

IDrive[®] BMR Pro

User Guide

Explore the features offered by IDrive BMR to get started with your disaster recovery plan.



| | |
|-------------------|-------|
| Overview | 1-1 |
| Sign in | 2-3 |
| Admin | 4-5 |
| Dashboard | 5-16 |
| Restore | 16-20 |
| Virtualization | 21-25 |
| Cloud Replication | 26-27 |
| Cloud Seeding | 28-30 |
| NAS | 30-35 |
| Settings | 35-40 |
| Statistics | 40-41 |
| Logs | 42-42 |
| Cloud Manage | 43-45 |



Overview

IDrive BMR offers cost-effective disaster recovery for SMBs.

Secure Physical Machines

You can backup entire Windows computers to the IDrive BMR device and restore them in the event of a disaster. The BMR backup includes the operating system, applications, and configurations.

Restore data from your backed-up physical machines through any of the following methods:

1. If you need quick access to a few files/folders from the backup, you can use the file-level restore method. Refer to 'File Restore (from physical machines backup)' under the ['Restore'](#) section.
2. Perform a bare-metal recovery to the same or a new target machine. Refer to 'System Restore (Bare-metal Restore using WinRE)' under the ['Restore'](#) section.
3. For faster recovery and business continuity, create a virtual instance of the protected machines on the IDrive BMR device or IDrive Cloud. Refer to the ['Virtualization'](#) section.

Secure VMware Machines

Backup your virtual machines hosted on VMware ESXi and vCenter servers by adding the servers and selecting VMs to backup to the IDrive BMR device. You can add or remove the VMs as needed.

Restore data from your backed-up VMware machines through any of the following methods:

1. For quick access to files/folders of a protected VM, use the file-level restore method. Refer to 'VMware File Restore' under the ['Restore'](#) section.
2. Perform a system restore to the same or a new VM on your esxi host or vCenter. Refer to 'VMware System Restore' under the ['Restore'](#) section.
3. For faster recovery and business continuity, create a virtual instance of the protected machines on the IDrive BMR device or IDrive Cloud. Refer to the ['Virtualization'](#) section.

Create, host, and backup network shares

Utilize your IDrive BMR device storage for convenient data storage and sharing by creating NAS/ iSCSI shares. You can capture instant local snapshots or schedule regular snapshots of your shares to ensure data security.

You can recover your NAS share data by creating a network recovery path over the SMB protocol. Your iSCSI shares can be restored to the same or a secondary iSCSI target. Refer to 'Restore the network shares on the IDrive BMR device' under the ['NAS'](#) section.

Cloud Replication and Seeding

You can also transfer the backups stored on your IDrive BMR device to an offsite location through cloud replication. Additionally, you can expedite initial data transfer through Cloud Seeding. (Transfer large volumes of data stored on the IDrive BMR device to your cloud account using an external storage device that will be shipped to you. This ensures fast transfer and zero bandwidth consumption.)

Sign in

Access the web interface of your IDrive BMR device from any network via cloud manage. Sign in to www.idrive.com with your IDrive BMR credentials. All your IDrive BMR devices are listed under the 'All BMR Devices' tab. Navigate to the required device and click the 'Connect' button corresponding to it to establish browser-based access to the device interface. Click 'Cloud Replication' to view the cloud backup statuses and view and manage the cloud recovery points.

Alternatively, you can access the device interface from any computer that is on the same LAN as the IDrive BMR device.

- Navigate to bmrdevice.idrive.com on your browser to get a list of all the IDrive BMR devices that are online on your network. Click the 'Connect' button corresponding to the required IDrive BMR device. This will launch the device interface in a new tab.
- Use the IDrive BMR device IP as the application URL. (To know your device IP, connect the device to a monitor and once the device has completed the start-up process, the dashboard will be displayed on the monitor along with the IDrive BMR device IP.)
- Enter the serial key of the IDrive BMR device followed by '.local' in small-case as the application URL.

For the initial sign in, use 'support123' as the password. We highly recommend you change the default password after the initial sign-in to the IDrive BMR device web interface.

Encryption settings

When you set up the IDrive BMR device for the first time, you will be prompted to configure your encryption settings. **You can only configure your encryption settings once.**

You can choose either of the following encryption methods:

Default Encryption: IDrive BMR will automatically set an encryption key to encrypt all your data.

Private Encryption: This option will allow you to set a self-defined encryption key. (This is the recommended option.) **Ensure that you store this key safely as we are unable to recover this key and will be unable to assist you with recovering any data without the private key.**

IDrive BMR uses AES-256 CCM encryption to secure your data when stored on the device and the cloud. Your data is also encrypted during the transfer to the cloud account; thereby, ensuring adequate protection for your data.

It is recommended to set a Private Encryption Key for enhanced security. This key is not stored anywhere on IDrive Cloud servers and therefore, it cannot be retrieved if lost. Ensure that you store this key safely for continued access to your data.

To configure encryption on your IDrive BMR device,

1. Sign in to the BMR web interface with your credentials.
2. Once you sign in, you will be prompted with a message to configure your device with encryption. Choose default encryption or private encryption based on your requirements.
3. To set 'Default encryption key', click 'Continue'.
4. Alternatively, to set 'Private encryption key', enter a private encryption key of your choice in the respective field and confirm the same. Click 'Continue'.

Note:

- *Once you set the encryption key (default or private), you will not be able to change this key in the future.*
- *IDrive does not store your private encryption key on its servers. It uses a special technique to encrypt your private encryption key so that it can be verified but not retrieved.*
- *It is recommended that you archive it safely. Without your private encryption key, you will not be able to retrieve your data. We will not be able to provide private encryption key information.*

Forgot password

This option lets you reset the password that you use to sign in to your IDrive BMR device interface.

To change the password,

1. On the 'Sign in' page, click 'Forgot Password'.
2. Click 'Confirm' in the confirmation window. An email with the security code will be sent to the admin email address.
3. Enter the security code and click 'Verify'.
4. Enter the new password, confirm the same, and click 'Reset password'.

A confirmation message will be displayed on the top.

Note: If you do not receive an email with a security code, click 'Resend security code' to resend the email. After this, if you still do not receive the mail, it could be due to the following reasons:

- *You may be checking the wrong email account. The address provided when placing the request for the device is the default email address for notifications.*
- *Your incoming email server might be rejecting the message.*

Admin

You can update the profile information such as the primary email address and password from the Admin menu.

Change Password

To change the password,

1. Sign in to the IDrive BMR device web interface.
2. Click 'Admin' displayed on the top-right corner of the page.
3. Click 'Change Password'.
4. Enter the new password, confirm the same, and click 'Change Password'. Once this is completed, you will receive a success notification.

Update Email Settings

To update your email settings,

1. Click 'Admin' displayed on the top-right corner of the page.
2. Click 'Email Settings'.
3. In the 'Email Notification' tab, navigate to the 'Server Alert Notification' section, click , enter the new admin email and click 'Save'. All device-related notifications will be communicated to this email address. You can add additional recipients in the 'Add Email' section below.
4. Next, navigate to the 'Backup Report Notification' section, enter the email addresses for receiving backup-related notification, click , and click 'Save'.

Configure two-factor authentication for the IDrive® BMR device interface

To enable two-factor authentication,

1. Sign in to the IDrive BMR device interface.
2. Navigate to 'Settings' > "Security" > 'Two-factor Authentication' and click 'Enable Two-factor Authentication'.
3. Select 'Email Address' or 'Phone Number' for the code verification process and click 'Confirm'.
In case you select 'Phone Number', enter your phone number and click 'Send Code'.
4. Enter the one-time authentication code sent to the admin email address / your phone number and click 'Verify and Enable'. The two-factor authentication feature will be enabled.

Power Options

You can perform the power operations of the IDrive BMR device from this menu. Following are the two available power options:

- ✓ **Restart** - Click this to restart the device.
- ✓ **Shutdown** - Click this to shut down the device.

Support

This section details the support options available for our product along with the contact and chat - support information.

Send Error Report

Use the 'Send Error Report' option to raise a support incident with our team. The relevant logs are attached to this ticket which will help us analyze the problem and provide resolution.

Dashboard

The 'Dashboard' tab displays important information such as the device health status, list of protected physical and VMware machines, backup summaries, restore summaries, local and cloud-storage overview.

Device Information

The 'Device Information' section displays the unique serial number of the IDrive BMR device, the IP address, networking information, and the device timezone.

Status

The 'Status' section gives a backup and restore summary of protected physical machines, VMware machines, and network shares.

Cloud Replication

This section displays the used quota of your BMR cloud space and the date and time of the latest cloud backup operation. You can click this section to go to the 'Cloud Replication' tab. Click  to recalculate the real-time usage of your cloud storage.

Local Storage

The 'Local Storage' section displays the total utilized storage space and a breakup for this storage between physical machines, VMware machines, and network shares.

System Health Status

The 'System Health Status' displays the health status of the storage RAID array and OS drive.

Health status and what they indicate:

- ✓ The drives are working fine and are healthy.
- ⚠ Failure detected. Contact the support team immediately.
- ⚠ Bad; Contact the support team immediately.

Note:

- The status 'Warning' doesn't always imply that there is a critical problem with the RAID storage array. Once you contact the support team, they will analyze the required reports and let you know if there is any issue and provide the necessary information to resolve them.
- A unique serial number will be provided to each storage device to identify and replace them if the health status is bad.

Firewall Checkpoints

Use this function to check for firewall and network restrictions on email delivery, cloud replication, remote manage, and other general services.

