DATALOGIC SHIELD FAQ

October 29th, 2026

This FAQ provides essential information about Datalogic Shield, including update processes, device support timelines, and security measures. It's designed to help you understand how we maintain the security and longevity of your devices.

Contents

General Information 3

Question 1: What products are currently covered by Shield? **3**

Question 2: How do I buy Datalogic Shield? **3**

Question 3: When should Shield be purchased? **3**

Question 4: Why should a customer buy Datalogic Shield? **3**

Question 5: Are there reasons why a customer might choose not to buy Shield? **4**

Question 6: Can I upgrade the major OS version of my device without Shield? **4**

Datalogic Zero Latency 4

Question 7: What is Datalogic Zero Latency? **4**

Question 8: How does Datalogic Zero Latency work? **4**

Question 9: When is Datalogic Zero Latency available? **4**

Question 10: What are the benefits of Datalogic Zero Latency? **5**

Question 11: What are benefits of Datalogic Zero Latency for an organization? **5**

Question 12: Which devices support Datalogic Zero Latency? **5**

Datalogic Arrow FOTA 5

Question 13: What is Datalogic Arrow FOTA? **5**

Question 14: How does Datalogic Arrow FOTA work with Datalogic Shield? **5**

Question 15: Is Datalogic Arrow FOTA required to receive Shield firmware updates? **6**

Question 16: What is the recommended distribution method for Datalogic Shield firmware updates? **6**

Question 17: Is Datalogic Arrow FOTA sold separately? **6**

Question 18: How do I use Datalogic Arrow FOTA with Shield? **6**

Question 19: Does Datalogic Arrow FOTA automatically install security updates? **7**

Question 20: Can I control when firmware updates are deployed? **7**

Question 21: Can Arrow FOTA update devices remotely? **7**

Question 22: Can Arrow FOTA be used with an MDM/EMM? **7**

Question 23: What happens if a device is offline when an update is released? **7**

Question 24: Does Arrow FOTA download the entire firmware image for every update? **7**

DATALOGIC SHIELD FAQ

Question 25: Are Shield firmware updates released through Arrow FOTA at the same time as the Android Security Bulletin? 7

Support Statuses 8

Question 26: What are the different support statuses under Datalogic Shield? 8

Question 27: Where is possible to check the current support status of my Device? 8

Question 28: How does Datalogic decide on the frequency of updates for devices under "Active – Variable Frequency" or "Transition – Variable Frequency"? 8

Question 29: What happens during the "Transition" period for an OS version? 8

Question 30: What does "Expired" support status mean? 9

Backporting 9

Question 31: What is backporting, and how does it work? 9

Question 32: How does Datalogic decide whether to backport a security patch? 9

Question 33: Are all security patches eligible for backporting? 9

CVEs and Security Patch Verification 9

Question 34: What is a CVE, and how does it work? 9

Question 35: How does Google handle CVEs, and how are they fixed? 9

Question 36: How does Datalogic verify security patches before deployment? 10

Incremental OTA Updates 10

Question 37: What are Incremental OTA Updates, and how do they work? 10

Question 38: What are the benefits of Incremental OTA Updates for customers? 10

Question 39: How are Incremental OTA Updates verified before deployment? 10

Question 40: Can customers choose between Incremental OTA Updates and full firmware updates? 10

Longevity 10

Question 41: How long will Datalogic devices be supported for? 10

Question 42: How many Android major versions are planned for Datalogic devices? 11

Question 43: How are Android major versions planned for Datalogic devices? 11

Question 44: What does it mean if I am notified that certain Shield PNs are no longer available? 11

Question 45: Does the discontinuation of a 5-Year Shield PN mean that 5 years of support is no longer possible? 11

Question 46: Why are certain Shield PNs being discontinued? 11

Question 47: Does this discontinuation affect the software support quality for my product? 12

Question 48: What options are available if I need extended support for a product with discontinued Shield PNs? 12

DATALOGIC SHIELD FAQ

Question 49: Can I combine shorter Shield PNs to create a longer coverage period?.....12

Question 50: Are there alternative support options if Shield coverage is unavailable?.....12

General Information

Question 1: What products are currently covered by Shield?

Shield is available on the following Datalogic Products:

- Joya Smart/+ Family
- Falcon X60/65 Family
- Skorpio X40/45 Family
- Memor 12/17 Family
- Memor 30/35 Family
- Smart Portal
- Memor 11 Family
- Skorpio X5
- Joya Touch 22

Question 2: How do I buy Datalogic Shield?

