What's New in Barracuda Backup

https://campus.barracuda.com/doc/5013563/

What's New in Version 6.6.04

Early Availability Release Date: December 6, 2022

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important:

- To prevent issues during the upgrade process, firmware upgrades have been disabled for customers with appliance serial numbers below 800000. For more details, contact Barracuda Networks Technical Support.
- This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that if you are updating from a firmware version prior to 6.5.04, the firmware update to 6.6.04 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.6.04, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.6.04 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Enhancements

- Official support for VMware vSphere Version 7 Update 3
- Official support for Microsoft Windows Hyper-V Server 2022
- Official support for macOS Version 12 Monterey
- Improvements to backup error messaging.

Fixes

- A fix has been implemented to improve VMware vSphere backup performance. [BNBS-49513]
- A fix has been implemented to improve file share (FS) backup performance. [BNBS-47831]
- Resolved an issue where restores from receiver appliances do not work unless the restore target exists on the sending appliance. [BNBS-47790]

- A fix has been implemented to enable download and recovery of `.VHDX` files backed up via the file system. [BNBS-29258]
- Resolved an issue causing virtual machines to be prematurely cleaned up in the Cloud LiveBoot system if the virtual machine name is too long. [BNBS-49842]
- Resolved an issue causing hung backups due to a race condition. [BNBS-49849]
- Resolved an issue causing reports with item-level failures to report as successful in the cloud interface. [BNBS-49819]
- Resolved an issue causing VMware vSphere backups to fail with “system aborted” due to a missing/deleted virtual machine in the backup schedule. [BNBS-48501]
- A fix has been implemented to re-enable the SNMP service. [BNBS-47745]
- Resolved an issue where report data gets stuck in the offsite replication queue, causing inaccurate dashboard and reporting information. [BNBS-50015]
- The APC UPS service has been upgraded to support connections via USB. [BNBS-49218]

What's New in Version 6.6.03

Early Availability Release Date: May 3, 2022

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: To prevent issues during the upgrade process, firmware upgrades have been disabled for customers with appliance serial numbers below 800000. For more details, contact Barracuda Networks Technical Support. This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that if you are updating from a firmware version prior to 6.5.04, the firmware update to 6.6.03 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.6.03, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.6.03 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Enhancements

- Official support for Microsoft Windows Server 2022
- Official support for Microsoft Windows 11
- Replication status for all offsite replication targets is now included in the daily email summary reports.
- A change has been made to the backup appliance health status, which now includes a warning status if the appliance is only partially checking in.

- Support has been added for LDM partitions for virtual machine browsing (LiveBrowse).

Fixes

- Improved browsing performance in the cloud UI restore browser. [BNBS-48068]
- Resolved a timestamp conversion issue causing Microsoft SQL databases to show “unknow transfer status” in the restore browser. [BNBS-48993]
- Resolved an issue where data was not getting purged for data sources and shares that have been removed from the cloud UI. [BNBS-47145]
- Improved mailbox scheduling and selection performance in the cloud UI. [BNBS-49110]
- Improved VMware virtual machine recovery. [BNBS-49183]
- Resolved an issue where the State or Province drop-down menu is not displaying properly on the appliance settings page of the cloud UI. [BNBS-49242]
- Resolved an issue where the daily email summary is sometimes sent multiple times per day. [BNBS-49109]
- Resolved an issue where the list of available virtual hardware components is incorrect when performing a local LiveBoot for a VMware virtual machine. [BNBS-49441]
- Resolved an issue where the external subnet mask is not visible in the cloud UI when performing a Cloud LiveBoot. [BNBS-48981]
- Resolved an issue where the last two items in the cloud UI restore browser are covered behind a blue line and inaccessible. [BNBS-43450]
- Improved error messaging for a virtual machine that fails with “system aborted”. The error message now states that the failure is due to the virtual machine no longer being available after explicit selection in the backup schedule. [BNBS-46712]
- Improve database performance by adjusting the frequency of the autovacuum process. [BNBS-47946]

What's New in Version 6.6.02

Early Availability Release Date: August 10, 2021

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: To prevent issues during the upgrade process, firmware upgrades have been disabled for customers with appliance serial numbers below 720000. For more details, contact Barracuda Networks Technical Support. This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that if you are updating from a firmware version prior to 6.5.04, the firmware update to 6.6.02 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.6.02, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system

reboot, then the completion of the firmware update when the device comes back online. The entire 6.6.02 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Enhancements

- Improved MacOS Support
  - Added official support for MacOS Catalina and Big Sur.
- Data Purging Enhancements
  - Improved the data purging process, making the process faster and more efficient.
- Support for APC Uninterruptable Power Supplies (UPS)
  - Added official support for APC UPS devices, which enables the Barracuda Backup appliance to gracefully shutdown in the event of a power failure.
- Security Enhancements
  - Added the ability for customers to disable remote access to their appliances from Barracuda Networks Technical Support.
  - Implemented a number of enhancements to improve the overall security of the platform and resolve any outstanding vulnerabilities.