Download Backup Agent

Download the agent software from 'Downloads' and install it on the computer you want to backup. The IDrive BMR device auto-detects the agent and starts a full image backup automatically for the first time, according to the schedule. In the rare instance that the agent fails to auto-detect the client, click the 'Having trouble adding a client?' link for instructions. For information on image backup, refer to [Backup Instructions](#). Alternatively, use the IDrive BMR MSI package to remotely install the BMR application on multiple PCs.

System Requirements for IDrive® BMR (Physical Machines)

IDrive BMR supports bare-metal backup from physical clients running on Windows OS.

The system requirements for IDrive BMR include the following:

Operating Systems:

- ✓ Windows Vista (with all Windows updates installed)
- ✓ Windows Server 2008 (with all Windows updates installed)
- ✓ Windows Server 2008 R2
- ✓ Windows 7
- ✓ Small Business Server 2011 (with all Windows updates installed)
- ✓ Windows 8
- ✓ Windows 8.1
- ✓ Windows 10
- ✓ Windows 11

- ✓ Windows Server 2012
- ✓ Windows Server 2012 R2
- ✓ Windows Server 2016
- ✓ Windows Server 2019

Note: CBT backup for faster incremental is not supported on Windows Vista and Windows Server 2008. [Read about CBT.](#)

Filesystem:

IDrive BMR supports backup from only NTFS formatted volumes

Disk Partition Style:

- ✓ MBR
- ✓ GPT

Note:

- *Backup and restore of dynamic (simple, mirrored, spanned, striped), logical, and Microsoft storage space (Raid-5 with resiliency type-parity) is supported for BMR firmware 8.4.0 and above. However, bare-metal recovery of dynamic OS disk with GPT partition is not supported. (In case you have upgraded to version 8.4.0 or above, make sure to install the latest backup agent that supports the latest backup features and perform at least one full image backup. If you attempt restoring from older versions of the client where the OS disk is dynamic, you may have OS boot issues. Similarly, use the updated WinRE Recovery Media Builder to create and upload a new WinRE recovery media to the IDrive BMR device.)*
- *The CBT feature is not supported for certain older operating systems such as Windows Vista, Windows Server 2008, and the 32-bit version of both Windows 7 and Windows Server 2008 R2.*

Physical Machines

This section displays all the registered clients and the client groups.

Clients

This section displays the following information for registered clients:

- ✓ **Host Name:** Name of the client added for backup
- ✓ **Status:** Displays the online or offline status of the clients
- ✓ **Last Backup Time:** Displays the date and time of the most recent backup for the client
- ✓ **Integrity Status:** Displays the backup integrity status of the most recent backup
- ✓ **Local Backup Status:** Displays the overall backup status per client
- ✓ **System Info:** Displays the IP address, OS, and assigned group of the physical machine

Status and what they indicate:

-  Backups are running fine
-  No recent backup, if there is no backup for an extended period of time

Advanced Settings

This tab allows you to configure advanced settings related to physical machine backup.

You can configure the following backup settings from this tab:

Max simultaneous backups - This option will limit the maximum number of simultaneous backups allowed at a time.

Max recently active clients - 'Max recently active clients' is the limit on the number of active clients and helps you manage your local storage space.

Note:

- The 'Max recently active clients' limit is applicable only when adding a new client. Even if one or more inactive clients turn online later and the limit is exceeded, the backup operations will continue as usual.*
- A client that has been offline for longer than 2 months is considered inactive.*

Max local network backup speed - Specify the bandwidth throttle to set the local network usage during backup.

Cleanup Settings

This tab allows you to configure settings related to the cleanup of physical and VMware backups on the local device.

Global soft file system quota - Set the storage utilization limit which will schedule the device to initiate a cleanup once the limit is reached. For more information, refer to [FAQ](#).

Cleanup time window - Schedule the cleanup operation from this section. The device will delete the old backups based on your backup retention settings and any incomplete backup, to help you manage your storage space. You can schedule daily, weekday, weekend cleanups or a custom-schedule by selecting the days and hours as required.

Cleanup Maintenance Page

If the local storage utilization on your IDrive BMR device exceeds the global soft filesystem quota, you will be redirected to the cleanup maintenance page to perform manual cleanup. All the backup and restore operations will be temporarily suspended until the utilized local storage is less than the Global soft filesystem quota.

To reduce the local storage,

1. Reduce the 'Min' and 'Max' image backups retention for all machines, as suitable, and click 'Cleanup Now'.

Note: If the cleanup does not reduce storage beyond the global soft filesystem quota, you will again be directed to the same page. To reinitiate the normal operations, you need to reduce the retention settings further and reattempt the cleanup.

2. Alternatively, you can click the 'Manage Recovery Points' button corresponding to any physical or VMware machine to view and manage their backups.

Backup Settings

This tab allows you to configure your global, client, and group backup schedule and settings for physical machines.

You can change the following settings related to the backup of physical machines:

Set backup interval - Set the interval between two consecutive backups of a physical machine.

Max backup speed - Select the 'Don't Limit' radio button to allow unrestricted network bandwidth for backups or select the 'Limit To' radio button and set the local network bandwidth for backup in Mbps.

Volumes - Choose to backup 'All' volumes of your client machines or select 'Custom' and specify the drives for backup, separated by commas. C: Drive is considered for backup by default and therefore does not need to be specified.

Note: Care fully specify the correct volumes for backup, especially when modifying global settings for backup. If volumes that do not exist are specified, the backup will fail.

Backup retention settings - Set the minimum and the maximum number of image backups the device should retain for a physical machine. The old backups will be removed during the cleanup operation.

Schedule backup - Schedule backups as 'Daily', on 'Weekdays', or on 'Weekends'. You can also select 'Custom' and select the days for backup. Also set the 'Start Time' and 'End Time' for backups.

Note: The 'Start Time' and 'End Time' are a soft cut-off. The actual start and end time are dependent on ongoing tasks.

Force full image backup - Select the 'Force a full image backup after every' checkbox and select the interval for forcing a full image backup. Full image backups require more time to complete and is better practice for data continuity.

Manage Recovery Points of Physical Machines

You can view and manually manage the recovery points of your physical machines. This is only available in BMR firmware 8.5.0 and above.

To view and manage the recovery points of a physical machine,

1. Sign in to the IDrive BMR device web interface and navigate to 'Dashboard' > 'Physical Machines' > 'Clients'.
2. Click corresponding to the required physical machine and select 'Manage Recovery Points'. This will open a page listing all the recovery points of the machine.

3. Select the recovery points you wish to delete and click 'Delete Recovery Points'. Until the recovery point is deleted, you can revert the operation by clicking 'Undo Delete'.
4. Click 'Yes' to confirm. These recovery points will be queued for permanent deletion from the IDrive BMR device. Click 'Refresh' to view the latest status of the recovery points.

Note: To view and manage the recovery points of an entire group, go to 'Groups' and in the groups tile-view and click .

Groups

A group is a collection of client machines organized together for collective backup scheduling and managing. You can create up to 30 groups, and a client machine cannot be added to more than one group.

This section displays all the created groups and the number of client machines added to the group. Here, you can perform an immediate full or incremental image backup or schedule the backup for the entire group.

Create Group

This option lets you create groups and add client machines to them. A group can have up to 25 client machines and you can create a maximum of 30 groups.

To create a group,

1. Sign in to the IDrive BMR device web interface and click 'Groups' on the 'Dashboard' page.
2. Click 'Create Group'.
3. Enter the name of the group in the 'Group Name' field.
4. Click 'Create group'.

Group Operations

You can perform the following operations on the created group:

- ✓ Add or remove client machines.
- ✓ Perform full or incremental image backup.
- ✓ Configure backup settings and schedule local backup.
- ✓ Delete the group.

To add client machines to an existing group,

1. Sign in to the IDrive BMR device web interface and click 'Groups' on the 'Dashboard' page. The created groups appear in the 'Groups' tab.
2. Click  on the required group tile. The 'Manage User Groups' page appears.

3. Select the required client machines from the 'Choose host machines' section under the 'Add' tab.
4. Click 'Save'.

To remove client machines from a group,

1. Sign in to the IDrive BMR device web interface and click 'Groups' on the 'Dashboard' page. The created groups appear in the 'Groups' tab.
2. Click  on the required group tile.
3. Click on the 'Remove' tab and select the client machines to remove from the 'Choose host machines' section.
4. Click 'Remove'.

To perform full or incremental image backup,

1. Go to the 'Dashboard' page.
2. Go to 'Physical Machines' > 'Groups'. Here the groups are displayed.
3. Click 'Backup Now' or select the 'Force Full Backup' checkbox on the required group tile to start the backup.

To apply local backup settings to a group,

1. Go to 'Dashboard' > 'Physical Machines' > 'Groups'. The created groups are displayed.
2. Click  on the required group tile. The 'Backup settings' page appears.
3. Set the backup interval and max backup speed. Choose the 'Backup retention settings' and schedule the backup.
4. Set the 'Volumes' you want to backup as 'All' or select 'Custom' and specify the volumes you want to backup.

Note: Carefully specify the correct volumes for backup. If volumes that do not exist are specified, the backup will fail.

5. Click 'Save & Close'

To delete a group,

1. Sign in to the IDrive BMR device web interface and click 'Groups' on the 'Dashboard' page. The created groups appear in the 'Groups' tab.
2. Click  in the required group section.
3. Click 'Yes' in the confirmation window.

Note: When you delete a group, the applied settings will be lost and all the client machines of that group will adopt global backup settings.

