## Contents

1. **About Acronis Cyber Appliance** .................................................. 1
   1.1 Acronis Cyber Appliance Exterior ................................................ 2

2. **Safety Instructions** .................................................................. 4

3. **Installing Acronis Cyber Appliance** ........................................... 5
   3.1 Unpacking Acronis Cyber Appliance ................................................. 6
   3.2 Mounting Acronis Cyber Appliance into Rack ................................. 6
   3.3 Connecting Cables to Acronis Cyber Appliance ............................ 9
   3.4 Configuring Acronis Cyber Appliance ........................................... 11

4. **Managing Licenses** ................................................................. 15
   4.1 Installing License Keys ............................................................. 16
   4.2 Installing SPLA Licenses ............................................................ 18

5. **Managing Updates** ................................................................. 19

6. **Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup** 22
   6.1 Deploying the Compute Cluster ................................................... 22
   6.2 Deploying the Acronis Cyber Backup “All-in-One” Appliance Virtual Machine 23
      6.2.1 Downloading the Acronis Cyber Backup “All-in-One” Appliance .......... 23
      6.2.2 Deploying the Acronis Cyber Backup “All-in-One” Appliance .......... 24
   6.3 Creating a Backup Gateway ....................................................... 26
   6.4 Performing Backup Operations .................................................. 27
      6.4.1 Adding Machines to Be Backed Up ........................................ 27
      6.4.2 Configuring a Backup Plan .................................................. 27

7. **Getting Technical Support** ...................................................... 30
8. Appendix: Specifications ................................................................. 32
   8.1 Technical Specifications ........................................................... 32
       8.1.1 Power Supply Specifications ............................................. 33
   8.2 Environmental Specifications .................................................... 33
       8.2.1 Air Quality Requirements .................................................. 34
About Acronis Cyber Appliance

Acronis Cyber Appliance provides a 5-node Acronis Cyber Infrastructure cluster in a 19-inch 3U rackmount server chassis. Acronis Cyber Appliance deploys into a universal and easy-to-use software-defined infrastructure solution that combines virtualization and storage. Powered by Acronis Cyber Infrastructure, it allows you to create and manage virtual machines and offers object, block, and file storage, including a local repository for cloud backups. You can also deploy Acronis Cyber Backup in the Acronis Cyber Infrastructure compute cluster, and have both the storage and the backup server running on Acronis Cyber Appliance.

Acronis Cyber Appliance comes in several models that vary by storage capacity:

<table>
<thead>
<tr>
<th>Model</th>
<th>Raw storage, TB</th>
<th>Usable storage*, TB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Capacity</td>
</tr>
<tr>
<td>15031</td>
<td>60</td>
<td>31</td>
</tr>
<tr>
<td>15062</td>
<td>120</td>
<td>62</td>
</tr>
<tr>
<td>15078</td>
<td>150</td>
<td>78</td>
</tr>
<tr>
<td>15093</td>
<td>180</td>
<td>93</td>
</tr>
<tr>
<td>15108</td>
<td>210</td>
<td>108</td>
</tr>
<tr>
<td>15124</td>
<td>240</td>
<td>124</td>
</tr>
</tbody>
</table>

* With the recommended redundancy scheme. Erasure coding 3+2 is recommended for capacity; replication=3 is recommended for performance.
1.1 Acronis Cyber Appliance Exterior

Acronis Cyber Appliance consists of five identical nodes. On the front of the appliance, under the front bezel are the power/reset buttons, a power LED of each node as well as the main power switch. The front panel also provides access to disks of each node: three per node, ordered left to right, i.e. the leftmost three disks are of node #1, the next three are of node #2, etc.

On the back of Acronis Cyber Appliance are two power sockets and a number of connectivity options.

Each node has its own network, IPMI, USB, and VGA ports.

