Technical Support Bulletin

# SFA OS$^{TM}$ Synchronization Issue with SED Authentication Keys

**ALERT!** A replacement controller added to a couplet running SFA OS 11.6.0 through 11.8.2 **may not synchronize its SED authentication key** to the primary controller. A second controller replacement could then remove the correct authentication key, resulting in SED data loss.

## Issue Summary

Self-encrypting drives (SEDs) automatically encrypt data on writes and decrypt data on reads in the drive hardware. An authentication key, which is different from the data encryption key, must be supplied to unlock the drive for data access. An administration authentication key, separate from the locking authentication key, may optionally be required to update firmware or make other administrative changes to the drive.

SFA OS generates the locking authentication key from a user-supplied password and other information. The authentication key is then stored for controller use in one of two ways. If the customer chooses to implement the Key Management Interoperability Protocol (KMIP), the authentication key is stored on the KMIP server. Otherwise, the authentication key is stored locally and mirrored on each controller.

It is possible for SED authentication keys stored locally on the two SFA controllers in a couplet to get out of sync. This occurs if all the following are true:

- SED authentication keys are stored on the local controllers and not on a KMIP server.
- SEDs were installed and the authentication key was generated under a version of SFA OS *prior* to 11.6.0.
- The storage is *currently* running SFA OS versions 11.6.0 through 11.8.2.
- A controller in the SFA couplet is replaced.

Under these conditions, the replacement controller will not mirror the primary controller's authentication key when it joins the couplet. This is due to a change in authentication key management in SFA OS 11.6.0 and higher.

The storage will continue to access SED data successfully if power to the SEDs has never been interrupted. It will also access SED data successfully if at least one of the two controllers stores the original authentication key.

But if the controller with the good key should later be replaced, access to the data on all SEDs in the array will be lost. Data will remain inaccessible even though two SFA controllers are present and operational, since neither controller will have the correct authentication key to unlock the SED drives in the array.

**ALERT!** If the authentication key for a self-encrypting drive (SED) is lost, **data on the affected drive cannot be recovered.**

### Affected Products

Declustered RAID (DCR) versions 11.6.0 through 11.8.2 of SFA OS are affected by this issue. Legacy RAID versions 3.1.5.x and earlier of SFA OS are *not* affected.

### Resolution

The synchronization issue for SED authentication keys will be resolved in SFA OS 11.8.3. Release is expected by year end 2020.

### Restoring Key Synchronization

Key synchronization can be restored by generating a new authentication key under SFA OS 11.6.0 or later. You do not need to know which controller has the good key, as the regenerated key will be propagated to both controllers. To do this:

1. On the primary controller, issue the following command at the SFA command line *three times*:

   ```
   set subsystem authorization_key password <your current password>
   ```

   **NOTE** You do not need to change your current password. Simply enter it three times.

2. *If the above command fails*, then the incorrect controller is currently primary. Determine which controller is the primary, then shutdown/restart the primary controller, wait for it to boot back up, and try the command again 3 times.
3. *Back up the generated authentication key* to external media. Two backup copies are strongly recommended.

   **ALERT!** Previous copies of the authentication key are now **obsolete** and should be discarded.

### Exporting Authentication Keys to External Media

In SFA configurations using local authentication keys, the *authentication keys MUST be backed up to external media* such as a USB stick for preservation, disaster recovery, or to replicate the same authentication keys over multiple storage systems. The procedure for doing so is described the in the *SFA OS User Guide*.

It is the *customer's responsibility* to maintain backup copies of the authentication key to ensure data access.

**ALERT!** A valid backup authentication key should always be on hand before controller replacement.

### Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or need assistance. Support can be reached by phone, by email, or on the web as listed below.

### Web

| | |
|---|---|
| *DDN Community Support Portal* | https://community.ddn.com/login |
| *Portal Assistance* | webportal.support@ddn.com |

### Telephone

| | |
|---|---|
| *DDN Support Worldwide Directory* | https://www.ddn.com/support/global-services-overview/ |

### Email

| | |
|---|---|
| *Support Email* | support@ddn.com |

### Bulletins & Notices

| | |
|---|---|
| *Support Bulletins* | http://www.ddn.com/support/technical-support-bulletins |
| *End-of-Life Notices* | http://www.ddn.com/support/end-of-life-notices |
| *Release Notes* | https://community.ddn.com/login |
| *Subscription Requests* | support-tsb@ddn.com |