CloudCollect
Simplifying Cloud Storage and Management

SURVEILLANCE BRIDGE

Dos and Don'ts

Important information for Support team members assisting customers using Surveillance Bridge.

What Surveillance Bridge does

- Bridge uses stub-files (pointers) to free up local space while maintaining access to the cloud
- Bridge deletes content in the cloud when local files (or stub files) are deleted
- In some cases (VMS specific), Bridge can synthesize video data (either black frames or informational messages) if cloud is not accessible.
- Bridge replicates and/or moves data to/from local disk and cloud
- Bridge is extremely resilient. If system is "rebooted or internet connectivity is lost, it resumes operations automatically
- Bridge can recover data from the cloud when the Disaster Recovery feature is enabled

What Surveillance Bridge will NOT do

- Bridge will NOT delete content in the cloud, unless local files are deleted
- Bridge will NOT interact with the VMS database

How the VMS interacts with Surveillance Bridge

- The VMS always reads and writes from/to the local drive (Bridge streams data from the cloud)
- The VMS sees a local drive that can contain an infinite amount of recordings
- The VMS sees a stub-file (just a pointer to the cloud) exactly like it sees a regular file
- The VMS will keep writing to the physical disk as long as there is free space

What to look for

- The VMS's retention period defines when recordings are deleted (local & cloud)
- Evidence locks remain in the cloud as long as the VMS does not delete them
- Archiver's storage "Max Size" setting on Management Client must take into account local drive AND cloud capacities
- **It is VERY important that the VMS NEVER runs out of local disk space as the archiver may attempt to delete stubs, thinking it is making space—but deleting stubs doesn't make local space, it only deletes content in the cloud. Some VMS look at the physical disk size instead of available free space to keep recording. We have the ability to make the local drive report a much larger size than it is—contact ADI for assistance if your VMS needs this to support the Storage Extension mode.**

What NOT to do

- Never delete files on the local drive unless you also want to delete the associated content in the cloud
- **Do NOT** use backup software on a Bridge-managed disk because backup software cannot backup stubfiles and will restore garbage instead of pointers to cloud.
- **Do NOT** uninstall Bridge or stop its services. If you need to stop them, make sure to restart them promptly as access to stub will result in file unavailable.
- Avoid moving cameras to a different archiver, as all associated recordings will need to be retrieved from the cloud. Such operation should be properly planned and executed.

It is perfectly safe to

- It is safe to stop or reboot the archiver (or any other VMS component)
- It is safe for the VMS to rebuild its database(s)
- It is safe to perform ALL normal VMS operations and run all supported plug-ins
- It is safe to temporarily lose connection to the cloud (as long as there is sufficient disk space locally to keep recording during the outage)