: We recommend using a 260x100 resolution image.

- Click the **Choose File** button and select your **logo file** from the local machine.
 - Click the **Upload** button to complete the upload process.
12. Click the **Shutdown and Reboot** section to shut down or reboot the GMP.



Integrating with ConnectWise

ConnectWise is a Professional Services Automation (PSA) platform for companies that sell, service, and support technology. If you use ConnectWise as your PSA platform, you can seamlessly integrate this platform with each Appliance and Vault that you manage to enable easy reporting, ticketing, and billing. You can centrally manage ConnectWise authentication and ticketing properties from the GMP.

When you integrate Replibit with ConnectWise, Replibit alerts trigger tickets within ConnectWise. Ticket status is then synchronized in both directions with the corresponding alert. You can also configure billing integration to track data usage in the Cloud.

If you receive an alert that highlights an issue, please reference the [Troubleshooting Guide](#) for support.

Configuring ConnectWise for Third-Party Integration

Before enabling ConnectWise Integration within Replibit, you must first ensure ConnectWise has been properly configured for Integration with third-party products.

Additionally, you need to ensure your ConnectWise environment meets the following prerequisites:

- Must include an active Customer account,
- Optionally, if you wish to enable billing support, the Customer account:
 - Must have an Agreement, and
 - Must have an Agreement Addition.

For complete requirements, please reference the [Replibit ConnectWise Integration Guide](#).

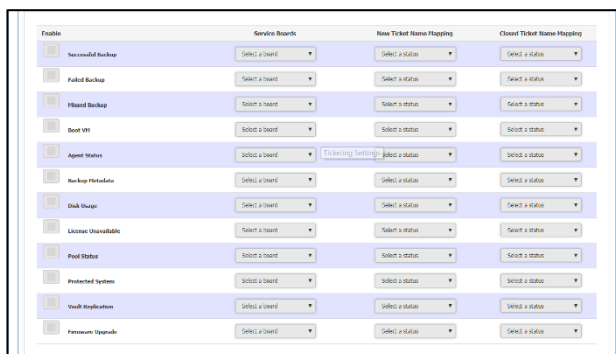
Configuring ConnectWise Settings in Replibit

After all prerequisites are configured in ConnectWise, you can create a default policy within the Global Management Portal. After these settings are configured, you can inherit these settings within each individual Managed System (Appliance and Vault).

Note: You can also utilize Replibit's Central Alerting feature in conjunction with ConnectWise. For more information, please reference the Managing Reports and Central Alerting section of this guide.

To integrate with ConnectWise:

1. In the GMP, click the **Policy Settings** tab. The *Policy Settings* page displays, allowing you to create a default ConnectWise policy, which can be inherited by Managed Systems (Appliances and Vaults).
2. Click to expand the **ConnectWise Credentials** section and enter your ConnectWise credentials, including the **Site URL** for your ConnectWise server, **Company name**, **API Key** and **API Secret**.
3. Click the **Test Connection** button to validate your settings.
4. Click the **Save Configuration and Credentials** button to save your credentials.
5. Click to expand the **Ticketing Settings** section and configure which Replibit Alert types should generate ConnectWise ticket by the Replibit product:
 - Click the **Enable** checkbox adjacent to each alert class you would like to turn on.
 - In the *Service Boards* drop down menu, select the appropriate **service board** configured in ConnectWise.
 - In the *New Ticket Name Mapping* drop-down menu, select the **status of new tickets** generated in the system.
 - In the *Closed Ticket Name Mapping* drop-down menu, select the **status of closed tickets** generated in the system.



6. When you are finished, click the **Save Configuration and Credentials** button.
7. When you are ready to inherit ticket settings and configure billing settings, log in to each Appliance and Vault that you manage and inherit settings:
 - In the Web interface of each Managed Device, click the **ConnectWise Settings** tab.
 - Click the **Inherit Configuration from GMP** checkbox. ConnectWise credentials and ticketing settings will be filled in using the values you defined on the GMP.
 - Click to expand **Ticketing Settings**.
 - In the *Service Ticket Company* drop-down menu, select a **Company** that is associated with this Appliance or Vault. This will ensure the correct Company in ConnectWise is mapped to this specific Customer Appliance.
 - Click the **Save Configuration and Credentials** button to save your changes.

The screenshot displays the 'ConnectWise Settings (Vault1)' configuration page. At the top, there is a checkbox labeled 'Inherit configuration from GMP' which is checked. Below this is the 'ConnectWise Credentials' section, containing four input fields: 'Site' (with a 'https://' prefix), 'Company', 'API Key', and 'API Secret' (masked with dots). A 'Test Connection' button is located below these fields. Further down are sections for 'Billing Integration' and 'Ticketing Settings', both currently collapsed. At the bottom of the page, there are four buttons: 'Save Configuration and Credentials', 'Reload Settings', 'Import Settings', and 'Export Settings'.

Note: *Service Ticket Company* assignment is unique to each Managed device and cannot be remotely configured or managed from the Management Portal. Likewise, Billing settings (Company, Agreement, and Addition) are unique to each device and cannot be managed globally.

Managing Replibit Licenses

You can add or delete license packs over time or adjust licensing models as your Customer needs grow and change. Please consider the following before making changes:

- Endpoint licenses are cumulative; you can add additional license packs over time to meet your needs.
- You can only assign *one* Storage license at a time to a Location.
- Endpoint and Storage licenses are mutually exclusive; you can only assign one or the other to a Location.

Note: If you need to switch licensing models, you will first need to remove all assigned licenses and then add the new license type

For a complete overview of Replibit licensing, please review the [Replibit Installation Guide](#).

Adding Licenses

Endpoint licenses come in two classes: Workstation and Server. For example, a Windows 10 operating system requires a Workstation license and a Windows Server 2012 operating system require a Server license. Each Location can be assigned any number of Endpoint Server and Workstation licenses, which allows you to back up the specified number of Protected Systems (Workstation or Server). Endpoint licenses are consumed automatically by Protected Systems when an Agent is installed, and the Protected System checks in with the Appliance.

Storage licenses allow you to back up an unlimited number of Protected Systems to a single Appliance, up to the storage license limit assigned to the Appliance.

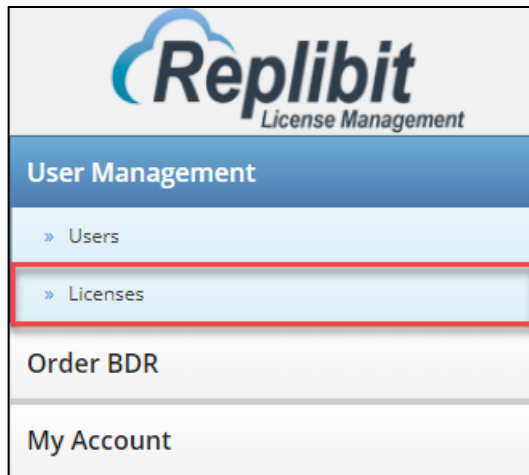
Note that the Agent automatically determines which type of license a given Protected System requires and this cannot be manually selected.

To add a license:

1. Log in to the [Replibit Licensing Portal](#).



2. From the *Replibit License Management* left pane menu, click to expand **User Management** and then select **Licenses**.



3. Locate the appropriate Customer and Location within the main window. Optionally, use the Search field to search by Customer name or Location. Customers and Locations are case sensitive.