Fixes

- Downloads from the cloud interface no longer time out and abort. [BNBS-48790]
- Large file downloads no longer fail due to a PHP memory limit. [BNBS-48611]
- The Amazon Machine Image (AMI) no longer fail during the restore/import process due to invalid characters in the virtual machine disk name. [BNBS-48636]
- Cloud LiveBoot does not hang in the “configuring” state due to a time out limit. [BNBS-48712]
- Items show properly in a virtual machine when browsing. [BNBS-48784]
- Browsing inside of a Hyper-V virtual machine due to an incorrect argument no longer occur. [BNBS-49012]
- Downloads no longer fail due to a connection time out failure. [BNBS-48799]
- Resolved an issue that prevented large email messages from being backed up due to a memory limitation issue. [BNBS-47559]
- The restore browser no longer exceeds 30 seconds to load or times out due to an inefficient query. [BNBS-47428]
- Cloud LiveBoot does not fail due to an invalid timestamp conversion. [BNBS-48715]
- Resolved an issue that caused Hyper-V partitions in the restore browser to be labeled “Backup Agent” due to an invalid timestamp. [BNBS-48742]
- Resolved an issue that caused the browsing of Hyper-V virtual machines to show no results and perform slowly due to an inefficient query. [BNBS-48725]
- Restore browser in the cloud interface does not display file revisions that no longer exist. [BNBS-48601]
- Cloud LiveBoot cleanup process does not fail due to a parenthesis in the virtual machine name. [BNBS-30248]

What's New in Version 6.6.01

General Availability Release Date: June 7, 2021

Early Availability Release Date: February 11, 2021

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: To prevent issues during the upgrade process, firmware upgrades have been disabled for customers with appliance serial numbers below 720000. For more details, contact Barracuda Networks Technical Support. This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that if you are updating from a firmware version prior to 6.5.04, the firmware update to 6.6.01 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.6.01, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.6.01 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Enhancements

- VMware vSphere 7 Support
  - Barracuda Networks has added official support for VMware vSphere 7 and ESXi 7 virtual environments. This also includes platform support for the Barracuda Backup virtual appliance (Vx).
- Support for LDAP over SSL (LDAPS)
  - Barracuda's Exchange Message-Level (EML) backup now supports Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL).

Fixes

- TLS v1.0 and v1.1 have been disabled. [BNBS-47156]
- Additional verbiage has been added to the confirmation prompt when a backup source has been deleted, warning that data will be deleted both locally and in the cloud. [BNBS-42949]
- Resolved an issue that will provide better backup performance for backup sources with many files. [BNBS-47765]
- Disk utilization calculations optimized, resulting in storage statistical information being updated more frequently in the user interface and a reduction in disk I/O operations. [BNBS-48043]
- User profile disks in Windows Server are now excluded by default, preventing undesired backup

errors. [BNBS-30964]
- VMware virtual machine backups does not fail due to an API call failure. [BNBS-46139]
- Resolved an issue causing file share (CIFS) backups to hang indefinitely instead of failing gracefully. [BNBS-46008]
- VMware backups optimized, resulting in faster CBT part checks. [BNBS-47264]
- Resolved an issue causing file share (CIFS) backups to be reported as a critical failure, even if the backup was successful. [BNBS-47498]
- Backup schedules are successfully saved if the start time is “00:xx”. [BNBS-47032]
- Data purge process optimized, resulting in faster data purging, especially in environments with many small files. [BNBS-47412]
- Resolved an issue causing file share backups using CIFS/SMB v2.1 to fail. [BNBS-39356]
- Microsoft Hyper-V disks can be displayed and browsed using the LiveBrowse feature. [BNBS-47408]
- Resolved an issue causing extremely slow performance in the local BBS console related to the appliance searching for a DHCP server. [BNBS-47857]
- Exchange Message-Level (EML) no long cause backup failures due to previously aborted backup jobs. [BNBS-47165]
- File share backups optimized to attempt to mount shares using newer versions of CIFS/SMB first. [BNBS-46319]
- Data backed up by the Barracuda Backup Agent for Linux are now included in the Large Items report. [BNBS-40982]
- Resolved an issue where data was sometimes not being purged on a receiving Barracuda Backup appliance. [BNBS-33603]
- Resolved an issue where the last backup time for a backup schedule set to repeat is not initiated. [BNBS-47176]
- Barracuda Backup Agent for Windows no longer crashes if it encounters a directory with an empty file name. [BNBS-45443]
- Tech Support Remote Access toggle no longer reverts to “ON” after navigating to another page. [BNBS-47685]
- Resolved an issue where email attachments are sometimes missing when downloading an email with an attachment. [BNBS-47300]
- Resolved an issue where RAID status is occasionally not reported correctly. [BNBS-46282]
- Modified the verbiage for encrypted files and directories that cannot be downloaded to a more appropriate message. [BNBS-46332]
- The message “Please enter a valid folder path” is no longer displayed when a valid path has been entered in the advanced file system selections window. [BNBS-46380]
- The local Barracuda Backup appliance updates to the currently specified time zone specified in the user interface. [BNBS-46971]
- The Advanced Backup Item Selection toggle no longer fails to save the specified setting. [BNBS-47707]
- Optimizations made to the automated replacement process when repopulating the device with cloud data. [BNBS-47001] [BNBS-42059]
- Exchange Message-Level (EML) backup FAQ link no longer goes to a page that is unavailable. [BNBS-46977]
- Pages accessed using an unsupported browser version are no longer blank, instead post a more appropriate error message. [BNBS-46360]

- SSL/TLS now has the ‘secure’ attribute cookie. [BNBS-43881]
- The ‘httpOnly’ cookie attribute no longer missing. [BNBS-43879]
- Resolved an issue where a VMware restore may fail due to a timeout error. [BNBS-46626]
- Two or more LVM partitions on a disk no longer prevents the disk from being browsed using the LiveBrowse feature. [BNBS-46465]
- Non-UEFI virtual machines can be restored as an AMI in AWS (Replication to AWS). [BNBS-48218]

