

logitech®

LOGI BOLT



Logitech's new standard for high performance wireless connectivity for people who create and produce in a world of congested wireless environments, evolving compatibility requirements and increasing security expectations.

LOGI BOLT

An inside view of developing Logitech's new standard for high performance wireless connectivity

Introduction

The proliferation of computer peripherals in the workplace, driven by the influx of millennials and Gen Z, has proven to be a boon for worker productivity, comfort and overall satisfaction. But the exponential growth of these devices, notably wireless mice and keyboards, has presented its own set of unintended consequences: security concerns, performance in noisy or congested wireless environments and compatibility issues culminating in costly, time-consuming calls to the company IT guru.

In response, **Logitech**, one of the world's leading manufacturers of computer peripherals, developed **Logi Bolt**, a next-generation wireless connectivity protocol engineered to not only address cybersecurity concerns and increasingly congested wireless environments but to also empower and grow alongside the future of work itself in the coming decade.

In addition to improved security, wireless reliability and connection strength, Logitech engineers were tasked with ensuring the technology works across multiple operating systems while enhancing the end user experience—a formula designed to lessen reliance on IT support. Based on *Bluetooth*® Low Energy wireless technology, Logi Bolt includes multiple security measures designed to minimize vulnerability risks in both office and work-from-home environments, ideally giving IT managers one less worry. Logi Bolt-enabled devices are featured prominently in Logitech's product line-up beginning this year.



Logitech MX Keys for Business and Logitech MX Master 3 for Business

Read ahead as this eBook breaks down the nuts and bolts of Logi Bolt and the thinking that drove its development.

Contents

- 1 Introduction
- 2 Leveraging a community
- 3 Fortified security
- 5 Robust connections
- 6 Near-universal OS compatibility
- 6 Pair up to 6 Logi Bolt devices
- 7 Flexible connectivity options
- 8 The Logitech way

Leveraging a community

Developing a new wireless protocol is no small undertaking. Beyond merely updating existing technology to meet the needs of the ever-evolving wireless office infrastructure, Logitech engineering and user experiences teams had to peer into the future and ask themselves “how can we ensure this technology will remain secure, robust and relevant five-to-ten years down the road?” This led to the adoption of *Bluetooth*®—or more precisely *Bluetooth* Low Energy—as a foundational technology upon which to build out the protocol architecture. It was a surprisingly easy choice. *Bluetooth* features multiple levels of built-in security, is reliable in noisy environments and is poised to remain relevant in a “dongleless” future—one where host computers may or may not include USB ports.



Logitech ERGO K860 Ergonomic Split Keyboard for Business and M575 Trackball Mouse for Business

While no technology is future proof, “future positioning” Logi Bolt became something of a guiding principle during its development. Product management leader, Barbara Vasconcelos, describes how the decision to leverage *Bluetooth* aligns with that objective. “There’s a whole community dedicated to the constant improvement and evolution of *Bluetooth* and Logitech is a part of that. We can’t predict what challenges the wireless environment of the future will present but we do know we’ll continue to leverage the collective efforts of the *Bluetooth* community and therefore be able to quickly evolve Logi Bolt in response so that it remains relevant, robust and secure.”



The Bluetooth SIG, Inc., of which Logitech is a member, is a global community of over 36,000 companies that are the caretakers and innovators of *Bluetooth* technology. The Bluetooth SIG, Inc. promotes the expansion of *Bluetooth* technology by fostering member collaboration to create new and improved specifications and facilitate global *Bluetooth* interoperability through a product qualification program.

www.bluetooth.com

Fortified security

Logi Bolt was designed to address growing security concerns resulting from an increasingly mobile workforce—work from home being an obvious example. It's engineered with *Bluetooth* security mode 1, level 4 (also known as Secure Connection Only mode), which is Federal Information Processing Standards (FIPS) compliant. That means Logi Bolt enforces security by means of encryption. Level 4 uses Authenticated LE Secure Connections (LESC) encrypted pairing—specifically, Elliptic Curve Diffie-Hellman P-256 (ECDH) and AES-CCM encryption. This ensures a Logi Bolt wireless product and its Logi Bolt receiver can only communicate with each other.

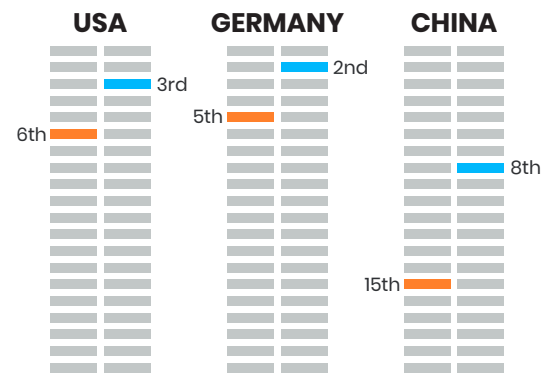


Federal Information Processing Standards (FIPS) is a set of data security and computer system standards created by the National Institute of Standards and Technology's (NIST's) Computer Security Division and applies to computer systems for non-military government agencies and government contractors. Organizations must adhere to these standards in order to be designated as FIPS compliant. Many private organizations have voluntarily adopted FIPS standards as a security benchmark.

