Cognyte Formerly a Verint company

Symphia NowForce

Policies Guide

For version 5.6.3 and above

March 07, 2021

Preface

Symphia NowForce's advanced dispatch and response technology provides comprehensive situational awareness. Symphia NowForce allows dispatchers, responders and third-party resources to share insights in real-time, creating faster response times to potential threats and active incidents. Symphia NowForce leverages an integrated system of live and historical event data, state-of-the-art mapping, and tailored mobile applications for responders' and reporters' input to ensure that the closest, best equipped and most appropriate personnel is dispatched.

About this Document

This guide provides an overview to the Policies feature. The guide includes:

- Introduction to the Policies user interface.
- Policy workflows in the NowForce system.
- The recommended sequence of tasks required to prepare, initiate and manage the use of Policies in your NowForce installation.

Contacting Cognyte Sales and Marketing

Cognyte is a global leader in security analytics software that empowers governments and enterprises with Actionable Intelligence for a safer world. Our open software fuses, analyzes and visualizes disparate data sets at scale to help security organizations find the needles in the haystacks. Over 1,000 government and enterprise customers in more than100 countries rely on Cognyte’s solutions to accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent threats to national security, business continuity and cyber security.

To schedule an online demo today, contact us on:

- https://www.cognyte.com/contact/
- insidesales@cognyte.com
- +1866-639-8482

Contacting Cognyte Service and Support

At Cognyte, we value our users and partners, and we strive to continuously improve the customer service experience. Cognyte Smart Support™ ensures 24/7, on-demand service and support. Enter support requests, access training and troubleshooting tips, initiate RMAs, check warranty status, access resources, and more.

If you encounter any type of problem after reading this document, contact your local distributor or Cognyte representative. For the main service and support page on the Cognyte web page, visit: https://www.cognyte.com/contact

For immediate assistance, contact the support team:

Cognyte Support™ App	Contact Support	
Android	Americas	Phone: +1-866-639-8482 or +1-303-254-7005 Email: symphia.support@cognyte.com CALA: Open 9:00 am to 5:00 pm (EST) Monday to Friday Canada/USA: Open 9:00 am to 5:00 pm (Local Time) Monday to Friday
iOS	Europe, Middle East, and Africa	Phone: +44 (0) 845-843-7333 Israel: +972 99624286 Email: symphia.support@cognyte.com Open 8:00 am to 6:00 pm (GMT) Monday to Friday
	Asia/Pacific	India: (+91) 124 415 9500 Singapore: (+65) 6549 7769 Email: symphia.support@cognyte.com Open 9:00 am to 5:00 pm Local Time (Monday to Friday)

Contents

Introduction

Symphia NowForce Policies is a fully integrated, complete workplace health and safety solution for your organization.

This guide covers:

- The prerequisites required for a successful policies deployment.
- The typical workflows for creating and managing polices in your NowForce installation.
- The user-system interactions, set at the organization level, that determine user participation in policies.
- The management of user privacy needs while maintaining desired levels of monitoring.

Who Should Read this Guide?

The guide assumes that the reader knows what NowForce does, how it works, and how to configure NowForce. To read more, see the NowForce User Guide.

The guide is intended for the following user personae: Administrators, Dispatch Operators and Mobile App Users (Field Supervisors and Employees).

The relevant sections for each personae is shown below:

User	Relevant Sections
Administrator	• "Overview of Policies" (page 7) • "Policies Prerequisites" (page 11) • "Policies Workflows" (page 12) • "Policy User Interface" (page 17) • "Creating a New Policy" (page 19)
Dispatcher/Operator	• "Applying Policies to Single Users" (page 27) • "Applying Policies to Multiple Users" (page 28) • "Monitoring Policies" (page 30)
Mobile App Users	• "Policies Use Cases" (page 14)

Overview of Policies

The NowForce Policies framework is a our Workplace Health and Safety Solution, designed specifically to assist your organization manage major disruptive events, like Covid-19. Policies enables you to create and manage dynamic guidelines for your organization to reduce risk and simplify your on-site process management.

Policies Framework

The main objectives of the Policies Framework are:

- Maximizing workforce potential for both mobile and facility-based workforces.
- Minimizing health and safety threats to your organization.
- Providing all levels of your organization clear visibility of the regulations, procedures, access control, mitigating ambiguities and misunderstandings.
- Empowering organizations to follow and implement local authority regulations.
- Respecting and preserving the privacy of your employees.

Typical Use Cases

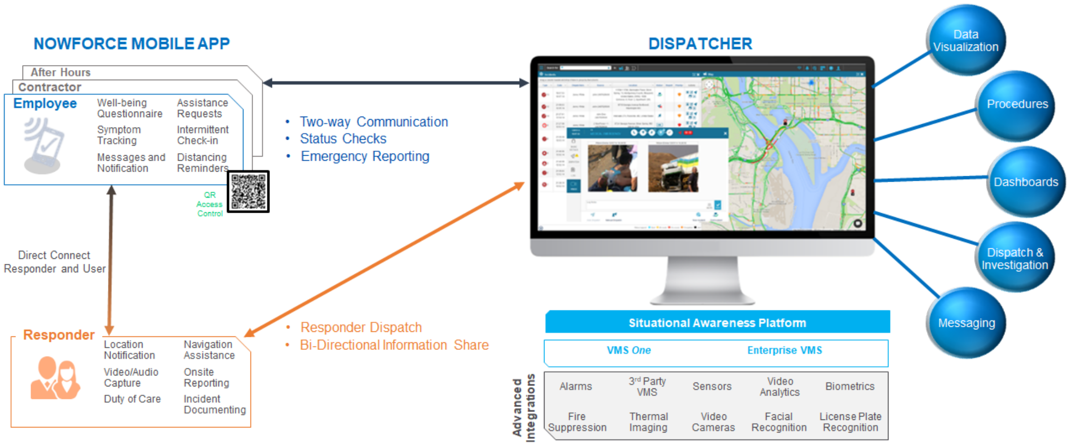
Typical use cases include:

- Granting and updating access privileges of permitted users/employees to company facilities.
- Coordinating the management of facility capacity, geographic capacity and workforce movement.
- Monitoring in real-time access to facilities with policy-specific QR codes.
- Collecting and monitoring manual and automatic user updates and forms on a routine basis.
- Automating smart mass messaging and response collection.
- Identifying at-risk employees (for example, users who have come into contact with a confirmed Covid-19 positive individual) and assigning those employees into a suitable policy for monitored management.

Integrating Capabilities

The Policies Framework integrates with the multiple features in the NowForce platform. Policies are administered in NowForce Dispatcher/Operator and can be applied to users with the Monitored Reporter or a higher license. Employees interact with policies via the NowForce Mobile App.

The diagram below illustrates the full capabilities of the NowForce modules that engage with Policies.



The Policies framework is designed to be entirely personalized to your organization.

Integrating Modular Customizable Capabilities

Policies settings are modular and customizable, and you have the flexibility to include some or all of the following when designing your policies:

- Access restrictions and privileges for specific sites.
- Transition (switching) rules that specify how users enter and exit a policy.
- User Updates, including detailed forms, for employees to complete and send.
- User Updates posted or logged to the system by a third-party (by the operator, devices, QR scanning).
- Smart Messaging that interprets each user's unique response to a bulk-sent message to apply the relevant policy to the user.

- Capacity management that allows you to define the specific percentage (or absolute number) of employees allowed on site or in a policy.
- Location tracking that monitors the entrance of employees into and out of specified geofences within a policy.

> Note
> NowForce's Adaptive Location tracking is monitored on the mobile device and can be switched off for specific user profiles or policies. Routine location coordinates are not shared with the server. Only if a user breaches a policy, for example entering/exiting a predefined geofence, is the breach communicated to the server.

