openpath

KiNGS SECURE TECHNOLOGIES

Adding Safety to Security:

Enforcing Wellness Attestations in the Workplace

A safer workplace starts at the door

openpath

A safer workplace starts at the door

As companies begin to safely reopen after a health crisis, there are increasing concerns over how to effectively create a safe workplace, adhere to governmental compliance requirements, and to reduce liability. From daily health self-attestations, to on-site temperature checks, to technology such as contact tracing and thermal cameras, organizations are searching for the best methods of making sure all employees and staff are well enough to enter the facility, without incurring prohibitive costs, taking up valuable time, or violating the privacy of their employees.

Openpath's open API offers added flexibility for organizations looking to quickly deploy added security measures with daily symptom attestations to safeguard their assets and prevent the spread of illnesses in the workplace.

Use Cases

Automating wellness attestation forms

Daily health and symptom attestations are the most common and often the most cost-effective way for companies to implement a symptom check-in for anyone entering the workplace. The wellness attestation form requires employees, staff and visitors to confirm health information such as that they do not feel sick, do not have a fever, have not come in contact with anyone who is sick, or have been cleared by a doctor after becoming ill. However, organizing and managing a daily form can become cumbersome and complicated to roll out, especially for multi-site organizations, not to mention there's still the challenge of enforcing the attestation when it comes to physical access to the building.

With Openpath, this process can be automated, as well as enforced at building entry points. By using a web application for the attestation forms, companies can then utilize Openpath's open API to associate the completion of the attestation form with the user's access control privileges.

Option 1: API-based activation or suspension of users for set periods of time

For example, each morning prior to entering the building, all required users must fill out a digital symptom self-attestation form pre-selected to meet the needs of the building. Once complete, their confirmation acts as a form of two-factor authentication in Openpath's platform. When they enter the building, their Openpath credentials will be active only if they've completed their self-attestation, allowing them access to the building for the next 24 hours—or any amount of time determined by the building. After the designated time period, their access privileges will be suspended. Any employee who has not completed their symptom self-attestation, or who has responded that they are ill, will not be granted building access and you can elect for the right individuals to be notified.

This type of use case is helpful for quick deployment, as it does not require you to maintain the state of a list of users, or manage your users in multiple databases. You can easily integrate this with most web/app-based solutions or enterprise attestation platforms.

What is needed:

- Openpath Access Control Platform
- Openpath admin login credentials
- API key for authentication
- Technical ability to make two REST API calls
- The end users' email addresses

You can determine how long a user's access privileges should be active or suspended with very simple API calls. View API configuration examples below for more information.

Option 2: API-based changes to user groups

With this method, you can create multiple groups of users. For example: users that have access, users that don't have access, and users that have not completed their symptom self-attestation yet. Then, with very few API commands you can move users into the right group as their status changes. The benefit of this structure is that you can easily view which users fall into which category within Openpath. However, the challenge with this structure is that it requires more management to maintain the state of the groups and users. You would need to know which users you want to move from one group to another, or remember after a set period of time if you need to remove a user from a group. Alternatively within this option, you can have a schedule that removes all users from a group every night, or at set intervals. This approach is not as granular on a per user basis, but it does offer some benefits.

What is needed:

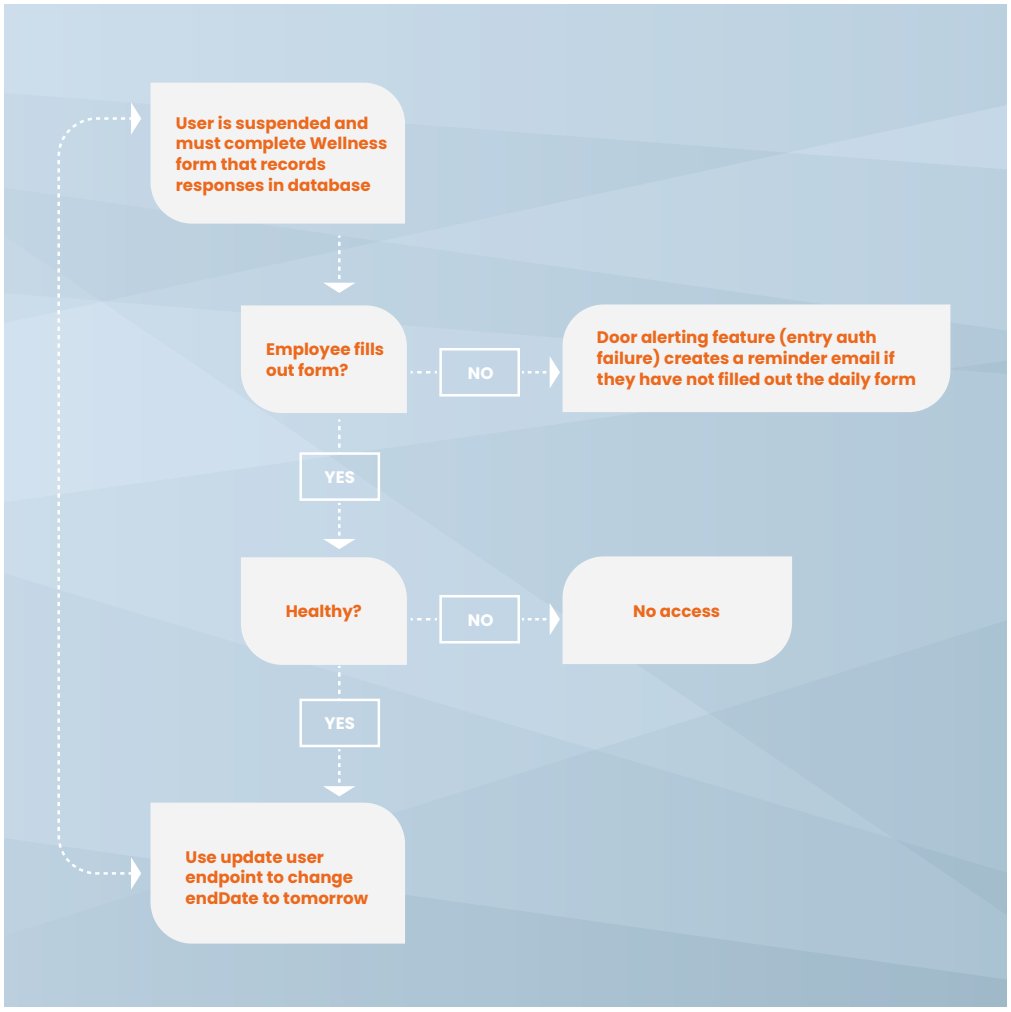
- Openpath Access Control Platform
- Openpath admin login credentials
- API key for authentication
- Technical ability to make a few REST API calls
- The end users' email addresses

API Configurations

There are a few ways to integrate a wellness self-attestation form with your access control using Openpath's open API.