Logi Bolt wireless products are securely paired to their USB receivers in the factory. Out of the box, the user simply plugs the Logi Bolt USB receiver into a USB-A port, powers on the Logi Bolt wireless mouse or keyboard and they're ready to work.

There are, however, two scenarios where a user would need to pair a Logi Bolt wireless product to a Logi Bolt receiver: when pairing more than one Logi Bolt mouse or keyboard to a single Logi Bolt receiver or when replacing a lost Logi Bolt USB receiver. The process for both cases is simple, only requiring a pairing app which can be downloaded for free at logitech.com/options.

Wireless security concerns ranked increasingly higher by ITDMs among evaluation criteria of computer peripherals.



Logitech proprietary research conducted among IT decision makers in companies with 1,000+ employees in the USA, Germany and China in July 2020 (n=804).

Legend:
Orange bar: Pre-Covid
Blue bar: Post-Covid

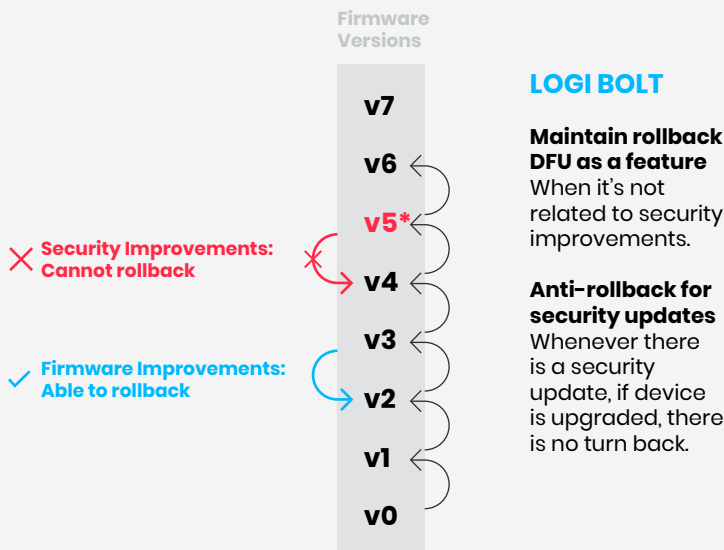
Logi Bolt products enforce LE Secure Connection (LESC). Pairing involves authenticating the identity of the two devices, encrypting the link, and computing encryption keys to allow security to be restarted on a reconnection. To authenticate a connection at pairing, Logi Bolt utilizes LEESC paskey which requires a series of clicks—a security measure common to keyboards but one that will also extend to Logi Bolt mice and across most enterprise operating systems—an industry first according to Logitech. The paskey method is considered superior to LE Legacy connections given its enhanced resilience to on-path attackers.

To help overworked IT managers maintain enterprise level security over an increasingly far-flung employee base, Logitech equipped Logi Bolt with self-service security measures that still allow for centralized oversight. When a pairing is attempted, the user receives a “new device alert.” Non-security related firmware updates can be rolled back by either the user or an IT manager should the need arise. Security updates, however, are permanent and can’t be rolled back providing a valuable check for IT.



