



# Nymi Connected Worker Platform FAQs

Version 1.66  
February 3, 2022

## Q: What biometrics data is captured and where is it stored?

User biometric data is stored in the form of a fingerprint template - a collection of unique features extracted from user fingerprint images. The original images are not retained and the fingerprint template is stored in protected memory space inside the Nymi Band™ microcontroller unit (MCU). The template is generated inside the MCU and never leaves or is accessible from outside the MCU.

For more information about fingerprint privacy, see: "Nymi Band: Secure Fingerprint Template Storage," which is included in the Nymi documentation package.

ECG data is used only during authentication to detect "liveness" (that you're a human being with a pulse). ECG data is not stored in the Nymi Band or used to identify the user.

Nymi does not store or process any biometric data outside of the Nymi Band.

## Q: Is Nymi a Software-as-a-Service or on-premise solution?

As of this writing (August 2021), the Nymi Connected Worker Platform (CWP) is 100% on-premise. No part of the solution is hosted or accessible by Nymi. However, Nymi may develop cloud-enabled features in the future for our customers who have adopted cloud technologies and want to get additional benefits from the Nymi CWP.

## Q: Can multiple fingerprints be enrolled to the Nymi Band?

The Nymi Band only supports enrollment of one user and one fingerprint at a time. Using multiple fingers during the enrollment process will degrade the performance of fingerprint authentication and, over time, authentication with the additional fingers may fail all together. Therefore, Nymi recommends using only a single finger during enrollment.

## Q: Is the user in control of their own biometric data?

The user's biometric data (the fingerprint template mentioned above) is securely stored on the Nymi Band and can never be accessed outside of the Nymi Band. A user can independently delete their biometric data in a security wipe feature by placing the Nymi Band on a charger and holding the bottom button for 10 seconds.



## Q: Is an Internet connection required from my environment?

No Internet connection is needed in the customer's environment, and the Connected Worker Platform is completely hosted on the customer's premise.

Optionally, CWP components can be hosted on cloud-based virtual environments.

## Q: What personal information is captured and where is it stored?

A document, "Storage and Transmission of Personal Data", is available from Nymi on this topic. By design, the Nymi Connected Worker Platform minimizes the amount of personal data stored.

How it works:

The fingerprint reader on the Nymi Band scans images of your fingerprint during the enrollment process to create a fingerprint template, which is an algorithm that gets stored securely on the Nymi Band. The images are immediately discarded once the template is created. (Note: The enrollment process is similar to setting up your smart phone for the first time, where you rest your finger on the fingerprint sensor, lift up, and repeat). The fingerprint template never leaves the Nymi Band and is deleted when a Delete User Data is performed on the Nymi Band.

The Nymi Band also checks for a human ECG trace every time the user authenticates with their fingerprint, by comparing the user's ECG signal to a generic human ECG signal. However, the Nymi Band does not store any information about the user's ECG signal and cannot uniquely identify the user by their ECG signal (only by their fingerprint). The ECG sensor is an added security measure that helps the Nymi Band to determine that it is on the assigned user at the highest confidence level.

When enabled, the Nymi Temperature Alerting feature gathers and processes Nymi Band user's wrist temperature. The temperature data is used to create a temperature profile, and then used for alerting user if their wrist temperature deviates from the baseline. No temperature data is stored on the Nymi Band. The temperature profile of the user is stored in the securely on the Nymi Band. The wrist temperature profile never leaves the Nymi Band and is deleted when a Delete User Data is performed on the Nymi Band.

## Q: Is the Nymi Connected Worker Platform secure?

Yes! The Nymi CWP is deployed into some of the most secure and highly regulated environments on Earth, including those of the leading Pharma Manufacturing, Medical Device, Healthcare and Financial Services enterprises. Please contact your Nymi representative to receive a copy of the "Connected Worker Platform Security White Paper" which details our security architecture.



## Q: Are Active Directory passwords stored by the Nymi Connected Worker Platform?

The Nymi Connected Worker Platform does not store a user's Active Directory password. If the CWP is deployed alongside third-party middleware, the middleware may store Active Directory passwords.

Nymi Lock Control™ is an optional application that provides Windows login and unlock capabilities based on user presence. If enabled, the Nymi Lock Control application stores an encrypted copy of the AD password in order to provide offline login functionality. By default, this capability is disabled. And, a quick reminder - all Nymi CWP components are on-premise and subject to the security controls and protocols managed by your company.

## Q: What is the Nymi Band made of?

The Nymi Band Generation 3 is comprised of hypoallergenic, ISO 10993-1 biocompatible components including a TPU strap and buttons, polycarbonate body and stainless steel ECG electrodes and clasping mushroom.

**Metals:** The Nymi Band contains two varieties of stainless steel; 430 Stainless Steel for the wrist-contact ECG electrode and 316 Stainless Steel with PVD-coated titanium for the fingerprint bezel sensor. Both materials have been tested for low nickel content and meet or exceed the requirements of the Derived No Effect Level (DNEL) for long-term local dermal effects with a sensitization endpoint, set by the European Chemicals Agency (ECHA). In other words, the Bands are comfortable and safe to wear for a long period of time.