Customer	Location	Server	Workstation	Storage	Used	Actions
partner (Used/Available)		-	-	-	-	-
Customer10	Main_Office	0	0	20K	No	Manage History

Note: Customers with more than one Location will appear in the list multiple times. Ensure that you have selected the correct Location when managing licenses. Customer and location names are case sensitive.

4. Click the **Manage** button. The *Manage Location* window displays.

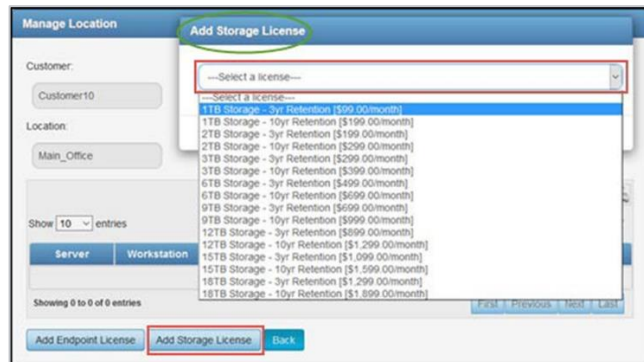
- To add an Endpoint license, click the **Add Endpoint License** button and update the following fields:
 - In the *Allocated* fields, enter the license count for Server(s) and Workstation(s) licenses as needed.
 - Click the **Submit** button.



Note: Endpoint licenses are cumulative; you can add additional license packs over time to meet your needs.

Note: Endpoint license billing *is not* prorated. Billing occurs on the last day of the month for all licenses that are allocated to a Location, regardless of whether the license is in use by a Protected System.

- To add a Storage license, click the **Add Storage License** button and update the following fields:
 - In the *Select a License* drop-down menu, select a Storage license option.
 - Click the **Submit** button.



Note: Only one Storage license can be assigned to a Location at a time. To change Storage licensing, first remove the existing license and assign a new one.

Note: Storage licensing *is* prorated and is billed based on the date licensing is assigned or removed.

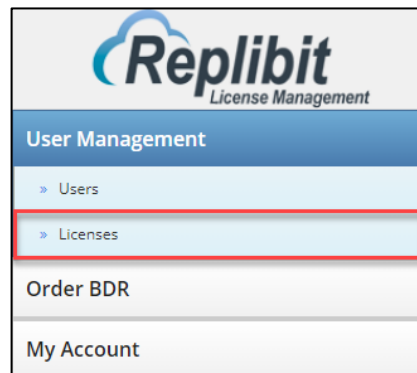
Removing Licenses

If you need to switch licensing models, you will first need to remove all assigned licenses and then add the new license type.

Note: If you are Replicating Protected Systems to the Axcient Cloud and you remove a Protected System from an Appliance, you will also need to delete the Protected System from the Vault to avoid future billing. Any Protected System remaining in the Axcient Cloud will be billed a full month at the Bundled Endpoint license rate, whether it still exists on its original Appliance or not.

To change a license:

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



2. Locate the appropriate Customer and Location within the main window.
3. Click the **Manage** button. The *Manage Location* window displays.
4. Find the license you would like to remove and click the **Delete** button.

Customer	Location	Server	Workstation	Storage	Used	Actions
Customer10 (Used/Available)	Main_Office	0	0	NAK	No	Manage

Note: You can remove a Protected System from the Axcient Cloud from the Vault Web interface.

Alternatively, you can remove a Protected System from the Appliance Web interface by deleting the Vault Replication configuration and selecting to also delete the Protected System from the Vault.

For instructions, please reference the [Deleting a Protected System](#) section of this guide.

Managing Protected Systems

After the Agent is installed on a Protected System, you should monitor the machine to ensure it remains in a healthy state. A few management and maintenance tasks associated with monitoring a Protected System include:

- Viewing Protected Systems status,
- Modifying the Agent (or Agent configuration settings), and
- Deleting or migrating a Protected System.

Viewing Protected Systems

You can view a list of registered Protected Systems from the Appliance or Vault Web Interface. From the Appliance or Vault Web interface, you can view the status of Protected Systems, the Operating System, view currently protected volumes, and more.

To view Protected Systems:

1. Log in to the Appliance or Vault Web interface. In this procedure, we are logging in to the Appliance Web interface.
2. In the left-hand navigation menu, click the Protected Systems tab.
3. Use the columns to view the details of each Protected System:
 - The *Status* column displays icons that indicate whether the system is currently running as a virtual machine (the first icon will be green) and if replication is enabled for the system (the second icon will be blue).
 - The *System Name* column lists the name of the Protected System and helps you identify each Protected System.



- The *Operating System Column* lists the Operating System of the Protected System.
- The *Currently Protected Volumes* field lists the volumes being backed up.
- If you are working in the Appliance Web interface, the *Schedule* column allows you to adjust the predefined schedule assigned to the Protected System. Schedules can be edited in the *Schedules* page of the Appliance Web interface. For complete instructions, please reference the Replibit Installation Guide.
- The *Actions* column allows you to delete or view the details of a Protected System.

Clicking **Delete** will prompt for the permanent deletion and removal of the Protected System and all recovery points. This action is permanent and cannot be undone.

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

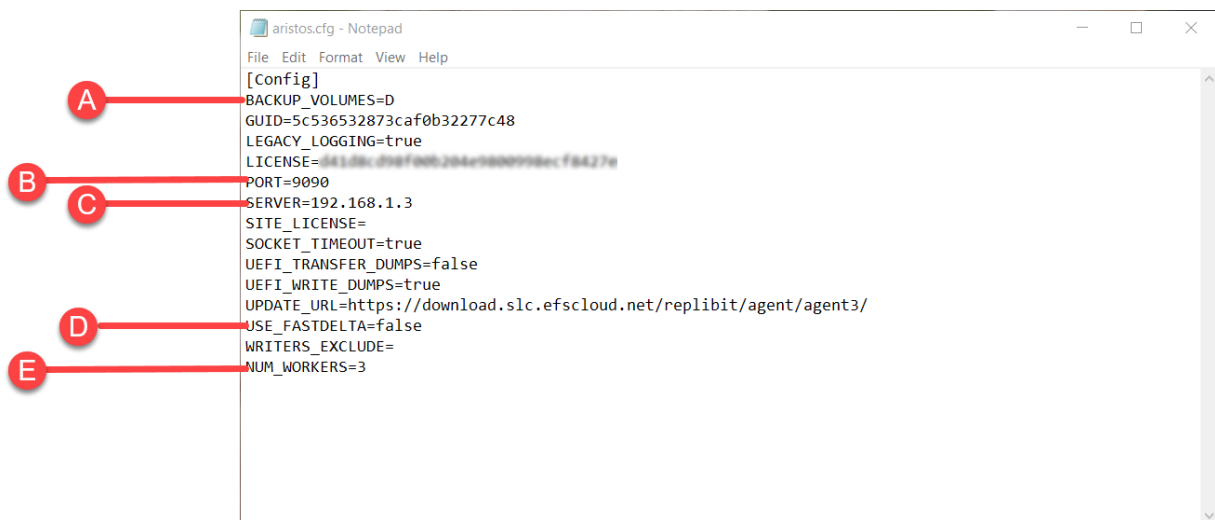
Modifying the Configuration File

In some instances, you might notice that a Protected System is not functioning as expected. For example, a Protected System might be backing up the wrong volume, or you might notice performance issues. You can use the Agent's configuration file (*aristos.cfg*) to adjust various settings.