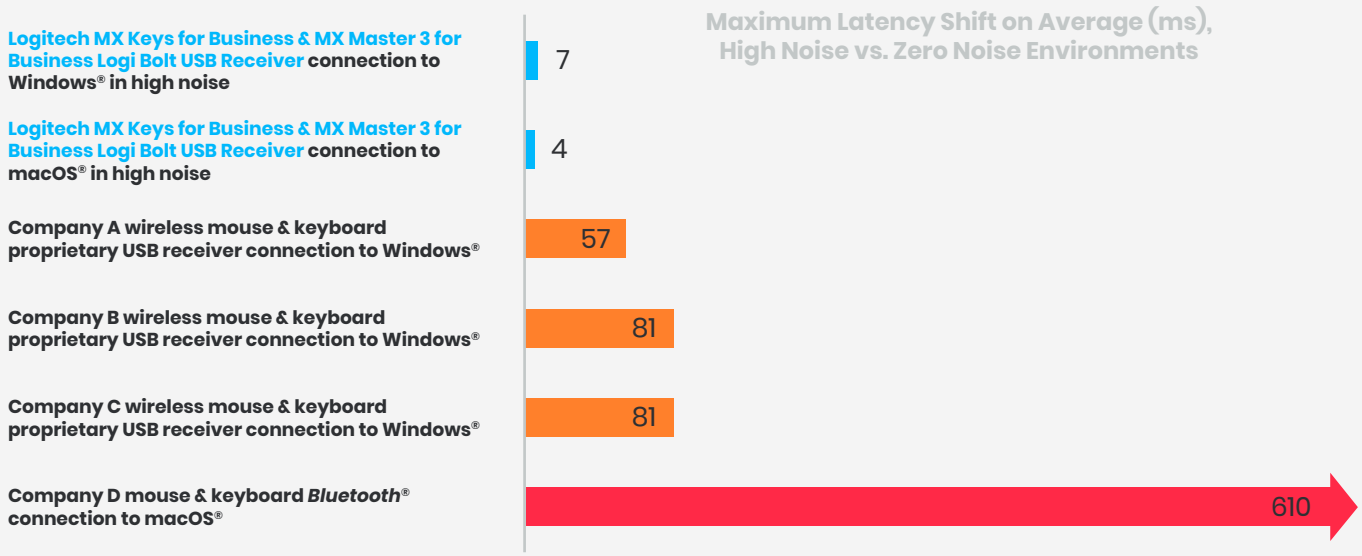
Logitech M575 Trackball Mouse for Business

Anti-rollback DFU



Logitech MX Master 3 for Business

Logi Bolt connection using a paired Logi Bolt USB receiver significantly outperforms other protocols in highly congested (noisy) environments



Robust connections

The future will certainly include more 2.4 GHz band (802.11) interference as that frequency is used by many types of devices including laptops, tablets, smartphones and remote sensors as well as wireless LANs, home WLANs—even baby monitors. Millennials and Gen Z-ers are pouring into the workforce and will comprise a majority by 2025. These younger workers are accustomed to the conveniences, comfort and enhanced productivity associated with wireless mice, keyboards and other computer peripherals. More important, they expect to find them in the workplace and forward-thinking employers are only too happy to provide them. But more wireless devices combined with denser Wi-Fi networks means more congestion and “noise” as various devices compete for space in the 2.4 GHz spectrum. More noise means more interference or on a practical level, potential device lag and signal drop. After that? Costly calls to IT.

Logitech’s solution to overcoming noise was to turbocharge Logi Bolt with a high RF link

budget—the power of the signal broadcast by the USB receiver. Connectivity innovation leader, Jean-Christophe Hemes, likens it to making yourself heard at a loud party. “If you’re trying to talk to someone in a noisy, crowded room you can either move closer to them or you can simply shout. Logi Bolt takes the latter approach, broadcasting a more robust, ‘louder’ signal that powers through ambient noise.”

Beyond its powerful transmission, Logi Bolt deftly employs a proprietary algorithm that makes frequency hopping more efficient. Laurent Gillet, Logitech Director of Engineering for Embedded Software compares it to an all-terrain vehicle. “Protocols built simply for speed were good ten years ago but not so much today given the huge increase in wireless noise. Picture a Ferrari stuck in a traffic jam. Logi Bolt on the other hand is more like an SUV. The hardware and algorithm we developed enable it go off road, if necessary, in order to maintain a robust link while still maintaining a high level of security.”

Near-universal OS compatibility

Logitech engineered Logi Bolt to be compatible with most enterprise operating systems (OS) when connected using the Logi Bolt USB receiver including Windows®, macOS®, Chrome OS™ and, Linux®.

Further, Logi Bolt-enabled products will also include the option to connect to host computers directly via *Bluetooth* which expands OS compatibility to include iPadOS®, iOS® and Android™*. This is especially important in the era of the mobile workforce. Enabled by the cloud and spurred on by the work-from-home trend, a typical employee now utilizes multiple computing devices during the course of the day—from a desktop computer in the office to a laptop at home or in a coffee shop to a tablet or smartphone from pretty much anywhere else. Cross-platform compatibility built into Logi Bolt saves IT the headache of having to decipher which employee needs which peripherals for which host computers while benefiting from the economies and simplicity of being able to make Logitech a global standard.

Pair up to 6 Logi Bolt devices

Logi Bolt wireless devices include a pre-paired USB receiver giving the user plug and play functionality right out of the box. An additional five devices can be paired with the same receiver for a total of six, a feature Logitech says is ideal for workers who split time working between the office and home. IT can issue an employee a set of peripherals for work and another for home with only the set-it-and-forget-it receiver being transported back and forth in the laptop.

Better still, a misplaced receiver can be replaced without having to repurchase the Logi Bolt wireless device it came with. Less expense via extended product utility. The user only needs to pair the new receiver using a secure, 6-digit authentication process.