What's New in Version 6.6.00

General Availability Release Date: September 16, 2020

Early Availability Release Date: March 11, 2020

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: To prevent issues during the upgrade process, firmware upgrades have been disabled for customers with appliance serial numbers below 720000. For more details, contact Barracuda Networks Technical Support. This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that if you are updating from a firmware version prior to 6.5.04, the firmware update to 6.6.00 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.6.00, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.6.00 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Fixes

- Backup schedule changes no longer fail to save periodically. [BNBS-30320]
- Exchange Message-Level backups now support NTLMv2. [BNBS-18400]
- Disk utilization reporting in the dashboard is now accurate. [BNBS-33899]
- Disk utilization reporting reflects accurate changes in a timely manner. [BNBS-43617]
- Ablility to ping Barracuda Backup devices on firmware version 6.6.00. [BNBS-47153]
- Barracuda Backup Agent for MacOS installer downloads as intended. [BNBS-46365]
- Invalid partition layout error no longer reported during bare metal recovery of Windows systems. [BNBS-30102]
- Warrning and error messages report when a VSS writer that was present for a previous backup

is no longer detected. [BNBS-44135]
- Barracuda Backup Agent “USN journal error” provides more detailed error messages. [BNBS-43425]
- Barracuda Backup Agent “Error Connecting to Agent” provides more detailed error messages. [BNBS-42959]
- Remediation of security vulnerability where HTTP (80/tcp) is being used in the local interface as opposed to HTTPS. [BNBS-43882]
- SMB v2 and v3 no longer fail to mount during CIFS backups. [BNBS-45689]
- Online reporting of replication targets does not report the target as offline if configured with a network port in addition to the IP address. [BNBS-44957]
- Barracuda Backup Agent works as intended when not finding the short file name for a given file. [BNBS-43962]
- Subscription information now displays in the Backup dashboard subscription widget. [BNBS-44967]
- Cloud Liveboot no longer fails with "Missing Volumes" error on revisions that are offsite vaulted. [BNBS-45572]
- The offsite replication storage values on the dashboard and in the replication page under **Backup > Replication** now match. [BNBS-45448]
- The Barracuda Cloud Storage option on the **Replication** page takes the normal amount of time to appear after activating the Barracuda Backup device. [BNBS-46262]
- Removing a share when it is the only one explicitly selected in a schedule will not remove that schedule even if it has servers explicitly selected. [BNBS-46353]
- Exchange Message-Level backups no longer fails with "Encountered Unknown SSL error". [BNBS-46080]
- Performing LiveBoot instant recovery from the cloud interface of a Barracuda Backup device acting as a “receiver” no longer fails. [BNBS-44507]
- CIFS shares successfully mount. [BNBS-45242]
- Successful bare metal restores are no longer reported as failing. [BNBS-46431]
- Several VMware backup and restore issues resolved by updating to the latest version of the VMware Virtual Disk Development Kit (VDDK).

What's New in Version 6.5.04

General Availability Release Date: May 12, 2020

Early Availability Release Date: November 21, 2019

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that the firmware update to 6.5.04 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.5.04, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.5.04 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Fixes

- Application of static routes no longer fail if the NTP check is unsuccessful. [BNBS-45563]
- Certain types of data are no longer being reported as double the size in the offsite replication graph (Transfer Remaining). [BNBS-45160]
- Exchange Message-Level restores initiated from a Barracuda Backup device acting as a receiver are no longer failing. [BNBS-44339]
- Restore Browser no longer hangs (spins indefinitely) when selecting a VMware virtual machine and attempting to browse it. [BNBS-46128]
- Audit log entries for file/directory downloads no longer fail. [BNBS-41530]
- Uploading a trusted certificate through the local user interface will not cause the local user interface to fail to reload/start. [BNBS-45734]
- When trying to navigate the cloud user interface, you are not redirected to the backup overview dashboard unless you do not have the correct permissions. Occasional json error is resolved. [BNBS-46586]

Known Issues

- Customers with appliance serial numbers less than 720000 may see a message stating that firmware upgrades have been disabled. This has been done to prevent device failure due to the lack of disk space required to perform the firmware and kernel upgrades. Customers will see the following message when attempting to upgrade from both the cloud and local user interface: "*We have detected that your Barracuda Backup device may not have the required space in order to perform a successful kernel and/or firmware update. To prevent device failure, we have disabled the firmware update action on this device. Please contact Barracuda Networks Technical Support for assistance with updating the device firmware.*" [BNBS-45769 & 45770]
  - Workaround**:** Contact Barracuda Networks Technical Support for assistance upgrading the device firmware.
- When using the **View all revisions** button in the Restore Browser, timestamps for VMware virtual machine revisions are occasionally incorrect, causing the wrong revision to be restored. [BNBS-46513]
  - Workaround**:** Selecting a revision using the calendar option will display the correct timestamps.

What's New in Version 6.5.03

Released September 11, 2019

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that the firmware update to 6.5.03 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.5.03, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.5.03 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification check that may cause increased backup windows.