The IPMI, USB, and VGA ports are only needed for advanced diagnostics. IPMI allows accessing the nodes
over the network for out-of-band management via a remote console. The default IPMI password to access the management node via SSH is Acronis!Infra%30 (it changes to a user-specified password during deployment). The USB and VGA ports allow you to connect a keyboard and a monitor to a node if the network is unavailable.

Day-to-day management of Acronis Cyber Appliance is done over the network through the admin panel, as described later in the guide.
Warning: Acronis Cyber Appliance may only be repaired by a certified service technician. You may only perform troubleshooting as authorized by the support team. Damage due to unauthorized repairs is not covered by the warranty.
CHAPTER 3

Installing Acronis Cyber Appliance

Before installing Acronis Cyber Appliance, make sure you have the following:

- 3U of server rack space in a standard 19-inch cabinet
- at least five free 1/10 GbE ports in a network switch (10 GbE recommended)
- at least five RJ45-to-RJ45 patch cables to connect the appliance to the switch
- two power sockets

If you want to set up network bonding, you will additionally need (a) five free 1/10 GbE ports in a network switch (10 GbE recommended) and (b) five RJ45-to-RJ45 patch cables to connect the appliance to the switch.

If you want to have access to the nodes from a remote console for out-of-band management, you will additionally need (a) six free 1 GbE ports in a network switch and (b) six RJ45-to-RJ45 patch cables to connect the appliance to the switch.

To install Acronis Cyber Appliance, perform the following steps:

1. Unpack Acronis Cyber Appliance.
2. Mount the appliance into rack.
3. Connect cables to the appliance.
4. Configure Acronis Cyber Appliance using the wizard.
5. Log in to the admin panel and install a license.
6. Set up the desired workloads in the admin panel.
Steps one through six are described in the following sections. For more information about step seven, refer to Administrator’s Guide.

### 3.1 Unpacking Acronis Cyber Appliance

Inspect the packaging contents for damage before mounting the appliance and connecting power.

Before continuing, make sure the following items are present in the packaging: the appliance chassis, mounting rails, two power cables, this quick start guide.

### 3.2 Mounting Acronis Cyber Appliance into Rack

The appliance comes with a set of server rails. Follow the steps further to install the rail and mount Acronis Cyber Appliance into the rack.

1. Separate inner and outer rails.

   Separate the inner rail from the outer rail by sliding the inner rail forward until the locking tab is visible, as per the illustration below. Depress the tab and separate the inner rail from the outer rail by sliding the two apart.
2. Attach the inner rail to the appliance.

   Align the rectangular cutouts on the inner rail to the pre-formed bayonets on the side of chassis. Secure the inner rail with a screw from the standard screw kit after all the bayonets go through the cutouts and properly engage.

3. Install the outer rail into the rack.

   When selecting the location, note that the rails are in the middle of the appliance. Make sure that you install the outer rails with 1U clearance above and below.

   Make sure that the safety lock is unlocked before mounting the brackets.

   Insert the locating pins into the upper and lower square holes on the rail from the back of rail. Push the safety lock forward to secure the bracket.
4. Mount the chassis into the cabinet.

**Important:** Two people are required to perform this step.

Insert the inner rail into the outer rail as shown on the figure.

**Important:** Make sure that the ball retainer is fully open before installing the chassis. Otherwise, you risk damaging the chassis!
3.3 Connecting Cables to Acronis Cyber Appliance

**Note:** For more details on configuring the network infrastructure, see the Installation Guide.

To prepare Acronis Cyber Appliance for configuration, do the following:

1. Connect the appliance to the electrical outlets using the supplied power cables.
2. On every node, connect any SFP+ or RJ45 network port (1 on the diagram) to a switch (2 on the diagram) with access to a dedicated subnet for your infrastructure. Then, connect the admin laptop (3 on the
3. (Optional) Connect the out-of-band management network interfaces of each node and the chassis (1 on the diagram) to a switch with access to the IPMI subnet for your appliance (2 on the diagram). The nodes have preconfigured IPMI IP addresses: 10.20.30.11 to 10.20.30.15. The chassis has the preconfigured IPMI IP address 10.20.30.10. Connect the admin laptop (3 on the diagram) to the same switch.

