Frequently Asked Questions – CrashPlan

**What is this?** CrashPlan is a desktop/laptop backup product that meets most of our campus requirements. More detailed information is available at http://www.crashplan.com/enterprise

**Why?** Risk of loss of encrypted drives, theft, audit, and all the other usual reasons.

**How does it work?** CrashPlan can do encrypted backups to USB local storage, a GT-operated cloud, or a commercial cloud. After the initial backup, CrashPlan PROe backs up changed files every 15 minutes or so. By default, the client only backs up user files and settings. Backed up files are encrypted before they leave the client and are available for restoration from the client application or from the web.

**Does it really work?** CoE has been running the product since 2009. With the addition of other Colleges and OIT, there are now 30 affiliated servers with about 1650 active clients.

**What is OIT offering?** OIT is providing storage servers in the GT cloud for faculty/staff use as well as assuming responsibility for operating the cloud master server from CoE. We currently have 300TB of storage and four servers on-line for this purpose. Other units are providing storage servers for their servers and research environments.

**Who is eligible to use the OIT-provided storage?** This service is offered through unit IT support organizations and the Technology Support Center in the Clough Commons. The OIT-operated storage is initially available for Institute-owned faculty and staff desktops and laptops. A benchmark of 40GB of storage (compressed & deduplicated) per client on each of two geographically distributed servers has been used to develop the project plan; units with aggregate usage that significantly exceed this amount may be asked to reduce usage or contribute to the storage pool. In other words, don’t plan on backing multi-petabyte research databases.

**What does it cost?** The current cost to the unit is $150 per user software license (5 years, average of 4 devices allowed per user) which is the direct cost from Code42. JulieBeth Golden is coordinating the purchases with the vendor. Licenses are reassignable as hardware changes.

**What is the process for obtaining licenses?** Have your unit send a request for the number of client licenses required to JulieBeth Golden (juliebeth.golden@oit.gatech.edu) along with a PeopleSoft account number and your unit’s spend-approver. JulieBeth will either aggregate orders so that we can purchase licenses in appropriate-sized chunks or issue a separate PO in BuzzMart charged to your PeopleSoft account. On receipt, we will add the license keys to the master server and increment your unit’s client license count on the master server.

**Who does the support?** Unit IT support organizations use this service to solve the problems of inadequate backups in their units. For the future, we have the full engagement of TSC and the distributed support program who will offer assistance to “orphans” that don’t have access to a unit IT support.

**What about personal machines?** There are several commercial products that provide cloud backup of personal equipment. In addition, CrashPlan offers a program called CrashPlan+ with cloud storage and
software clients for personal use. They offer a discount for Georgia Tech students, faculty, and staff at http://crashplan.com/gtstudent. Several of us have personally purchased their Family plan that covers all the machines in our household. Because of Open Records laws and restrictions on personal use of state resources, you would not want to use the OIT-provided storage for personal backups.

**What about graduate students, research machines, and other needs?** At the present time, storage for those backups can’t be hosted on the OIT storage. (Of course, graduate students with assistantships are employees and eligible to participate if they are assigned Institute-owned equipment.) We are pleased to assist units in adding their own storage servers to the GT cloud – the unit retains physical and operational control of the servers, but their CrashPlan clients can select that server as a destination for backups.

**Can I try it out?** OIT and the College of Engineering are happy to lend out a few licenses and storage to units so they can experiment with the product. Since all of the licenses are kept on the server cluster, it is easy to move them around.

**Who do I talk to?** Dan Forsyth and Jerry Swann are the acting service managers, dan.forsyth@oit.gatech.edu, jerry.swann@oit.gatech.edu. Suggestions are welcome.

**Departmental CrashPlan Administration**

**Documentation and Support**

The CrashPlan support site is a good place to start. You’ll find summaries of the user interfaces as well as instructions for common tasks. There are a number of good support articles at Answers from Support.