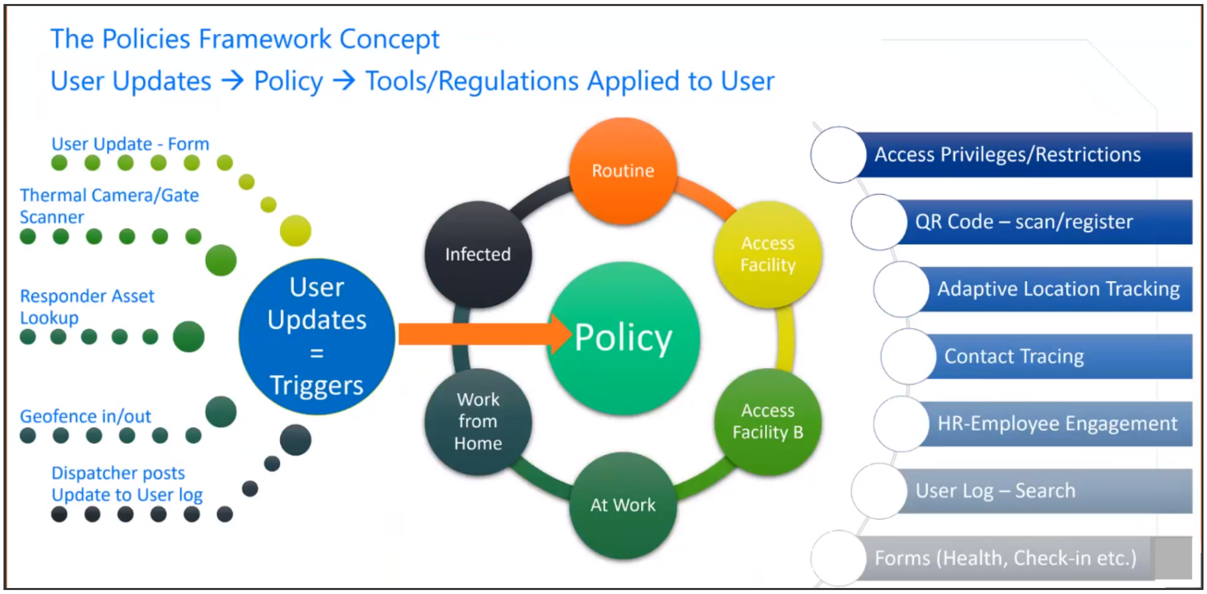
- Exposure monitoring (contact tracing) via Bluetooth contact tracing of via location cross-checking. The contact tracing protocol is managed and monitored automatically on the devices remotely. No personal information is shared unless the user/employee actively chooses to notify the operators.

Simplifying Policies Transition Rules

The ability to automate thousands of user-system interactions under a single coherent and logical set of rules is the mainstay of the Policy framework. Simplifying and adapting the policy transition rules to enable dynamic matching to shifting public policy, local regulations or company needs.

You can set automated logical triggers for users, that define a user's transition from one policy to another. These triggers are shown on the left-hand side of the diagram, and include: user update form, images and scans, entrance or exit of a geofence, and dispatcher posts to user updates logs.

The NowForce system processes updates received and can automatically transition users into the relevant policy. All changes are logged in the system and retrievable from the users' logs.



The Policies Framework Concept

User Updates → Policy → Tools/Regulations Applied to User

You can create multiple policies to manage different routine and non-routine scenarios for your organization. Typical use cases are described in the "Policies Use Cases" (page 14) section.

Policies Prerequisites

The following requirements are mandatory to enable the Policies feature:

Requirement	Performed by
Policies-relevant system configurations must be enabled.	NowForceSupport
A Monitored Reporter (or higher) license must be applied to all mobile users participating in the Policies framework.	Administrator
Download and installation of the NowForce Mobile App version 5.6 or higher on user's mobile devices.	Users
Optional: Purchase of BT (Bluetooth) Exposure Notification (Covid-19) licenses. Note Required only for BT Exposure Notification functionality.	Administrator
Optional: Application of BT (Bluetooth) Exposure Notification (Covid-19) licenses to required user profiles.	Administrator

Required licenses per user:

License Requirement	Required for
Monitored Reporter (or higher) license	All users/employees participating in the Policies framework.
Advanced Responder (or higher) license	All field supervisors participating in the Policies framework who require scanning of QR codes.
Dispatcher Operator	All operators (security, safety, HR etc) managing the application of Policies in the NowForce system.
Administrator	All administrators configuring and defining Policies in the NowForce system.

For further details see the NowForce Licensing Guide.

Policies Workflows

New policies are created by the administrator and then assigned to users by either the operator or administrator. Users engage with the policy feature via their NowForce Mobile App and their responses are monitored in the NowForce Dispatcher.

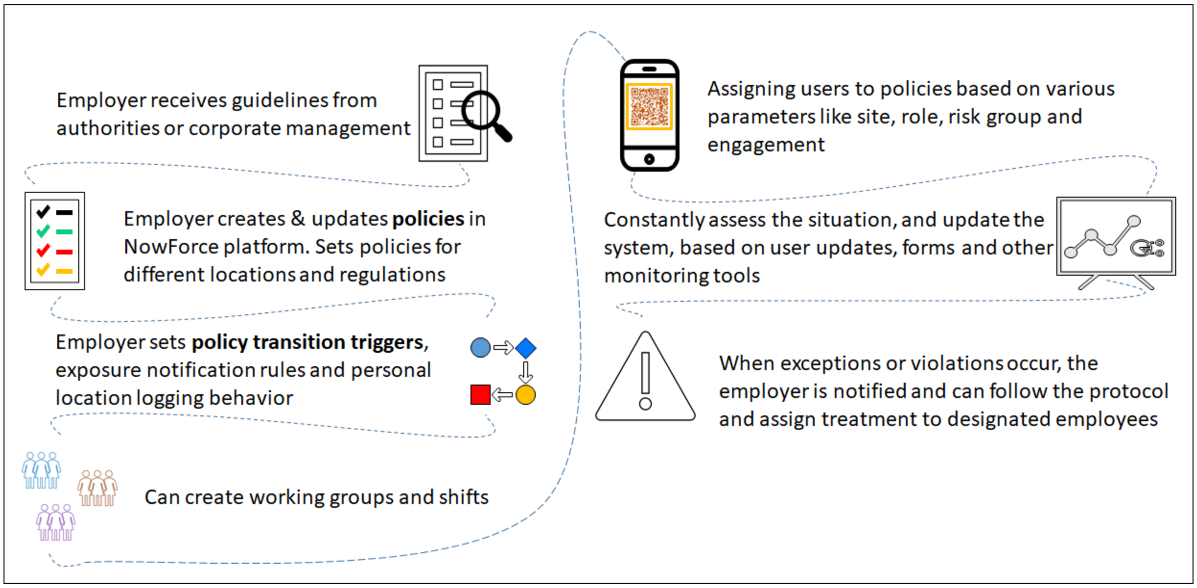
Before you begin

Ensure your organization's workplace health and safety requirement guidelines are clearly defined, so you are able to action these guidelines when creating a new policy.

Task	Steps	Location in NowForce	Performed by
Developing a New Policy	Ensuring all "Policies Prerequisites" (page 11) for licensing and system requirements are met.	• Profiles Settings • License Settings • Organization Configuration Settings	Administrator
	"Creating a New Policy" (page 19)	Policy Settings page	Administrator
Managing Policies	"Applying Policies to Single Users" (page 27)	User Management window	Dispatcher
	"Applying Policies to Multiple Users" (page 28)	User Panel	Dispatcher
	"Monitoring Policies" (page 30)	Dashboard window	Dispatcher

Getting Started Workflow

The Getting Started workflow demonstrates how a workplace health and safety policy is initially planned and implemented using NowForce. For more information about how the Policies feature integrates with your NowForce deployment, see "Overview of Policies" (page 7).