The Agent configuration file lists key parameters that control Agent behavior. In most instances, you will *not* need to access or modify this file. However, you may need to edit this file for troubleshooting purposes, performance improvement, or to turn on advanced features.

For example, you can manage the following parameters:

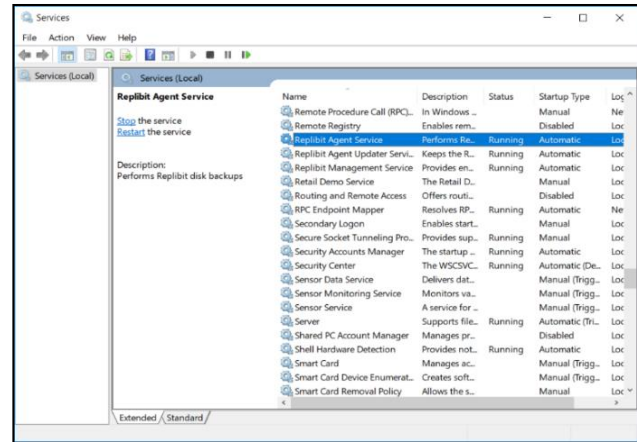
- A. The BACKUP_VOLUMES parameter is an inclusion list, specifying which NTFS volumes are to be backed up by the Agent. By default, the value is blank, prompting a backup of all detected NTFS volumes. To define an inclusion list, enter each volume, separated by a comma.
- B. The PORT parameter lists the port open between the Protected System and the Appliance.
- C. The SERVER parameter lists the IP address of the Appliance.
- D. The USE_FASTDELTA parameter is used to turn on or off the Fast Delta feature. Fast Delta is a block-change scanning tool that improves the backup performance of large database applications, such as Microsoft Exchange or Microsoft SQL. By default, this parameter is set to *false*. This parameter should only be set to *true* when supporting Microsoft Exchange or Microsoft SQL servers.
- E. The NUM_WRITERS parameter is not listed in the default configuration file, but it can be inserted to adjust the number of worker threads utilized by the Agent. Lowering this value will reduce the speed of backups. If you are noticing CPU performance issues on a local machine with an installed Agent, you can modify this value to lower CPU usage. By default, the Agent uses four worker threads per processor core.



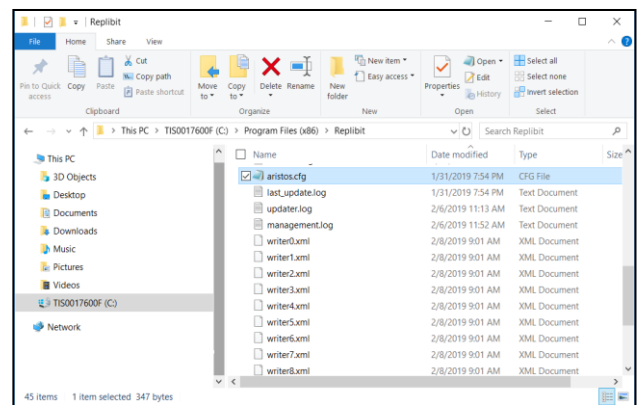
Note: Additional configuration options are available for special use cases. Please contact Axcient Support for assistance in troubleshooting and configuring advanced Agent settings.

To modify the Agent configuration file:

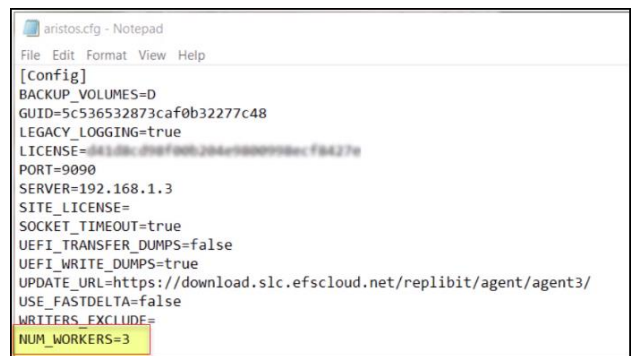
1. From the Services app on the target machine, stop and disable the *Replibit Agent Service*.



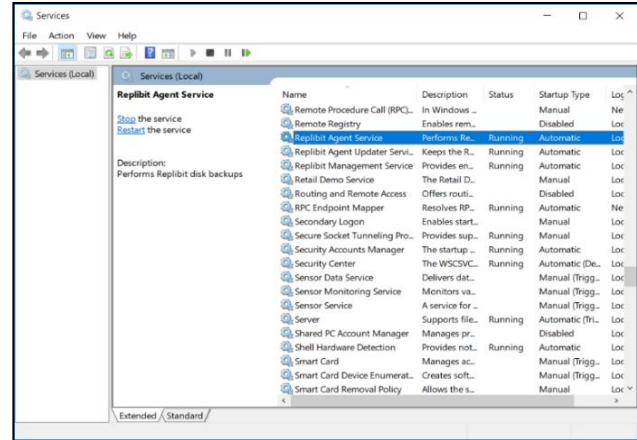
2. Using Windows Explorer, navigate to the Replibit Agent installation folder (for example, *C:\Program Files (x86)\Replibit*).
3. Open the *aristos.cfg* file with administrative privileges.



4. Modify the appropriate parameters.
5. Save the file when you are finished.



6. Enable and restart the *Replibit Agent Service*.



Deleting a Protected System

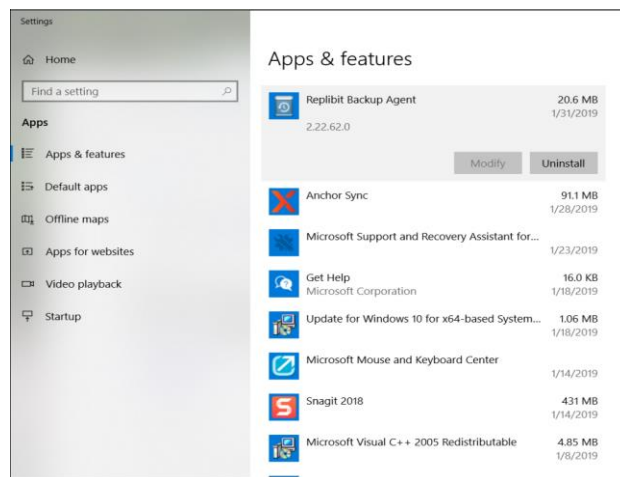
If you need to delete a Protected System, remember that removing a license does *not* stop the billing process. To stop the billing process, you must complete each of the following steps:

- Uninstall the Replibit agent.
- Delete the Protected System from the Appliance.
- Delete the Protected System from the Vault.
- Remove the license in the Replibit Licensing Portal.

