IBM Z
April 2024

IBM Fibre Channel Endpoint Security

Frequently Asked Questions

Requirement for adoption of IBM Fibre Channel Endpoint Security on FICON-attached devices

Question:
What is IBM Fibre Channel Endpoint Security?

Answer:
IBM Fibre Channel Endpoint Security (IFCES) is an end-to-end solution that is designed to provide a means to help ensure the integrity and confidentiality of all data flowing on Fibre Channel links between authorized server and storage devices, creating a trusted storage network that encrypts data in flight.

Question:
What are the products/components required to deploy IBM Fibre Channel Endpoint Security?

Answer:
The IBM Fibre Channel Endpoint Security solution is currently available on IBM z15® and IBM z16™ servers and IBM DS8900F storage controllers. The z15 and z16 systems also require purchase of the Endpoint Security feature enablement as well as inclusion of the non-priced Central Processor Assist for Cryptographic Functions (CPACF) feature. External key manager support is provided by the IBM Security® Guardium® Key Lifecycle Manager (GKLM) product. Multiple instances of GKLM are set up in a Multi-Master configuration to achieve continuous availability of synchronized data across multiple instances of IBM Security Guardium Key Lifecycle Manager. No operating system software is required for the enablement of IFCES, although some operating systems provide some level of visibility to the current security state of each link as well as notifications of link state and key change events that can be recorded to provide a security trail.

Question:
What are the options for deploying the IBM Guardium Key Life Cycle Manager product in support of IBM Fibre Channel Endpoint Security?

Answer:
IBM Guardium Key Life Cycle Manager can be deployed on any one of Linux®, Windows®, or AIX® operating systems, or within a containerized environment under Linux on x86-64, Linux on POWER®, or Linux on IBM Z® when used as part of the IBM Fibre Channel Endpoint Security solution. GKLM is also supported running in a zCX environment, but such a configuration is not currently supported when using GKLM in the IFCES solution.

Question:
We have a third-party License Server deployed. Can we use it for IFCES instead of GKLM?

Answer:
IBM Guardium Key Life Cycle Manager is the only external key manager that is supported as part of the IBM Fibre Channel Endpoint Security solution today. New intellectual property was added into IGKLM in support of establishing unique secure keys to be exchanged between server and storage pairings participating in the solution.

Question:
What non-IBM FICON® storage controllers currently support IBM Fibre Channel Endpoint Security?

Answer:
The IBM DS8900F is the only IBM FICON storage controller supporting IBM Fibre Channel Endpoint Security in the market today. Clients who currently deploy other vendor FICON products should contact those vendors to understand their current offerings and plans for future support of IFCES.

Question:
Does this Statement of Direction also apply to FCP-attached devices?

Answer:
No, this Statement of Direction only applies to FICON-attached devices. While IBM Fibre Channel Endpoint Security is supported on connections between FCP channels on z15 and z16 servers and DS8900Fdevices that support the SCSI protocol, at this time IBM is not requiring the use of IFCES with FCP-attached devices.

Question:
On the DS8900F there are settings on a per port basis for 'audit mode' and 'enforced'. How are these settings affected by this SoD?

Answer:
The port settings on the DS8900F reflect how the DS8900F will respond based on the success of negotiating a security association between the endpoints. This Statement of Direction is about the response of the FICON channels on the zNext+1 server to the FICON-attached device's participation in the IBM Fibre Channel Endpoint Security negotiation process for establishment of the necessary security association. It is indicating that FICON channels on that IBM Z server will not allow a successful connection to be maintained with the attached device if it was introduced into the market after December 31, 2024 and it does not support the security association negotiation process of IBM Fibre Channel Endpoint Security.

Question:
Will IFCES reduce my FICON channel performance? If so, by how much?