Datalogic Shield is included as part of our mobile device maintenance plans (Ease of Care) or by purchasing a separate software-only Datalogic Shield contract.

Question 3: When should Shield be purchased?

Shield should be purchased together with the mobile computer hardware from the beginning. Datalogic may consider a late purchase of Shield depending on the specific case. However, customers should not wait to buy Shield only when they need a Shield update, as there may be an added cost.

Question 4: Why should a customer buy Datalogic Shield?

The following three points summarize the main reasons why a customer should buy shield.

Proactive Cybersecurity: In today's digital landscape, cybersecurity threats are constantly evolving. Datalogic Shield ensures your devices are always protected with the updated security patches, addressing vulnerabilities identified by Google.

Continuous Innovation: Shield is more than just security; it's about keeping your devices at the forefront of technology. Firmware updates include performance enhancements, new features, and upgrades to Datalogic Mobility Suite tools, ensuring your devices are always operating at peak efficiency.

Futureproofing with Major Upgrades: Shield includes major Android upgrades that bring significant new features and improvements. This keeps your devices compatible with the latest applications and services, ensuring they remain valuable assets to your operations.

DATALOGIC SHIELD FAQ

Question 5: Are there reasons why a customer might choose not to buy Shield?
If a customer's use case involves devices that do not require regular updates, major Android version upgrades, or the latest features, they may choose not to purchase Shield. However, this comes with the risk of leaving devices vulnerable to cybersecurity threats and missing out on the continuous improvements that enhance device performance and longevity.

Question 6: Can I upgrade the major OS version of my device without Shield?
Android major upgrades are part of the Shield offering. If a customer doesn't have Shield, they are not entitled to dessert upgrades (e.g. Android 13 to 15).

Datalogic Zero Latency

Question 7: What is Datalogic Zero Latency?
Datalogic Zero Latency represents the pinnacle of security support in the Android market.
It's an enhanced level of service of the Shield program that guarantees the immediate integration of Google's monthly security patches with zero delay in terms of months. This means that as soon as Google releases a security patch, Datalogic ensures it is integrated into your devices before that Google provides the security update for the next month. Most of the time this means Datalogic can provide last security patches within 1 Month from the Google Date of publication.

This potentially guarantees Monthly FW Updates available, up to 12 per year on a specific Android OS version.

Question 8: How does Datalogic Zero Latency work?
Upon the release of a new security patch in the Android Security Bulletin by Google, Datalogic immediately integrates this patch into the firmware of supported devices. This seamless process ensures that security updates reach your devices as quickly as possible, minimizing any potential exposure to cybersecurity threats. With Datalogic Zero Latency, you receive the latest security patches with zero months of delay from the date of publication from Google.

Question 9: When is Datalogic Zero Latency available?
Datalogic Zero Latency is available on the latest OS update provided by Datalogic for your device during the period while the operating system is still supported by Google and by the chipset vendors consistently with the version of all specific SW Components running on the device.

Once Google and chipset vendors end support for that OS version or for the specific SW Components used in the Datalogic devices, the availability of high-frequency updates such as those provided by Zero Latency ceases.

However, software updates will continue at a quarterly cadence, with new features and enhancements along with relevant security patches backported when they provide clear benefits without compromising device stability, and compatible with software architecture of the target operative system version.

DATALOGIC SHIELD FAQ

Question 10: What are the benefits of Datalogic Zero Latency?

Instant Security Protection Zero Latency ensures your devices receive the latest security patches immediately, eliminating delays and reducing the risk of exposure to vulnerabilities. This immediate protection keeps your devices secure against emerging threats.

Minimized Disruption: By applying security updates as soon as they are available, Zero Latency reduces the potential for security-related downtime. This helps maintain continuous operations, allowing your business to run smoothly without unexpected interruptions.

Peace of Mind: With Zero Latency, you can trust that your devices are always up to date with the latest security measures. This provides confidence that your systems are protected, allowing you to focus on your core business activities without worrying about security gaps.

Question 11: What are benefits of Datalogic Zero Latency for an organization?

Datalogic Zero Latency enables organizations to respond quickly to critical vulnerabilities, with security patches delivered within the same month a vulnerability is identified. This rapid response helps minimize the window of exposure and reduces the risk of exploitation, data breaches, financial loss, and reputational damage.

Question 12: Which devices support Datalogic Zero Latency?