Employer receives guidelines from authorities or corporate management

Employer creates & updates **policies** in NowForce platform. Sets policies for different locations and regulations

Employer sets **policy transition triggers**, exposure notification rules and personal location logging behavior

Can create working groups and shifts

Assigning users to policies based on various parameters like site, role, risk group and engagement

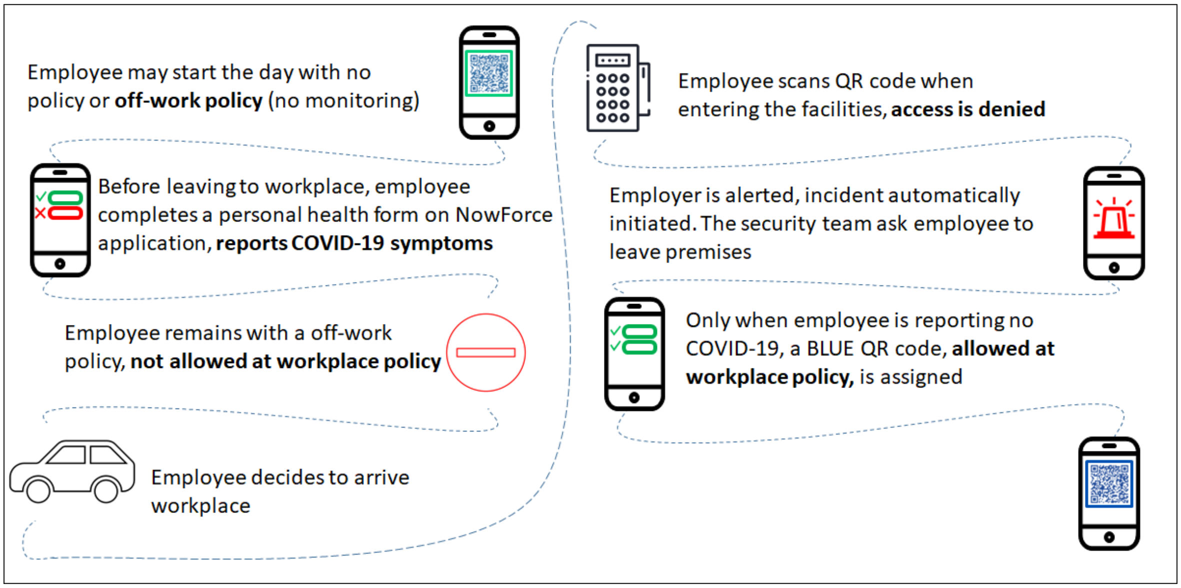
Constantly assess the situation, and update the system, based on user updates, forms and other monitoring tools

When exceptions or violations occur, the employer is notified and can follow the protocol and assign treatment to designated employees

Policies Use Cases

Policies are designed to monitor workplace health and safety. The use case describes how an employee reports their COVID-19 positive symptoms via the NowForce Mobile App.

1. The user sends in a user update, the system receives the update, and the user is automatically transitioned into a "not allowed at workplace" policy.
2. When the user arrives at the workplace and present their QR code for scanning, they are denied access.
3. Only once they send a user update that indicates they are healthy, will they be assigned into an "allowed at work" policy and receive a QR code that allows them to enter the facilities.

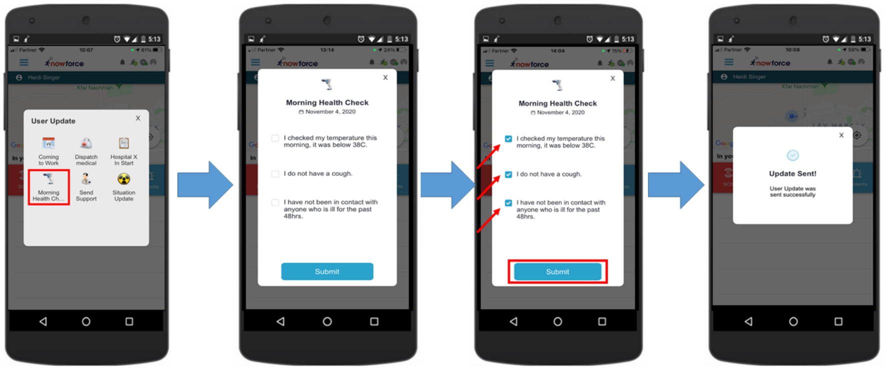

Employee may start the day with no policy or **off-work policy** (no monitoring)
Before leaving to workplace, employee completes a personal health form on NowForce application, **reports COVID-19 symptoms**
Employee remains with a off-work policy, **not allowed at workplace policy**
Employee decides to arrive workplace
Employee scans QR code when entering the facilities, **access is denied**
Employer is alerted, incident automatically initiated. The security team ask employee to leave premises
Only when employee is reporting no COVID-19, a BLUE QR code, **allowed at workplace policy,** is assigned

The typical workflows for an All Healthy Declaration and a Declaration of Symptoms in the NowForce system are described below:

All Healthy Declaration Use Case

In this example, users that complete health declarations (or any other type of update or form that indicates they are healthy) are assigned into an "allowed at work" policy as follows:

1. A health declaration is available on the user's mobile device according to the user's assigned policy.
2. From their NowForce Mobile App the user sends an update indicating that they are healthy.



Morning Health Check
November 4, 2020

□ I checked my temperature this morning, it was below 38C.
□ I do not have a cough.
□ I have not been in contact with anyone who is ill for the past 48hrs.

Submit

Morning Health Check
November 4, 2020

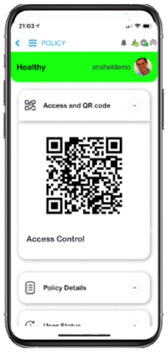
☑ I checked my temperature this morning, it was below 38C.
☑ I do not have a cough.
☑ I have not been in contact with anyone who is ill for the past 48hrs.

Submit

Update Sent!

User Update was sent successfully

3. The NowForce system automatically applies the policy transition rule and the user is moved into a "allowed at work" policy.
4. Scanning the user's QR code on their NowForce Mobile App at the access point grants the user access to the premise.
5. The user remains in the "allowed at work" policy until a transition trigger for exiting (revoking) the "allowed at work" policy is received - this could be the expiration of a set time allocation or upon exit of the geofence or other.
6. The user receives a notification in the NowForce Mobile App to indicate they have been moved into a different policy.



Declaration of Symptoms Use Case

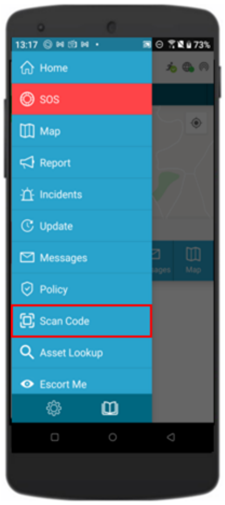
1. Based on the current assigned Policy, the user (employee) will have an option to send an update with a form, in this example, a health declaration indicating symptoms.

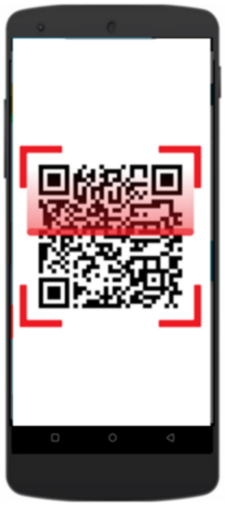
2. If the user sends a health form indicating existence of symptoms, this triggers a transition to a "Blocked access" policy.

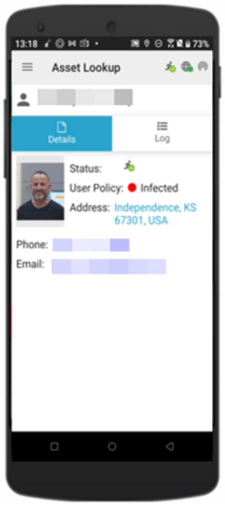
3. The NowForce system automatically applies the transition rule and the user is moved into an "Cannot enter" policy, with no access allowed to the workplace.

4. A 'no access allowed' message and QR code is sent to user's NowForce Mobile App.

5. If the employee attempts to enter the office facility and the guard at the entrance scans the employee's QR code on their NowForce Mobile App a message that a 'no access allowed QR was scanned' in NowForce Dispatcher.

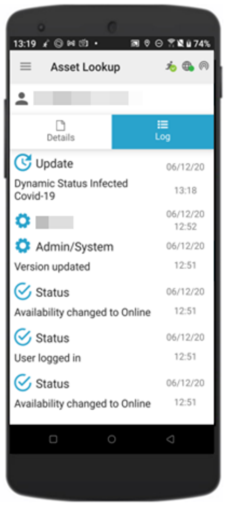






[redacted]

Status:
User Policy: ● Infected
Address: Independence, KS 67301, USA
Phone: [redacted]
Email: [redacted]



[redacted]

Update 06/12/20
Dynamic Status Infected Covid-19 13:18

[redacted] 06/12/20 12:52

Admin/System 06/12/20
Version updated 12:51

Status 06/12/20
Availability changed to Online 12:51

Status 06/12/20
User logged in 12:51

Status 06/12/20
Availability changed to Online 12:51

6. The guard can either add a text entry to the user's log indicating the user was refused entry or even create an incident in the system to trigger dispatch of other officers to address the situation.