Enhancements

- Extended Microsoft Platform Support
  - Barracuda Networks has added official support for Microsoft Exchange 2019
    - Backup and recovery support for Exchange 2019 databases.
    - Barracuda message-level protection to enable granular email message and folder recovery.
- Expanded Configuration Options
  - Barracuda Backup appliances can now be configured via the on-board serial port to assist with deployment for a scenario in which a monitor and/or keyboard cannot be added to a Barracuda Backup appliance during the initial configuration or to make configuration changes.
- Enhanced Audit Logging
  - Reboot, shut down, and wipe actions initiated from the Barracuda Backup local interface are now logged in the audit log report to help meet compliance requirements.

Fixes

- VMware backup jobs no longer report as failing due to segfault error at the end of the backup. [BNBS-40311]
- Disk space graphs now load properly on the **Advanced Graphs** page. [BNBS-29704]
- Barracuda Networks resellers are able to successfully link replacement Barracuda Backup devices to their client accounts. [BNBS-38930]
- Fixed an issue where the warning message “A volume (drive) that was previously backed up is no longer there and being backed up” does not specify which volume is no longer present. [BNBS-22605]
- DNS hostnames (FQDN) can be used when configuring replication targets. [BNBS-27745]

- Ports added to the end of an IP address can be used when configuring replication targets. [BNBS-41614]
- After manually purging an item in the **Restore Browser**, the item is no longer shown. [BNBS-29690]
- Authentication issues to VMware no longer reported as an empty error message. [BNBS-32535]
- The Backup Export Tool now loads VTL drives hosted by AWS. [BNBS-43361]
- Files with periods or spaces at the end of the filename can now be opened and backed up during a CIFS/SMB backup. [BNBS-42523]
- VMware VMs are successfully exported using the Backup Export Tool. [BNBS-42521]
- Complete file system restores of a Windows Server 2019 system to the original location no longer result in a failure to restore the Windows Defender directories and contents located in C:\ProgramData and C:\Program Files. [BNBS-41652]
- A complete system state restore of a Windows Server 2019 system no longer fails due to the Windows Defender directories and files. [BNBS-41655]
- TLS certificates for the local interface are now signed using SHA-256. [BNBS-42599]
- Actions performed in the local interface are now shown in the cloud interface Audit Log. [BNBS-27140]
- The current confirmation message when updating firmware from the cloud UI has been revised to avoid miscommunication. [BNBS-41950]
- Changing the name of a VMware VM when attempting to restore to vSAN does not cause the restore to fail. [BNBS-39268]
- New warning notification when the **Purge** button is clicked on the Large Items report. [BNBS-32680]
- Graphs now load properly on the **Advanced Graphs** page. [BNBS-28314]

What's New in Version 6.5.02

Released April 24, 2019

Note: For the best experience, all devices attached to an account or replicating site-to-site should be updated to the same firmware version.

Important: This release does not support locally controlled Barracuda Backup devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

The 6.5.01 early availability release has been merged into 6.5.02.

Please be advised that the firmware update to 6.5.02 includes a kernel update, which will require a reboot of this Barracuda Backup device. Before updating the device firmware to 6.5.02, it is recommended that you have physical access to the device in the event of a failure. The kernel update will occur first, followed by a system reboot, then the completion of the firmware update when the device comes back online. The entire 6.5.02 firmware update process may take 30-60 minutes to complete. After the update, the next scheduled backup will undergo a one-time data verification

check that may cause increased backup windows.

Enhancements

- Extended Microsoft Platform Support
  - Barracuda Networks has added official support for the following Microsoft platforms:
    - Microsoft Windows Server 2019
    - Microsoft Hyper-V Server 2019
    - Microsoft SQL Server 2019
- Improved Barracuda Backup Agent Security
  - The Barracuda Backup Agent now uses TLS 1.2 (128-bit AES) to both authenticate with a Barracuda Backup device and encrypt the connection between the Barracuda Backup Agent and the Barracuda Backup device. This enhancement provides secure encrypted communication and helps prevent potential man-in-the-middle attacks.
- Expanded Configuration Options with Static Routes
  - Static routes can now be configured from the Barracuda Backup cloud interface. Static routes are used to connect the Barracuda Backup device to a specific network or sub-network in cases where the routing is not happening automatically.
- Enhanced Bare Metal Recovery for Microsoft Windows
  - The new bare metal recovery (BMR) kit creates a bootable ISO using the latest Windows ADK (Windows Assessment and Deployment Kit) and WinPE (Windows Preinstallation Environment) add-on from Microsoft. This provides the latest software from Microsoft, improving reliability.

Fixes

- If the Barracuda Backup device loses NTP synchronization during a backup, the backup reports as failed immediately, when it should wait until the backup has finished. [BNBS-37639]
- Failed backup reports will show an error header that states the number of issues in the backup, but no details for the errors are shown in the report. [BNBS-31178]
- The Barracuda Backup Agent for MacOS fails to backup data underneath a directory when that directory returns a “no data available” error code during a backup. [BNBS-37783]
- When clicking on the purge button on the Large Items page, there is no warning notification about purging/deleting data. [BNBS-32680]
- Restores from replication partners may fail if parts are not present locally (Private Key Encryption configurations only). [BNBS-37698]
- Writing more than 4TB to removable drives with the Backup Export Tool will fail. [BNBS-37680]
- Unable to LiveBrowse (granular recovery) a Hyper-V virtual machine from an offsite replication destination (receiver). [BNBS-38708]
- When switching from the interface of a specific Barracuda Backup device back to the overview dashboard showing all devices on the account, the device name, model, serial number, and IP address of the prior device show in the header when they shouldn't. [BNBS-31644]
- When using LiveBoot, some errors can leave a back trace on the page. [BNBS-31134]
- The data migration options (hardware replacements) page is showing "Migrate from Barracuda Cloud" for devices that have been replicated to AWS. [BNBS-37710]
- Restore actions on a privately encrypted receiver will always prompt for the LOCAL passphrase