Datalogic Zero Latency is available on the Datalogic device:

- Joya Smart/+ Family
- Falcon X60/65 Family
- Skorpio X40/45 Family
- Memor 12/17 Family
- Memor 30/35 Family

Datalogic Zero Latency is automatically included in all current and new Shield contracts, ensuring that your devices are always at the forefront of security.

Datalogic Arrow FOTA

Question 13: What is Datalogic Arrow FOTA?

Our firmware-over-the-air service for securely and automatically distributing Shield firmware updates to supported Datalogic devices. Sold as an add-on, must be bought separately from a Shield or EoC service contract.

Question 14: How does Datalogic Arrow FOTA work with Datalogic Shield?

Shield provides the firmware update commitment, while Arrow FOTA provides an automated mechanism for distributing those firmware updates to devices.

DATALOGIC SHIELD FAQ

Question 15: Is Datalogic Arrow FOTA required to receive Shield firmware updates?

No. Shield firmware updates can be distributed through downloading firmware from the Shield Portal and distributing through 3rd party management software. Arrow FOTA is Datalogic's recommended automated distribution method for customers who want to remotely manage firmware deployment.

Question 16: What is the recommended distribution method for Datalogic Shield firmware updates?

For customers managing devices remotely, Datalogic recommends Arrow FOTA for automated, scalable firmware distribution. Other supported deployment methods may also be used depending on the customer's environment.

Question 17: Is Datalogic Arrow FOTA sold separately?

Yes, Arrow FOTA is licensed separately from Shield, allowing customers to use its firmware deployment capabilities independently of Shield. Arrow FOTA is offered either through a direct or indirect distribution model:

Direct: each device connects to the cloud service and maintains its own license.
Indirect: each device connects to a local proxy server that pulls firmware from the cloud service.

Because of the difference in licensing between direct/indirect, with licenses based on the number of proxies rather than devices, this model can deliver significant cost savings at scale, as a single licensed proxy can serve a large fleet without requiring a separate FOTA license for every device.

Question 18: How do I use Datalogic Arrow FOTA with Shield?

To use Datalogic Arrow FOTA with Shield, update your existing MDM OEMConfig profile to configure the required licenses and firmware update settings.

1. **Enable Shield:** Ensure devices have a valid Datalogic Shield license.
2. **Choose your distribution model:** For direct cloud connectivity, configure the optional Arrow FOTA direct-to-cloud license. For proxy-based distribution, deploy a licensed Arrow FOTA Proxy server on your network and configure devices to connect through it.
3. **Configure update policies:** Use OEMConfig to define your update strategy, including scheduling, automation, update types, and delivery options.
4. **Deploy your profile:** Apply the updated OEMConfig profile through your MDM to configure Arrow FOTA across your device fleet.

Once configured, Arrow FOTA can distribute firmware updates according to your policies, helping keep devices secure and up to date with less manual effort. Technical documentation for both device and proxy settings can be found here: https://datalogic.github.io/fota/overview

DATALOGIC SHIELD FAQ

Question 19: Does Datalogic Arrow FOTA automatically install security updates?

Yes, to get automatic updates set **firmware selection** to **latest**. If only security patches are desired, disable both **Allow OS Updates** and **Allow maintenance release updates.**

Question 20: Can I control when firmware updates are deployed?

Yes, add **Polling windows** to control when updates occur. Either create weekly schedules or set specific dates to create an update period. Additionally, an **update delay** can be set so devices are updated with a new release a set period of days after each release.

Question 21: Can Arrow FOTA update devices remotely?

Yes, both direct and indirect distribution methods distribute the firmware remotely. If **Zero Touch Updates** is enabled there is no need for any user interaction with the device to trigger an update.

Question 22: Can Arrow FOTA be used with an MDM/EMM?

Yes, settings are exposed through OEMConfig. Simply update your existing configuration profiles to configure the Datalogic Arrow FOTA service.

Question 23: What happens if a device is offline when an update is released?

The device can receive the update when it reconnects and is able to communicate with the Datalogic Arrow FOTA service, subject to the configured deployment policy.

Question 24: Does Arrow FOTA download the entire firmware image for every update?

Datalogic Arrow FOTA supports optimized firmware delivery to reduce the amount of data transferred during updates. Incremental OTA packages can be significantly smaller than a complete firmware image when supported, generally 2-4% of a full firmware image.

If **Update policy** is set to **Prefer incremental updates**, with **firmware selection** to **latest**, then an incremental will be used if available to get to the latest. If **Update policy** is set to **Incremental-only updates**, then the next incremental update will be used to advance the firmware version. This will continue, laddering updates, until the latest valid version is reached.