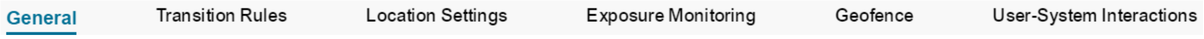
7. The user remains in an "Cannot enter" policy until either a preset expiry time passes or manually by the HR operatorthe user sends an update that triggers their transition into an"Allowed access" policy.

Policy User Interface

This section describes the layout and key terms in the Policy Settings page.

Policy Settings Layout

You can access the policy setting using the following tab:



- In the General tab you set a name and policy description, and set the policy access control requirements.
- In the Transition Rules tab you to set the automated entrance and exit rules for the policy.
- In the Location Settings tab you set the requirements and exceptions for mobile location tracking in the policy.
- In the Exposure Monitoring tab you set the contact tracing parameters of the policy. See "Add-On Feature BT (Bluetooth) Exposure Notification " (page 31).
- In the Geofence tab you set the primary and additional geofences for the policy.
- In the User-System Interactions you define QR scans and User Updates for the policy.

See "Creating a New Policy" (page 19) for the detailed tasks required to create a new policy for your organization.

Policy Terms and Definitions

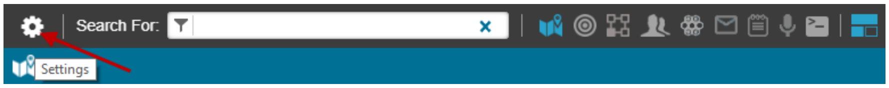
Term	Definition
Access Control	Specifies locations that users assigned to this policy can access. Locations can be added to the configurable list.
Access Restrictions	The free text fields where the Administrator describes the restrictions and limitations of the policy.
Access Privileges	The free text field where the Administrator details available access privilege of the policy.
Adaptive Location Settings	The location settings that can be configured for different frequency and accuracy of mobile device tracking. Note • Only applies if mobile location monitoring of users is enabled. • These routine locations are saved only to the users mobile device (for geofencing and future contact tracing purposes) and are not shared with the server.
Exposure Tracking	Tracking and saving of intersections of mobile devices, between two or more individuals using the Bluetooth tool on the app. A time threshold for each exposure can be preset.
Exposure Match	When an one individual alerts the system they have been infected and applications on other individual devices identify the an intersection with the infected individual.
User Update	Continuous updates registered to the User’s log. These updates can be posted by the monitored user via the NowForce Mobile App or by another authorized Supervisor/Operator via the mobile or desktop applications.
Geofence	Circular areas defined by a center address and radius. The Policies settings allow defined monitored geofences that trigger alerts in the system.
Rule Violation	User action that violates a determined policy restriction.
Transition Trigger	A user action that can automatically transition a user from one policy to another. Triggers can include user updates, form submission, entering or exiting a geofence, elapsed time, exposure notifications etc. These are set as transition rules in the policy settings.
Entrance Rule	An associated user action that triggers a change in the user policy granting (or restricting) the user access. Specific updates can be set to transition the user into a higher or lower level policy.
Exit Rule	A time defined as expiry for a policy.
Limitations	Maximum number of individuals, either absolute or percentage of workforce, whether in a location or in a policy.

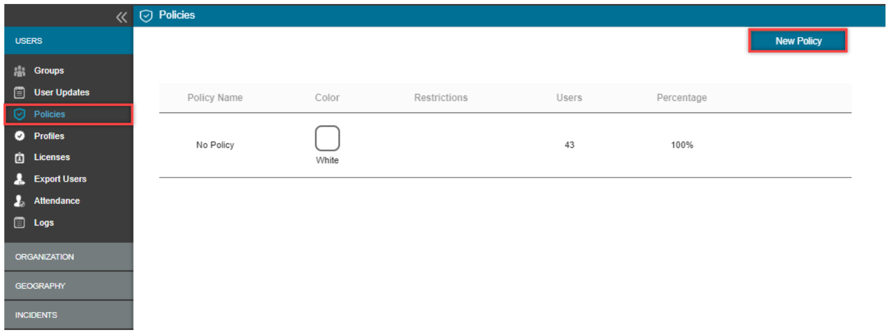
Creating a New Policy

This section describes how an administrator creates a new policy in NowForce.

▼ To create a new policy

1. In the corner of the Main screen, click **Settings** (gear).



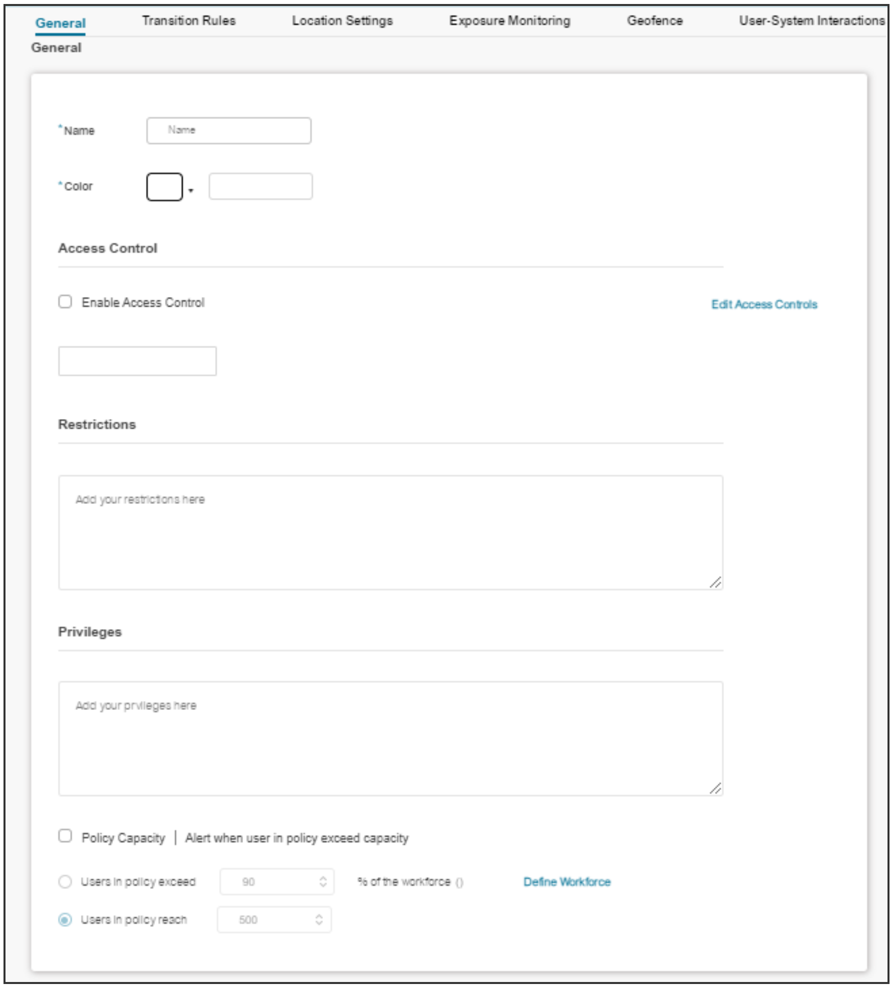


Policy Name	Color	Restrictions	Users	Percentage
No Policy	□ White		43	100%

2. Click the **Policies** tab and **New Policy** to create a new policy.

   The new policy screen opens in the **General** tab.

> **Note**
> All fields marked with an asterisk are compulsory.