* iOS and Android support available for Logi Bolt keyboards only

Flexible connectivity options

OS compatibility was only part of fulfilling Logitech's goal that users find Logi Bolt "simply works with what I have." Going a step further, Logitech engineers outfitted Logi Bolt devices with dual connectivity methods—via the pre-paired USB receiver or by direct *Bluetooth* connection—the second method being ideal for when the host computer doesn't have available USB ports. Logi Bolt product manager, Barbara Vasconcelos, sees a future where IT must account for "dongleless" connectivity. "You're starting to see tablets, phones and other devices without USB ports used for productivity and creativity. Mobile workers on a train, for example, will connect a keyboard to their phone, grab files from Google Docs and start working—and with IT-approved security."

Logitech says the fact that Logi Bolt devices are pre-paired with the receiver at the factory and also the self-service method of securely pairing additional devices has the potential to lower costs for IT departments. Boris Siebert, head of Business-to-Business and Go-to-Market at Logitech explains. "Because Logi Bolt products are ready for use out of the box, IT is spared the time and expense of fielding helpdesk requests put in by employees—some working remotely—who are using a newly issued mouse or keyboard for the first time. And because pairing additional Logi Bolt devices to that same receiver requires authentication—mice included—IT can be comfortable with an employee doing it themselves and without worrying about security breaches."

Logi Bolt is based on *Bluetooth*, but it may ... counterintuitively ... be especially appealing to the estimated 20% of companies that ban direct *Bluetooth* connections on company computers due to heightened security requirements. Siebert continues. "In companies with heightened security requirements, IT will sometimes disable *Bluetooth* on all computers which essentially forces users to connect via the Logi Bolt USB receiver—the method offering the higher level of security. Yes, there's still a *Bluetooth* signal involved, but through an end-to-end closed system where a Logi Bolt receiver is emitting an encrypted signal that only connects with Logi Bolt products. So the receiver can't be paired with any non-Logi Bolt device. And because Logi Bolt works with most enterprise operating systems and is securely paired right of the box, it makes procurement and set up that much easier. Assign a Logi Bolt mouse or keyboard to an employee and then pretty much forget it."



Logitech MX Keys for Business and MX Anywhere 3 for Business.

The Logitech way

Talk with any Logitech employee about Logi Bolt and you'll immediately detect an undercurrent of pride. That's because they hold up Logi Bolt as a vivid example of the type of innovation upon which Logitech was built and ultimately what the company is all about. General Manager & VP Business Group, Delphine Donne-Crock, ties it to Logitech's brand promise. "Our brand stands for plug and play, peace of mind, compatibility, durability, quality and support. Logi Bolt exemplifies all of those things."



Learn more about Logi Bolt and Logi Bolt wireless products by visiting connection.com/logibolt

Logi Bolt Wireless Protocol Technical Specifications

Logi Bolt wireless devices:

- USB 2.0 Type-A
- *Bluetooth* Low Energy 5.0 or higher.
- Backwards compatible to *Bluetooth* 4.0 or higher hosts when in direct *Bluetooth* connection.
- *Bluetooth* power class is class 2 with transmission operating ranges of approximately 30 feet (10 meters) within a line of sight. This range will vary depending upon computing and environmental conditions.

		Logi Bolt Mouse	Logi Bolt Keyboard
Bluetooth Security Mode	Paired with Logi Bolt USB receiver	Security Mode 1 – Security Level 4	Security Mode 1 – Security Level 4
	Direct connect to host computer via <i>Bluetooth</i>	Security Mode 1 – Security Level 2 (if the host computer can)	Security Mode 1 – Security Level 3 (if the host computer can)
Authentication	Paired with Logi Bolt USB receiver	10-click passkey (which means an entropy of 2 ¹⁰)	6-digit passkey (which means an entropy of 2 ²⁰)
	Direct connect to host computer via <i>Bluetooth</i>	Just Works Pairing is used per industry standard as there is no Passkey pairing standard for mice	Passkey is requested per industry standard

© 2021 Logitech. Logitech, Logi, Logi Bolt and the Logitech logo are trademarks or registered trademarks of Logitech Europe S.A. and/or its affiliates in the U.S. and other countries.

Logitech
7600 Gateway Blvd.
Newark, CA 94560-9998
USA

NASDAQ: LOGI

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Logitech is under license.

macOS, iPadOS®, iOS® are trademarks of Apple Inc., registered in the U.S. and other countries.

Windows® is a trademark of Microsoft Inc., registered in the U.S. and other countries.

The "Android" name, the Android logo, the "Google Play" brand, and other Google trademarks, are property of Google LLC in the US and other countries.