Authentication Station Guide

Overview

Due to the inherent nature of biometrics, some users may have difficulty authenticating to the Nymi Band in certain environments and circumstances over the lifetime of the product.

Similar to any biometric solution, Nymi recommends that customers implement a back-up to on-band biometric authentication in cases where a user has difficulty authenticating the Nymi Band with their fingerprint.

Authentication challenges result when the fingerprint comparison fails, or the Nymi Band cannot detect the user's ECG signal (via the built-in ECG sensor). Some causes may include:

- Damage to the user's fingerprint because of cuts and scrapes that may have occurred before enrollment, or afterwards
- Excessively wet or dry skin
- Debris between the fingerprint sensor and the fingerprint
- Users with a weak ECG signal, which results in Liveness Detection challenges.

For users who experience authentication challenges, Nymi's recommended solution is to authenticate to the Nymi Band at an Authentication Station.

An Authentication Station is a terminal workstation or tablet which is connected to the Nymi Enterprise Server, which allows a user to authenticate to their band by logging into the Nymi Band Application with their corporate credentials. This enables a user to bypass biometric authentication.

Requirements

Review the following requirement to deploy an Authentication Station:

- Ensure that the Authentication Station has a network connection to the Nymi Enterprise Server (NES) system.
- Install and configure the Nymi Band Application
- Connect and enable the Bluetooth Adaptor
- Enroll the user to a Nymi Band[1] and ensure that the user wears the Nymi Band securely on their wrist.
- Enable Corporate Credentials Authentication in the NES Administrator Console. Corporate Credentials Authentication can be enabled globally or per-user[2]. The following figure shows a group policy with the global Corporate Credentials Authentication option selected.
- Ensure that users can access the Authentication Station as needed. See **Deployment Considerations** below for further details.

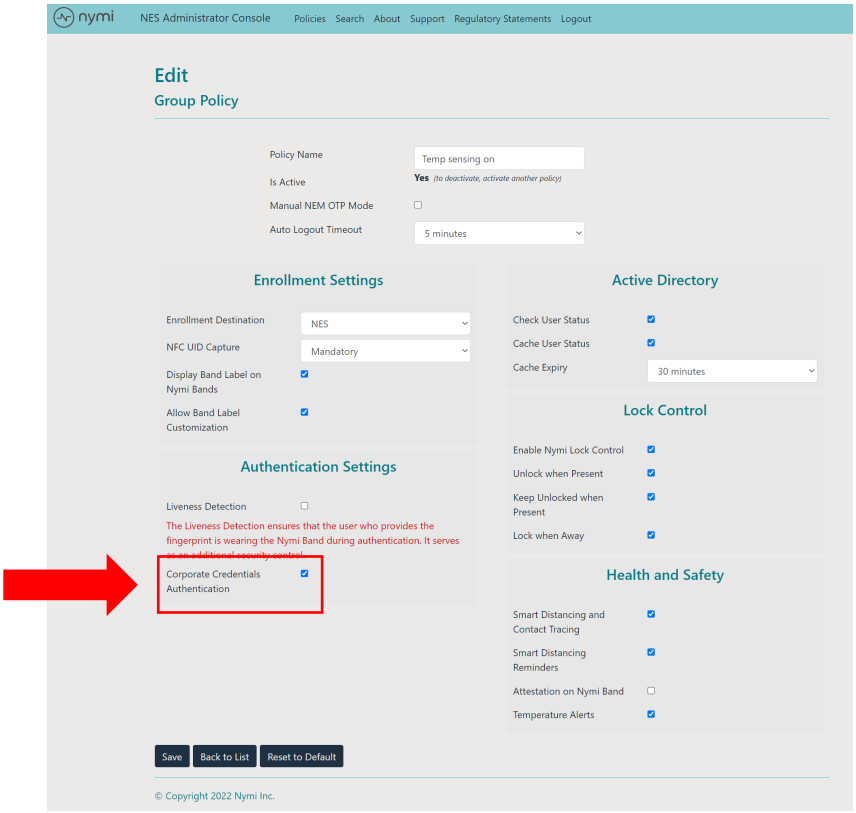

Figure 2: NES Administrator Console with Corporate Credentials Authentication highlighted

[1] For further instructions on Enrollment, please see the Nymi Knowledge Base at support.nymi.com.
[2] Please note Per-User Policies is only available in CWP 1.3 and beyond. For further information, please speak to your Nymi Solutions Manager.

User Workflow

A user performs the following steps to authenticate to the Nymi Band by using an Authentication Station:

1. Open the Nymi Band Application on the Authentication Station Terminal.
2. Type their Corporate Credentials (username and password) to log into the Nymi Band Application. The Nymi Band Application will navigate automatically to the "Authenticate to your Nymi Band" screen.
3. Click the Authenticate button, as shown in Figure 3. The Nymi Band authenticates. Figure 3, below, shows the Authentication screen with the Authenticate button highlighted.