regardless of whether the data would require it or if the passphrase is correct. [BNBS-37725]
- Barracuda Backup Agent backups failing due to “no reconnect info” errors. [BNBS-41267]
- Data migrations where data is pulled from the cloud are failing due to connection errors. [BNBS-40127]
- Backup errors generated for non-Microsoft reparse points. [BNBS-38690]
- CIFS/SMB backups are failing to back up files with special characters. [BNBS-29482]
- The Barracuda Backup Agent for Windows locks the EFI partition, causing other processes requiring access to it to fail. [BNBS-34604]
- Microsoft SQL backups fail if all SSL/TLS protocols other than TLS 1.2 are disabled. [BNBS-35008]
- CIFS/SMB backups cannot read the contents of directories with names that end with dots or spaces. [BNBS-41936]
- VMware backup jobs failing due to exceeding timeout period on the vSphere web client session. [BNBS-41660]

Known Issues

- VMware backup jobs reported as failing due to segfault error at the end of the backup. [BNBS-40311]
    - Workaround: Contact Barracuda Networks Technical Support for resolution, patch available for firmware version 6.5.02.
- Complete file system restore of a Windows Server 2019 system to the original location will result in a failure to restore the Windows Defender directories and contents located in C:\ProgramData and C:\Program Files. [BNBS-41652]
    - Workaround: Windows Defender directories and contents can be downloaded or restored to an alternate location. The directories can also be recovered by performing a Windows Bare Metal Recovery.
- A complete system state restore of a Windows Server 2019 system will fail due to the Windows Defender directories and files. [BNBS-41655]
    - Workaround: The entire Windows Server 2019 system can be recovered by performing a Windows Bare Metal Recovery.

What's New in Version 6.5.00

Released September 18, 2018

Note: For the best experience, upgrade all devices attached to an account or replicating site-to-site to the same firmware version.

Important: This release does not support *locally controlled Barracuda Backup* devices. The current Local Control release for Barracuda Backup is firmware version 6.4.03.

Be advised that the firmware upgrade to 6.5.00 from any version prior to 6.4.06 requires all data

sources protected using the Barracuda Backup Agent to undergo a data verification check, known internally as a second-pass backup, on the next scheduled backup. The one-time data verification check will cause increased backup windows. For this reason, Barracuda Networks recommends upgrading device firmware over a weekend or during a scheduled maintenance period.

Enhancements

- Private encryption of cloud data
- Automated migration option for cloud data and configuration
- Barracuda Backup Agent security enhancements
- Enhanced single file downloads to support browser restart capability
- Improvements to support tunnel stability and user experience

Fixes

- Microsoft SQL backups that are configured to use SQL server authentication credentials are failing. [BNBS-39158]
- Barracuda Backup Agent stops logging. [BNBS-38454]
- Failure to obtain SQL server version from the registry causes backups to fail. [BNBS-37371]
- Large number of unchanged records can cause backups to fail. [BNBS-37178]
- Hung VMware backup reports due to segfault in backup process. [BNBS-36427]
- Support tunnel binding to incorrect port causing conflicts between processes. [BNBS-33520]
- Subscription expiration date on dashboard showing as “Invalid date”. [BNBS-33655]
- Hung backup reports in web UI due to incorrect report data transfer. [BNBS-36363]
- Agent backups failing on UNC paths in System State. [BNBS-35277]
- VMware backup jobs failing when a VM is no longer present. [BNBS-34855]
- VMware historical revisions selected for offsite vaulting are not being purged locally. [BNBS-35821]
- Incorrect NTP server values causing time sync issues on some Barracuda Backup devices. [BNBS-36716]
- Slow load performance of VM list in Cloud LiveBoot VM selection dialog. [BNBS-29234]
- Restores of VMware VMs backed up on vSAN failing. [BNBS-30847]
- Network File Share backups can fail when encountering a single directory with a higher than average number of files and sub-directories. [BNBS-24302]
- User accounts fail to sync to the local Barracuda Backup device if notifications for that user are disabled. [BNBS-33690]
- Restores of offsite vaulted data can fail if first attempt at part retrieval fails (retry logic issue). [BNBS-35491]
- VMware CBT backups not properly verifying the existence of previously backed up parts. [BNBS-33577]
- Non-critical backup errors for Agent backups are not being reported properly. [BNBS-35355]
- Microsoft Hyper-V .avhd and .avhdx files not displayed in the Restore Browser. [BNBS-25701]
- Microsoft Hyper-V backups failing when VMs are configured using UNC paths. [BNBS-35776]
- VMware VMs using a virtual SATA controller fail to restore. [BNBS-33469]
- VMware VMs backed up with multiple virtual hard disks are only being restored with one hard disk in some cases. [BNBS-33893]

