BLACK BOX
NETWORK SERVICES

Product Technical Advisory for
iPath KVM Manager

Product Code(s): *ACR1000A-CTL-(24-ULT), second generation iPath controllers in 1RU form*
Product Name(s): *iPath KVM Manager*
Date Advised: *February 6th, 2017*

Technical Advisory: When the iPath controllers are configured in a Primary / Backup mode using firmware other than version 4.0.40623 (*older systems*) or 4.4 (*newer systems*), the SSD has been found to wear out faster due to excessive communication between both controllers. This reduces the lifespan of the on-board SSD memory.

Systems that are not at risk: The following controllers are not at risk of this technical advisory:

-Systems not setup in a Primary / Backup system
-Older iPath controllers (*first generation*) running firmware 3.3 or older
-Systems using Primary / Backup with newer iPath controller (*second generation*) running firmware 4.0.40623 or 4.4.40323
-See the last page for Controller Definitions if you need to verify which unit you have

Solution: Upgrade the Primary & Backup iPath managers to firmware version 4.0.40623 (*older systems*) or 4.4 (*newer systems*), which will stop the excessive communication between the devices. It will not undo any existing wear, but will normalize the iPath technology and provide alerts about the SSD drive when it is 75% worn (*early warning*) and additional warnings when the system senses the SSD is beginning to fail. These warning messages are displayed in the iPath web interface. Endpoints will also need to be upgraded accordingly. (*Endpoints have their own technical advisory, see document*).

Details: Second generation iPath controllers configured in a Primary / Backup mode use excessive communication in firmware versions other than version 4.0.40623 (*older systems*) or 4.4 (*newer systems*), which could reduce the MTBF of the on-board SSD. Stand-alone first / second generation iPath controllers do not have the excessive communication issue and are not at risk. An industrial grade SSD has been installed on iPath controllers since October 2016 which has 4X more life compared to the released version.

Next Steps / Call to Action: To be sure you have a successful upgrade, please follow these steps. There are two scenarios outlined below (*in red*), you should only need to follow one of them unless you have mixed systems.

- **Mixed endpoints running v3.3 to v3.7 firmware w/ Primary & Backup iPath**
  Product Codes: *ACR1000A, ACR1000A-R2, ACR1002A, ACR1020A, ACR1012A-T*

  Step 1 Download iPath Firmware: Download iPath firmware 4.0.40623

  Downloads Available (*be sure to read release notes*):
  iPath 4.0.40623

  Step 2 Download Endpoint Firmware: Download the endpoint firmware that is compatible to this version.

  Stability Update: Downloads Available (*be sure to read release notes*):
  ACR1000A v3.6
  ACR1000A-R2 v3.6
  ACR1002A v3.6
  ACR1012A v3.6
  ACR1020A-T v3.6

  Reliability Update: Downloads Available (*be sure to read release notes*):
  ACR1000A v3.7
  ACR1000A-R2 v3.7
  ACR1002A v3.7
  ACR1012A v3.7
  ACR1020A-T v3.7

  Step 3 Perform Backup*: Download a local copy of the iPath configuration in the iPath web interface and save it in a secure location. If for any reason the upgrade fails, we can use this to work from to get the system working again.

  Step 4 Perform Upgrade: Update all endpoints first, and then update the iPath controller.

Note* In the event an update has failed and you lose your database, you can always upload the backup configuration file that was saved in **STEP 3**. Once the file is uploaded to the iPath manager, all endpoints will appear to be "offline" because the TLS certificate is not present. You can get the units back online by performing a factory reset on each endpoint and the original settings in the configuration file will automatically be copied (Name, IP Address, etc). This is considered a last resort if a failure has occurred.

- **Newer Systems running v4.x Firmware Code**
  Product Codes: *ACR1000A-R2, ACR1002A, ACR1020A, ACR1012A-T*

  Step 1 Download iPath Firmware: Download iPath firmware 4.4.40323

  Downloads Available (*be sure to read release notes*):
  iPath 4.4.40323

  Step 2 Download Endpoint Firmware: Download the endpoint firmware that is compatible to this version.

  Stability Update: Downloads Available (*be sure to read release notes*):
  ACR1000A-R2 v4.3
  ACR1002A v4.3
  ACR1012A-T v4.3
  ACR1020A-T v4.3

  Reliability Update: Downloads Available (*be sure to read release notes*):
  ACR1000A-R2 v4.4
  ACR1002A v4.4
  ACR1012A-T v4.4
  ACR1020A-T v4.4

  Step 3 Perform Backup*: Download a local copy of the iPath configuration in the iPath web interface and save it in a secure location. If for any reason the upgrade fails, we can use this to work from to get the system working again.

  Step 4 Perform Upgrade: Update all endpoints first, and then update the iPath controller.

Note* In the event an update has failed and you lose your database, you can always upload the backup configuration file that was saved in **STEP 3**. Once the file is uploaded to the iPath manager, all endpoints will appear to be "offline" because the TLS certificate is not present. You can get the units back online by performing a factory reset on each endpoint and the the original settings in the configuration file will automatically be copied (Name, IP Address, etc). This is considered a last resort if a failure has occurred.

iPath Controller Definitions: We currently have two types of iPath controllers in the field, the First Generation is an older model which is not affected, only the Second Generation iPath (1RU) is affected.

Second Generation iPath (1RU)

-Current model, affected by this Technical Advisory
-Latest firmware version available:
*Systems using older ACR1000A-T/R units controlled by Second Generation iPath: 4.0.40623
*Systems not using older ACR1000A-T/R units controlled by Second Generation iPath: 4.4.40323

First Generation iPath

-No longer available
-Latest firmware version available: 3.3.30913