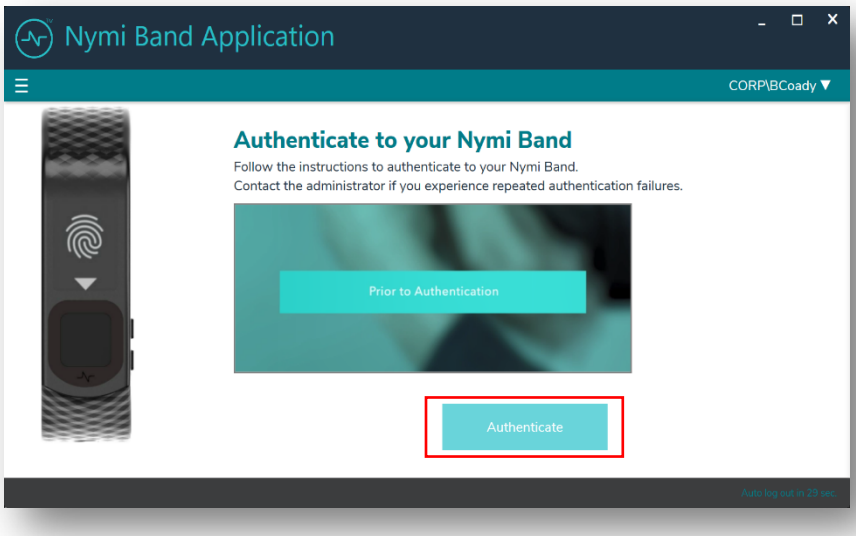

Figure 3: Nymi Band Application: Authentication Screen with Authenticate Button Highlighted

The entire process should take less than 2 minutes.

If a user cannot authenticate by using the Authentication Station, ensure that your environment has met all the requirements in the Authentication Station Requirements section. If the issue persists, contact Nymi Support for further assistance.

Deployment Considerations

Nymi recommends deploying an Authentication Station on a fixed terminal workstation or on an approved tablet.

Review the following recommendations and requirements to deploy the Authentication Station:

- Use a Windows-based fixed terminal workstation or tablet.
    - The following tablet models have been verified to work with the Connected Worker Platform (though other tablet models may be suitable):
        - Getac F110
        - Microsoft Surface Pro
- Connect the Bluetooth Adaptor.

Further installation requirements may exist depending on the deployment environment. Contact Nymi Support for further assistance.

Placement

Different work environments and Nymi Band use cases may require different considerations when determining where to place an Authentication Station.

1. In environments that allow **unsupervised alternative authentication**, Nymi recommends mounting a tablet or placing a fixed terminal workstation in one of the following areas:
    a. Centralized location, such as an entrance.
    b. Centralized meeting point such as outside a Locker Room or cafeteria.
    c. Where users charge and store the Nymi Bands.
2. In environments that require **supervised alternative authentication**, Nymi recommends that organizations deploy a tablet with a supervisor. Users with biometric authentication issues can request support from a supervisor, who can provide them with the tablet to authenticate by using the Nymi Band Application.
3. In environments that **use the Nymi Band to gain physical access**, Nymi recommends deploying the authentication station at the security desk or install the Nymi Band Application on their work laptop and direct the user to authenticate with their corporate credentials prior to entering the work environment
4. In situations where **a user is experiencing repeated biometric authentication challenges**, Nymi recommends installing the Nymi Band Application on their work laptop or workstation.
    a. If the user uses the Nymi Band for physical access, they can authenticate on their laptop with their corporate credentials before they enter the work environment
    b. If the user uses the Nymi Band to perform authentication tasks on their workstation, they can authenticate with their corporate credentials on their workstation when they arrive at their work area.

For further support on understanding the best option for your environment and use case, contact your Nymi Solution Consultant.

Security Considerations

Nymi recommends that customers consider impacts on security When using an Authentication Station does pose some security considerations as it provides an alternative to biometric security that is used by the Nymi Band.

Before deploying an Authentication Station to provide an authentication alternative to biometric authentication, review the following security considerations:

Authentication Collusion

It is possible for a user to provide their enrolled Nymi Band to another user, and then use the Nymi Band Application to authenticate the Nymi Band, while the Nymi Band is on the wrist of the other user.

Nymi recommends one of the following actions to prevent this form of collusion:

- Place an Authentication Station in a centralized location to increase visibility.
- Place an Authentication Station in a supervised area.

As the Nymi Band maintains non-repudiation through On-Body Detection, if a user is found to be using a Nymi Band that is not enrolled to them, it can be reasoned they must have had support from the enrolled user.

For additional support about how to maintain security when you deploy an Authentication Station, contact your Nymi Solution Consultant.

Enrollment Collusion

When the Nymi Band Application is installed on an Authentication Station, the machine also acts as an Enrollment Terminal.

As a result, a user can enroll an unenrolled Nymi Band on an Authentication Station when the following conditions are met:

- The user has access to the Authentication Station.
- The user is not currently enrolled to an active Nymi Band.

A user cannot perform a security wipe of their enrolled Nymi Band and re-enroll the Nymi Band on Authentication Station, nor can the user provide the Nymi Band to another user to perform an enrollment on the Authentication Station. An attempt to collude in this manner fails because the Nymi Enterprise Server (NES) database maintains a record of the Nymi Band to user association until an NES Administrator removes the association or removes the Is Primary option for the Nymi Band.

When a user wears a security wiped Nymi Band and attempts to perform the enrollment, the Nymi Band Application detects the existing Nymi Band association and enrollment does not continue.

Additionally, Nymi recommends users enroll their bands initially while supervised by an administrator to ensure users are trained correctly on using the Nymi Band and the enrollment is successful.

On-Body Detection

When a user authenticates to the Nymi Band by using an Authentication Station, the Nymi Band still enables On-Body Detection, which causes the Nymi Band to deauthenticate when the user removes the Nymi Band from their wrist. This maintains non-repudiation between the Nymi Band and the user wearing the Nymi Band.