**Administrator Access**

Your account should have the Org Admin or Org Manager role set to allow you to administer your organization. Pretty much all administration takes place on the master server: https://crashmaster.gatech.edu:4285

If you want to view the logs on a slave server, use the hostname of the slave server, port 4285, and log in with an account that has the "Storage Server Manager" role. Typically, you shouldn’t modify any settings there.

**Creating (Authorizing) Accounts**

Even though CrashPlan authenticates using GTED, you must add each user’s account to the CrashPlan master server to authorize its use. You do this by going to the form at Organizations>organization-name. Then choose Add a user... from the "gear" menu on the right. For our campus implementation, you need to enter the GTED username (the user’s GT account) to create the account.

Because of a little bug, the email address is sometimes not being picked up from GTED. Therefore, after creating the account, you may want to check the email address: Enter the GT account name into the Smart Search box at the upper left. Then click on the GT account name in the list that appears. You should then see the email address at the top of the panel on the right. If it’s empty, then choose Edit...
from the "Gear" menu on the right. Add the Email Address (and any administrator roles) and click the Update User button.

The default of no quota is usually adequate, but you may change it if you wish. If you wish to empower an organization administrator, add the Org Admin role in the roles tab.

The default backup destinations for devices created by the account you've created will be assigned based on the Organization>organization-name, then Gear menu>Device Defaults, then the Backup panel.

Account Ownership, Deactivation, and Deletion

When a user leaves your department or the Institute, it's entirely appropriate to Deactivate the account. This causes the account to no longer be usable for backups and it moves the archives into Cold Storage for several months. Unless you really need to reclaim the storage space or the user license, leaving it in this state for several months is the best practice so you could retrieve backup files if necessary. You can deactivate the devices and purge the archives in cold storage at any time to reclaim the user's space and licenses, but those backups are irrevocably destroyed at that point.

When you create an account in CrashPlan, it associates the login credentials with the GTED account of the same name. It also maintains an internal identifier so the CrashPlan account exists independently of account name, user name, or email address. In other words, you can change any of those attributes. CrashPlan doesn't make it practical to delete user accounts, but you can rename an account so that you can create another one with the original. This means you can rename an existing account (by using Edit...) to a nonsense account name and user name that has no devices and no storage and hence uses no licenses. Then you're free to create a user new account for that account name or not as appropriate.

Creating Child Organizations

If you want to apply different policies to different subgroups in your organization, CrashPlan lets you create child organizations which can each have their own default user settings and their own backup administrators. Go to Organization>organization-name>. Then under the "Gear" menu, choose Add a child organization.... Name the child organization with a prefix identifying your organization -- the child organization names must be unique across the master.

You may move existing accounts into different sub organizations with the Change Organization... entry in the Gear menu on the right. An account can only existing in a single organization at a time.

If you do create child organizations, do not move your account with administrator privileges into a child organization. If you do, you will become the administrator of only that child organization and be unable to move your account back to the organization level. Then the CrashPlan administrators will get a chuckle at your expense. And don't ask us how we know this happens.

Choosing Storage Destinations

You will be setting the defaults for all of your organization (or for each sub-organization that you create) by using the Organization>organization-name then "gear" menu>Device Defaults... panel. These settings are applied initially as each client device adds itself to your servers. Destinations that are listed here but
without checkmarks in the Auto Start Backup box will be available in the CrashPlan client to be chosen as a backup destination, but will not automatically be used. If you check the box and then use the Push icon to the right of it, all existing devices in the organization will be directed to start using the destination.

In version 3.6, it appears that it takes master system administration permissions to change the list of available Destinations. These are shown under the ORG INFO Destinations panel when you display the organization. If you need to change this list, please contact the service managers and we'll make the changes for you.

You can alter the specific settings of a client device by drilling down to the device in the Users, Organizations, or Devices pane. From there you can start or stop backups for that client on particular servers, just as can be done by the user in the CrashPlan client application.