- Hyperlinks to SQL databases in backup reports are not properly going to the object in the Restore Browser. [BNBS-16858]
- Slow performance when transferring statistical and report data used in the web UI. [BNBS-37483]
- The Current Tasks widget on the dashboard should not show Replication as “In Progress” if there is no binary data in the offsite transfer queue. [BNBS-31140]
- Unable to successfully link replacement devices when the option to migrate only the configuration is selected. [BNBS-33960]
- Invalid time zone of ‘ ‘ prevents backup jobs from running. [BNBS-35828]
- Backups failing when encountering nested volumes on btrfs filesystems. [BNBS-31165]
- Connection issues between ESXi host and Barracuda Backup during backup reads causing backups to fail in some cases. [BNBS-35313]
- Transfer graphs on dashboard not loading for AWS replication destinations. [BNBS-35906]
- UUID sometimes being displayed in Restore Browser instead of file/object name. [BNBS-35267]
- Unable to remove offsite replication partners after a migration. [BNBS-35411]
- Changed block tracking is not enabled” warning in backup reports used in cases where CBT cannot be used for different reasons or CBT is not being used at all. [BNBS-35424]
- Offsite replication destinations/targets should display serial number instead of id used internally by Barracuda. [BNBS-25907]
- Bare metal restore failing when the system has an EFI partition with a volume GUID. [BNBS-35562]

Known Issues

- Restores from replication partners may fail if parts are not present locally. (When data is sent to both a cloud destination and another Barracuda Backup device, Barracuda will attempt to pull file parts from the cloud if they cannot be found on the Barracuda Backup replication partner during a restore job. If private encryption of cloud data is configured for the cloud target, the restore will fail as the parts are privately encrypted.) [BNBS-37698]
  - Workaround: Contact Barracuda Networks Technical Support for assistance with recovery.
- Writing more than 4TB to BET fails for removable drives. This issue exists in previous versions and is included in Barracuda Backup 6.5.01. [BNBS-37680]
  - Workaround: Contact Barracuda Networks Technical Support for assistance in resolving this issue.

What's New in Version 6.4.07

Released October 30, 2018

Note: For the best experience, all devices attached to an account or replicating site-to-site should be upgraded to the same firmware version.

Important: This release does not support locally controlled Barracuda Backup devices. The current

Local Control release for Barracuda Backup is firmware version 6.4.03.

Please be advised that the firmware upgrade to 6.4.07 from any version prior to 6.4.06, requires all data sources protected using the Barracuda Backup Agent to undergo a data verification check, known internally as a 2nd pass backup, on the next scheduled backup. The one-time **data verification check will cause increased backup windows**. For this reason, Barracuda Networks recommends upgrading device firmware over a weekend or during a scheduled maintenance period.

Fixes

- Barracuda Backup Agent stops logging. [BNBS-38454]
- Failure to obtain SQL server version from the registry causes backups to fail. [BNBS-37371]
- Large number of unchanged records can cause backups to fail. [BNBS-37178]
- Unable to export data using the Backup Export Tool. [BNBS-37091]
- Incorrect NTP server values causing time sync issues on some Barracuda Backup devices. [BNBS-36716]
- Hung VMware backup reports due to segfault in backup process. [BNBS-36427]
- Hung backup reports in web UI due to incorrect report data transfer. [BNBS-36363]
- Clicking on "Configure Permissions" on a user on the BCC users page results in a dead link (404 error). [BNBS-36054]
- NTP Sync call prevents backups from being performed. [BNBS-36044]
- Issues with user sync, causing an empty list of users within Barracuda Backup. [BNBS-35911]
- Navigation issues causing a loop where the user must select a Barracuda Backup device over and over. [BNBS-35885]
- VMware historical revisions selected for offsite vaulting are not being purged locally. [BNBS-35821]
- Microsoft Hyper-V backups failing when VMs are configured using UNC paths. [BNBS-35776]
- Incorrect web version being passed to customers on pre-6.4 firmware. [BNBS-35746]
- Having no users configured for notifications can cause incorrect user sync in the rest of Barracuda Backup. [BNBS-35726]
- An account with no Barracuda Backup devices cannot hit the migrations page. [BNBS-35625]
- Liveboot web request queuing only tries once before failing. [BNBS-35417]
- Agent backups failing on UNC paths in System State. [BNBS-35277]
- VMware backup jobs failing when a VM is no longer present. [BNBS-34855]
- Support tunnel binding to incorrect port causing conflicts between processes. [BNBS-33520]

What's New in Version 6.4.06

Enhancements

- Improved activation of Barracuda Backup devices and Cloud-to-Cloud Backup
- Barracuda Backup macOS Agent
- Support for VMware vSphere 6.7

Fixes

- Incorrect storage usage numbers reported after upgrades from 6.2.04 to 6.4.05. [BNBS-34837]
- The RAID status is not being updated for new Barracuda Backup devices that replaced a device with a critical RAID status. [BNBS-34398]
- The backup size for Microsoft SQL backups using VDI are being reported incorrectly. [BNBS-34054]
- LDAP referral errors in Microsoft Exchange Message-Level backups cause an unnecessary number of warnings in backup reports. [BNBS-32835]
- Restoration of directories containing hundreds of thousands of files or more is failing due to inefficient memory consumption. [BNBS-32694]
- Incorrect disk usage reported due to missing directory. [BNBS-32636]
- Barracuda Backup devices showing as offline in UI, despite being online and functional. [BNBS-30547]
- When configuring an external interface on Cloud LiveBoot VMs, IP, Subnet, and MAC address information is not displaying correctly [BNBS-29656]