General

*Name: Name

*Color

Access Control

□ Enable Access Control

Restrictions

Add your restrictions here

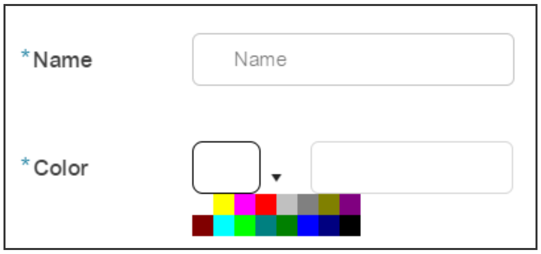
Privileges

Add your privileges here

□ Policy Capacity | Alert when user in policy exceed capacity

○ Users in policy exceed 90 % of the workforce ()

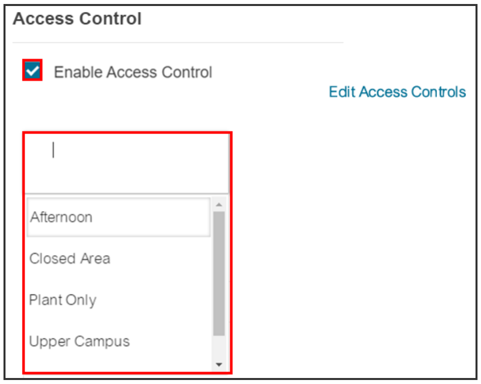
● Users in policy reach 500



*Name: Name

*Color

3. Enter a **Name** and select a policy identifier **Color** from the dropdown.



Access Control

☑ Enable Access Control

Afternoon

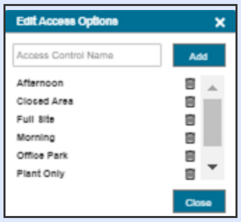
Closed Area

Plant Only

Upper Campus

4. To define Access Control for this policy, select the **Enable Access Control** checkbox and the relevant access control option from the field below.

> ## Note
>
> To add a new access control option, click **Edit Access Controls**, add a new access control option, and click **Add**. When the option becomes available, click **Close**.



Edit Access Options

Afternoon

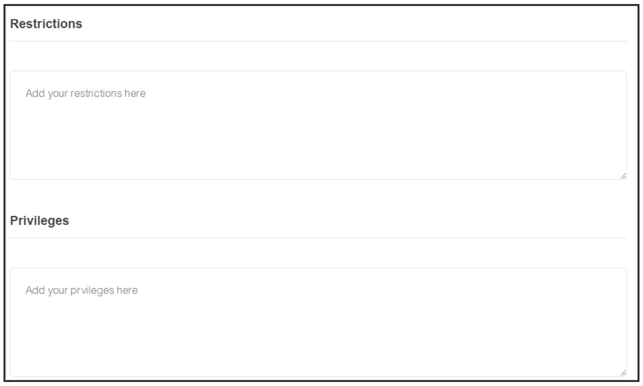
Closed Area

Full Site

Morning

Office Park

Plant Only



Restrictions

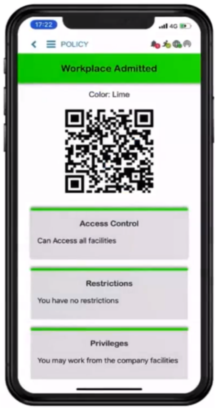
Add your restrictions here

Privileges

Add your prvileges here

5. Complete the **Restrictions** and **Privilege** text boxes.

   The Access Control, Restrictions and Privileges display in the mobile app.



Workplace Admitted

Color: Lime

Access Control

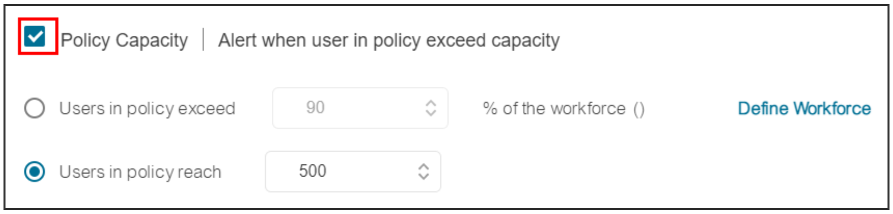
Can Access all facilities

Restrictions

You have no restrictions

Privileges

You may work from the company facilities



☑ Policy Capacity | Alert when user in policy exceed capacity

○ Users in policy exceed 90 % of the workforce () Define Workforce

● Users in policy reach 500

6. Select **Policy Capacity** to include a user threshold in the policy.

   An alert will sent to the Dispatcher when the capacity cap set in the policy is reached.

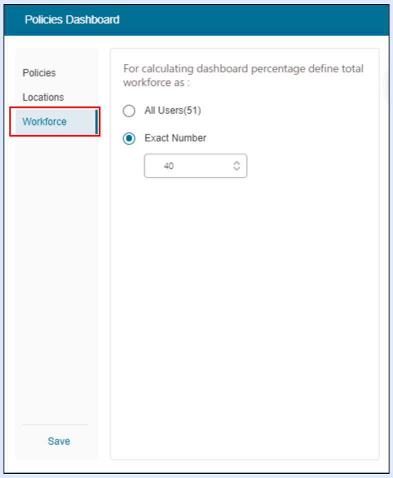
   > Note
   >
   > You can set the capacity parameters to either a percentage of your workforce or absolute number of users in the policy.

7. To set your capacity threshold:

   a. As percentage of your workforce, select **Users in policy exceed** and enter the % value of the workforce in the field, or

   b. As an absolute number, select **Users in policy reach** and enter the number in the field.

   > Note
   >
   > To define your workforce, select **Define Workforce**. This opens the Policies Dashboard. Select the **Workforce** tab and either the **All Users** or **Exact Number** to define your workforce.

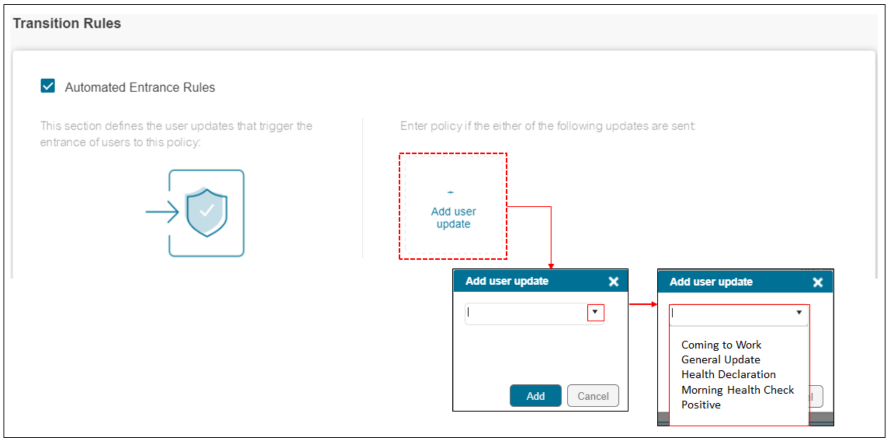


For calculating dashboard percentage define total workforce as :

○ All Users(51)

● Exact Number

40



Transition Rules

☑ Automated Entrance Rules

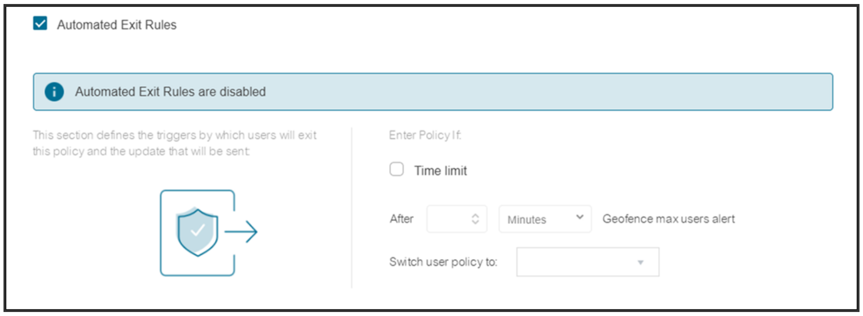
This section defines the user updates that trigger the entrance of users to this policy:

Enter policy if the either of the following updates are sent

8. Select the required **Transition** rule for the policy.

   a. Select the **Automated Entrance Rules** and from the dropdown select the required **User Updates**.

   > Note
   >
   > To add a new User Updates option, click **Add** in the User Update window.