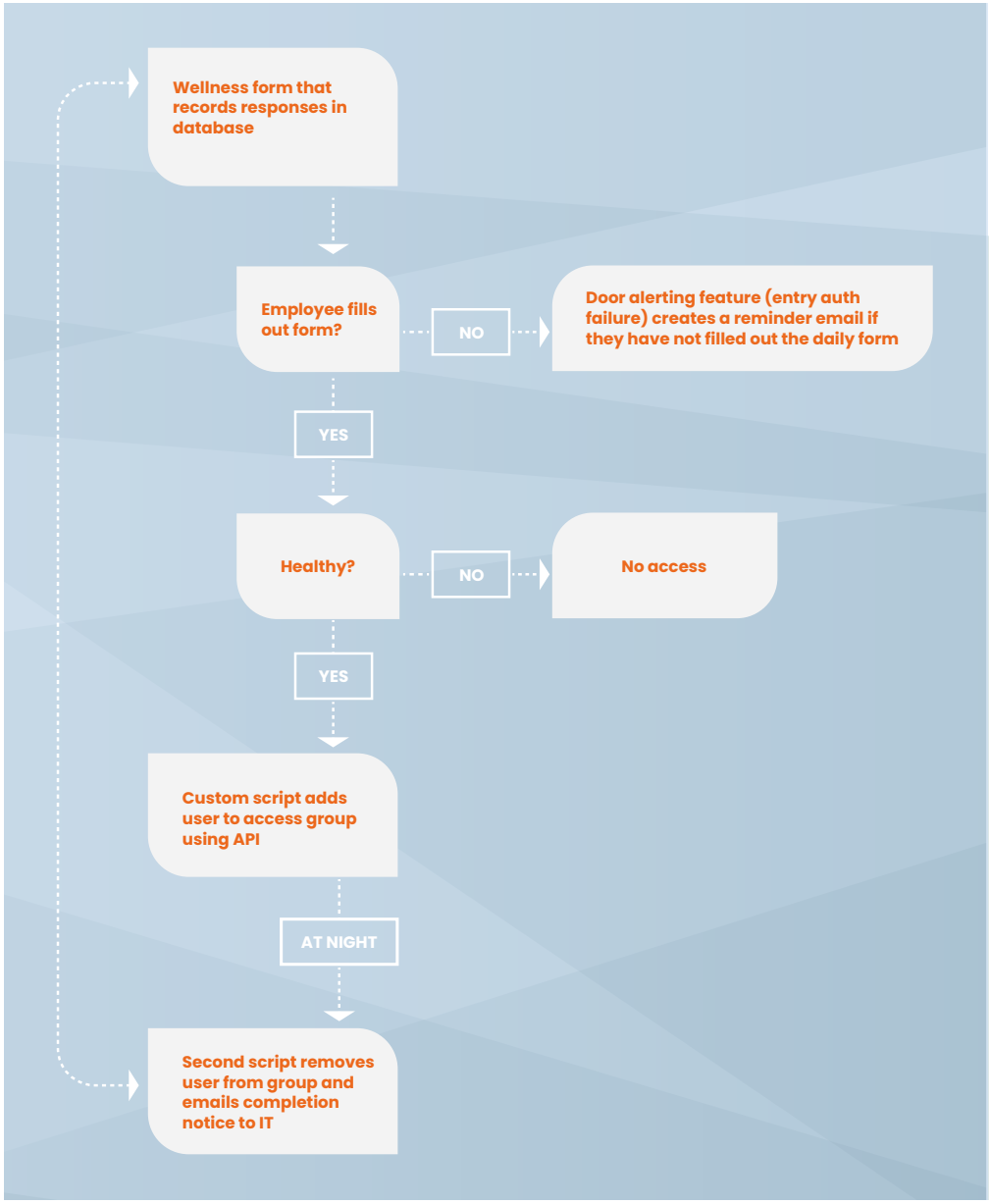
Option 1: API-based activation or suspension of users for set periods of time

You can activate users for a set period of time, or you can suspend users until they have completed an attestation form. This method forces a user to fill out the attestation form or they will not be granted access. Use the update user endpoint to reset the user's endDate to the following day after they complete the form.



Option 2: API-based changes to user groups

If your users already share an access group, then you can use the set user's groups endpoint to easily add and remove the user group. Use Openpath's built-in alert settings to be notified when an entry authorization fails, informing you when an employee without access (incomplete form) attempts to unlock the door.



APIs Used

Authenticate with the API: **POST** https://api.openpath.com/auth/login
List all users in an org: **GET** https://api.openpath.com/orgs/orgId/users
Update users' endDate: **PATCH** https://api.openpath.com/orgs/orgId/users/userId
Set users' groups: **PUT** https://api.openpath.com/orgs/orgId/users/userId/groupIds

For more information about Openpath APIs please visit the Developer Hub at https://openpath.readme.io/

Conclusion

Using Openpath to automate and enforce workplace self-attestations at a single site or across multiple locations can help organizations comply with guidance from local health authorities. Openpath's cloud-based software gives administration the benefit of remote management, enabling companies to grant and revoke access, update door schedules, and customize their health screening procedures from a single interface. With flexible configuration options, Openpath is able to enforce physical door security for any size business, without the need to hire additional staff to guard doors or collect forms. The open API offers quick deployment options by integrating seamlessly with online wellness attestation forms, as well as easy configurations to integrate with thermal camera technology in an efficient manner.

Similar deployments can be configured for solutions with contact tracing, off-site temperature checks, antibody testing and virus testing. With Openpath, personal data is kept safe and secure with end-to-end encryption. When health and security go hand in hand, readily protect your most valuable assets with Openpath.