Activities

This section displays information about ongoing local backups of physical and VMware machines. During a backup operation, the 'Activities' section provides the following options:

1. Stop - Click to force stop the ongoing local backup
2. Show Logs - Click to view detailed information of local backup

VMware

You can backup all the registered virtual machines running on ESXi and vCenter servers from this section.

System Requirements:

ESXi Hosts: IDrive BMR supports ESXi server versions 5.5, 6.0, 6.5, 6.7, and 7.0; we do not support free ESXi

VMs guest OS: Works for any application, file-system and operating system that is supported by VMware

IDrive BMR supports the following operating systems to enable VMware file-system restores:

| Microsoft Windows | Linux | BSD, Solaris | Mac | Disk Types | RAID |
|-------------------|------------------|--------------|------|---------------------------------------|---|
| FAT, FAT32 | ext2, ext3, ext4 | UFS | HFS | Basic and Dynamic disks are supported | Mirrored RAID volumes are supported. Since there are two disks with the same data, both the VMDK images will be mounted for file restore. |
| NTFS | ReiserFS | UFS2 | HFS+ | | |
| | JFS | | | | |
| | XFS | | | | |
| | Btrfs | | | | |

Note:

1. Microsoft Windows - ReFS is not supported
2. Linux - ZFS is not supported; Linux LVM is supported, however, encrypted LVM volumes are not supported
3. BSD, Solaris - Limited support for variants of UFS, used in the following systems - SunOS, Sun X86, HP-UX, NeXTSTEP, OpenStep
4. RAID - All other types of RAID configurations are not supported; Striped volumes, and split volumes are not supported

ESXi

This section displays the VMs running on ESXi hosts, added for backup to the IDrive BMR device.

Add ESXi Host

You need to add VMware ESXi host to the IDrive BMR device to backup data from the VMs hosted on the server.

To add ESXi host,

1. Sign in to the IDrive BMR device web interface.
2. Go to the 'VMware' tab and click 'Add ESXi Host'.
3. Provide details such as ESXi name, IP address, and username and password, and click 'Next'.
4. Select the required virtual machines and click 'Next'.

Note: IDrive BMR follows VMware's naming conventions and restrictions for virtual machines. Hence names with the special characters colon, quotation marks, and slash (;, ", \, and /) are not supported.

5. Set the required backup schedule parameters in the respective tabs and click 'Next'. (Select the 'Disable Schedule' checkbox if you want to disable backup.)
6. A summary of the backup operation is displayed. The backup of the VMs will be performed as per the schedule. Verify the details and click 'Confirm' to add.

Once this is completed, the ESXi host is added to the IDrive BMR device successfully and backup for the selected VMs will occur as per the schedule.

After you have added an ESXi host, you can perform an immediate full image and incremental backup, change the backup schedule, view integrity and backup status, and view the last backup time for each ESXi host. You can also add new VMs to an ESXi host at a later time.

To add VMs to the VMware ESXi,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'ESXi'.
3. Click  on the required ESXi.
4. Select the required VMs to add and click 'Next'.

Note: IDrive BMR follows VMware's naming conventions and restrictions for virtual machines. Hence names with the special characters colon, quotation marks, and slash (;, ", \, and /) are not supported.

5. Verify the details and click 'Confirm'.

To perform an immediate backup,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'ESXi'.
3. Click 'Backup Now' or select the 'Force Full Backup' checkbox to perform an immediate incremental or full image backup respectively.

To reschedule data backup for an ESXi host,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'ESXi'.
3. Click  on the required ESXi Host.

4. On the 'Schedule Backup' screen, change the required parameters. You can click 'Disable Schedule' to disable backup.
5. Click 'Confirm' to save the changes.

To delete an ESXi host,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware > ESXi'.
3. Click  on the required ESXi Host.
4. Click 'Yes' in the confirmation window.

Note: The list of deleted ESXi hosts will be displayed at the bottom of the page and all the data will be permanently removed from the device during cleanup. You can click 'Do not remove' to retain the required ESXi host.

vCenter

This section displays the VMs running on the vCenter server, added for backup to the IDrive BMR device.

Add vCenter server

You can backup virtual machines running on multiple ESXi hosts that are managed through a VMware vCenter server. All you need to do is add the vCenter server to the IDrive BMR device and schedule the backup. In the case of multiple ESXi hosts managed by a single vCenter server, this is the recommended method of adding all the ESXi hosts in one go.

To add a vCenter server,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware Backup' > 'vCenter'.
3. Click 'Add vCenter Server'.
4. Provide details such as vCenter name, IP address, and username and password, and click 'Next'.
5. Select the required virtual machines and click 'Next'.

Note: IDrive BMR follows VMware's naming conventions and restrictions for virtual machines. Hence names with the special characters colon, quotation marks, and slash (;, ", \, and /) are not supported.

6. Set full or incremental backup schedule parameters in the respective tab and click 'Next'.
7. Verify the details and click 'Confirm' to add.

Once you have added a vCenter server, you can perform immediate full image and incremental backup, change the backup schedule, view integrity and backup status, and view the last backup time for each vCenter server. You can also add new VMs to a vCenter server at a later time.

To add VMs to the VMware vCenter,

1. Sign in to the IDrive BMR device web interface.

2. Go to 'VMware' > 'vCenter'.
3. Click  on the required vCenter tile.
4. Select the required VMs to add and click 'Next'.

Note: IDrive BMR follows VMware's naming conventions and restrictions for virtual machines. Hence names with the special characters colon, quotation marks, and slash (;, ", \, and /) are not supported.

5. Verify the details and click 'Confirm'.

To perform an immediate backup,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'vCenter'.
3. Click 'Backup Now' or select the 'Force Full Backup' checkbox to perform an immediate incremental or full image backup respectively.

To reschedule data backup,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'vCenter'.
3. Click  on the required vCenter.
4. On the 'Schedule Backup' screen, change the required parameters. You can click 'Disable Schedule' to disable backup.
5. Click 'Confirm' to save the changes.

To delete a vCenter server,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'VMware' > 'vCenter'.
3. Click  on the required vCenter.
4. Click 'Yes' in the confirmation window.

Note: The list of deleted vCenter servers will be displayed at the bottom of the page and all the data will be permanently removed from the device during cleanup. You can click 'Do not remove' to retain the required vCenter server.

Manage Recovery Points of VMware Machines

You can view and manually manage the recovery points of your VMware machines.

To view and manage the recovery points of a VMware machine,

1. Sign in to the IDrive BMR device web interface and navigate to 'Dashboard' > 'VMware'.
2. Navigate to the required ESXi or vCenter server tile under the respective tab and click . This will open a page listing all the recovery points of VMs of the selected ESXi / vCenter server.
3. Select the ESXi server from the 'Choose ESXi' dropdown (This step is not relevant if you navigated here from the ESXi tab).

4. Choose a VM from the 'Choose VM' dropdown.
5. Select the recovery points you wish to delete and click 'Delete Recovery Points'. Until the recovery point is deleted, you can revert the operation by clicking 'Undo Delete'.
6. Click 'Yes' to confirm. These recovery points will be queued for permanent deletion from the IDrive BMR device. Click 'Refresh' to view the latest status of the recovery points.

Alternatively, click on the ESXi / vCenter server tile-header and navigate to the required VM. Click and select 'Manage Recovery Points' to view and manage the recovery points.

Restore

This tab lets you perform the various restore operations for protected physical machines, VMware machines, and NAS data.

File Restore (from physical machines backup)

You can access all backed-up files using this option. Create a network share from the required recovery point to access your files.

To create a network share path for a recovery point,

1. On the 'File Restore' tab, select the client from 'Choose a System' drop-down menu.
2. Select the recovery point from the 'Choose Recovery Point' drop-down menu.
3. Specify the drive.
4. By default 'Enable user authentication' will be selected as 'No'. This will create an open share that is accessible to all on the network. However, if you want the share to be secured, we recommend you authorize it with a username and password. To create a secure share, select 'yes' and perform the following steps:
 - a. Select the username from the 'Mount username' drop-down menu.
 - b. Enter the mount password.
5. Click 'Create'. The network share is created using the CIFS / SMB protocol.

Note: You can create a maximum of 5 simultaneous network shares from the recovery points, irrespective of the authentication type selected.

Once the network share for the recovery point is successfully created, a summary of it will be displayed in the 'Mount Path Summary' table. You can use the path displayed under 'Mount Path' to access your backed-up data using the SMB client/protocol.

System Restore (Bare-metal Restore using WinRE)

You can perform a bare-metal restore to a target machine that is on the same network as your IDrive BMR device. First, create a bootable USB or media device using the Recovery Media Builder app available for download in the 'Downloads' menu of the IDrive BMR device interface. Then boot your target replacement machine using the USB or media device.

Pre-requisites for performing a bare-metal restore:

1. USB drive with a minimum of 4 GB storage - to create USB recovery media.
2. Ensure that the drives on your target computer are healthy (run SMART checks on the drives if necessary).
3. The target computer must be bootable from a USB storage device.
4. The IDrive BMR device and the target computer should be on the same LAN.
5. The target computer should have a wired network connection to the LAN (DHCP is recommended).
6. If the target computer has hardware RAID, it should be configured before initiating the restore process.

For optimal performance during bare-metal restore, stop any ongoing backup operation.