Known Issues

- Default energy setting in mac OS High Sierra and Sierra causes the disk(s) to sleep and the Barracuda Backup mac OS Agent to lose its connection back to the local Barracuda Backup device. [BNBS-35379]
  - Workaround: Deselect the **Put hard disks to sleep when possible** option in **Energy Saver**. For details, see the Apple Support article Use the Energy Saver settings on your Mac.
- mac OS Agent will report non-critical errors and fail to backup '/private' directory. [BNBS-35345]
  - Workaround: Deselect the **/private** directory in the backup schedule or create an exclusion rule for the **/private** directory to prevent non-critical backup errors from appearing in the backup report.
- Inconsistent delivery of daily Backup Summary Reports. [BNBS-33856]

What's New in Version 6.4.05

Features

- Replication to AWS support for EMEA region [BNBS-30053]
- Automated migrations: User can choose not to migrate [BNBS-30015]
- Automated migrations: User can select to migrate configuration only [BNBS-30016]
- Admin is notified when a backup job takes more than 24 hours to complete [BNBS-27008]
- Advanced selections: specify a path to back up [BNBS-28914]

Fixes

- Barracuda Backup Appliance model 790 linking as Cloud-to-Cloud Backup [BNBS-32753][BNBS-30773]
- Restore Browser does not properly show some data backed up after backup failure [BNBS-30961]
- File System backups can hang due to failing health status [BNBS-30830]
- Downloading certain directories will fail in the web UI; use Local UI for these items [BNBS-30453]
- Backup job fails due to failed mount path [BNBS-30349]
- Backup Agent can get stuck in a rebuild loop [BNBS-30124]
- Offline email notifications sometimes not sending [BNBS-29815]
- Purge on demand fails on the Large Items page [BNBS-29786]
- Cannot add port to replication settings [BNBS-23394]
- Audit log entries stored in incorrect time zone [BNBS-21175]
- Differential SQL VSS backups should display the changed size and not the full database size in the Backup Report and Restore Browser [BNBS-16331]
- Incorrect timestamp for non-incremental restores in Restore Browser [BNBS-29533]

Known Issues

- Large Items page does not load in the local UI: view in the web UI [BNBS-32638]

What's New in Version 6.4.04

Fixes

- Unable to restore VM that does not exist on the host [BNBS-29952]
- Backup reports can fail to send [BNBS-29655]
- Cloud LiveBoot does not prefetch all disks [BNBS-29622]
- File Systems can fail to restore from the Local UI [BNBS-29562]
- Cluster Shared Volumes (CSV) not excluded from backup [BNBS-29242]
- Report shows successful when backup fails with 0 btyes of data [BNBS-29096]
- Verbose Agent error description in Backup Reports [BNBS-29056]
- Cloud LiveBoot displays incorrect machine state [BNBS-28820]
- Support for Hyper-V Cloud LiveBoot non-primary boot disks [BNBS-28756]
- Agent per-object schedules can cause purger to incorrectly remove runs for database objects [BNBS-28611]
- Open support tunnel can fail in the Local UI [BNBS-28577]
- Summary reports are sometimes incomplete or not sending [BNBS-28483]
- Web records can show inaccurately due to caching [BNBS-27998]
- LiveBrowse not working with VHDX files [BNBS-27592]
- Backups with FQDN can fail to connect to the agent after upgrade [BNBS-17102]

Known Issues

- File System backups can hang due to failing health status [BNBS-30830]
- Cannot add port to replication settings [BNBS-23394]
- Purge on demand fails on the **Large Items** page [BNBS-29786]
- Downloading certain directories will fail in the web UI - use Local UI for these items [BNBS-30453]

What's New in Version 6.4.03

- This release adds several fixes that were identified in 6.4.02.
- Version 6.4.03 is the latest (current) local control release

What's New in Version 6.4.02

Features

- Replication and Restore to Amazon Web Services (AWS)
  - Replication to AWS (S3) – Barracuda Backup now supports replication to AWS as replication option in addition to Barracuda Cloud
  - Restore to AMI – Restore Barracuda Backup virtual image backups to an AWS EC2 instance

Enhancements

- Open support tunnel from the web UI [BNBS-28823]
- SMB versions 2 and 3 support [BNBS-28423]
- Cloud LiveBoot HyperV: VHDX Generation 2 support [BNBS-27388]
- Link to purge items directly from the Large Items report [BNBS-27013]

Fixes

- Backup jobs fail due to other process [BNBS-29081]
- Multi-select restore fails without timestamp [BNBS-28587]
- Warn before offsite vaulted data is removed by a user [BNBS-28573]
- Once enabled, Offsite Vaulting cannot be disabled. [BNBS-28571]
- Backup schedules skipped intermittently [BNBS-28557]
- Summary reports not sending for some schedules [BNBS-27904]
- LiveBrowse not working with vhdx files [BNBS-27592]
- Show custom retention policies in the web UI [BNBS-26935]

What's New in Version 6.4.00

Features

- New Barracuda Backup Dashboard and Overview pages
- Physical Barracuda Backup to Receiver Vx Replication
  - Available on Barracuda Backup models 190 through 690
  - Receiver Vx can be provisioned directly from within the web UI
  - Priced as an additional subscription added to the Barracuda Backup

Enhancements

- HTTPS support for uploading a CA-signed certificate in Local UI
- Virtual Barracuda Backup can now replicate to and from a physical Barracuda Backup