In terms of policy, please remember that the OIT Rich and OIT BCDC destinations are currently provided only for the backup of employee’s work data on machines that are owned by the institute. These resources are not intended to house backups of large research and academic data sets. As backup administrator, you are responsible for helping to see that these storage resources are used appropriately. You may of course use any storage servers belonging to your organization for whatever purposes suit your organization.

Please don't use servers belonging to any other organization without their approval. If you see servers available in your organization that shouldn't be available to your clients, please notify one of the service managers and they can help you see that they are removed from your menus.

**Adding a Storage Server and Destination**

The server software is available from:


1. **Version.** We're running version 3.6.5.1 at the time of this writing, but you can confirm the master version by logging into [https://crashmaster.gatech.edu:4285](https://crashmaster.gatech.edu:4285) and looking for the version at the top of the Settings page. There is no wiggle room: your storage node and the master must be running the exact same version.

2. **Master Key.** The server is “free” to download but to federate it with the GT master server, you must generate a connection string and use the master key we already have. So tell the web page you already have a master key. And get the master key from one of the services managers because you will need it to start your server.

3. **Certificate.** You will ultimately need an InCommon certificate for the server that matches its name. The self-signed certificate that’s automatically generated is good enough to get started, but it won't support restores from the web GUI, among other things.

The initial installation of PROe Server requires the master key you said you had -- and you'll need to use the GT master key. Before you get started, ask one of the service managers to send it to you.
1. Install CrashPlan PROe Server.
2. Sign into the admin console
3. Go to **Settings > Server**
4. Enter a Primary and Secondary Network Address and save (At GT we don't use the secondary address; the primary address should be the DNS name of the storage server, should match the InCommon certificate name, and should use 4282 as its port).
5. From the Action menu, select Make Storage Server
6. Copy the connection string that is presented
7. Send the connection string to one of the service managers to add to the master server

The vendor documentation for adding storage is at:


which is from where the above is excerpted and which has more detailed information on the process of adding servers, store points, and destinations.

You will need to open the firewall in front of your server to allow TCP/4280, 4282, and 4285 from the world. This allows future clients to back up to it and also allows the master to see the storage server. You also need to obtain an InCommon certificate for the DNS name of the server to make web restores function correctly. We can help with getting and installing the certificate.

**Network Ports**

The following network ports are used by CrashPlan storage servers. CrashPlan clients need no open network ports.

- TCP 4280: HTTP access to the Console and device upgrades
- TCP 4282: Listening port on PROe Servers for device to server, mobile device to server, and server to server communication
- TCP 4283: Communication between servers within a destination (open to store points within a destination)
- TCP 4285: HTTPS access to the Console (Documentation doesn't mention that web-based restores also get redirected to the appropriate storage servers
- TCP 4286: Communication between servers within a destination

**Georgia Tech Recommendations:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Master Server</th>
<th>Storage Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>4280</td>
<td>World Campus</td>
<td>World Campus</td>
</tr>
<tr>
<td>4282</td>
<td>World World</td>
<td>World World</td>
</tr>
<tr>
<td>4283</td>
<td>Subnet (other store points)</td>
<td>Subnet (other store points)</td>
</tr>
<tr>
<td>4285</td>
<td>World World (Web-based restore gets redirected to the storage server)</td>
<td>World World (Web-based restore gets redirected to the storage server)</td>
</tr>
<tr>
<td>4286</td>
<td>Subnet (other store points)</td>
<td>Subnet (other store points)</td>
</tr>
</tbody>
</table>
Hints for Large Servers on Version 3.6

Although backups of large servers are not the focus of this product, it is possible to make it work. Some constructive suggestions:

- The single setting that has the greatest impact on the client data transfer speed is setting Data-deduplication to "minimal". Data-deduplication still occurs at a level claimed to be 90%+ without all the processing overhead.
- When dealing with the millions of files issue on Linux, I've had to allocate up to 30GB memory for the client to work properly without crashing, especially when going over 10+ million files. You have to set this manually in:

  /usr/local/crashplan/bin/run.conf

  And change this value:

  -Xmx29696m

  For 30GB, these clients are handling between 20-40 million files and yes the first backup can take 1-2 months, but after this it is generally smooth sailing.