Note:

1. *After restoring a machine, Windows may prompt you to re-activate your license.*
2. *Bare-metal recovery of dynamic (simple, mirrored, spanned, striped), logical, and Microsoft storage space (Raid-5 with resiliency type-parity) is supported by version 8.4.0 and above. However, bare-metal recovery of dynamic OS disk with GPT partition is not supported.*
3. *In case you have upgraded to version 8.4.0 or above, make sure to install the latest backup agent that supports the aforementioned advanced backup and perform at least one image backup. If you attempt restoring exclusively from older versions where the OS disk is dynamic, you may have OS boot issues. Similarly, use the updated WinRE Recovery Media Builder to create and upload a new WinRE recovery media to the IDrive BMR device.*

Setup instructions to build WinRE recovery media

To build WinRE recovery media for future use,

1. Launch the setup.
2. Select 'Future Use'.
3. Select a target destination and click 'Next'.
4. The ISO build progress will be displayed on the page. You will receive a success message once the ISO build is completed.
5. Enter the IP address of the IDrive BMR device, click 'Next', enter your IDrive BMR device credentials, and click 'Next'.
6. The ISO will now be uploaded to the IDrive BMR device. Once completed, you will receive a success message.

To build a WinRE recovery media for immediate use,

Refer to the steps given below to create a bootable CD or USB with the recovery media for immediate use.

1. Navigate to 'Downloads' > 'BMR Recovery Builder'.
2. Launch the setup.
3. Select 'Immediate Use'.
4. Choose 'Create a Bootable ISO file', select the target destination, and click 'Next'.
5. The ISO build progress will be displayed on the page and you will receive a success message once it is completed.

To create a bootable USB for immediate use,

1. Navigate to 'Downloads' > 'BMR Recovery Builder'.
2. Launch the setup.
3. Select 'Immediate Use'.
4. Select 'Create a bootable USB'. Then select the partition style and the USB device from the respective drop-down menus to create the boot device and click 'Next'.
5. The USB creation progress will be displayed.
6. You will be notified once the USB bootable device is successfully created along with further instructions to use the bootable device.

Note:

- If the setup is not able to find the .wim file, you will be prompted to download ADK after selecting the 'Future Use' or 'Immediate Use' option.
- The new page that appears will ask the user to download ADK from the link given in the instruction. After the ADK setup is completed the next button will be enabled.
- Click 'Next' to proceed with the aforementioned options.

Steps to perform a bare-metal restore (WinRE Restore)

To initiate restore,

1. Boot your target replacement machine using the USB or CD-ROM device created earlier.
2. Select one of the options below to connect to the IDrive BMR device:
 - With the 'Auto-detect IP Address' option (recommended), you can connect automatically to any available IDrive BMR device within the network.
 - With the 'Specific IP Address' option, you can connect to a particular IDrive BMR device. This is useful when you want to connect to a specific device in a network having multiple IDrive BMR devices installed.
3. Sign in to the IDrive BMR device with your device credentials.
4. Choose the system and recovery point from the respective drop-down menu.
5. Choose the required volumes and then click 'Next'.

Note: If you click the 'Back' button on this page, you will be signed out of the device. You will have to sign in again to the device.

6. Select a destination drive.

Note: Once the restore process is initiated, any previously existing data on the chosen destination drive will be deleted.

7. You will receive a confirmation message when the restore is completed.

VMware Restore

This tab allows you to restore the protected VMs to the ESXi host or vCenter server.

VMware System Restore

To restore a VM running on an ESXi host,

1. Sign in to the IDrive BMR device web interface and go to the 'Restore' tab.
2. Go to 'VMware Restore' > 'ESXi'.
3. Select 'VM restore'.
4. Select the required ESXi host you want to restore.
5. Select a VM and the required recovery point.
6. Select 'Same VM' if you wish to restore data to the selected VM.
7. To restore data to another VM, select 'New VM'. In the 'New VM' section, choose an ESXi host, enter a name for the new VM, and select a data store.

Note: The required ESXi host needs to be on the IDrive BMR device.

8. Click 'Restore'.
9. The progress is displayed in the 'Activities' section.

Note: In some cases, the progress may take some time to appear.

To restore a VM running on vCenter server,

1. Sign in to the IDrive BMR device web interface and go to the 'Restore' tab.
2. Go to 'VMware Restore' > 'vCenter'.
3. Select 'VM Restore'.
4. Select the vCenter server and the ESXi host.
5. Select a VM and the required recovery point.
6. Select 'Same VM' if you wish to restore data to the selected VM.
7. To restore data to another VM, select 'New VM'. In the 'New VM' section, select a vCenter server and ESXi host for the new VM, enter a name for the new VM, and select a data store.

Note: The required vCenter server needs to be on the IDrive BMR device.

8. Click 'Restore'.
9. The progress is displayed in the 'Activities' section.

Note: In some cases, the progress may take some time to appear.

VMware File Restore

You can also restore individual files/folders, irrespective of the type of operating system on the VM.

To restore files/folders from a protected VM on the ESXi host,

1. Sign in to the IDrive BMR device web interface and go to the 'Restore' tab.
2. Go to 'VMware Restore' > 'ESXi'.
3. Select 'File Restore'.
4. Select the required ESXi host.
5. Select a VM and the required recovery point.
6. Select a username and enter the password.
7. Click 'Create Mount' to initiate the restore process. A network path is created in the 'Mount Summary' table. The network share is created using the CIFS / SMB protocol.

To restore individual files/folders from a backed-up virtual machine on the vCenter server,

1. Sign in to the IDrive BMR device web interface and go to the 'Restore' tab.
2. Go to 'VMware Restore' > 'vCenter'
3. Select 'File Restore'.
4. Select the required vCenter server.
5. Select an ESXi host.
6. Select a VM and the required recovery point.
7. Select a username and enter the password.
8. Click 'Create Mount' to initiate the restore process. A network path is created in the 'Mount Summary' table. The network share is created using the CIFS / SMB protocol.

Virtualization

This tab allows you to create virtual instances of your protected physical and VMware machines, providing a time-efficient means to data recovery in the event of a disaster. You can create up to 4 local virtual instances on the device and assign memory based on the RAM configuration of your device. Similarly, you can create up to 4 virtual instances on the cloud, considering the memory available for cloud virtualization.

Local Virtualization

You can create a local virtual instance of your backed-up physical and VMware machines from this section using the built-in KVM hypervisor.

To create a local virtual instance of a physical machine,

1. Sign in to the IDrive BMR server web interface.
2. Go to 'Virtualization' > 'Local Virtualization' and click the 'Create a Virtual Machine' button. A new pop-up will appear.
3. On the 'Physical Machines' tab, select the required client from the 'Choose a System' drop-down menu.
4. Choose a recovery point.
5. Select the number of processors for the virtual machine.
6. Allocate required memory for the virtual machine in the 'RAM' field.

Note: Memory value should be greater than 512 MB. You can decide the memory value depending on the available memory displayed below the 'Memory' field.

7. Select a network source.
8. Next, select the appropriate network model.
9. Choose the required storage controller for the virtual machine. SATA is recommended.
10. Select a graphics option from the drop-down menu.
11. Click 'Build Virtual Machine'.

Once this is completed, your virtual machine is built. You can now connect to it and access data.

Note: When a machine with dynamic disks is virtualized, the created virtual instance will have basic disks with randomly assigned drive letters. You may have to sign in to the VM and change the drive letter associations as necessary.

To connect,

1. Navigate to the new local virtual instance click the 'Copy VNC Password' button on the right-hand side.
2. Click 'Connect' against the virtual instance.
3. In the new window that appears, paste the password. Click 'Send Password'.

Remote connection to the virtual machine will be established.

Note: All the created virtual instances will be unmounted and the changes made in the virtual machine will be lost when you restart your IDrive BMR device. You can also click  to unmount the virtual machine manually.

To create a virtual instance of your VMware server,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'Virtualization' > 'Local Virtualization' and click the 'Create a Virtual Machine' button. A new pop-up appears.
3. In the 'VMware' tab, choose the required server from the 'Choose Server' drop-down menu.
4. Select the ESXi Host from the 'Choose ESXI Host' drop-down menu.
5. Select a VM from the 'Choose VM' list.
6. Choose the required recovery point.
7. Specify the boot firmware. Refer to the virtual machine's hardware configuration on the VMware server to set the firmware to UEFI or Legacy BIOS.
8. Assign the number of processors for the virtual machine from the 'Processors' drop-down menu.
9. Allocate required memory for the virtual machine in the 'RAM' field.

Note: Memory value should be greater than 512 MB. You can decide the memory value depending on the available memory displayed below the 'RAM' field.

10. Select a network source.
11. Next, select the appropriate network model.
12. Choose the required storage controller for the virtual machine. LsiLogicSAS is recommended.
13. Select a graphics option from the drop-down menu.
14. Click 'Build Virtual Machine'.

Once this is completed, your virtual machine is built. You can now connect to it and access data.

To connect,

1. Navigate to the new virtual instance, click the 'Copy VNC Password' button on the right-hand side
2. Click 'connect' against the virtual machine.
3. In the new window that appears, paste the password. Click 'Send Password'.

A remote connection to the virtual machine will be established.

Note: All the created virtual instances will be unmounted and the changes made in the virtual machine will be lost when you restart your IDrive BMR device. You can also click  to unmount the virtual machine manually.

Cloud Virtualization

You can create a cloud virtual instance of your backed-up physical and VMware machines from this section using the built-in KVM hypervisor.