☑ Automated Exit Rules

Automated Exit Rules are disabled

This section defines the triggers by which users will exit this policy and the update that will be sent

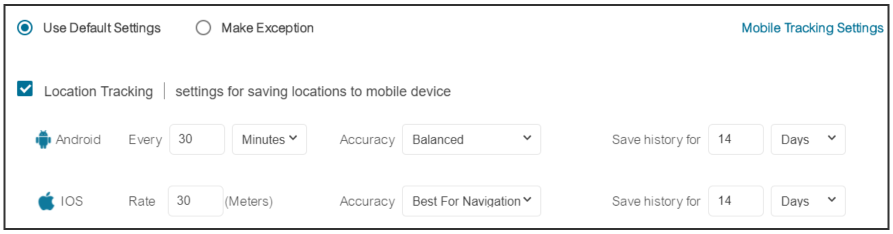
Enter Policy If:

□ Time limit

After Minutes Geofence max users alert

Switch user policy to:

   b. Select the **Automated Exit Rules** checkbox and set the **Time limit** and **Switch user to policy** options.



● Use Default Settings ○ Make Exception

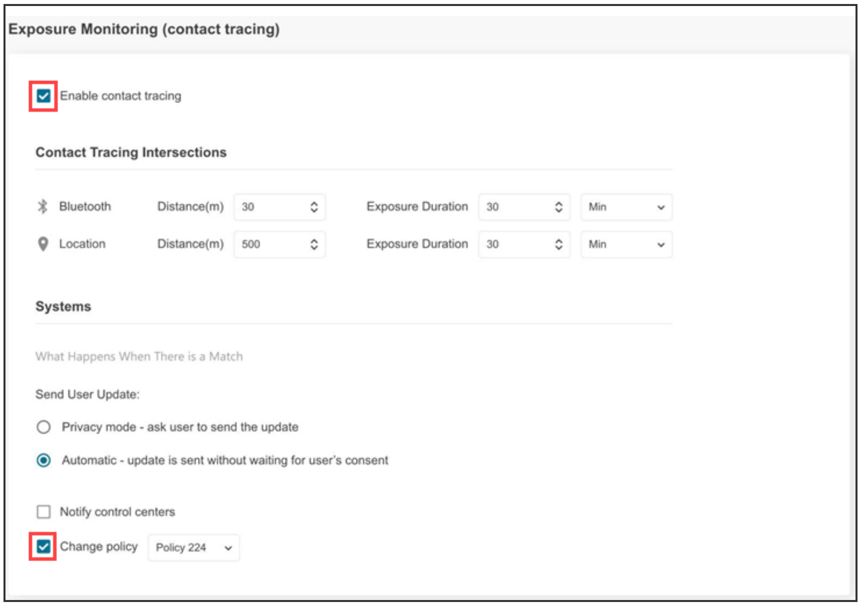
☑ Location Tracking | settings for saving locations to mobile device

Android Every 30 Minutes Accuracy Balanced Save history for 14 Days

IOS Rate 30 (Meters) Accuracy Best For Navigation Save history for 14 Days

9. If you require location tracking select **Enable Mobile Tracking** and adjust the Android and iOS frequency settings.

   > Note
   >
   > To view the full location tracking and sharing controls in the system select the **Mobile Tracking Settings** link to open the **Mobile Tracking Settings** page.



Exposure Monitoring (contact tracing)

☑ Enable contact tracing

Contact Tracing Intersections

Bluetooth	Distance(m)	30	Exposure Duration	30	Min
Location	Distance(m)	500	Exposure Duration	30	Min

Systems

What Happens When There is a Match

Send User Update:

○ Privacy mode - ask user to send the update

● Automatic - update is sent without waiting for user's consent

□ Notify control centers

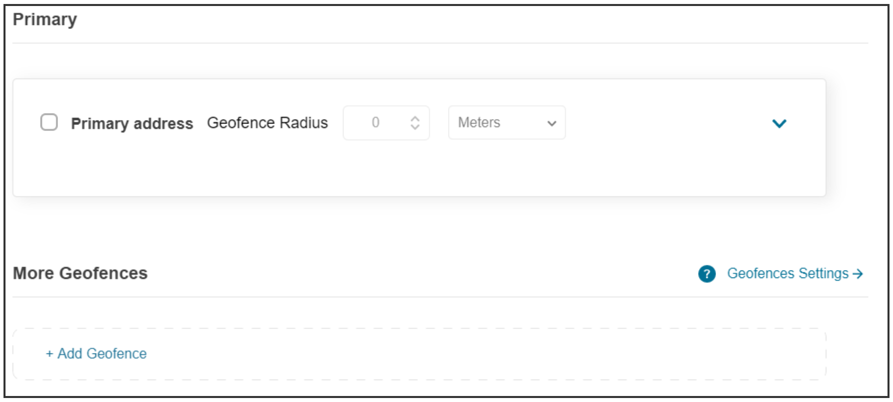
☑ Change policy Policy 224

10. If you require Exposure Notification (Contact Tracing) select the **Enable contact tracing** option.

> Note
> You can adjust the Bluetooth and Location settings.

11. Select the preferred **What Happens When There is a Match** option.

12. Select **Change policy** to automatically change the users policy the policy selected from the list.



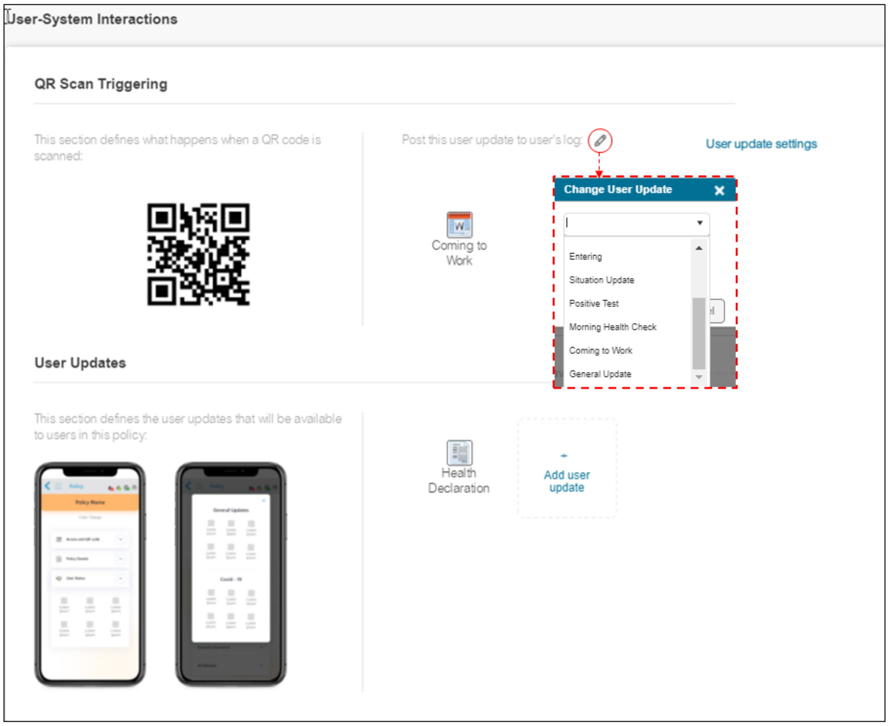
Primary

□ **Primary address** Geofence Radius 0 Meters

More Geofences

13. In the Geofence tab select **Primary address**. You can add more geofences by clicking **Add Geofence.**

> Note
> Clicking **Geofence Settings** will exit you from the Policy settings. You will be prompted to save your changes to your new policy before your exit.



User-System Interactions

QR Scan Triggering

This section defines what happens when a QR code is scanned:

Post this user update to user's log:

User update settings

Change User Update

Entering
Situation Update
Positive Test
Morning Health Check
Coming to Work
General Update

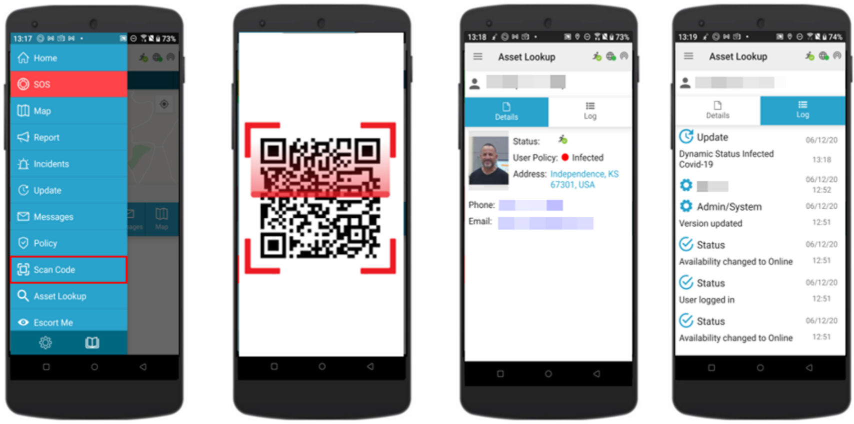
User Updates

This section defines the user updates that will be available to users in this policy:

14. In **User-Sytem Interaction** tab:

   a. In **QR Scan Triggering** define what happens when a QR code is scanned. Select 🖉 to select the Change User Update that will be posted to the user's log.