**Plastics:** The Band composition is from TPU elastomer. This blend of material is frequently used in fitness trackers, smart watches, and other wearables. The Band material contains no latex or similar material and has been lab tested to simulate end-use conditions; in those tests no organic compounds were found.

**Battery:** Lithium-ion

For more information, please see [Material Composition](#).

## Q: How do I clean the Nymi Band?

The Nymi Band meets IP66 and IP67 Ingress ratings (dust tight, protection against water jets and submersion up to 1 meter for 30 minutes.). The Nymi Band is durable against wiping and gentle brushing. It can be cleaned daily using a 70% isopropanol, or a mild soap and water solution.

## Q: Is the Nymi Band a multi-factor authenticator?

The Nymi Band is a first of its kind one-step multi-factor authenticator. As a biometrically enabled wearable, its innovative design combines "something you have" (i.e. the Nymi Band being a user-specific security token) with "something you are" (i.e. biometrics identification).



## **Q: How do I authenticate to the Nymi Band if I'm wearing gloves?**

You should authenticate to your Nymi Band at the beginning of your shift, prior to putting on your gloves, gown, and other equipment. Upon successful authentication, the Nymi Band remains active and ready-to-use until it detects it has been removed from your body. Therefore, it is fully compatible to function under PPE.

## **Q: How long does the battery last, and how long does it take to charge?**

The battery lasts for approximately 3 days with regular use (about 300 authentications per day), but we recommend that you charge it every day. It takes 2 hours or less to fully charge a Nymi Band, and about 10-15 minutes to charge a completely depleted Nymi Band to last a full day.

## **Q: Is the Nymi Band rated as intrinsically safe, or suitable for use in hazardous locations?**

The Nymi Band has not been rated for use in hazardous locations. Contact your Nymi representative on how we can best meet your needs.

## **Q: How does Nymi validate their claims around reliability and product lifetime?**

Nymi tests the Nymi Band through accelerated lifetime testing to meet a minimum of 3-years of reliable operation. For details, please contact your Nymi representative for a copy of the Nymi Band 3.0 Reliability specification.

## **Q: How long does it typically take to validate/qualify Nymi per Good Automated Manufacturing Practices (GAMP)?**

Nymi has been validated for multiple GXP environments in over 15 countries. Where Nymi is being introduced to a system and environment that is already validated, the process is quite minimal. For example, when Nymi is introduced for e-signing with an existing, validated MES system, there is no change to the business process or validated system; Nymi simply provides a user the option to either type in their username and password, or tap their Nymi Band to a Nymi-enabled endpoint to provide their credentials. No other processes are changed, including how the validated application stores or processes data, therefore there is no need to revalidate the operation.

The specific customer validation process does vary from company to company, however, Nymi is able to provide a series of templates which can provide comprehensive assistance to a company seeking to validate our solution.



Nymi can provide validation templates and help build test cases and test plans. We also enable our customers to take advantage of our own validation efforts, and we can provide consumable test cases and reports to lessen the burden of validation to prevent duplication of testing.

If required, Nymi can also provide guidance, best practices and other consulting resources to help you define SOPs for cleaning, storage and other operational aspects of the solution. Typically, during an initial deployment, Nymi will work with your QA team to develop plans for validation so that ensure a clear path to a successful production rollout.

## **Q: Can Nymi Bands be used in a cleanroom environment?**

We worked with the top global Pharms and Medical Device manufacturers to design the Nymi Band specifically for use in highly regulated, cleanroom environments, while still making it comfortable and sleek enough for regular office use.

The Nymi Connected Worker Platform has been deployed in GxP-validated environments in more than 15 countries, including at 9 of the top 10 global Pharmaceutical manufacturers. The following points address specific concerns that customers have raised in the past:

“But, we have SOPs that strictly prohibit watches, jewelry and personal affects into our cleanroom and production areas; can we still use the Nymi Band?”

Our customers consider the Nymi Band as industrial equipment (e.g. similar to a barcode scanner) rather than jewelry. The devices do not tell time, are strictly controlled by company policies, and configured to aid specific work activities and use cases. We often assist our customers in developing appropriate SOPs for cleaning, storage, and daily use in accordance with existing policies regarding work equipment.

The Nymi Band is designed to work through multiple layers of Personal Protective Equipment (PPE). It is always worn under PPE and therefore is not exposed to the air in a cleanroom environment. It is designed to be cleaned frequently to industrial standards.

Customers with high-grade cleanrooms often choose to store and charge their Nymi Bands in the gowning/staging area, or locker room, so that the devices never leave controlled areas. Nymi provides bulk charging and storage solutions, please ask your Nymi representative for more information!

The Nymi Band is a workplace wearable rather than a personal affect. Its active features are controlled by company policy and provide none of the distractions of smart watches or cell phones.

## **Q: Are the Nymi Bands designed to break away if someone gets stuck? How much force is required?**

During evaluation, work is often undertaken with the on-site EHS team to determine any potential risks or safety issues associated with using the Band, particularly around moving machinery. The Nymi Band strap is not designed to break away, but the band is designed with a low profile and must be worn snugly on the user’s wrist to operate, often under PPE, thus greatly reducing the likelihood of it becoming caught.