To create a cloud virtual instance of a physical machine,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'Virtualization' > 'Cloud Virtualization' and click the 'Create a Virtual Machine' button. A new popup will appear.
3. Select the 'Physical Machines' tab, select the required client from the 'Choose a System' drop-down list, and choose a recovery point.
4. Select the number of processors for the virtual machine and allocate the required memory for the virtual machine in the 'RAM' field, taking into account the memory available for cloud virtualization.
5. Select a network source and the appropriate network model.
6. Choose the required storage controller for the virtual machine (SATA is recommended) and select a graphics option from the drop-down.
7. Click 'Build Virtual Machine'.

Once this is completed, your virtual instance is built. You can now connect to it and access data.

Note: When a machine with dynamic disks is virtualized, the created virtual instance will have basic disks with randomly assigned drive letters. You may have to sign in to the VM and change the drive letter associations as necessary.

To connect,

1. Navigate to the new cloud virtual instance click the 'Copy VNC Password' button on the right-hand side.
2. Click 'Connect' against the virtual instance.
3. In the new window that appears, paste the password. Click 'Send Password'.

A remote connection to the virtual machine will be established.

To create a cloud virtual instance of your VMware server,

1. Sign in to the IDrive BMR device web interface.
2. Go to 'Virtualization' > 'Cloud Virtualization' and click the 'Create a Virtual Machine' button. A new popup appears.
3. Select the 'VMware' tab, choose the required server from the 'Choose Server' dropdown, and select the ESXi Host from the 'Choose ESXi Host' dropdown list.
4. Select a VM from the 'Choose VM' list and choose a recovery point that will be used to create the virtual instance.
5. Assign the number of processors for the virtual machine from the 'Processors' drop-down list and allocate required memory for the virtual machine in the 'RAM' field, taking into account the space available for cloud virtualization.
6. Select a network source and select the appropriate network model.
7. Choose the required storage controller for the virtual machine (LsiLogicSAS is recommended) and select a graphics option from the drop-down.
8. Click 'Build Virtual Machine'.

Once this is completed, your cloud virtual instance is built. You can now connect to it and access data.

To connect,

1. Navigate to the new cloud virtual instance, click the 'Copy VNC Password' button on the right-hand side.
2. Click 'Connect' against the virtual machine.
3. In the new window that appears, paste the password. Click 'Send Password'.

A remote connection to the virtual machine will be established.

Perform power operations on the virtual instances

You can perform power operations on the virtual machine. Additionally, you can send the keyboard inputs such as windows, Ctrl+Alt+Del, Alt+Tab, and F8 to the virtual machine.

To perform power operations,

1. Sign in to the IDrive BMR device interface and go to the 'Virtualization' tab.
2. Click  to power on a virtual instance.
3. Click  to power off a virtual instance. You will be prompted with a confirmation window. Click 'Force Shutdown'.

Note: Use the shutdown option in the OS of the virtual instance to shut down the machine. Force shutdown from the IDrive BMR device interface only as a last resort when facing system issues.

To restart a virtual instance,

1. Click  in the menu of the required virtual instance.
2. You will be prompted with a confirmation. Click 'Restart'.

Reconfigure a virtual instance

Typically, to reconfigure the hardware of a virtual instance, you will need to backup the virtual instance and create a new virtual instance with the backed-up data. You can skip this hassle with IDrive BMR as you can simply shut down the virtual instance and click 'Configure' to reconfigure the hardware parameters.

You can reconfigure the following parameters of a virtual instance:

Specify the boot firmware - Change the boot firmware to BIOS / UEFI. (applicable only for local virtual instances for VMware machines)

Processors - Use the 'Processors' drop-down list to reassign the number of processors for the virtual machine.

RAM - Reallocate the required memory for the virtual machine.

Network Source/Model - Change the network source and reassign a network model if needed.

Storage Controller - Change the required storage controller for the virtual machine.

Graphics - Update the graphics option from the drop-down.

Install performance-enhancing drivers for a local virtual instance

Configure your virtual instances with performance-enhancing drives to achieve better performance.

To install performance-enhancing drivers for a local virtual instance,

1. Shut down the virtual instance and click 'Configure'.
2. Attach the ISO file (virtio-drivers(For_Windows_VMs).iso) containing high-performance drivers for network and graphics hardware in the virtual instance and click 'Save'.
3. Power-on the virtual instance.
4. Use the 'Device Manager' to locate the drivers on the attached ISO file.
5. Install the necessary drivers using the 'Update Driver Software' wizard.
6. Upon completion, reboot to begin using the virtual instance with the enhanced drivers.

Troubleshooting: Windows OS booting issues in a local virtual instance

In the case of OS boot issues during virtualization, especially for Windows OS, you can upload the pre-built Windows recovery media to correct the boot issues. You can also build a WinRE recovery media for immediate use

- *IDrive BMR does not provide the OS recovery media.*
- *The total upload limit is 20 GB.*

To upload recovery media, for future use in case of boot issues,

1. Shut down the virtual instance and click 'Configure'.
2. Click 'Upload ISO Image'.
3. Browse and choose the OS recovery ISO file and click 'Upload'.
4. To view the ISO files uploaded to BMR, click the 'Uploaded Files List'. (virtio-drivers(For_Windows_VMs).iso) is available by default and cannot be deleted.

To troubleshoot booting issues in a virtual instance,

1. Shut down the virtual instance and click 'Configure'.
2. Enable 'Attach ISO', and select the relevant OS recovery ISO file.
3. Configure the virtual machine's boot order to 'CD/DVD-ROM', set up boot menu timeout if necessary, and repair the operating system boot issues.

Note: It is recommended to set a boot timeout of 10 seconds or above.

4. Once the boot issue is resolved, change the boot order to 'Hard Disk' and detach the ISO file.
5. Reboot your virtual instance.

Cloud Replication

The Cloud Replication tab lets you replicate the data backups of physical and VMware machines on the IDrive BMR device to the cloud account. Additionally, you can use the cloud seeding service, also called IDrive BMR Express, to transfer data to your cloud account via an external device. Listed below are the various sections of the Cloud Replication UI with a brief explanation.

IDrive Account Information

This section provides information about your IDrive cloud account to which the data will be transferred. Information such as username and account status will be displayed

Cloud Replication Settings

You can perform an immediate cloud backup or schedule cloud replication from the 'Cloud Replication Settings' section. The following options are available to perform backup:

Select clients for manual backup/Select ESXi/vCenter VMs for manual backup - Select clients / server and VMs to perform an immediate backup. Click 'Backup Now'.

Schedule Backup

Select clients to backup/Select ESXi/vCenter VMs for backup - Select the required clients / server and VMs. Click 'Select All' to select all the computers.

Scheduled backup time - Set the time at which your scheduled backup should start. Select 'Daily' to perform the backup every day or select the specific days for the backup to run.

Backup end-time - Disable cut-off on backup end time or configure a soft or hard cut-off for the end time.

Note: Hard cut-off will terminate backup on the specified end time. For soft-cut off the actual end time is dependent on the ongoing tasks that are in progress.

Bandwidth throttle - Enter the bandwidth throttle value to set the Internet usage for your backups. By default, this value will be set to 100 Mbps.

Note: Bandwidth throttle value should be between 1-1000 Mbps.

Schedule summary

This section displays a summary of the scheduled backups. Information such as computers selected for backup and the day and time of the next scheduled backup will be displayed.

Click 'Delete Schedule' to delete all upcoming scheduled backups.

Activities

This section displays the ongoing cloud replication status. Information such as computer/server and VM name, drive selected for backup, recovery point, the amount of data transferred to the cloud, time taken for backup, Internet speed, and the estimated time for backup are displayed.

Cloud Replication Status

This section displays the status of the last backup, including information such as hostname/VM name, last backup time, and the size of the data transferred. You can even search for the required hostname and device by using the search field.

Last Backup Log

View detailed information on the last cloud replication in the 'Last Backup Log' section.

View Logs

Click 'View Logs' to view a comprehensive log of cloud replication activities of your physical clients and VMware machines.

Cloud Seeding

You can quickly transfer large amounts of data stored on the IDrive BMR device to your cloud account via physical shipment of data in a temporary storage device. The Cloud Seeding UI is for data transfer between your Express device and IDrive BMR device.

Place an order for BMR Express device via the web console

Sign in to www.idrive.com with your BMR credentials and navigate to the 'IDrive BMR Express™' tab. Fill out the shipment form with all the necessary information including a key, which will be used to encrypt your data for enhanced protection during transit. You will be contacted by our team after we receive your order. Once you confirm the order, we will ship the device to you with all the required accessories.

Transfer data from the IDrive BMR device to the Express device

After receiving the Express device, you need to follow these instructions for transferring data from the IDrive BMR device to the Express device:

1. Sign in to the IDrive BMR device web interface and click the 'Cloud Replication' tab.
2. Click the 'Switch to Cloud Seeding' button.
3. Connect the Express device to the IDrive BMR device.
4. Click the 'Mount' button.
5. To transfer backups of the physical machines, go to the 'Physical Machines' tab. To transfer backups of your VMware server, go to the 'VMware' tab.
6. In the 'Cloud Seeding Settings' section, select the clients to transfer from the respective dropdown.
7. Set the backup throttle. By default, this value will be set to 100 Mbps.
8. Click 'Transfer Now'.

Once the data is successfully transferred to the Express device, you can eject the device and ship it back to IDrive. The time required to transfer data to your cloud account depends on the volume of data and our representative will update you on the same once we receive the device from you

Cloud replication will be re-enabled from the cloud-server side once the cloud seeding process is complete and the cloud backups will continue from where it had paused.

To cancel cloud seeding after initiating it, you should contact the BMR support team.