**Important:** The nodes have preconfigured IP addresses: 10.20.20.11 to 10.20.20.15.
3.4 Configuring Acronis Cyber Appliance

Perform the following steps to configure Acronis Cyber Appliance:

1. Turn on the power: (a) press and hold down the main switch for five seconds, (b) press the power buttons of each node.

2. Connect an admin laptop (from which you will configure Acronis Cyber Appliance) to the network. Assign a static IP address to it from the same subnet that nodes are in, e.g., 10.20.20.100. As mentioned before, the nodes have preconfigured IP addresses: 10.20.20.11 to 10.20.20.15.

3. On this computer, open a web browser and visit the default primary node IP address 10.20.20.11. The wizard has been tested to work in the latest Firefox, Chrome, and Safari web browsers.

4. Once the configuration wizard is displayed, click Configure.

5. Review and accept the license agreement. Then, click Next.
6. On the next step, enter the following:

- New host names for all nodes (or leave the default names). You can rename the nodes to fit your organization's naming policies or make them relevant to your organization.

- New static IP addresses for the network interfaces connected on all the nodes. If you leave the fields empty, the default addresses 10.20.20.11 to 10.20.20.15 will be used.

- Virtual IP address at which you will access the highly available admin panel. You can read more about high availability in the Administrator’s Guide.

- Network mask. Consult your network administrator for the proper network/subnet mask.

- At least one local DNS server.

- Gateway. Consult your network administrator for the proper gateway address.

- Domain name (optional). If this system will be visible from the Internet or if you wish to bind it to your organization's domain, provide the domain prefix and suffix.

- Time zone and time. Since nodes communicate with each other, they must be on the same time zone and have the same time in order to ensure proper synchronization. Click Change time settings to set the correct time zone and time.
### Important:
Entered values cannot be changed later.

### Configure appliance

#### Configure network parameters
Enter new IP addresses for the currently connected network interfaces on each node and provide other details.

<table>
<thead>
<tr>
<th>Node</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>10.20.20.11</td>
</tr>
<tr>
<td>node2</td>
<td>10.20.20.12</td>
</tr>
<tr>
<td>node3</td>
<td>10.20.20.13</td>
</tr>
<tr>
<td>node4</td>
<td>10.20.20.14</td>
</tr>
<tr>
<td>node5</td>
<td>10.20.20.15</td>
</tr>
<tr>
<td>Virtual IP address for HA management</td>
<td>10.20.20.100</td>
</tr>
</tbody>
</table>

- **Network mask**: 255.255.255.0
- **Gateway**: 10.20.20.1
- **DNS server**: 8.8.8.8
- **2nd DNS server (optional)**: 8.8.4.4

7. On the next step, enter the cluster name (you cannot change it later) and the cluster administrator password.

---

If one or more nodes are not reachable from the primary node, they will be marked as offline. In this case, make sure the nodes are powered on and connected to the correct network. Deployment will be blocked until all nodes are green (accessible and configurable by the primary node).

### Note:
You will be able to configure bonds and VLANs later in the admin panel.

Click **Next**.
Chapter 3. Installing Acronis Cyber Appliance

Click **Submit**. Configuration will begin, as indicated on the progress bar.

8. Wait until the progress bar reaches the end, and change the IP address of the admin laptop to a free one from which you can access Acronis Cyber Appliance.

9. Once configuration is completed, you will see a link to the cluster admin panel. Log in with the username `admin` and the specified password. The admin panel has been tested to work at resolutions 1280x720 and higher in the latest Firefox, Chrome, and Safari web browsers.

10. Proceed to **SETTINGS > Licenses** and upgrade the default trial license either by a key or SPLA (for more details, see *Managing Licenses* (page 15)). If you do not have a license, contact your sales representative.