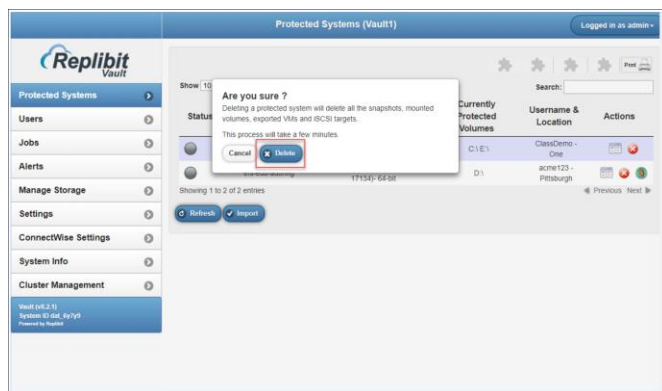
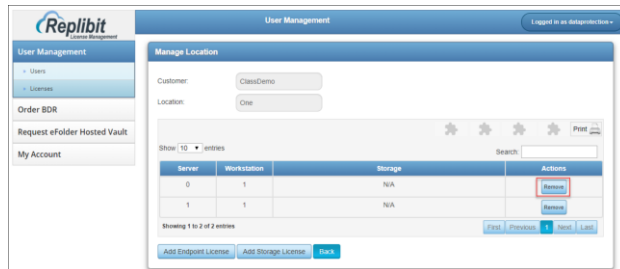
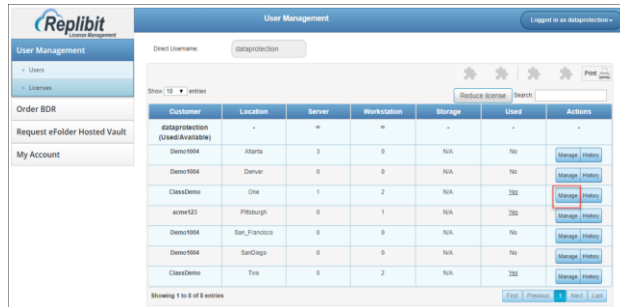
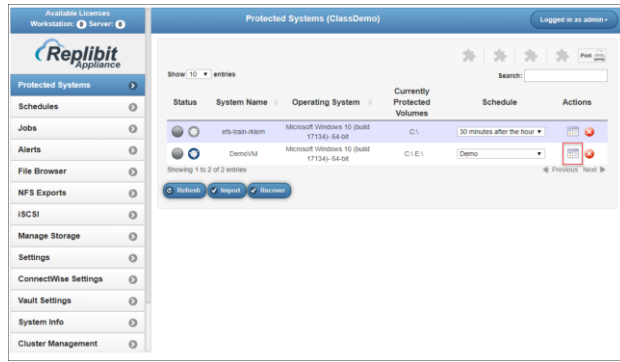
Note: To avoid billing charges, you *must* remove the Protected System from all Axcient Vaults. If you are Vaulting to your own Private Cloud, you can leave the system on your self-hosted Vault without incurring any additional charges.

To delete a Protected System:

1. On the Protected System, open the Control Panel.
2. Uninstall the Replibit Agent from the Protected System using the *Apps & Features* tool.



3. Log in to the Appliance Web interface.
4. Click the Protected Systems tab. The *Protected System* page displays, listing all Protected Systems registered to the Appliance.
5. Find the Protected System and click the Delete button.
6. Log in to the Replibit Licensing Portal.
7. Click the User Management tab to expand the menu and then click the Licenses tab.
8. Find the Location you want to manage and click the Manage button.
9. In the *Manage Location* page, find the license you want to delete and click the Remove button to remove.
10. Log in to the Vault Web interface.
11. Click the Protected Systems tab. The *Protected System* page displays, listing all Protected Systems being replicated to the Vault.
12. In the *Protected Systems* page, find the Protected System you want to delete and click the Delete button.



Managing Appliances

After you deploy the Appliance at the Customer Location, you should perform periodic checks to ensure the Appliance is functioning as expected. You can perform various management tasks within the Appliance Web Interface to:

- Monitor, view, and respond to alerts,
- Manage storage, and
- View system information.

Monitoring Alerts in the Appliance Web Interface

The *Alerts* tab shows the status of any active or recent alerts generated by the Appliance. For example, you can track missed backups, Vault replication status, storage failures, and more.

System Name	Host Name	Type	Title	Created	Resolved	Occurrence	Status	Action
DemoVM	Class Demo	Agent Status	Agent disconnected	Wed 02-06-19 02:38 PM	Wed 02-06-19 02:46 PM	1	Success	
efs-train-rklem	Class Demo	Vault Replication	Vault ingestion in TrainingVault (rb-training1.rb.ams.efscld.net) is delayed by 6 days	Sat 02-02-19 04:10 AM	Tue 02-12-19 06:48 AM	1	Warning	
DemoVM	Class Demo	Agent Status	Agent disconnected	Thu 01-31-19 05:59 PM	Mon 02-04-19 11:44 AM	1	Success	
DemoVM	Class Demo	Agent Status	Agent disconnected	Wed 01-30-19 10:15 PM	Thu 01-31-19 05:21 PM	1	Success	
DemoVM	Class Demo	Agent Status	Agent disconnected	Tue 01-22-19 10:59 PM	Tue 01-22-19 11:00 PM	1	Success	
DemoVM	Class Demo	Agent Status	Agent disconnected	Sat 01-19-19 05:43 AM	Sun 01-20-19 10:56 PM	1	Success	
DemoVM	Class	Failed	Backup failed, please check	Fri 01-18-19 12:34	Fri 01-18-19	1	Warning	

The following alerts can be generated by the Appliance:

Missed Backup

The Missed Backup alert is generated if a Protected System did not complete the last scheduled backup.

This alert will display in the *Alerts* tab. Optionally, you can configure an Email alert or a ConnectWise alert.

Failed Backup

The Failed Backup alert is generated if a backup process fails.

	This alert will display in the Alerts tab. Optionally, you can configure an Email alert or a ConnectWise alert.
No Transmission to Vault for 48 Hours	<p>The No Transmission to Vault for 48 Hours alert is generated if the Appliance is not able to connect with the Vault within a 48-hour time period.</p> <p>This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.</p>
Degraded Storage Volume in ZFS Pool	<p>The Degraded Storage Volume in ZFS Pool alert is generated if an Appliance storage volume has been marked as degraded.</p> <p>This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.</p>
ZFS Pool Offline	<p>The ZFS Pool Offline alert is generated if the entire ZFS Storage Pool is offline.</p> <p>This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.</p>
Storage Pool at 80% Capacity	<p>The Storage Pool at 80% Capacity alert is generated when storage capacity for the Appliance is over 80% full.</p> <p>This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.</p>
End User Disk Quota	<p>The End User Disk Quota alert is generated if disk quota configured for a Customer reaches the specified limit.</p> <p>This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.</p>
Boot VM Check	The Boot VM Check email report provides a complete list of Boot VM Check results. You can also access this information in the Global Management Portal.

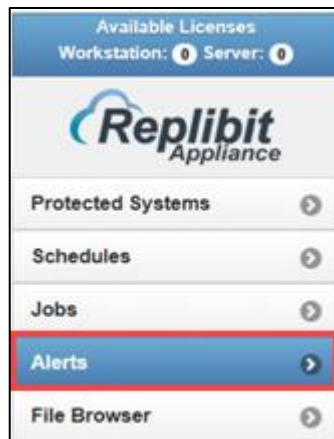
For instructions on integrating with ConnectWise, please reference the [Integrating with ConnectWise](#) section of this guide.