Express Restore

Retrieve data transferred to the cloud via BMR Express.

To raise a request with the support team for Express restore,

1. Sign in to www.idrive.com with your BMR credentials and navigate to the 'IDrive BMR Express™' tab.
2. Navigate to the 'Express Restore' tab.

3. Select the required clients from the 'Granular Restore Service' section to request the data.
4. Provide the contact information and shipping address in the respective sections.
5. Check the 'I agree to the terms of the Hard Drive Shipment agreement' checkbox, and click 'Submit Request'.

When you get the Express Drive for restore,

- You can perform files/folder-level restore, if you only need certain files from the backup.
- Restore the entire system using IDrive BMR's bare-metal restore functionality.

Contact support once you receive the Express device for restore. Our technical team will assist you with your preferred choice of data recovery.

View Logs

The 'View Logs' option here would take you to a page with a comprehensive log of cloud seeding activities of your physical clients and VMware machines.

Activities

This section displays the status of the ongoing data transfer to or from the external device. Information such as machine name, recovery point, the amount of data transferred, time taken so far to transfer, the data-write speed, and the estimated time of completion are displayed.

Cloud Seeding Settings

You can select the client machines for transfer, set the bandwidth throttle, and also add the email address for receiving notifications related to cloud seeding.

The following options are available:

Select clients to transfer - You can select the required client machines to transfer data from the IDrive BMR device to the external device. Click 'Select All' to select all the client machines.

Backup throttle - Set the speed of the backup to the express device and optimize load on the IDrive BMR device. By default, this value will be set to 100 Mbps.

Note: Bandwidth throttle value should be between 1-1000 Mbps.

Last Backup Log

View detailed information on the last cloud seeding operation from the 'Last Backup Log' section.

Express Drive Information

This section provides information about the Express device sent by IDrive. Information such as status of the device (mounted or unmounted) and disk utilization will be displayed.

Cloud Seeding Status

This section displays the status of the data transfer, including information such as the hostname/VM name, date and time of the last transfer, and the size of the data that was transferred. You can even search for a required machine using the 'Search' field.

NAS

The NAS tab lets you leverage the BMR storage space for hosting network-attached shares. You can create NAS file share and collaborate with associates over file-based sharing protocols such as SMB, NFS, AFP, and SFTP. Alternatively, you can create iSCSI shares or block-level datastores that imitate locally-attached disks. Additionally, you can secure your datastores locally via scheduled snapshots.

You can create the NAS and iSCSI shares on the IDrive BMR device from any external network via the Cloud Manage feature. However, to access the content of the share, you need to be on the same network as the IDrive BMR device.

Choosing the type of network share:

When creating a network share on the IDrive BMR device, choose the share type based on your requirement.

- *NAS share offers file storage which is suitable for sharing files and folders. These shares are accessible as mapped drives on the client machines.*
- *iSCSI shares, however, offer block-level storage and can be imported as a disk on the client machine running the iSCSI initiator client.*

BMR network shares and storage space

You can create and host unlimited network shares on the IDrive BMR device. The network shares are created within your BMR local device quota therefore, for seamless performance, monitor your local storage utilization.

For storage details of the NAS and iSCSI shares on the IDrive BMR device, navigate to 'Statistics' > 'Storage Insights'. On the same page, you can scroll down to the 'NAS' tab below to view and download the backup statistics of your network shares.

Host and access NAS share on the IDrive BMR device

Create NAS shares on the BMR device and collaborate across SMB, AFP, NFS, and SFTP protocols.

To create a NAS share with IDrive BMR,

1. Sign in to the IDrive BMR device interface.
2. On the 'NAS Share' tab, click 'Create a new share'.
3. Select 'NAS Share' as the share type and click 'Next'.
4. Assign a name to the network share under the 'Share Settings' tab.

5. Select 'Apply New settings' and configure the share settings. Alternatively, choose the 'Use the configurations of an existing share' option to replicate the configuration of an existing share.
6. Click 'Next'.
7. Set the snapshot frequency in the 'Local Snapshot' tab, using the drop-down against 'Capture a local snapshot every _'.
8. Select the days for local backup as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.
9. Set the start and end time of the backup.

Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

10. Use the slider under 'Snapshot Retention Settings' to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a network share.
11. Click 'Next'.
12. In the 'Confirm Share' tab, review the local snapshot summary, and click 'Create'.
13. The new share will be displayed in the 'BMR NAS' tab.

To configure your NAS share,

1. Sign in to the IDrive BMR device interface.
2. Navigate to the 'NAS Share' tab to view all the network shares on the IDrive BMR device.
3. Click 'Configure Share Settings' corresponding to the required NAS share.
4. Under the 'Manage Share Access' tab, set the access permission as public or private. In the case of private access, assign users to the share in the 'Manage Share Users' section below.
5. Under the 'Share Protocols' section, select the network protocols that will be used for accessing the shares.

Note: SMB protocol access is configured by default.

6. Enable write access for all users, if required.
7. Under the 'Configure Local Snapshot' tab, set the frequency for capturing the local snapshots and schedule the backups as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.
8. Set the start and end time of the backup.

Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

9. Use the slider in the 'Snapshot Retention Settings' section to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a NAS share.
10. Click 'Save' to save the local snapshot settings.

Host and access iSCSI share on the IDrive BMR device

To create an iSCSI share with IDrive BMR,

1. Sign in to the IDrive BMR device interface.
2. Go to the 'NAS Share' tab and click 'Create a new share'.
3. Select 'iSCSI Share' as the share type and click 'Next'.
4. Assign a name to the iSCSI share under the 'Share Settings' tab.
5. Select 'Apply New settings' and configure the share settings. Alternatively, choose the 'Use the configurations of an existing share' option to replicate the configuration of an existing share.
6. Assign disk space for the iSCSI target and configure the block size.

Note: Sector sizes 8128 Bytes or 64 KB are supported for IDrive BMR device firmware version 8.6.0 and above. For older firmware, select 512 Bytes or 4 KB.

7. Click 'Next'.
8. Set the snapshot frequency in the 'Local Snapshot' tab, using the dropdown against 'Capture a local snapshot every _'.
9. Select the days for local backup as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days
10. Set the start and end time for backup.

Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

11. Use the slider under 'Snapshot Retention Settings' to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a network share.
12. Click 'Next'.
13. In the 'Confirm Share' tab, review the local snapshot summary, and click 'Create'.
14. The new share will be displayed in the 'BMR NAS' tab.

To configure your iSCSI share,

1. Sign in to the IDrive BMR device interface.
2. Navigate to the 'NAS Share' tab to view all the network shares on the IDrive BMR device.
3. Click 'Configure Share Settings' corresponding to the required iSCSI share.
4. In the 'CHAP Authentication' section, configure CHAP Authentication and Mutual CHAP Authentication.

Note:

- CHAP authentication is recommended for the identity verification of the remote client(s).
- CHAP authentication can be negotiated in both directions for mutual authentication between the client and the iSCSI target, via Mutual CHAP Authentication.
- CHAP authentication needs to be enabled for configuring Mutual CHAP Authentication.

5. Under the 'Configure Local Snapshot' tab, set the frequency for capturing the local snapshots. Schedule the backups as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.
6. Set the start and end time of the backup.

Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

7. Use the slider in the 'Snapshot Retention Settings' section to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a NAS share.
8. Click 'Save' to save the local snapshot settings.

Backup the network shares on the IDrive BMR device

Maintain a backup of your network share on the BMR device via local snapshots.

To schedule local snapshots for a network share on the IDrive BMR device,

1. Sign in to the IDrive BMR device interface.
2. Go to the 'NAS Share' tab to view all the existing network shares.
3. Click 'Configure Share Settings' corresponding to the required network share.
4. In the 'Configure Local Snapshot' section, set the frequency for capturing the local snapshots and schedule the backup.
5. Click 'Save'.

Note:

In the case of iSCSI share backup, IDrive BMR uses data compression and deduplication mechanism for efficient storage space utilization. The local storage used to store the iSCSI share backups can be lesser or greater than the actual amount of data physically stored.

To pause the local backup of a network share on the IDrive BMR device,

1. Sign in to the IDrive BMR device interface.
2. Go to the 'NAS Share' tab to view all the existing network shares.
3. Click 'Configure Share Settings' corresponding to the required network share.
4. In the 'Configure Local Snapshot' section, move the slide toggle to read 'Disabled'.

Restore the network shares on the IDrive BMR device

To restore your NAS share data from the local snapshots,

1. Sign in to the IDrive BMR device interface.
2. Navigate to the 'Restore' > 'NAS Restore'.
3. Choose 'NAS' as the share type.
4. Select the required share and recovery points.

5. By default, user authentication is disabled. Meaning, the share will be accessible to everyone on the network. To create a secure share.

Note:

- Select 'Yes' and enable user authentication.
 - Select the username from the 'Mount username' drop-down menu
 - Enter the mount password.
6. Click 'Create'. The data is shared over the SMB protocol. Based on the OS you are using, you can use the SMB client native to the OS, or install a dedicated application specific to your OS platform to access the data.

To restore your iSCSI share data as a secondary iSCSI target,

1. Sign in to the IDrive BMR device interface.
2. Navigate to the 'Restore' > 'NAS Restore'.
3. Choose 'iSCSI' as the share type.
4. Select the required share and recovery points.
5. Select 'Create a secondary iSCSI target'.
6. Configure CHAP and Mutual CHAP authentication, if required.

Note: CHAP authentication needs to be enabled for configuring Mutual CHAP Authentication.