   The users' QR code is scannable on a field supervisor's mobile device. The scanning of the QR code displays the user's details and updates their User Log, this is shown below.



Status:
User Policy: ● Infected
Address: Independence, KS 67301, USA
Phone: [redacted]
Email: [redacted]

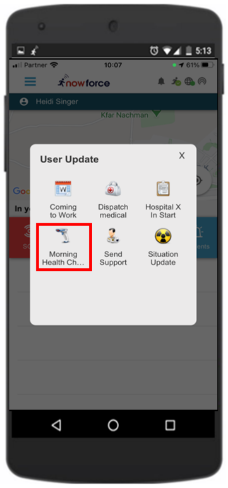
Update 06/12/20
Dynamic Status Infected Covid-19 13:18
[redacted] 06/12/20 12:52
Admin/System 06/12/20
Version updated 12:51
Status 06/12/20
Availability changed to Online 12:51
Status 06/12/20
User logged in 12:51
Status 06/12/20
Availability changed to Online 12:51

z

> **Note**
>
> Clicking **User Updates Setting** will exit you from the Policy settings. You will be prompted to save your changes to your new policy before you exit.

b. In the **User Update** section click **+** to add the user updates available to users in the policy.

The available User Updates display in the mobile app.



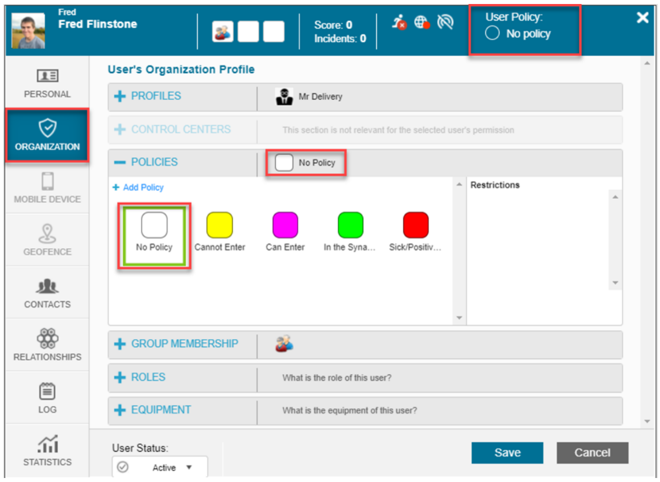
15. Click **Save**.

Applying Policies to Single Users

This section describes how you can set a policy for a single user.

▼ To apply a policy to a single user.

1. In the Main screen, select 👤 **Users icon** from the taskbar.
2. In the Users Panel, stand on the user's image displayed in the **Actions** column and select **Edit** from the popup menu. The User Management window opens.
3. In the User Management window, select the **ORGANIZATION** tab and then select the **POLICIES**.



Fred
Fred Flinstone

Score: 0
Incidents: 0

User Policy:
○ No policy

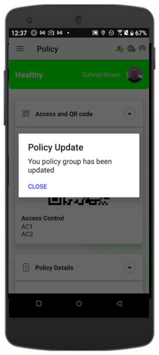
User's Organization Profile

+ PROFILES	Mr Delivery
+ CONTROL CENTERS	This section is not relevant for the selected user's permission
− POLICIES	□ No Policy
+ GROUP MEMBERSHIP	
+ ROLES	What is the role of this user?
+ EQUIPMENT	What is the equipment of this user?

User Status: Active

4. Select a policy.
5. Click **Save**.

   The user receives an alert indicating that their policy has been changed.



12:37 67%

Policy

Healthy Gabriel Noam

Access and QR code

Policy Update

You policy group has been updated

CLOSE

Access Control
AC1
AC2

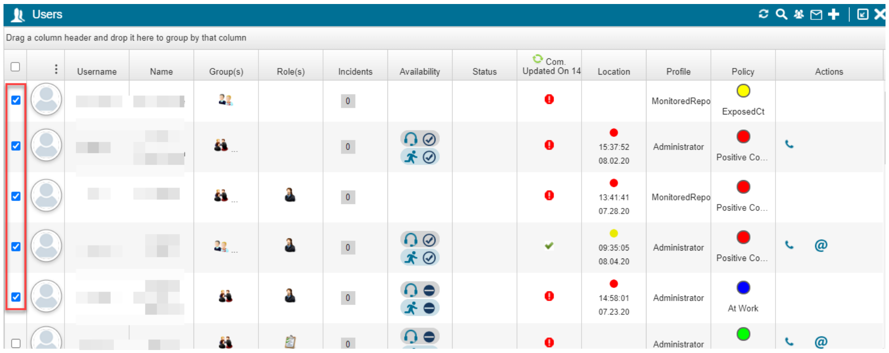
Policy Details

Applying Policies to Multiple Users

This section sets how you can set a policy to multiple users.

▼ To apply a policy to multiple users

1. In the Dispatcher screen, select **Users icon** from the taskbar top open the Users Panel.
2. In the **Users Panel** select the users.

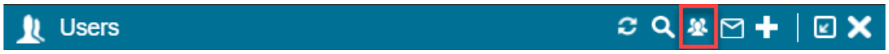


Users

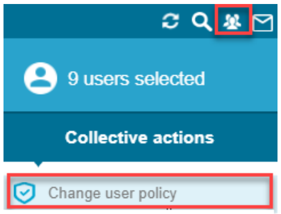
Drag a column header and drop it here to group by that column

☐	⋮	Username	Name	Group(s)	Role(s)	Incidents	Availability	Status	Com. Updated On 14	Location	Profile	Policy	Actions
☑		[redacted]	[redacted]			0			!		MonitoredRepo	● ExposedCt	
☑		[redacted]	[redacted]	...		0	✓ ✓		!	● 15:37:52 08.02.20	Administrator	● Positive Co...	☎
☑		[redacted]	[redacted]	...		0			!	● 13:41:41 07.28.20	MonitoredRepo	● Positive Co...	
☑		[redacted]	[redacted]	...		0	✓ ✓		✓	● 09:35:05 08.04.20	Administrator	● Positive Co...	☎ @
☑		[redacted]	[redacted]			0	⊖ ⊖		!	● 14:58:01 07.23.20	Administrator	● At Work	
☐		[redacted]	[redacted]			0	⊖		!		Administrator	●	☎ @

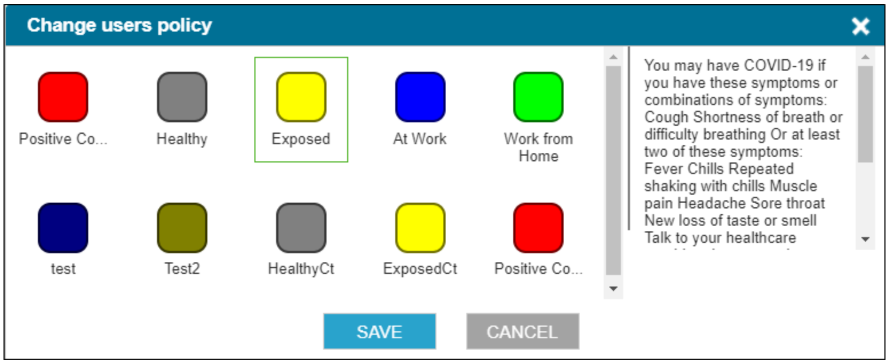
3. Select the **Bulk Users** icon on the panel toolbar.



4. Click **Change user policy**.



The **Change users policy** window opens.