11. If you need to make additional changes to network configuration, e.g., create bonds and VLANs, connect cables to other network ports and follow the instructions in the **Administrator’s Guide**.

After deployment, update the product to the latest version (see *Managing Updates* (page 19)). Then, you can configure the cluster for using Acronis Cyber Backup (see *Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup* (page 22)), or other desired workload as described in the **Administrator’s Guide**.
CHAPTER 4

Managing Licenses

Acronis Cyber Appliance is licensed for two types of deployments:

- Hybrid cloud. Comes with a 3-year hardware warranty and requires a subscription for Acronis Backup Cloud. After 3 years, the hardware warranty needs to be renewed for another 1 or 3 years.
  
  For this deployment type, you will need to install a SPLA license as described in *Installing SPLA Licenses* (page 18).

- Private cloud. Comes with a 3-year license for Acronis Cyber Infrastructure and hardware warranty. After 3 years, both the license and warranty need to be renewed for another 1 or 3 years.
  
  For this deployment type, you will need to install a license key as described in *Installing License Keys* (page 16).

For more details on licensing options, see the Knowledge Base article #62324.

Acronis Cyber Infrastructure supports the following licensing models for production environments:

- License key. Implementing the provisioning model, keys are time-limited (subscription) or perpetual and grant a certain storage capacity. If a commercial license is already installed, a key augments its expiration date or storage limit.

- Services provider license agreement (SPLA). SPLA implements the pay-as-you-go model: it grants unlimited storage capacity and customers are charged for the actual usage of these resources. With SPLA, Acronis Cyber Infrastructure automatically sends reports to Acronis Cyber Cloud once every four hours. If no reports have been received for two weeks, the license expires. For reports to reach destination, the cluster must be able to access the Acronis datacenter that has been used to enable SPLA. Make sure that TCP port 443 is open.
Note: SPLA license is valid for Cloud Partners. If SPLA is enabled, you can connect Backup Gateway only to Acronis Backup Cloud and not to Acronis Backup 12.5 or Acronis Backup Advanced 12.5. To connect Backup Gateway to these products, you will need to use license keys. Furthermore, Acronis Backup Gateway usage is not counted in SPLA in Acronis Cyber Infrastructure. SPLA only counts universal usage that is not related to backup. Backup usage is shown in the Acronis Backup Cloud section of Acronis Cyber Cloud.

You can switch the licensing model at any time:

• Switching from a license key to SPLA terminates the key even if it has not yet expired. Terminated keys cannot be used anymore.

• Switching from SPLA to a license key changes the licensing model to subscription or perpetual. After doing so, ask your service provider to terminate your SPLA by either disabling the Storage application for your account or deleting the account.

Important: If a license expires, all write operations to the storage cluster stop until a valid license is installed.

4.1 Installing License Keys

To install a license key, do the following:

1. If you are switching from SPLA, ask your service provider to terminate the agreement by either disabling the Acronis Cyber Infrastructure application for your account or deleting the account.

2. On the SETTINGS > Licenses screen, click Upgrade and Register key.
3. In the **Register license key** window, paste the license key and click **REGISTER**.

4. Back on the **Licenses** screen, click **Activate** if you are activating from a trial or choose one of the following:

   - **Upgrade**, to add storage capacity to the active license.
   - **Prolong**, to prolong the soon-to-be-expired license.

   And click **Activate**.
The expiration date or storage capacity will change according to what the key grants.

4.2 Installing SPLA Licenses

To install a SPLA license, do the following:

1. On the SETTINGS > Licenses screen, click Upgrade and Use SPLA.

2. In the Use SPLA window, select a region from the drop-down list and click Activate. You will be redirected to a login page of Acronis Cyber Cloud.

Note: For more information on datacenters, see https://kb.acronis.com/servicesbydc.