To view alerts in the Appliance Web interface:

1. Log in to the Appliance Web interface.

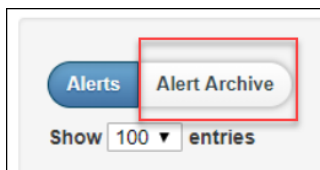
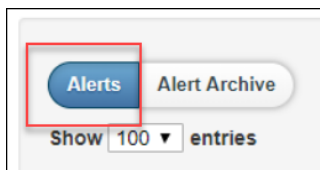


2. In the left-hand navigation menu, click the Alerts tab. The Alerts page displays, listing active alerts.



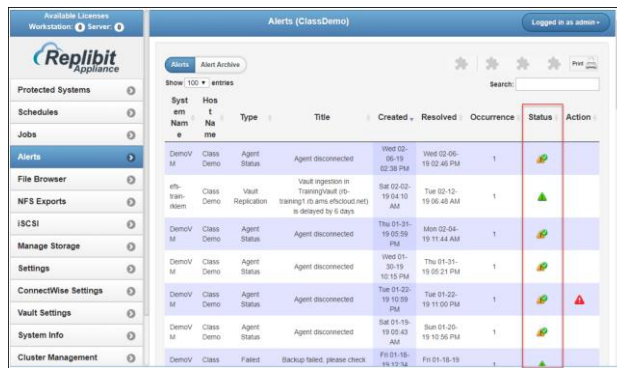
3. In the Alerts page, you can optionally toggle between active and archived alerts.

- Click the Alerts tab to view active alerts.
- Click the Alert Archive tab to view historical alerts.



Note: Retention of archived alerts is controlled by Jobs Auto Delete Settings, which is accessible by clicking the Settings tab.

4. In the *Alerts* page, read each alert to understand important events that occur in the system.
5. Use the *Status* column to view the status of alerts. Alert status can be *Active*, *Closed*, or *Auto Cleared*.
6. Hover your mouse over icons in the *Status* column to read their text label.

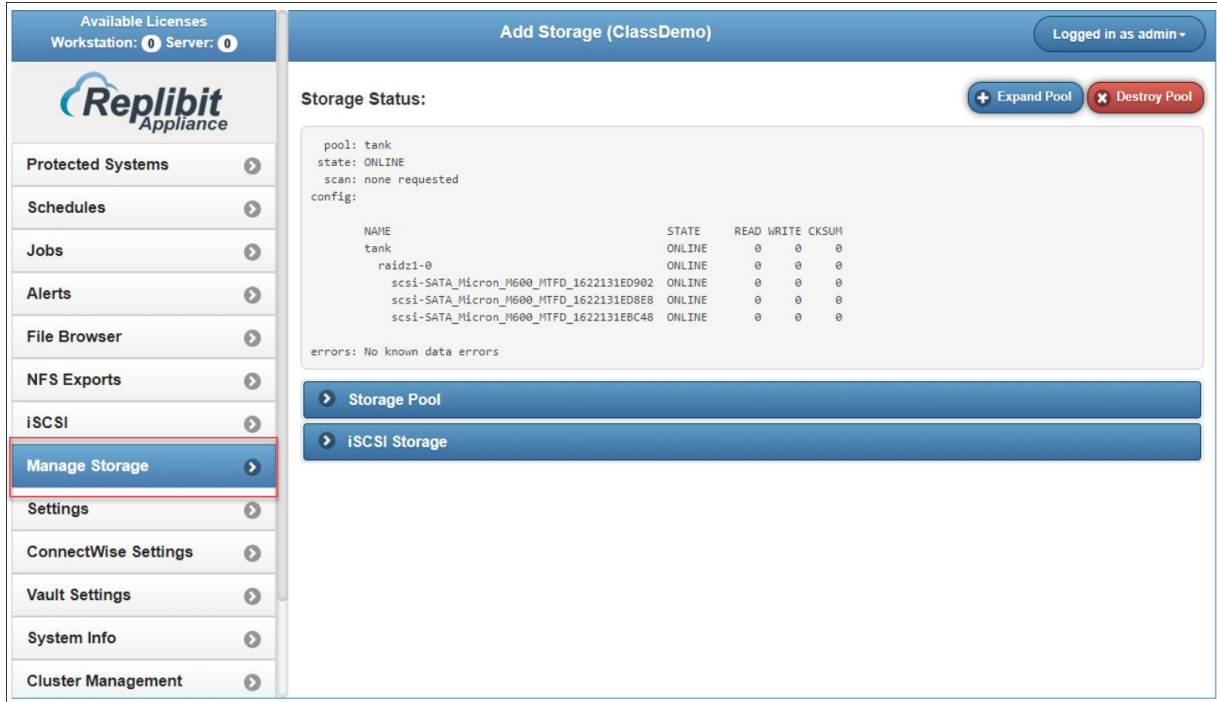


7. Optionally, click the **Action** button to manually close an Alert. Most alerts will be automatically cleared if the next attempt to perform the failed action succeeds.



Viewing Storage Settings for the Appliance

The *Manage Storage* page allows you to see the status and configuration of the Storage Pool and all disk volumes active within the system. From this menu pane, you can create or destroy the Storage Pool, replace failed disks and perform a rebuild of the Storage Pool, or add disks to the Storage Pool to expand storage capacity.

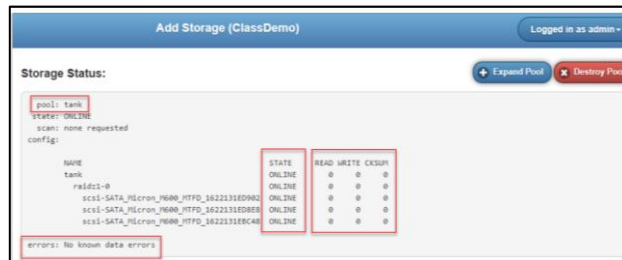


To view storage settings for the Appliance:

1. Log in to the Appliance Web interface.



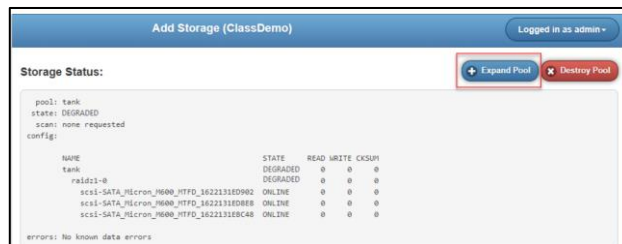
2. In the left-hand navigation menu, click the **Manage Storage** tab. The *Manage Storage* page displays, giving you access to storage settings.
3. In the *Storage Status* section, review the current configuration and status of the Storage Pool. For example:
 - The *Pool State* field should be marked as **Online**.
 - The *State* field should be marked as **Online**.



- The *State of each disk volume present* field should be marked as **Online**.
- The *Read, Write, and CKSum error count* columns should be marked as **0**.
- The *Errors* field should be marked as **No Known Errors**.

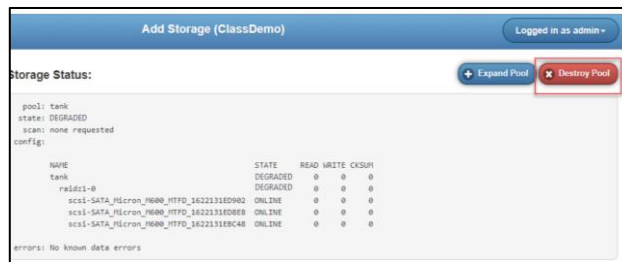
Note: Please contact Axcient Support if the Storage Status section does not display expected values.

- Optionally, click the **Expand Pool** button to scan for the Storage Pool size, change, and add the new storage space to the Pool.