Question 25: Are Shield firmware updates released through Arrow FOTA at the same time as the Android Security Bulletin?

Yes, Shield releases are made available to Arrow FOTA same day.

DATALOGIC SHIELD FAQ

Support Statuses

Question 26: What are the different support statuses under Datalogic Shield?

The description of the different support statuses can be found here, and are the following:

Active: SW updates are made available periodically including Google security patch updates and bug fixing.

Active – variable frequency: SW updates are made available, but the frequency of the updates is not guaranteed anymore due to lack of support from Datalogic partners for such OS versions. Datalogic will solely assess each security vulnerability reported in the ASB (Android Security Bulletin) and determine if it is possible to backport.

Transition: A more recent OS version has been released, SW updates for the previously existing version are made available, but it is recommended to update to the latest OS version to continue to get updates in future.

Transition – variable frequency: SW updates are made available, a more recent OS version has been released, and it is recommended to update to the latest OS
version to continue to get updates. In addition, the frequency of the updates is not guaranteed anymore due to lack of support from Datalogic partners for such OS versions. Datalogic will solely assess each security vulnerability reported in the ASB (Android Security Bulletin) and determine if it is possible to backport.

Expired: SW updates have been released and are still available for download, however no further releases will be made available.

Question 27: Where is possible to check the current support status of my Device?

On the download page of your device you can find a table on top reporting for each operative system released what is the current support status.

Question 28: How does Datalogic decide on the frequency of updates for devices under "Active – Variable Frequency" or "Transition – Variable Frequency"?

Datalogic prioritizes your security by maintaining updates as long as possible. When support from partners diminishes such as Google or the chipset platform vendor, we adjust the frequency but continue to assess and address critical vulnerabilities on a case-by-case basis.

Question 29: What happens during the "Transition" period for an OS version?

During the "Transition" period, Datalogic continues to provide updates for the previous OS version while recommending an upgrade to the newer version. This ensures your devices remain secure and compatible with the latest software, offering you a clear path forward in your technological journey. The duration of the Transition period is 18 months.

DATALOGIC SHIELD FAQ

Question 30: What does "Expired" support status mean?

“Expired" status means no new updates will be provided, but existing updates remain available for download. This status signifies the end of active support, and customers should consider upgrading to maintain security and performance.

Backporting

Question 31: What is backporting, and how does it work?

Backporting is a process where Datalogic adapts security patches or updates originally developed for newer versions of the Android OS to work with older versions not supported anymore by Google or the chipset vendor. This ensures that even older devices continue to receive relevant security updates, reflecting Datalogic’s commitment to extending the life and security of your investments.

Question 32: How does Datalogic decide whether to backport a security patch?

Datalogic assesses each vulnerability reported in the Android Security Bulletin. If a vulnerability is critical and backporting is feasible, Datalogic ensures that the patch is adapted for older OS versions, maintaining a high standard of security and quality across all supported devices.

Question 33: Are all security patches eligible for backporting?

Not all patches can be backported due to technical limitations or the potential risks they may introduce to system stability.

CVEs and Security Patch Verification

Question 34: What is a CVE, and how does it work?

A CVE (Common Vulnerabilities and Exposures) is a standardized identifier assigned to known security vulnerabilities. Once a CVE is identified, it’s published in the Android Security Bulletin (ASB), detailing the vulnerability, its severity, and the necessary patch to resolve it. Datalogic uses the ASB in two stages: first, as a guide to apply the latest security patches on supported and active operating systems, and second, to assess which CVEs can be backported when official support ends.

Question 35: How does Google handle CVEs, and how are they fixed?

Google identifies vulnerabilities and assigns them CVEs, which are then detailed in the Android Security Bulletin. Google develops patches to address these vulnerabilities and provides them to manufacturers like Datalogic. With Datalogic Zero Latency, these patches are immediately integrated into your devices, ensuring that your organization is always protected with the latest security measures.

DATALOGIC SHIELD FAQ

Question 36: How does Datalogic verify security patches before deployment?

Every firmware update made available to customers undergoes rigorous testing to ensure compatibility, performance, and security integrity. This comprehensive verification process includes leveraging third-party laboratories approved by Google to validate the security and functionality of the updates.

Incremental OTA Updates

Question 37: What are Incremental OTA Updates, and how do they work?

Incremental Over-the-Air (OTA) updates are designed to deliver targeted fixes and improvements more efficiently. Instead of requiring a full system update, incremental OTA updates only include the most recent changes since the last update, resulting in faster downloads and installations. This method ensures a faster deployment and distribution of the FW Updates.