3. Log in to Acronis Cyber Cloud.

4. In the Register cluster window, accept the license agreement.

5. In the registration confirmation window, click Done.

The registered cluster will show up in Acronis Cyber Cloud. You will be able to monitor its resource usage and download reports.
CHAPTER 5

Managing Updates

Acronis Cyber Infrastructure supports non-disruptive rolling updates. Cluster nodes are updated one by one, with the data availability unaffected. During the update, the node enters maintenance mode and its workloads and VMs are migrated to other nodes. After the update, the node returns to operation. For more information on the maintenance mode, see Performing Node Maintenance.

Take note of the following before you start updating nodes:

• To check for and download updates, the cluster must be healthy and each node in the infrastructure must be able to open outgoing Internet connections. This means, in particular, that cluster DNS must be configured and point to a DNS able to resolve external host names. For more details, see Adding External DNS Servers.

• Unassigned nodes cannot be updated.

• Updates are applied to one storage cluster node at a time.

• If you enable any third-party repositories like EPEL, make sure that packages from the official repository, hci.repo, are never overwritten by packages from the third-party repositories. Disable such repositories when you do not need them anymore. Otherwise, product stability may be at risk.

To update the storage cluster from the admin panel, do the following:

1. Open the SETTINGS > Updates screen. The date of the last check is displayed in the upper right corner. Click the round arrow to check for new updates. If updates are available for a node, that node’s update status changes to Available.
2. Click Download in the upper right corner to get the updates. When the updates are downloaded to a node, its update status changes to Ready to install. After the updates have been downloaded for all of the nodes, the button will change to Install. Click it to continue.

3. In the Install updates window, choose how to proceed if a node needs to be rebooted but cannot enter maintenance mode. To avoid downtime, nodes that need to be rebooted are placed in maintenance mode one by one during the update. Nodes that cannot enter maintenance mode are skipped and not updated by default. By selecting the checkbox, you can instead stop the update if some of the nodes cannot enter maintenance mode. Nodes that have already been updated will remain so.

Click Install.

While the updates are being installed, you can pause or cancel the process.

4. If you have chosen to abort the update if some of the nodes cannot enter maintenance and it happens, a window will open showing the reasons why the nodes cannot enter maintenance. You will need to decide how to proceed. You can cancel the update, solve the issues, and retry updating without
downtime. Or you can force the update on the listed nodes at once. In the latter case, the nodes in question will be rebooted, potentially causing a downtime of services running on them.

After the update is complete, node statuses will change to **Up to date**.

To update the kernel with ReadyKernel, consult *Updating Kernel with ReadyKernel*. 
CHAPTER 6

Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup

This section describes how to deploy and configure the Acronis Cyber Backup in form of “All-in-One Appliance” virtual machine in Acronis Cyber Infrastructure. You can then connect your Acronis Cyber Appliance cluster to Acronis Cyber Backup as a storage backend. As a result, you will have both the storage and the backup server running on Acronis Cyber Appliance.

6.1 Deploying the Compute Cluster

Before creating a compute cluster, make sure the network is set up according to recommendations in Managing Networks and Traffic Types. The basic requirements are: (a) the traffic types VM private, VM public, Compute API, and VM backups must be assigned to networks; (b) the nodes to be added to the compute cluster must be connected to these networks and to the same network with the VM public traffic type.

Once you've configured the networks, you can proceed to create the compute cluster:

1. On the COMPUTE screen, click Create compute cluster and configure the cluster settings in the Configure compute cluster window as follows.

2. In the Nodes section, select all the nodes and make sure the network state of each selected node is Configured. Then, click Next.
If node network interfaces are not configured, click the cogwheel icon, select networks as required, and click **Apply**.

3. In the **Public network** section, leave the IP address management disabled if you want the IP address for Acronis Cyber Backup Appliance virtual machine to be allocated by an external DHCP server. Otherwise, you can enable it. For more information, refer to [Creating the Compute Cluster](#).

4. In the **Summary** section, review the configuration and click **Create cluster**.

You can monitor compute cluster deployment on the **Compute** screen.