7. Click 'Create'.

To restore your iSCSI share data to the existing iSCSI target,

1. Sign in to the IDrive BMR device interface.
2. Navigate to the 'Restore' > 'NAS Restore'.
3. Choose 'iSCSI' as the share type.
4. Select the required share and recovery points.
5. Select 'Restore to the existing iSCSI target'.
6. Click 'Restore'.
7. A pop-up window will appear requesting confirmation to proceed with the restore.

Note:

- Restoring your network share will effectuate the following changes.
- Data created after the selected recovery point will be permanently lost.
- Restore mounts of the time range beyond the recovery point will be automatically deleted.
- All active iSCSI connections will be terminated.

Click 'Confirm' to continue with the restore.

User Management for BMR NAS

In the case of NAS shares, you can collaborate on the datashares across SMB, AFP, NFS, and SFTP protocols. To manage network share collaboration, IDrive BMR has introduced the 'Users' section under 'Settings'.

To add users to BMR,

1. In the IDrive BMR device interface, go to 'Settings' > 'Control Panel' > 'Users'.
2. Click 'Add User'.
3. Provide the user details and configure the user access with a password.
4. Click 'Add'. The new user is created and listed in the 'Users' tab.

To delete the user(s), select the user(s) and click .

To update user details at a later time, click  corresponding to the required user, update the details, and click 'Save'.

Settings

From this tab, you can change the device and network settings and configure email notifications. You can also perform power operations such as shut down and restart the device.

Mail

You can change the mail server settings as per your requirements from this tab. Also, you can configure the email addresses for receiving backup and device health notifications.

Email Notification

Server Alert Notification

Change the primary / admin email address and add additional email addresses to receive alerts on device health information from this section.

To change the admin email address,

1. Sign in to the IDrive BMR device web interface.
2. Click 'Settings' on the menu bar.
3. Go to 'Mail' -> 'Email Notification' tab.
4. Click , enter the new email address.
5. Select the checkbox 'Send alert when the IDrive BMR device is offline for more than 48 hours (Applicable only if cloud replication is enabled).' It is recommended to select this option and enable periodic monitoring of the device health.

Note: For devices with firmware 8.4.0 and above, cloud replication is enabled by default.

6. Click 'Save'.

To add additional email addresses,

1. Sign in to the IDrive BMR device web interface.
2. Click 'Settings' on the menu bar.
3. Go to 'Mail' > 'Email Notification' tab.
4. Click , enter email addresses separated by a comma in the 'Additional Email' field.
5. Click 'Save' to save the changes.

Backup Report Notification

This section lets you add email addresses for receiving backup notifications.

To add email addresses,

1. Sign in to the IDrive BMR device web interface.
2. Click 'Settings' on the menu bar and go to 'Mail' > 'Backup Report Notification'.
3. Click  to add the email addresses in the 'Send backup report(s) to' field. Click 'Save' to save the changes. Select the checkboxes 'Notify on success' and 'Notify on failure' if needed.
4. If you want the recipients to also receive notifications for the virtual boot verification of physical machine backups, move the slider in the 'Virtual Boot Verification' section to 'Enabled'.

Note:

- *Virtual boot verification feature is only available for IDrive BMR firmware 8.6.0. It is an integrity check for physical machines backups. The IDrive BMR device creates virtual instances of the backups, boots the system, and finally verifies the boot process with a screenshot.*
- *The feature is not supported for legacy operating systems such as Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7. For these operating systems, verify the virtualization status manually at least once every week to ensure restore-readiness.*

If any physical or VMware machine is not backed up for more than 30 days: You will receive email notification with the list of machines that have not been backed up to the local IDrive BMR device and cloud.

Mail Server Settings

You can change the mail server settings from this section.

To change the mail server settings,

1. Sign in to the IDrive BMR device web interface.
2. Go to the 'Settings' tab and click 'Mail'.
3. Click 'Mail Server Settings'.
4. Select the mail server option from the 'Mail Relay Server' drop-down menu.
5. Define the other required parameters and click 'Save'.

By default, the IDrive BMR device uses the Amazon SES server for mail communications. It is recommended to use this setting. However, you can change it to the local BMR network or your preferred network.

You can also check if the Firewall is enabled for the selected port.

Control Panel

This tab allows you to configure or change the network settings and perform the power operations of the device. You can even change the time settings of the device depending on your location from this tab.

Network Settings

Change the network settings of your device from this tab.

Configure the network settings of the IDrive BMR device

The IDrive BMR device may feature one or two network Ethernet ports. You can view the ethernet settings of the port(s) in 'Control Panel' > 'Network Settings'.

The following parameters are displayed for the network port(s):

IP Mode - Specifies the configured IP mode, whether static or DHCP.

IP Address - Displays the IP address or the network location of the IDrive BMR device. The IP address is how you can identify the IDrive BMR device.

Netmask - Displays the netmask value.

Gateway - Displays the gateway address of the router / network device.

MAC Address - Displays the unique hardware address of the Ethernet port on the IDrive BMR device.

Jumbo Frames - IDrive BMR supports 'Jumbo Frames' for the Maximum Transmission Unit of up to 9216 bytes. Enable 'Jumbo Frames' if you wish to improve data transmissions, and by extension the network performance.

Note: For the switch to be effective, ensure all devices and hardware in your network infrastructure support Jumbo Frames.

Set static IP address and network configuration for the IDrive BMR device

To configure a static IP address for an Ethernet port,

1. Click  against the required ethernet port entry. The 'Network Settings' window appears.
2. Select the 'IP Mode' as 'Static' and provide the required information such as IP address, Netmask, and Gateway in the respective fields.
3. Click 'Apply Settings'.

Note: Ensure the availability of the required static IP to avoid losing access to the device. In case the specified static IP is not available, you will lose connection to the IDrive BMR device. In which case, you will need to connect to the device's physical monitor to reset the network settings.

Configure the DNS settings for your BMR appliance

To change DNS settings,

1. In the 'DNS Settings' section, select 'Use the following DNS server address'.
2. Provide primary, secondary, and tertiary DNS server addresses in the respective fields and click 'Apply'.

Check firewall for blocked ports

Firewall Checkpoint is a function within the IDrive BMR device that helps you check firewall restrictions, if any. Through this function, network restrictions on services such as email delivery, cloud replication, and so on are identified.

In the 'Firewall Checkpoint' section of 'Settings' > 'Control Panel', click 'Check Now' to run a firewall check for general, mail relay server, and cloud replication configurations. (You can check this from the 'Dashboard' page by clicking 'Firewall Checkpoints'). Either of the following statuses will be displayed:

 **Successful**

 **Failure**

The status 'Successful' implies that there are no firewall restrictions and you can continue to use all services related to BMR. If the Firewall check returns 'Failure' alert, troubleshoot as necessary / contact your network admin and check again.

Steps for troubleshooting:

- ✓ In case of issues with the general Firewall settings, unblock Port '80' and Port '443' for 'www.idrive.com' and 'www1.idrive.com' servers.
- ✓ If you are facing issues with the mail settings, check your Mail Server Port details and unblock the port, if blocked.
- ✓ To resolve an issue related to cloud Replication, contact the BMR support team for the Port details. Then share the received information with your network admin to unblock the respective ports.
- ✓ To resolve issues related to Remote Manage - Devices with firmware 8.3.0 or below, unlock port 5349 for bmrturn.idrivelite.com. Devices with firmware 8.4.0 or above, unlock port 443 for us-west-1.idrivetunnel.com and accessbmr.idrive.com.

Reset the BMR network

Go to 'Settings' > 'Control Panel' > 'Network Settings' and click 'Reset Network' to configure all the network interfaces on the IDrive BMR device to operate on DHCP mode. After a network reset, the device will try to obtain DHCP-provided IP from your network. You will need to connect to the IDrive BMR device with a physical monitor to view the new device IP.

Note: Before resetting the network stop any ongoing backup operation and delete any virtual instances on the device.

Time Zone

Change the time zone settings of your device as per your location from this tab.

To change the time zone,

1. Sign in to the IDrive BMR device web interface.
2. Go to the 'Settings' > 'Control Panel' and click 'Time Zone'.
3. Choose your region from the 'Select Time Zone' drop-down menu.
4. Select your country and zone.
5. Click 'Save'.

Security

Enable two-factor authentication

Enable two-factor authentication for enhanced security and to prevent unauthorized access to your account. Once two-factor authentication is enabled for the device interface, in addition to the device password, you will be required to enter a verification code sent to the admin email address.

Below are the steps to enable two-factor authentication,

1. Sign in to the IDrive BMR device interface.
2. Go to 'Settings' > "Security" > 'Two-factor Authentication'.
3. Click 'Enable 'Two-factor Authentication'.
4. Select 'Email Address' or 'Phone Number' for the code verification process and click 'Confirm'.
Note: In case you select 'Phone Number', enter your phone number and click 'Send Code'.
5. Enter the one-time verification code, received at your admin email address/phone number and click 'Verify & Enable'. You will see a success message indicating that two-factor authentication is successfully enabled.

Signing in after two-factor authentication is enabled

Once two-factor authentication is enabled for the device interface, in addition to the device password, you will be required to enter a verification code sent to the admin email address.

To sign in after two-factor authentication is enabled,

1. On the sign-in screen, enter the username and password and click 'Sign in'.
2. You will be prompted to enter the verification code you received on the admin email address. Enter the code.
3. Click 'Verify'.