Fixes

- Summary reports display incorrect share names [BNBS-27913]
- VSS SQL Backup does not fail when Differential chain is broken, causing incomplete revisions [BNBS-14279]
- Message Level schedules shown in duplicate [BNBS-22684]
- Cloud LiveBoot list of virtual machines does not always load [BNBS-27669]
- Uncaught Message-level exception causes backup failure [BNBS-27371]
- User roles created in the web UI do not sync locally for Helpdesk and Overview users [BNBS-28391]
- VSS SQL Backup does not fail when Differential chain is broken, causing incomplete revisions [BNBS-14279]
- Summary reports not sending for some schedules [BNBS-27904]
- Bare Metal Restore ignores drive selections [BNBS-16441]
- Sending multiple email alerts after firmware upgrade [BNBS-27633]
- Bare Metal Restore ignores drive selections [BNBS-16441]
- Uncaught message-level errors cause backup failure [BNBS-27170]
- Agent fails on VSS components containing relative paths [BNBS-27304]
- "No disks found" for LiveBoot causes boot failure [BNBS-27861]

What's New in Version 6.3.04

Features

- Cloud LiveBoot updated web interface and support for Microsoft Hyper-V
- LiveBoot updated web interface
- Added Helpdesk and Status user roles

- Support for VMware vSphere version 6.5

What's New in Version 6.3

Features

- Performance enhancements
  - New Backup Agent introduces multi-streaming improving initial backup and restore times
  - New replication queueing system eliminates bottlenecks with highly transactional data sets
  - File shares backups with large directory trees spawn streams more efficiently
- Backup Export Tool expanded functionality
  - Archive to AWS Storage Gateway-VTL
  - Added support for VMware image exports
- Barracuda Cloud-to-Cloud Backup for Office 365
  - Microsoft SharePoint Online
- Other enhancements
  - Multi-account management view switcher
  - Hyper-V restores to an alternate host
  - SQL VDI flat file restores from web UI
  - Ability to boot a virtual machine Clone using Barracuda LiveBoot

What's New in Version 6.2

Features

- On-Demand Purging
- Granular Scheduling – Item selection has moved to the backup schedule which allows you to granularly select specific sets of data to back up and the ability to configure multiple schedules for each source, each with different sets of data selected
- Keep or Remove Data Options in Granular scheduling
- Manually Send a Summary Report
- Configure Daily Summary Reports
- Download a Detailed Backup Report
- Configure Agent-Based Data Sources
- New VMware Data Source Configuration

What's New in Version 6.1

Features

- Barracuda introduces Cloud-to-Cloud Backup for Microsoft Office 365
  - Go to https://www.barracuda.com/directtocloud to learn more and sign up for a risk-free trial
- Back up historical revisions to external media using Yosemite Server Backup
- Support physical to virtual restores to VMware and Hyper-V with the Barracuda Backup Agent
- Backup Export Tool Archive allows you to export historical revisions of data backed up and stored on a Barracuda Backup appliance
- Barracuda Cloud-to-Cloud Backup for Office 365
  - Microsoft OneDrive for Business
  - Microsoft Exchange Online

What's New in Version 6.0

Features

- New web interface look and feel
- Improved Hyper-V Support
  - Browse Hyper-V VHD files through the Restore Browser
- Local Control
  - Manage Barracuda Backup in a cloudless state
  - Replicate data from one or more Local Control appliances
  - Configure alternate rate limits
  - SMTP Server configuration
- Generate large item reports

What's New in Version 5.4

Features

- Offsite Vaulting
  - Store older backup data revisions offsite
  - Specify monthly and yearly offsite retention policies
- Granular SharePoint Restores
  - Use Kroll Ontrack to restore SharePoint objects

    Kroll Ontrack
    You must have an active Kroll Ontrack license.
- Continuing support for Microsoft applications:
  - Microsoft SQL Server 2012
  - Microsoft Exchange 2013
  - Microsoft Windows 8 / 2012 (including ReFS)

    - Microsoft Hyper-V 2012 Standalone
    - Microsoft Hyper-V 2012 Clustering
    - Microsoft Hyper-V 2008R2 Clustering
- Introduction of the Barracuda Backup Agent (Linux):
    - Adds ACL protection
    - Adds alternate stream protection
    - Adds extended attributes protection
- Parallel VMware Backups:
    - Multiple guests on the same host will be backed up concurrently
- Improved Restore Browser:
    - Adds ability to search for items
    - Adds ability to select multiple items for restore
- Advanced Graphs

What's New in Version 5.2

Features

- Barracuda LiveBoot in the Cloud for VMware:
    - Instantly boot to your VMware virtual machine using Barracuda Networks' deduplicated cloud storage.
    - Centralized management of LiveBoot instances

The following feature has been deprecated in version 5.2

- Watched Files – The seldomly used Watched Files feature has been deprecated in versions 5.2, and will not be supported for new Barracuda Backup Servers. Note that existing Watched File Rules will continue to function as expected.

What's New in Version 5.1

Features

- Backup Analytics:
    - View a detailed list of large items by source or file name in the **REPORTS > Large Items** page.

What's New in Version 5.0

Features

- Barracuda LiveBoot for VMware:
  - Instantly boot to your VMware environment any backed up snapshot using de-duplicated storage on Barracuda Backup Server
- Barracuda LiveBrowse for VMware:
  - View and traverse file structure inside all backed up VMware snapshots
  - Download Files and Directories within VMware snapshots
- Improved Restore Browser:
  - Cloud UI Restore Browser displays in the Barracuda Backup web interface
  - Download file system directories as ZIP files
  - Download email mailboxes and folders as ZIP files
- Reporting:
  - Cloud UI Reports available in the Barracuda Backup web interface
  - Size, Duration, Speed, and Type details are included in Reports
  - Enhanced Backup and Restore reporting data organization