### 6.2 Deploying the Acronis Cyber Backup “All-in-One” Appliance Virtual Machine

#### 6.2.1 Downloading the Acronis Cyber Backup “All-in-One” Appliance

1. Go to [https://account.acronis.com/](https://account.acronis.com/) and log in to your account. If you do not have one, you will need to create it—refer to [Registration at Acronis Website](#).

2. Register your Acronis products, if not done before. Refer to [Registering Acronis products at the website](#).

3. In the **Products** section, locate the Acronis Cyber Backup download links. Refer to [Downloading the Latest Build of Acronis Software](#).

4. Download **AcronisBackup_All-in-One_Appliance.zip**.

5. Extract **AcronisBackupAppliance.iso**.

6. Add this image to the Acronis Cyber Infrastructure compute cluster as follows:

   6.1. On the **COMPUTE > Virtual machines > IMAGES** tab, click **Add image**.

   6.2. In the **Add image** window, click **Browse** and select the ISO file.

   6.3. Specify the image name and select the **Generic Linux** OS type. Click **Add**.

   For more information, refer to [Uploading, Editing, and Removing Images](#).
6.2.2 Deploying the Acronis Cyber Backup “All-in-One” Appliance

The Acronis Cyber Backup “All-in-One” Appliance is a pre-configured virtual machine that you deploy in Acronis Cyber Infrastructure. For more information about the appliance, refer to Acronis Backup appliance.

1. On the COMPUTE > Virtual machines > VIRTUAL MACHINES tab, click Create virtual machine. A window will open where you will need to specify VM parameters.

2. Specify a name for the new VM.

3. In Deploy from, choose Image.

4. In the Images window, select AcronisBackupAppliance.iso and click Done.

5. In the Volumes window, you do not need to add any volumes. The volume added automatically for the system disk is sufficient for Acronis Cyber Backup installation.

6. In the Flavor window, choose the large flavor and click Done. This flavor will provide 4 vCPUs and 8 GB of RAM for the Acronis Cyber Backup virtual appliance.

7. In the network window, click Add, select a public virtual network interface and click Add. It will appear in the Network interfaces list. For more information on the interfaces, refer to Creating Virtual Machines.

8. Back in the Create virtual machine window, click Deploy to create and boot the VM.

9. On the COMPUTE > Virtual machines > VIRTUAL MACHINES tab, select the created virtual machine. Then, click Console and install the Acronis Backup OS by using the built-in VNC console.
9.1. On the initial installer screen, select **Install or update Acronis Backup** and press **Enter**.

![Installer Screen](image)

**Note:** The initial installer times out after 15 seconds, and the system attempts to boot from the newly created virtual volume. If you see the message “Booting from local disk... No bootable device”, restart the virtual machine by clicking **Send keys > Ctrl + Alt + Del**

9.2. Specify the installation settings: a host name (optional) and a password for the root user.
Chapter 6. Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup

After the installation completes, the login screen details for the Acronis Backup console are displayed. Use the Acronis Cyber Backup console to configure and manage backup operations.

![Acronis Backup appliance initial setup](image)

After the installation completes, the login screen details for the Acronis Backup console are displayed. Use the Acronis Cyber Backup console to configure and manage backup operations.

**Note:** To install the full Acronis Cyber Backup license, refer to [Acronis Backup licensing](#).

### 6.3 Creating a Backup Gateway

1. In the Acronis Cyber Infrastructure admin panel, navigate to **Storage Services**, and then to **Backup Storage**. Here, you can see all the nodes in the storage cluster that can be used as backup destinations. Select all the nodes, and then click **Create gateway**. In the right panel, click **This cluster**.

2. Make sure the correct network interface is selected in the drop-down list. Click **NEXT**.

   If necessary, click the cogwheel icon and configure node's network interfaces on the **Network Configuration** screen.