You may have COVID-19 if you have these symptoms or combinations of symptoms: Cough Shortness of breath or difficulty breathing Or at least two of these symptoms: Fever Chills Repeated shaking with chills Muscle pain Headache Sore throat New loss of taste or smell Talk to your healthcare

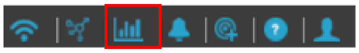
5. Select the policy you want to change the users too. A green box appears around the policy.
6. Click **Save**.

Monitoring Policies

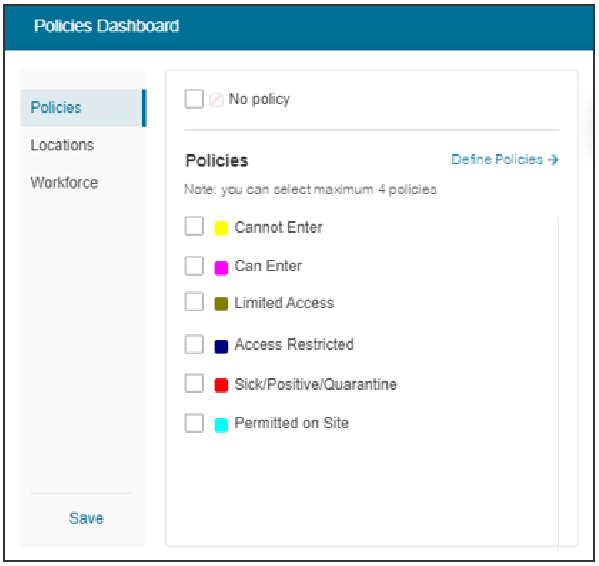
This section sets out the steps required by the Administrator to monitor policies in NowForce.

▼ To monitor a policy

1. On the task bar, in the upper right corner of the **Dispatcher** screen. Select the Dashboard icon.



2. Select the **Policies** option and the **Policies Dashboard** opens.



Policies Dashboard

□ No policy

Policies

Note: you can select maximum 4 policies

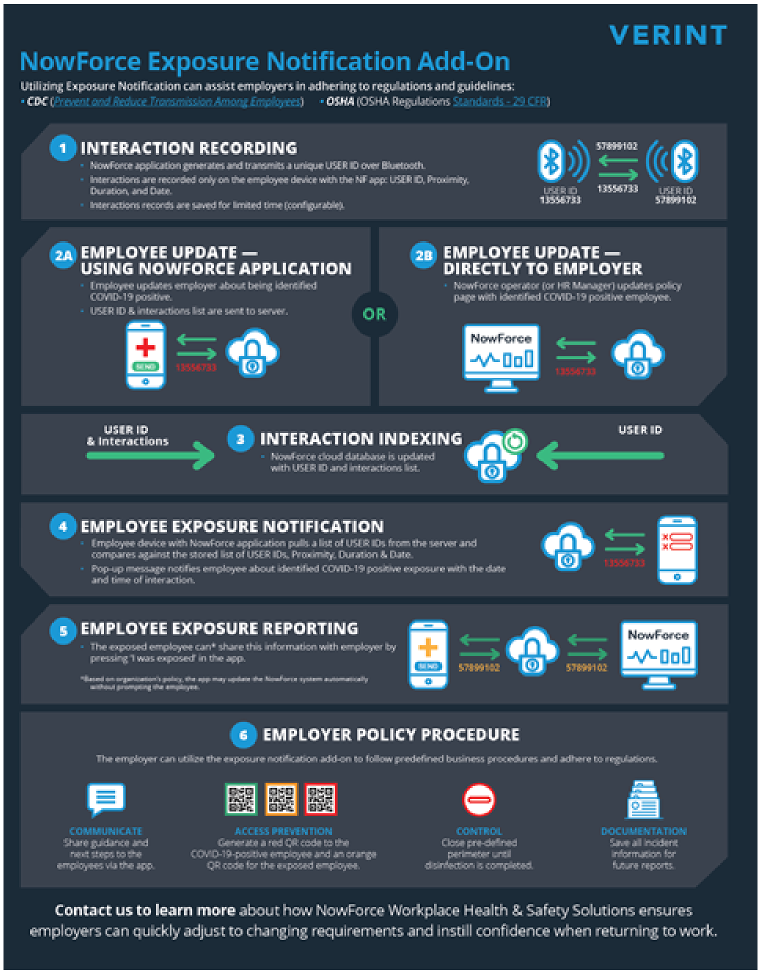
- □ 🟨 Cannot Enter
- □ 🟪 Can Enter
- □ 🟫 Limited Access
- □ 🟦 Access Restricted
- □ 🟥 Sick/Positive/Quarantine
- □ 🟦 Permitted on Site

The number of users in each policy appears on the right hand side. You can also view policy related **Locations** (geofences) and the **Workforce** settings.

Add-On Feature BT (Bluetooth) Exposure Notification

BT (Bluetooth) Exposure Notification (Contact Tracing) is an add-on installed as part of the NowForce Mobile App. The BT Exposure Notification requires users to have a license of monitored reporter or higher functionality. The BT Exposure Notification utilizes Bluetooth to provide accurate measurements of interaction (intersection) between employees' mobile devices. To ensure user privacy, mobile devices are identified by a NowForce Anonymous ID.

> Note
>
> - BT Exposure Notification works with the Android app in the background.
> - The iOS app can be in the background to receive and register other devices, but must be in foreground in order to transmit the NAI (NowForce Anonymous ID).



VERINT

NowForce Exposure Notification Add-On

Utilizing Exposure Notification can assist employers in adhering to regulations and guidelines:

- CDC (Prevent and Reduce Transmission Among Employees)
- OSHA (OSHA Regulations Standards - 29 CFR)

1 INTERACTION RECORDING

- NowForce application generates and transmits a unique USER ID over Bluetooth.
- Interactions are recorded only on the employee device with the NF app: USER ID, Proximity, Duration, and Date.
- Interactions records are saved for limited time (configurable).

2A EMPLOYEE UPDATE — USING NOWFORCE APPLICATION

- Employee updates employer about being identified COVID-19 positive.
- USER ID & interactions list are sent to server.

OR

2B EMPLOYEE UPDATE — DIRECTLY TO EMPLOYER

- NowForce operator (or HR Manager) updates policy page with identified COVID-19 positive employee.

3 INTERACTION INDEXING

- NowForce cloud database is updated with USER ID and interactions list.

4 EMPLOYEE EXPOSURE NOTIFICATION

- Employee device with NowForce application pulls a list of USER IDs from the server and compares against the stored list of USER IDs, Proximity, Duration & Date.
- Pop-up message notifies employee about identified COVID-19 positive exposure with the date and time of interaction.

5 EMPLOYEE EXPOSURE REPORTING

- The exposed employee can* share this information with employer by pressing 'I was exposed' in the app.

*Based on organization's policy, the app may update the NowForce system automatically without prompting the employee.

6 EMPLOYER POLICY PROCEDURE

The employer can utilize the exposure notification add-on to follow predefined business procedures and adhere to regulations.

COMMUNICATE
Share guidance and next steps to the employees via the app.

ACCESS PREVENTION
Generate a red QR code to the COVID-19-positive employee and an orange QR code for the exposed employee.

CONTROL
Close pre-defined perimeter until disinfection is completed.

DOCUMENTATION
Save all incident information for future reports.

Contact us to learn more about how NowForce Workplace Health & Safety Solutions ensures employers can quickly adjust to changing requirements and instill confidence when returning to work.

A typical BT Exposure Notification workflow in the NowForce system is described in the sequence below:

1. The user installs the NowForce Mobile App and a NowForce Anonymous ID (NAI) is automatically generated by the system and assigned to their mobile device.
2. The Administrator purchases BT EN (Bluetooth Exposure Notification) licenses and adds to the Profiles.
3. The Administrator applies the Profiles to Users and adds them to a BT Exposure Notification enabled Policy.
4. The User submits a User Update via the NowForce Mobile App indicating Covid-19 positive status.
5. Their response triggers an automatic BT exposure match review of the user's NAI and all other employees NAIs.
6. Discovered exposure matches receive an automated anonymous notification message from the NowForce system alerting them to their potential exposure.

7. The potentially exposed employees can share this information by sending a User Update in NowForce Mobile App and this can subsequently trigger a policy transition.
8. The user remains in this new policy until either sending a further update from their NowForce Mobile App or if a predefined time has expired (in which case the policy can switch to a "Healthy" or "Allowed to Enter" policy).