Question 38: What are the benefits of Incremental OTA Updates for customers?

Incremental OTA updates are smaller, allowing for quicker download and installation, minimizing downtime and keeping your operations running smoothly. These updates are much smaller, sometimes as little as 5% the size of a full OTA file, making them ideal for environments where network bandwidth is limited.

Question 39: How are Incremental OTA Updates verified before deployment?

Just like full firmware updates, Incremental OTA updates undergo a thorough testing process at Datalogic. We ensure each update is compatible, effective, and secure, maintaining the highest standards of performance and reliability. Our rigorous verification process guarantees that these updates enhance your devices without compromising their stability.

Question 40: Can customers choose between Incremental OTA Updates and full firmware updates?

Yes, customers can choose between Incremental OTA updates and full firmware updates. Incremental OTA updates are available for customers who have kept their devices up to date with each OS release. However, full OTA updates are required when performing a major OS upgrade (e.g., from Android 11 to Android 13) or when updating between non-consecutive firmware versions.

Longevity

Question 41: How long will Datalogic devices be supported for?

Datalogic devices are supported throughout the entire lifecycle of the product, and for at least two years after the product reaches its End of Life (EoL). Depending on the platform's longevity, the support period can be even longer. During this time, Datalogic continues to provide OS updates, security patches, and performance enhancements.

DATALOGIC SHIELD FAQ

Question 42: How many Android major versions are planned for Datalogic devices?

Typically, Datalogic plans to support two major Android versions for each device. However, this can vary depending on the specific platform, and in some cases, it could be extended to three or more major versions. The exact number of supported versions depends on the hardware capabilities and the longevity of the platform.

For our current fleet of devices based on the Qualcomm Dragonwing™ QCM4490 chipset, we guarantee support up to at least Android 19, and depending on future confirmation from Qualcomm, potential support up to Android 21. These include the following devices:

- Joya Smart/+ Family
- Falcon X60/65 Family
- Skorpio X40/45 Family
- Memor 12/17 Family
- Memor 30/35 Family
- Smart Portal

Question 43: How are Android major versions planned for Datalogic devices?

Datalogic plans Android major version updates with the goal of providing continuous and extended security support. We align these updates with Google's security support timeline to ensure that your devices remain secure and up to date for as long as possible. By carefully planning these updates, we aim to maximize the longevity and security of your devices.

Question 44: What does it mean if I am notified that certain Shield PNs are no longer available?

This means that for the specified products, some Shield PNs are being discontinued. However, this does not necessarily imply that longer-term support is completely unavailable. If the bulletin indicates that shorter-term Shield PNs remain available, it means extended support will require periodic feasibility assessments and may be granted on a year-by-year basis.

Question 45: Does the discontinuation of a 5-Year Shield PN mean that 5 years of support is no longer possible?

Not necessarily. While a 5-Year Shield PN might not currently be available, support could still be extended incrementally. For instance, a customer may purchase 3 years of Shield coverage initially, and if subsequent assessments confirm feasibility, additional 1-year increments can be purchased to achieve a total of 5 years or more.

Question 46: Why are certain Shield PNs being discontinued?

Discontinuation occurs when extended support cannot be guaranteed due to uncertainties in the software architecture roadmap or platform supplier support. These factors impact our ability to commit to longer-term coverage at the time of the communication.

DATALOGIC SHIELD FAQ

Question 47: Does this discontinuation affect the software support quality for my product?

No, the quality of software support remains unchanged for active Shield PNs. The discontinuation solely affects the availability of pre-defined, longer-term support options, which now require periodic feasibility evaluations.

Question 48: What options are available if I need extended support for a product with discontinued Shield PNs?

Customers can still purchase shorter-term Shield PNs (e.g., 1-year or 3-year options). Feasibility assessments conducted closer to the end of the purchased period may allow for additional incremental coverage based on the availability of platform support.

Question 49: Can I combine shorter Shield PNs to create a longer coverage period?

You cannot purchase all shorter Shield PNs together to combine them into a longer period. However, after the expiration of an active Shield PN, and if feasibility assessments confirm continued support, customers can extend coverage by purchasing additional increments (e.g., adding another year after a 3-Year Shield expires). This process allows for potentially extended support, subject to feasibility confirmation.

Question 50: Are there alternative support options if Shield coverage is unavailable?

In cases where Shield coverage cannot be extended, Datalogic may explore other support mechanisms to ensure customers receive the necessary level of service. Contact our support team for more details.