3. Select the **Encoding 3+2** redundancy mode.

4. Specify a DNS name that will be associated with the selected cluster and used to register that cluster within Acronis Cyber Backup (like `backup.example.com`). The new DNS name is associated with each node's IP address in the selected cluster. A specific node for backup operations is selected.
automatically by the backup agent. Click Next.

5. To register this storage in backup software, specify the URL with IP address or hostname of the machine to access the Acronis Cyber Backup console (example: http://192.168.128.212:9877). If you use https, make sure the SSL certificate is trusted. Provide the credentials of the local management server administrator (e.g. “root”). Click Next.

6. Finally, click DONE.

6.4 Performing Backup Operations

6.4.1 Adding Machines to Be Backed Up

Before you can back up a machine, you must install a backup agent. Agents are applications that perform data backup, recovery, and other operations on the machines managed by Acronis Cyber Backup. Choose an agent, depending on what you are going to back up. For more information, see the full list of supported operating systems and environments.

1. Open Acronis Cyber Backup console in your browser and log in.

2. To add a machine to the management server, click All devices > Add. You will be asked to select the setup program based on the type of the machine that you want to add.

3. Once the setup program is downloaded, run it locally on that machine.

6.4.2 Configuring a Backup Plan

A backup plan is a set of rules that specify how data will be protected on a given machine. To create a backup plan, follow the steps:

1. Select the machines that you want to back up.

2. Click Backup. The new backup plan template opens.
3. Click **Where to back up**.

4. Click **Add location**, and select **Acronis Cyber Infrastructure**.
5. Click **Done**.

6. Click **Create to create a new plan**. To run an existing backup plan, click **Run now**.

For detailed information on how to configure and use Acronis Cyber Backup, see the **product documentation**.
CHAPTER 7

Getting Technical Support

If you need technical support, please contact Acronis as follows:

1. Visit the contact support page at https://www.acronis.com/en-us/support/contact-us/.

2. Log in to your account.

3. Select the product you are using.

4. Choose how you would like to contact the support team: via e-mail or phone.

Please be ready to provide support engineers with remote access to your Acronis Cyber Appliance, per your Service Level Agreement. To maintain security, it is recommended to whitelist only specific IP addresses communicated to you by support engineers and block external access from any other addresses. For more information, see the Knowledge Base at https://kb.acronis.com/sdiremote.

You can also use the following self-service resources:

• Knowledge base, https://kb.acronis.com/, a repository of frequently asked questions, step-by-step instructions, and articles about known issues. Visit the following knowledge base sections for information on Acronis Cyber Appliance and related software solutions:
  • Acronis Cyber Appliance, https://kb.acronis.com/acronis-appliance
  • Acronis Cyber Infrastructure, https://kb.acronis.com/acronis-cyber-infrastructure
  • Acronis Backup Cloud, https://kb.acronis.com/acronis-backup-cloud
  • Acronis Backup 12.5, https://kb.acronis.com/acronis-backup-12-5

• User documentation, guides describing how to use Acronis Cyber Appliance as well as Acronis software, https://www.acronis.com/support/documentation.
For information on Acronis Cyber Appliance warranty, see the Support section at https://www.acronis.com/en-us/support/hwappliance-support.
This chapter lists technical and environmental specifications of Acronis Cyber Appliance.

### 8.1 Technical Specifications

The following table lists Acronis Cyber Appliance hardware parts.