- Crashplan has been known to miscalculate the time estimate when dealing with very small files and way overestimate the time to completion.

Troubleshooting

New Versions

We are currently supporting version 3.6.4.1. When the servers are upgraded, your client should automatically upgrade itself. Don't use a client version newer than than the servers.

Go to the Source

CrashPlan has good advice on their support site, including a category for troubleshooting:

Announcements Forum

This link also gets you started on searching their troubleshooting articles:

http://support.code42.com/Administrator/Latest/Troubleshooting

Basic troubleshooting advice:

- Start the CrashPlan client application. Does the client application wake up correctly? If the client application can't contact the local client engine, you may see the message "Unable to connect to the local backup engine." If this happens, follow the instructions on the support page to restart your backup engine. Then you may need to check your local firewall to be sure than you can connect to tcp localhost:4243 so that the application can communicate with the backup engine.
- Look at the Backup tab. Are the servers accessible? If the green dot to the left of the server name is not present, you have a network connectivity issue or the server is down. If the green dot is present, the client is able to communicate with the server.
You will likely be backing up to more than one server, since this is how we manage redundancy on the service. All of your listed servers do not need to be active for you to have good backups and the ability to restore files. If you occasionally find one of your servers unavailable for a few hours, that is a normal operational situation. If none of your servers are green and you have good network connectivity, then you may have a problem on your system.

- Check the messages next to each server. Is the client backing up? The CrashPlan client only backs up to a single destination server at a time. You will often notice "Waiting for backup" messages as the client engine round-robins through the destination servers. If the engine is backing up to one server and the others are "Waiting," then this the desired situation. This is especially noticeable when you are doing your initial backup or have changed large files on your system.

- If you see the message "Destination Unavailable" next to a server, but the dot to the left is green, this means that the problem lies on the server and not your client. If this condition persists, please contact your unit's backup administrator. CrashPlan supplies a guide for Troubleshooting a Client from the server that may be of interest to you.

Other issues:

*Backups are working but my network performance is bad*

There is an adjustment to throttle the backup engine so that it doesn't take your entire network connection. The campus networks (both wired and wireless) usually have the capacity to handle anything that the backup engine can throw at them. Home networks (DSL and cable) and public networks are generally not that fast and can be choked by a prolific backup engine. Home DSL networks often have upload speeds of 128 - 512 kbps and the engine can overwhelm them, especially if you're doing an initial backup.

To throttle your network speed, in the CrashPlan Pro client application, choose the Settings pane and then the Network tab. Change the four Limit Sending... pulldowns to 100kbps and press Save. This will greatly slow your backup progress, but make sure you are a good citizen on just about anybody's network. An initial backup at this speed can take months(!) though. Use the None or 2mbps settings when connected to a campus network until your initial backups are complete; then you are pretty safe using the 100kbps or 200kbps settings all the time because incremental backups are generally very small.

*My initial backup is taking forever!*

Even on a fast network, initial backups can take a day or two. For fastest results, plug in to a wired campus network and make sure your settings in the CrashPlan Pro client application in the Settings pane under Network have the Limit Sending... pulldowns set to None. Next best is a campus wireless network connection through the GTwifi network.

*I want to be able to restore quickly*

Backing up to "the cloud" is great for integrity and portability, but your restore time is limited (greatly) by the bandwidth of your network connection. In other words, a restore from "the cloud" is going to take at least as long as the backup did, which is not very fast. If you want fast restores, connect a USB...
drive with sufficient free space and use the Destinations pane with the Folders tab to choose a folder for CrashPlan on your USB drive to store backups. CrashPlan will update backups to this folder any time the USB drive is available. This USB drive makes an excellent source from which to restore all your files quickly.