Disable two-factor authentication

To disable two-factor authentication for your account,

1. Sign in to the IDrive BMR device interface.
2. Go to 'Settings' > "Security" > 'Two-factor Authentication'.
3. Click 'Disable'. You will see a success message indicating that two-factor authentication is disabled.

Statistics

This tab displays information about system health and provides storage insights about the IDrive BMR device.

Storage Insights

This tab displays information about storage usage and backup statistics for your physical machines, VMware machines, and network shares.

1. Storage details of physical and VMware machines include the actual utilized storage space, the total number of mounts for file restore and virtualization, and the space used by the virtual instances of physical and virtual machines.
2. Storage details of NAS share include the total utilized storage space and the space used by the NAS and iSCSI restore mounts.
3. The 'Storage' section displays the storage utilized by physical machines, VMware machines, and the network shares in the IDrive BMR device. Here, you can perform cleanup for your physical and VMware machines.

To perform a manual cleanup,

1. Choose 'All', 'Physical Machine', or 'VMware Machine' as the 'Cleanup Type' from the drop-down menu.
2. Click 'Cleanup'.
3. Click 'Confirm' in the confirmation window.

Backup Statistics

This section displays information about the storage used by each client, VMware machine, and network share.

- The 'Data Size' section displays the actual storage space utilization, which is far less than the original drive size. The IDrive BMR device employs deduplication mechanism and compression in the backend to optimize the storage space.
- You can check which physical machine or VM has an active file restore, virtual instance, and scheduled cloud replication. In the case of NAS, you can check if the network share has an active restore mount.
- You can view and manually manage the recovery points or recovery snapshots of your physical machines, VMs and NAS shares.
- You can also search for a required client, VM, or network share using the 'Search' field.

System Health

This tab provides information about the health status of RAID devices, hard drives, memory used, and the network port. You can also perform the cleanup operation if the storage utilization reaches 80%.

RAID Health Status

This section displays the health status of RAID devices. If one device stops working the other acts as a backup.

RAID Health statuses and what they indicate:

ONLINE - The drives are working as expected.

DEGRADED - The drive experienced an issue and is predicted to fail.

FAULTED - The drive is not found or is inaccessible.

Contact the support team immediately if any of the RAID devices stop working. Our team will analyze the problem and send a replacement device after processing the issue. Once you receive the device, our team will assist in replacing the device over chat or phone support. After the device is successfully replaced and identified by the device, the rebuild operation will start. You can see the rebuild operation status in the 'RAID health status' section.

OS Drive Health Status

You can check the individual health status of the hard drive (OS and storage) under the 'OS Drive Health Status' section.

OS Health statuses and what they indicate:

GOOD - Drives are working fine.

BAD - Contact support team immediately.

Predicted to Fail - Contact support team immediately.

General Info

This section gives information about the time since the IDrive BMR device is up and running and also about RAM usage.

Network

The 'Network' section displays information about network settings such as IP address and the mode of network.

Logs

This tab displays information about activities performed on the device. These logs will help support the team to analyze the cause of backup failure.

Physical Machines And VMware

Backup Logs

This tab displays information about backup activities of the registered physical clients and VMware machines. Click  to view detailed information about the activity.

IDrive Cloud Logs

This tab provides information about all logs related to cloud backups. This includes the date, hostname/VM name, volume, recovery point, type, backup status, and integrity information.

Cloud Seeding Logs

The tab displays information about all logs related to cloud replication initiated via BMR Express.

Restore Logs

This tab displays information about restore activities of the registered clients and VMware machines.

Delete Logs

This tab displays information about the recovery point deletions.

NAS Logs

View comprehensive logs of BMR network shares, backups, restore, and delete operations.

System Logs

This tab displays information about system activities such as sign in, sign out, and so on.

Export

This option allows you to download the logs in CSV, Excel, and PDF format. You can also print and copy the logs. Click 'Export' in the respective tab and click the required format from the drop-down menu to download the logs.

Cloud Manage

Cloud Manage enables browser-based management and access of the IDrive BMR device interface from external networks.

To connect to your IDrive BMR device,

1. Go to www.idrive.com and sign in with your BMR cloud account credentials.
2. The 'All BMR Devices' tab displays the list of IDrive BMR devices.

If any device appears offline, click  to update the status.

Note: The refresh option is displayed only for IDrive BMR version 8.4.0 and above.

3. Click 'Connect' against the required device. Access to the device web interface is established in a new tab. From here, you can perform local backups, create restore points, view logs, and also monitor the health of the machines on the device. For more information, refer to the [BMR FAQs](#).
4. Click 'Cloud Replication' to view the cloud replication statuses. You can also view and manage the cloud backup recovery points of individual physical and VMware machines on the IDrive BMR device.

Note:

- *In the case of IDrive BMR devices with firmware version 8.3.0 or older, access to the device web interface is established via a remote access window.*
- *If the IDrive BMR device is purchased through a reseller, the reseller will have access to your device with automatic sign in through the 'Partner Management' feature. You can disable this access any time via the IDrive BMR device interface, under 'Settings' > 'Control Panel' > 'Partner Manage'.*

Cloud virtualization on IDrive® BMR web console

Create and access cloud virtual instances associated with your IDrive BMR device from the IDrive BMR web console.

Signing in after two-factor authentication is enabled

To create a cloud virtual instance via the web console,

1. Sign in to <https://www.idrive.com> with your IDrive BMR cloud account credentials.
2. Click 'Cloud Virtualization' next to the required device. This will open the cloud virtualization screen and display any cloud virtual instances associated with the device.
3. Click 'Create a Virtual Machine'.
4. The 'Physical Machines' tab is selected by default. To create a virtual instance of a VMware machine, switch to the 'VMware' tab.
5. Choose the required physical machine or VMware server and machine.
6. Select a recovery point.
7. Select the number of processors for the virtual machine.

- Allocate memory for the virtual machine in the 'RAM' field, taking into account the memory available for cloud virtualization.
- Select a network source and a suitable network model.

Note:

- Disconnected and NAT (Firewalled) network sources are available for cloud virtualization.*
- Disconnected, NAT (Firewalled), and Bridged network sources are available only for local virtualization. To create or access local virtual instances, connect to the local device interface.*

- Select a storage controller for the virtual machine.

Note: SATA is recommended for virtualizing physical machine backups. LsiLogicSAS is recommended for creating virtual instances of VMware machines.

- Select a graphics option from the dropdown.
- Click 'Build Virtual Machine'. A virtual instance of the machine will be created. You can now connect to it and continue working.

Note on virtual instances of physical machines: When a machine with dynamic disks is virtualized, the created virtual instance will have basic disks with randomly assigned drive letters. You may have to sign in to the virtual instance and change the drive letter associations as necessary.

Access cloud virtual instances via the web

To access a cloud virtual instance from the web console,

- Sign in to <https://www.idrive.com> with your IDrive BMR cloud account credentials.
- Click 'Cloud Virtualization' against the required device. The cloud virtual instances associated with the particular device will be listed.
- Click 'Copy VNC Password' and then 'Connect' corresponding to the required virtual instance.
- Sign in to the virtual instance with the copied VNC password.

View Tickets

View the support tickets for your account in the 'View Tickets' tab of the BMR web client. Below are the steps:

- Navigate to www.idrive.com and sign in to your BMR cloud account.
- In the 'View Tickets' tab, you can view all the support tickets associated with your account. You can also view information such as ticket ID, subject, status, and last updated time.
- Enter the ticket ID in the search bar to view a specific ticket.
- Click on the ticket ID for more details.

You can filter out the tickets based on their status.

Two-factor authentication for your IDrive® BMR cloud account

Enable two-factor authentication for enhanced security and to prevent unauthorized access to your account.

Below are the steps to enable two-factor authentication,

1. Navigate to www.idrive.com and sign in to your BMR cloud account.
2. Go to the top-right corner, click the drop-down menu, and select 'Two-factor Authentication'.
3. Click 'Enable'.
4. Select the preferred method for receiving the one-time verification code, 'Email Address', 'Phone Number', or Time-based OTP authentication, and click 'Confirm'.
 - *In the case of email address verification, the OTP will be sent to the email address in your 'Profile Information' section.*
 - *If you choose 'Phone Number', enter the same and click 'Send Code'.*
 - *If you choose Time-based OTP authentication, launch any Time-based OTP authenticator app on your mobile device and scan the QR code. Click 'Next', copy the recovery code, and click 'Continue'.*
5. Enter the verification code, received on the phone number / email address or displayed on the TOTP application, and click 'Verify & Enable' / 'Activate'. You will see a success message indicating that Two-factor verification is successfully enabled.

To sign in after two-factor authentication is enabled,

1. Navigate to www.idrive.com and enter your username and password.
2. Click 'Sign in' and you will be prompted to enter a verification code sent to your phone number / email address or displayed on the TOTP application.
3. Enter the verification code and click 'Verify' / 'Submit Code'.

Note: If you are unable to receive the SMS with the OTP, you can choose to receive the verification code via email address or a TOTP application. Click 'Receive verification code via email address' or 'Verify code via Time-based OTP Authenticator app (Supported Apps)' on the two-factor authentication page.

Disable two-factor authentication

To disable two-factor authentication for your account,

1. Navigate to www.idrive.com and sign in with your IDrive BMR cloud account credentials.
2. Go to the top-right corner, click the drop-down menu, and select 'Two-factor Authentication'.
3. Click 'Disable'.

We hope you found this User Guide useful to get started with IDrive BMR. For additional information, you may click  and refer to the help slides or read the [BMR FAQs](#).

If you did not find what you need, write to us at support@idrive.com.