<table>
<thead>
<tr>
<th>Chassis</th>
<th>3U, 435x130x600 mm (WxHxD), 34.5 kg</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Atom C3958 @ 2.00GHz, 16 cores, 31W TDP, VT-d support, w/o Hyper-Threading</td>
</tr>
<tr>
<td>RAM</td>
<td>32GB (up to 256GB), Samsung, 2x16GB DDR4-2400 ECC</td>
</tr>
<tr>
<td>OS drive</td>
<td>1x Intel S4600 240GB 2.5-inch SSD</td>
</tr>
<tr>
<td>Cache drive</td>
<td>1x Intel S4600 240GB 2.5-inch SSD</td>
</tr>
<tr>
<td>Storage drives</td>
<td>3x Seagate 4/8/10/12TB enterprise SATA HDD per node, 15x in total</td>
</tr>
<tr>
<td>Network</td>
<td>2x 1/10GbE RJ45, 2x 10GbE SFP+</td>
</tr>
<tr>
<td>Power supply</td>
<td>750W 1+1, current share and cold redundancy depending on power loads (also see table below)</td>
</tr>
<tr>
<td>IO ports</td>
<td>Rear: 2x USB 2.0, 1x VGA, 2x 1/10GbE RJ45, 2x 10GbE SFP+, 1x GbE RJ45 management</td>
</tr>
<tr>
<td>Software</td>
<td>Acronis Cyber Infrastructure 3.5</td>
</tr>
<tr>
<td>Data protection</td>
<td>Replication and erasure coding via storage policies</td>
</tr>
</tbody>
</table>

Continued on next page
Table 8.1.1 – continued from previous page

| Redundancy                                      | Hot-swappable data disk drives |
|                                                | 2x hot-swappable power supplies |
|                                                | No single point of failure     |
|                                                | Non-disruptive online software upgrades |

| Monitoring, management                        | CLI, GUI, API, IPMI |

8.1.1 Power Supply Specifications

The following table lists appliance power supply specifications.

| Voltage, frequency                           | 100-240 V, 50/60 Hz |
| Power consumption, W                        | 750                |
| Heat dissipation max (BTU/hr)               | 2,300              |
| Max inrush, A                               | 40                 |
| Input current                               |                    |
| AC input                                    |                    |
| 100–127 Vac, 8.8 A                          | Max. current       |
| 200–240 Vac, 4.3 A                          |                    |
| Power supply efficiency                     |                    |
| (Platinum class)                            |                    |
| 10% load                                    | 20% load           |
| 80%                                          | 90%                |
| 50% load                                    | 94%                |
| 100% load                                   | 91%                |
| Input power factor correction*              |                    |
| Output power                                |                    |
| 20% load                                    | 50% load           |
| Power factor                                |                    |
| >0.80                                       | >0.95              |
| >0.95                                       | >0.95              |

* Tested at 230 Vac, 50 Hz and 115 Vac, 60 Hz. The input power factor is greater than values in the table at power supply's rated output and meets Energy Star® requirements.

8.2 Environmental Specifications

Acronis Cyber Appliance environmental specifications are listed in the following tables.

| Store temperature                          | -40°C to 85°C (-40°F to 185°F) |
| Store temperature gradient                | 20°C (68°F) per hour           |
| Operating temperature                     | 10°C to 35°C (50°F to -95°F)   |
| Operating temperature gradient            | 20°C (68°F) per hour           |

Continued on next page
<table>
<thead>
<tr>
<th>Table 8.2.1 – continued from previous page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative humidity percentage range for storage</td>
</tr>
<tr>
<td>Relative humidity percentage range for operating</td>
</tr>
<tr>
<td>Vibration for storage</td>
</tr>
<tr>
<td>Vibration for operating</td>
</tr>
<tr>
<td>Shock for storage</td>
</tr>
<tr>
<td>Shock for operating</td>
</tr>
<tr>
<td>Altitude for storage</td>
</tr>
<tr>
<td>Altitude for operating</td>
</tr>
</tbody>
</table>

### 8.2.1 Air Quality Requirements

The air must be free of:

- corrosive dust and/or corrosive contaminants
- conductive dust or conductive particles (such as zinc whiskers)

Airborne residual dust must have a deliquescent point* less than 60% relative humidity. (*The relative humidity at which crystalline materials begin adsorbing large quantities of water from the atmosphere.)

Gaseous corrosion level in terms of (in Angstrom) as per ISA:

- Copper reactivity rate must be less than 300 A/month, class G1(ANSI/ISA71.04-1985).
- Silver reactivity rate must be less than 200 A/month (AHSRAE TC9.9).