Answer:
IBM internal performance benchmarks performed on an IBM z16 server with FICON Express32S adapters demonstrated that enabling IBM Fibre Channel Endpoint Security encryption had negligible impact on CPU consumption, elapsed job execution time and I/O completion rate. See the published performance whitepaper for more detail regarding the workloads tested and the results at this link: https://www.ibm.com/support/pages/system/files/inline-files/IBM%20z16%20FEx32S%20Performance_3.pdf

Question:
If this feature is mandatory in the future, will IBM continue to charge a 'per channel' fee for its enablement on IBM Z through FC1146?

Answer:
No, as of now FC1146 is a 'no charge' feature code. The cost of deployment of IBM Fibre Channel Endpoint Security now only consists of the associated GKLM license fees.

Question:
How will we handle the enforcement of the use of the IBM Fibre Channel Endpoint Security feature in sanctioned countries or regions where it is not available? Will IBM Z no longer connect to storage controllers in those geographies?

Answer:
In such sanctioned countries/regions where support for IBM Fibre Channel Endpoint Security is not provided by IBM, the attachment to FICON devices will continue to function without the use of encryption.

Question:
Since the IBM TS7700 product is FICON-attached, but does not support IBM Fibre Channel Endpoint Security today, is it affected by this Statement of Direction? If so, what are the plans for this device to support IFCES? If it is not affected by this Statement of Direction, why not?

Answer:
Since the TS7700 is a FICON-attached device this Statement of Direction does apply to it. Any new TS7700 models introduced after December 31, 2024 will support IBM Fibre Channel Endpoint Security.

Question:
Does this SoD only apply to IBM FICON-attached devices, or are other vendor FICON-attached products also affected?

Answer:
All FICON-attached devices (disk, tape, virtual tape) are affected by this Statement of Direction, regardless of manufacturer.

Question:
If I purchase a FICON-attached storage controller after December 31, 2024, but it is a model that was first introduced into the market prior to that date, will it continue to connect to a zNext+1 system without the use of IBM Fibre Channel Endpoint Security enabled?

Answer:
Yes, storage controller models first introduced into the market prior to December 31, 2024 will not be required to support IBM Fibre Channel Endpoint Security when attached to a zNext+1 generation IBM Z or IBM® LinuxONE.

Question:
Will this requirement for use of IBM Fibre Channel Endpoint Security on the zNext+1 generation of IBM Z systems also apply to IBM® LinuxONE systems of the same generation?

Answer:
Yes, the requirement for use of IBM Fibre Channel Endpoint Security will apply to all FICON attachments on both zNext+1 and the IBM® LinuxONE family of the same generation system.

Question:
If I purchase a new storage controller model that was first introduced after December 31, 2024 and it does not support IBM Fibre Channel Endpoint Security, what will happen when I attempt to use FICON channels on a zNext+1 system to connect to and communicate with it?

Answer:
If an attempt is made to use FICON channels on a zNext+1 generation system to connect to and communicate with a storage controller model that was first introduced after December 31, 2024 and the storage controller does not indicate support for IBM Fibre Channel Endpoint Security, then the FICON channels will not maintain the connection (they will 'drop light') and further communication will be disabled.

Question:
If I purchase a model of storage controller that was introduced after December 31, 2024 which does support IBM Fibre Channel Endpoint Security, but something in the setup prevents successful communication with the GKLM server required to successfully establish a security association between the zNext+1 server and the storage controller, what will happen?

Answer:
If the storage controller model is one that was introduced after December 31, 2024 and it indicates support for IBM Fibre Channel Endpoint Security but an error is reported to the channel indicating an inability to access the key server and successfully complete the establishment of a security association, the channel will report an error to the IBM Z Support infrastructure but will allow communication with the storage controller to proceed without the use of encryption.

Question:
How widespread is the deployment of IFCES today?

Answer:
As with most new technologies introduced onto IBM Z, adoption of IFCES has grown fairly slowly, but steadily. We encourage clients who have not yet begun to adopt IFCES to begin to familiarize themselves with the components required and to plan to take the necessary steps.

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.