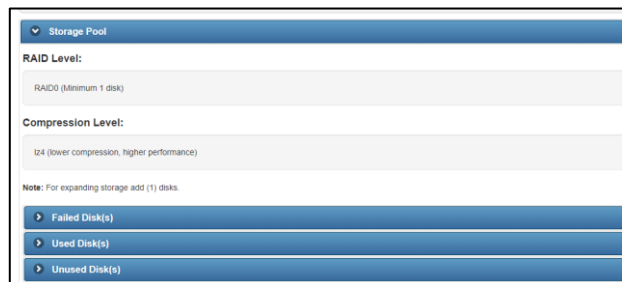
- Click the **Destroy Pool** button to delete the Storage Pool and all data.

Note: Use this option with caution. If you click Destroy Pool, the system will delete the Storage Pool and *all data and is irreversible*.



- Click the **Storage Pool** section to view failed, used, and unused disks.

- Click the **Failed Disks** sub-section to identify disks that have failed. You can also use this section to replace failed disks, if necessary. For more information, please reference the [Managing Failed Disks](#) section of this guide.
- Click the **Used Disks** sub-section to identify disks in use. This section is useful to view disk

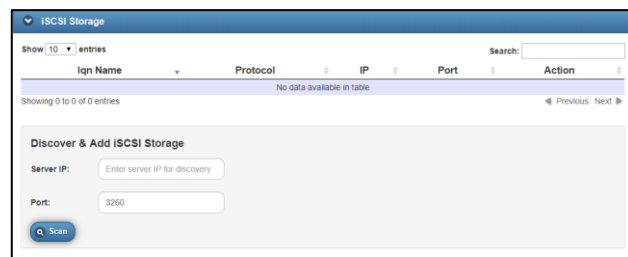


information, including disk status and size.

- Click the **Unused Disks** sub-section to identify disks not yet in use. This section can be used to expand the capacity of the Storage Pool, if necessary. For more information, please reference the [Expanding the Storage Pool](#) section of this guide.

7. Click the **iSCSI Storage** section to view any external iSCSI disk volumes.

iSCSI utilizes the network layer instead of a dedicated storage controller when performing disk and storage operations.



Note: We do not recommend mixing Local storage with iSCSI storage devices when creating the Storage Pool.

Managing Failed Disks

If you encounter critical errors with your storage pool, including a degraded or failed disk, you will need to replace these disks as soon as possible to reduce the risk of data loss.

To replace a failed disk:

1. Log in to the Appliance Web interface.
2. In the left-hand navigation menu, click the **Manage Storage** tab. The *Manage Storage* page displays, giving you access to storage settings.



3. In the *Manage Storage* page, click to expand the **Failed Disk** section. Failed disks will be listed in this section.
4. Click the **Replace** button to start the failed disk recovery process.
5. In the Replace Disk dialog box, select an unused disk that will be used to replace the failed disk.
 - In *Unused Disk* drop-down menu, select an **available disk** that is as large as or larger than the original failed volume.
 - Click the **Replace** button to begin rebuilding the RAID set onto the replacement drive.



Expanding the Storage Pool

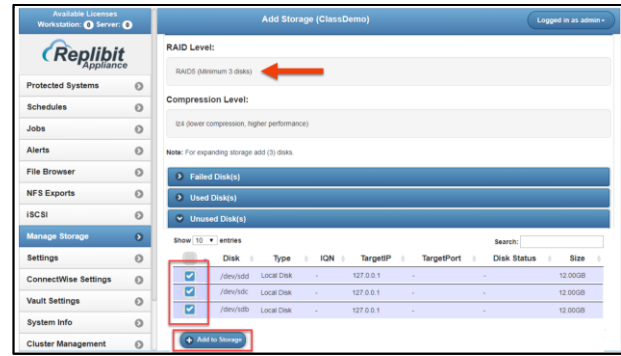
You can expand your Appliance storage pool if you need additional space for your Appliance. The *Unused Disks* section of the *Manage Storage* page can be used to expand the capacity of the Storage Pool, if necessary.

To replace expand the storage pool:

1. Log in to the Appliance Web interface.
2. In the left-hand navigation menu, click the **Manage Storage** tab. The *Manage Storage* page displays, giving you access to storage settings.



- In the *Manage Storage* section, click to expand the **Unused Disks** section. Unused disks will be listed in this section.
- Use the *Disks* checkboxes to select a set of disks that are the same size. The size does *not* have to be the same as other RAID sets already assigned to the Storage Pool.



Note: You will need to select the required *minimum number* of disks. *Minimum Disks* is defined as the number of disks used to initially create the Storage Pool.

- Click the **Add to Storage** button to create a new RAID set and add it to the existing Storage Pool.

Managing iSCSI Storage

You can optionally utilize iSCSI storage within your Appliance storage pool.

iSCSI utilizes the network layer instead of a dedicated storage controller when performing disk and storage operations. Keep in mind that multiple network adapters should be employed when utilizing iSCSI for the Storage Pool in order to prevent network performance bottlenecks.

We do *not* recommend mixing Local storage with iSCSI storage devices when creating the Storage Pool.

To manage iSCSI storage:

- Log in to the Appliance Web interface.
- In the left-hand navigation menu, click the **Manage Storage** tab. The *Manage Storage* page displays, giving you access to storage settings.



- In the *Manage Storage* page, click to expand the **iSCSI Storage** section.

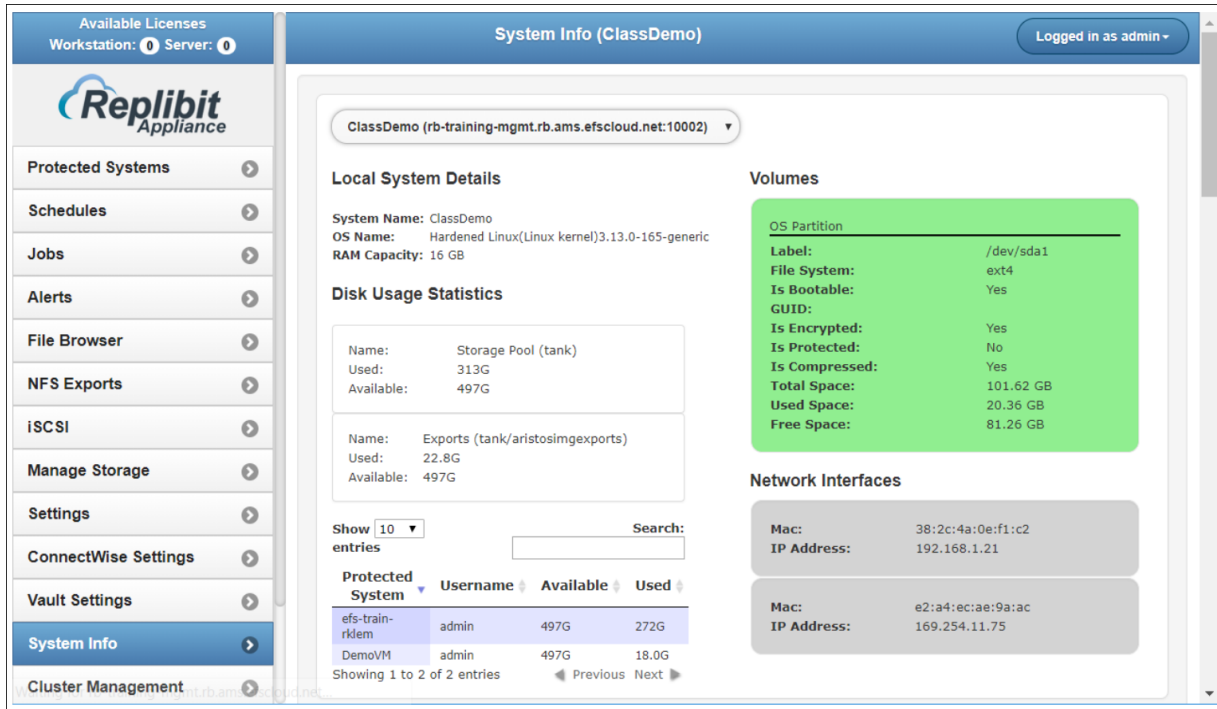
4. In the *iSCSI Storage* section, discover and add iSCSI storage:
 - In the *Server IP* field, enter the iSCSI Target Server IP address.
 - In the *Port* field, enter the port number if it has been changed from the default port.
 - Click the **Scan** button to search for accessible storage targets.
 - Use the drop-down menu to select from a list of discovered *iSCSI Targets*.
 - Optionally, if you need to configure CHAP authentication, click to enable **CHAP Logon Information** and enter the **username** and **password**.
 - Click **Connect** to save attach the iSCSI volumes.