For those employees, such as technicians, who are required to reach into heavy machinery, an SOP can be developed to limit potential risk. For example, wearing the Nymi Band on their non-dominant hand, or removing it entirely before doing potentially dangerous work.

## **Q: Can the Nymi Band be reassigned to new users?**

Yes, Nymi Bands can be assigned to new users, and the re-enrollment process only takes a few minutes.

## **Q: Can we share the Nymi Bands between shifts?**

This is technically possible, but not recommended. Once a user is enrolled to a Nymi Band the unique ID of that Band represents the user's identity. If that Band ID changes users constantly it can be more difficult to audit who was assigned a Nymi Band at what time. Also, having to enroll to a new Nymi Band every day may be very inconvenient for the user, particularly if many people are trying to re-enroll at an enrollment station at once (at the beginning of a shift for example).

## **Q: What happens if a Nymi Band stops working in the middle of the day?**

The journey to becoming a passwordless enterprise is iterative, and our Customers often configure the Nymi solution with an alternate authentication method when they are starting out. Therefore, if a user loses their Nymi Band during the day, or it stops working, the user can continue with their workday by simply typing their username/password.

However, Nymi enables users to use far more complex and secure passwords without sacrificing convenience, because the user is unlikely to have to type their password anymore for Nymi-enabled applications. Furthermore, Nymi can be configured for a completely passwordless experience once your company is ready to eliminate passwords all together.

Finally, most customers keep spare Nymi Bands on-site to quickly replace any bands that have been lost or that become inoperable.

## **Q: Will the Nymi Band work with my computer/endpoint?**

The Nymi Band communicates over two different technologies: 1) Near-field Communication (NFC) and 2) Bluetooth Low Energy (BLE). Depending on your use case, the endpoint (laptop, desktop, tablet, HMI, etc.) will need to be enabled with either NFC or BLE, or both. Currently, Nymi can only be used with endpoints running Windows 10 OS, with some exceptions. Please ask your Nymi representative for more information about technical requirements for your particular use case.



## Q: Can we use Nymi Bands for visitors?

Yes! Visitors can quickly and simply enroll to Nymi Bands, temporarily syncing to the physical and logical access systems controlled by your company with specifically-configured visitor access rights.

## Q: How does the Nymi Band know my credentials/password?

The Nymi CWP links your corporate username to your Nymi Band ID, and the system connects to your company's physical access, and identity access management systems to provide your Nymi Band with the appropriate access privileges. The Nymi CWP does not grant you any access rights to anything, but instead it simply relays the credentials stored in your company's Active Directory, physical access control system(s), or other identity access management systems.

## Q: What if I use different username/passwords to access different applications? Can I still use just one Nymi Band?

Yes! The Nymi CWP enables a user to access different applications that require different credentials using just one Nymi Band. Often the reason that users must maintain multiple credential sets, or "identities", is that the applications they are accessing reside on different networks that link to different authoritative sources. Nymi is helping leading enterprises address this difficult security/user experience paradox by enabling companies to preserve their network security segmentation and eliminate password re-use between network segments (which is convenient for users but undermines security segmentation) by providing users with an authentication method that's easier than typing a password - and can eliminate passwords all together. The Nymi Band!

Learn more about "[Resolving the IT OT Connection Paradox](#)" on the GSK Tech Blog.

## Q: What is Liveness Detection and should I enable it?

Liveness Detection is an optional system that uses electrocardiogram (ECG) during activation to increase confidence that the presented fingerprint is from a human wearing the Nymi Band. This takes about 10 seconds.

Liveness Detection increases confidence that the assigned user is wearing the Band while authenticating the device, however this feature alone cannot prevent them from sharing it with someone else. Like any security control (biometrics included), it can be beaten through collusion, where two or more employees are actively working together to subvert the security control.

The Nymi Band offers the key advantage of "non-repudiation", or undeniable evidence that the enrolled user was complicit in sharing the credential. Unlike a password, key card, or FOB, if an unauthorized user has another user's active Nymi Band on their wrist, there is no denying the enrolled user participated in the act, which acts as a significant deterrent to this type of behavior.

The use of Liveness Detection is optional either on a per-user basis or globally for all users.



Nymi's Customer Success Team will consult with customers to determine the best setting for their deployment.

Read more about [Operational Considerations for Liveness Detection here](#).



## About Nymi

Nymi, a Toronto-based company, creates a wrist-worn connected worker platform that unifies and enhances workplace connectivity for the digital future.

The Nymi Band™ consolidates workplace connectivity onto a platform that unifies the workplace across multiple environments by securing the point at which the worker and technology converge. By moving identity to the secure edge, organizations are able to eliminate silos and gain a complete view of their business with new applications enabled exclusively through a connected worker approach. As part of its diverse, global customer base, Nymi serves the world's largest enterprises with deployments across 15 countries.

Learn more at [nyimi.com](https://nyimi.com) or [info@nyimi.com](mailto:info@nyimi.com)