The screenshot shows a web interface titled "Discover & Add iSCSI Storage". It contains the following elements:

- Server IP:** A text input field containing "192.168.90.251".
- Port:** A text input field containing "3260".
- Scan:** A blue button with a magnifying glass icon.
- iqn List:** A dropdown menu showing two identical entries: "iqn 2004-04.com.qnap:ts-451plus.iscsi.test.0f88b9".
- CHAP Logon Information:** A checkbox that is checked.
- Username:** A text input field with a password icon.
- Target Secret:** A text input field with a password icon.
- Buttons:** "Cancel" and "Connect" buttons at the bottom.

Viewing Appliance System Information

You can monitor Appliance system information from the *System Info* page in the Appliance Web interface. The *System Info* page displays detailed information about CPU usage, running processes, network data, disk usage, and more.

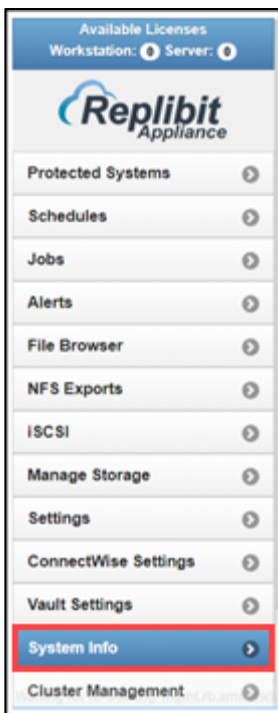


To view Appliance system information:

1. Log in to the Appliance Web interface.

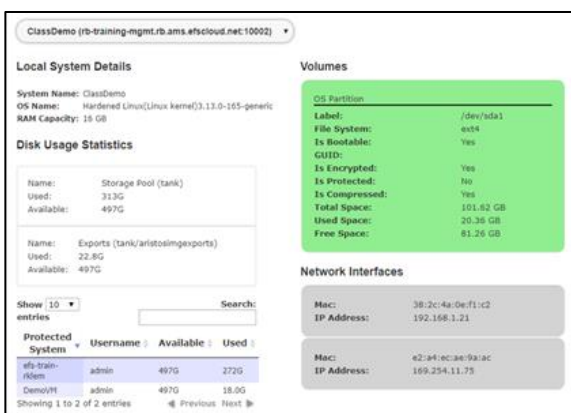


- In the left-hand navigation menu, click the **System Info** tab. The *System Info* page displays, showing an overview and summary of the system status of the Appliance.



- In the *System Info* page, review the following sections:

- In the *Local System Details* section, review the system name, operating system, and RAM capacity details.
- In the *Disk Usage Statistics* section, review information about each disk. You can view the name of the disk, as well as space used and space available.
- In the *Volumes* section, review information about the Operating System volume. For example, you can view the encryption status, total space, used space, and free space.
- In the *Network Interfaces* section, review network details, such as the MAC and IP address.



4. In the *System Detail Graphs* section, review the graphs in each panel. You can view the following information about the localhost:

- Load, memory, CPU, network activity, and packets in and out over the past hour.
- CPU idle, CPU user, CPU nice, CPU system, CPU nice, CPU wio over the past hour.
- Disk space available, total disk space, and maximum disk space over the past hour.
- Fifteen, five, and one minute load average over the past hour.
- Memory buffers, cached memory, and free memory over the past hour.
- Free Swap space over the past hour.
- Bytes received, bytes sent, packets received, and packets sent over the past hour.
- Total running processes and total processes over the past hour.



Managing Vaults

The Replibit Vault is the datacenter component of Replibit. Because the Vault receives replicated Protected System data, it is important that you perform basic administrative tasks to ensure the integrity of your data.

Whether you are vaulting to the Axcient Cloud or to your own Private Cloud datacenter, you can perform various management tasks within the Vault Web interface. For example, you can:

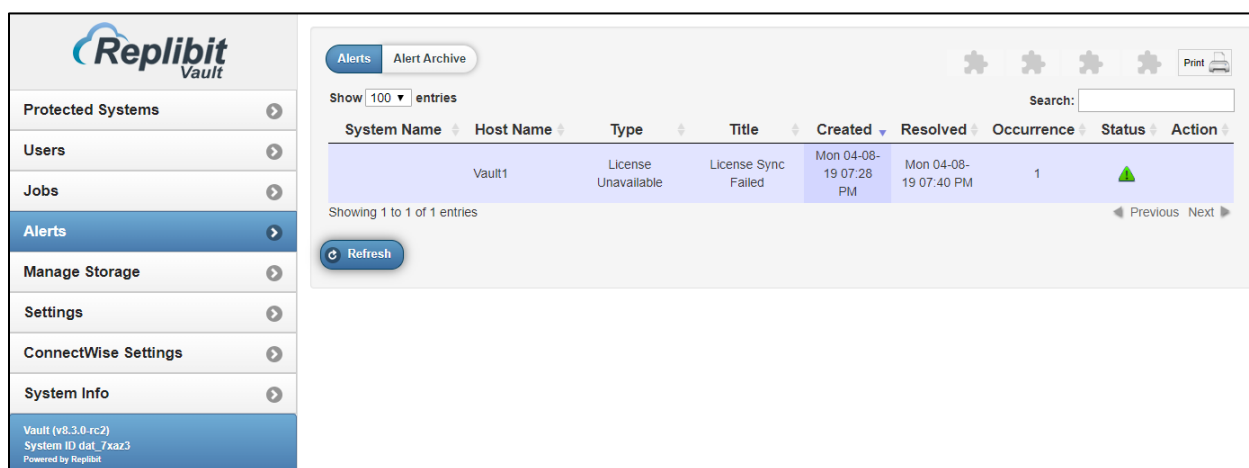
- Monitor alerts, and
- View system information.

If you vault to your own Private Cloud datacenter, you are responsible for performing hardware maintenance tasks. You can review recommendations and best practices in our [Knowledgebase](#).

If you vault to the Axcient Cloud, these tasks are performed for you by the Axcient team.

Monitoring Alerts in the Vault Web Interface

The *Alerts* tab shows the status of any active or recent alerts generated by the Vault. For example, you can track replication status, storage failures, and more.



The following alerts can be generated by the Vault:

Degraded Storage Volume in ZFS Pool

The Degraded Storage Volume in ZFS Pool alert is generated if a Vault storage volume has been marked as degraded.

	This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.
ZFS Pool Offline	The ZFS Pool Offline alert is generated if the entire ZFS Storage Pool is offline. This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.
Storage Pool at 80% Capacity	The Storage Pool at 80% Capacity alert is generated when storage capacity for the Vault is over 80% full. This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.
End User Disk Quota at 80% Capacity	The End User Disk Quota alert is generated if disk quota configured for a Customer reaches 80% of the specified limit. Replication will become blocked for the customer when storage usage reaches 100% of the defined limit. This alert will display in the <i>Alerts</i> tab. Optionally, you can configure an Email alert or a ConnectWise alert.
Boot VM Check	The Boot VM Check email report provides a complete list of Boot VM Check results. You can also access this information in the Global Management Portal.

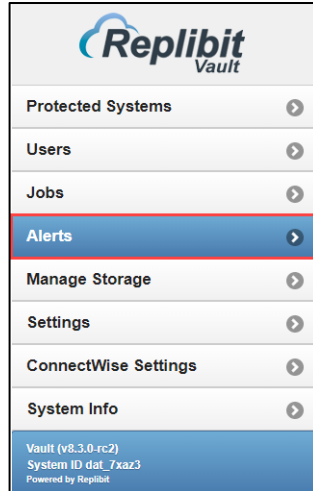
For instructions on integrating with ConnectWise, please reference the [Integrating with ConnectWise](#) section of this guide.

To view alerts in the Vault Web interface:

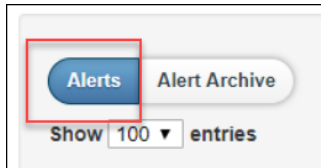
1. Log in to the Vault Web interface.



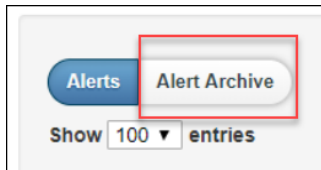
- In the left-hand navigation menu, click the Alerts tab. The Alerts page displays, listing active alerts.



- In the Alerts page, you can optionally toggle between active and archived alerts.

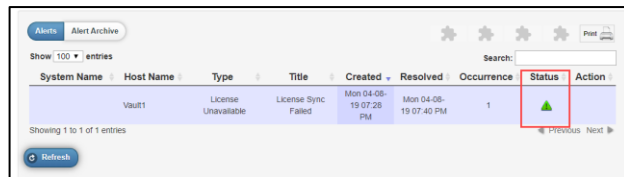


- Click the Alerts tab to view active alerts.
- Click the Alert Archive tab to view historical alerts.



Note: Retention of archived alerts is controlled by Jobs Auto Delete Settings, which is accessible by clicking the Settings tab.

- In the Alerts page, read each alert to understand important events that occur in the system.
- Use the Status column to view the status of alerts. Alert status can be Active, Closed, or Auto Cleared.
- Hover your mouse over icons in the Status column to read their text label.



- Optionally, click the Action button to manually close an Alert. Most alerts will be automatically cleared if the next attempt to perform the failed action succeeds.

Wed 02-06-19 02:38 PM	Wed 02-06-19 02:46 PM	1	
Sat 02-02-19 04:10 AM	Tue 02-12-19 06:48 AM	1	
Thu 01-31-19 05:59 PM	Mon 02-04-19 11:44 AM	1	
Wed 01-30-19 10:15 PM	Thu 01-31-19 05:21 PM	1	
Tue 01-22-19 10:59 PM	Tue 01-22-19 11:00 PM		

Viewing Vault System Information

You can monitor Vault system information from the *System Info* page in the Vault Web interface. The *System Info* page displays detailed information about CPU usage, running processes, network data, disk usage, and more.

System Info (ClassDemo) Logged in as admin

ClassDemo (rb-training-mgmt.rb.ams.efscld.net:10002)

Local System Details

System Name: ClassDemo
 OS Name: Hardened Linux(Linux kernel)3.13.0-165-generic
 RAM Capacity: 16 GB

Disk Usage Statistics

Name:	Storage Pool (tank)
Used:	313G
Available:	497G

Name:	Exports (tank/aristosimgexports)
Used:	22.8G
Available:	497G

Volumes

OS Partition

Label: /dev/sda1
 File System: ext4
 Is Bootable: Yes
 GUID:
 Is Encrypted: Yes
 Is Protected: No
 Is Compressed: Yes
 Total Space: 101.62 GB
 Used Space: 20.36 GB
 Free Space: 81.26 GB

Network Interfaces

Mac:	38:2c:4a:0e:f1:c2
IP Address:	192.168.1.21

Mac:	e2:a4:ec:ae:9a:ac
IP Address:	169.254.11.75

Protected Systems

Protected System	Username	Available	Used
efs-train-rklem	admin	497G	272G
DemoVM	admin	497G	18.0G

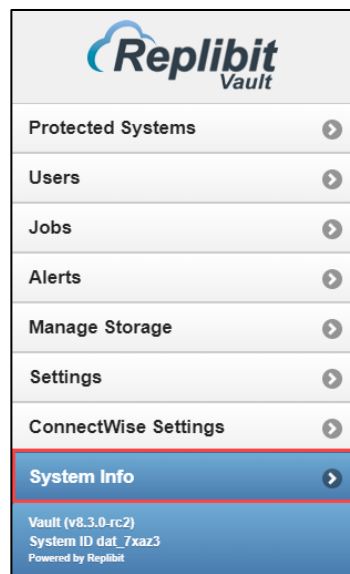
Showing 1 to 2 of 2 entries

To view Vault system information:

1. Log in to the Vault Web interface.

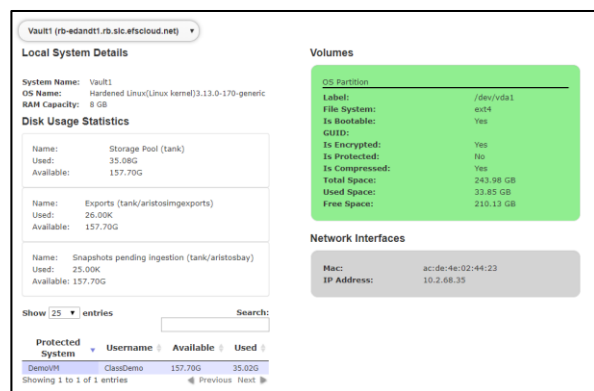


2. In the left-hand navigation menu, click the *System Info* tab. The *System Info* page displays, showing an overview and summary of the system status of the Vault.



3. In the *System Info* page, review the following sections:

- In the *Local System Details* section, review the system name, operating system, and RAM capacity details.
- In the *Disk Usage Statistics* section, review information about each disk. You can view the name of the disk, as well as space used and space available.
- In the *Volumes* section, review information about the Operating System volume. For example, you can



view the encryption status, total space, used space, and free space.

- In the *Network Interfaces* section, review network details, such as the MAC and IP address.
4. In the *System Detail Graphs* section, review the graphs in each panel. You can view the following information about the localhost:
- Load, memory, CPU, network activity, and packets in and out over the past hour.
 - CPU idle, CPU nice, CPU system, CPU user, and CPU wio over the past hour.
 - Disk space available, total disk space, and maximum disk space over the past hour.
 - Fifteen, five, and one minute load average over the past hour.
 - Memory buffers, cached memory, and free memory over the past hour.
 - Free Swap space over the past hour.
 - Bytes received, bytes sent, packets received, and packets sent over the past hour.
 - Total running processes and total processes over the past hour.

