Dynamic IP Whitelist

Monitor is a web-based application which by default can be accessed over the internet from anywhere, including mobile data networks; Organisations may wish to restrict to networks within their control.

One option available to do this and keep both Monitor and the Care app secure, is to Maintain the permitted IP addresses dynamically using the Care app and location tags. The Dynamic IP whitelist ensures secure access to Monitor is maintained, by logging the location IP addresses through using the NFC tags with the Care app.

In addition, this feature can also secure access to the Care App from outside the location, by ensuring a Location tag is required to login.

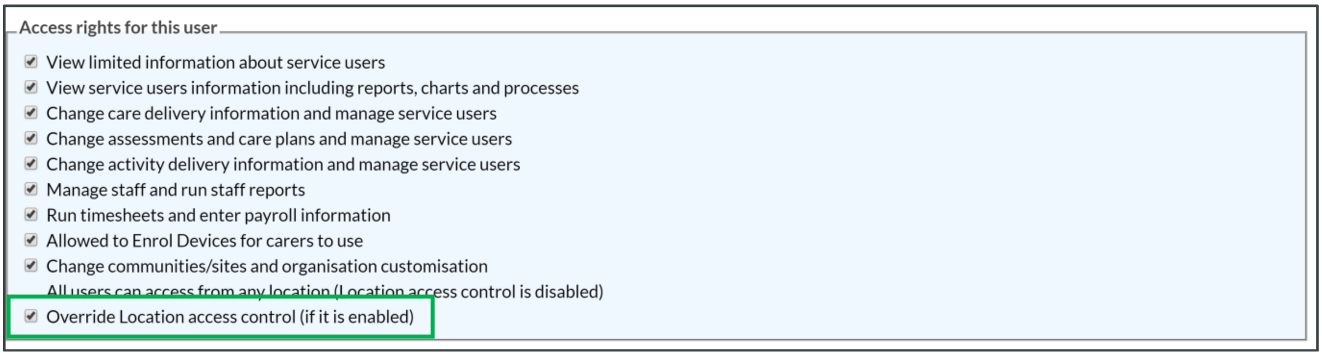
Note: this is separate to restricting access to the Care App using a static IP.

Considerations when deciding how to restrict access from IP address

There are various considerations you will need to make when deciding which option(s) to choose. The following are a list of factors you may wish to consider:

- Do the locations where access is required have static IP addresses?
- What are the contingencies when the primary network is unavailable (e.g. often homes may tether from mobile data if their organisations network connectivity is down)?
- Do any of your team need to access the system remotely (e.g. from home networks)?
- Will your internal IT team be able to provision any changes to the whitelist when required?
- Are there any exceptions to the rule(s)?
- Mobile devices generate a different IP address each login, which can cause problems if on a 4G network and not using the organisation's network.
- Are you accessing Monitor on a different network to the Care App i.e. via a VPN or using a Wifi Dongle? The IP addresses for the Dynamic IP Whitelist are stored when logging in to the Care App. Therefore, if you are not using Monitor on the same network as the Care App, this feature should not be used.

If the whitelist functionality is enabled, it is possible to override this setting at an Employee record level by enabling the **Override Location access control** setting. This will ensure that the Employee can log on from their device without the requirement of being on the whitelist.



Access rights for this user

☑ View limited information about service users
☑ View service users information including reports, charts and processes
☑ Change care delivery information and manage service users
☑ Change assessments and care plans and manage service users
☑ Change activity delivery information and manage service users
☑ Manage staff and run staff reports
☑ Run timesheets and enter payroll information
☑ Allowed to Enrol Devices for carers to use
☑ Change communities/sites and organisation customisation
All users can access from any location (Location access control is disabled)
☑ Override Location access control (if it is enabled)

It is essential to ensure that Admin users, users that need to access Monitor from home, or those that are "on-the-road", such as regional managers, owners, or out-of-hours IT support that may be carried out from outside the corporate network, have this setting enabled in their worker record. This setting must enabled before the IP Whitelist settings are turned on, to make sure there are users who can access Monitor at all times.

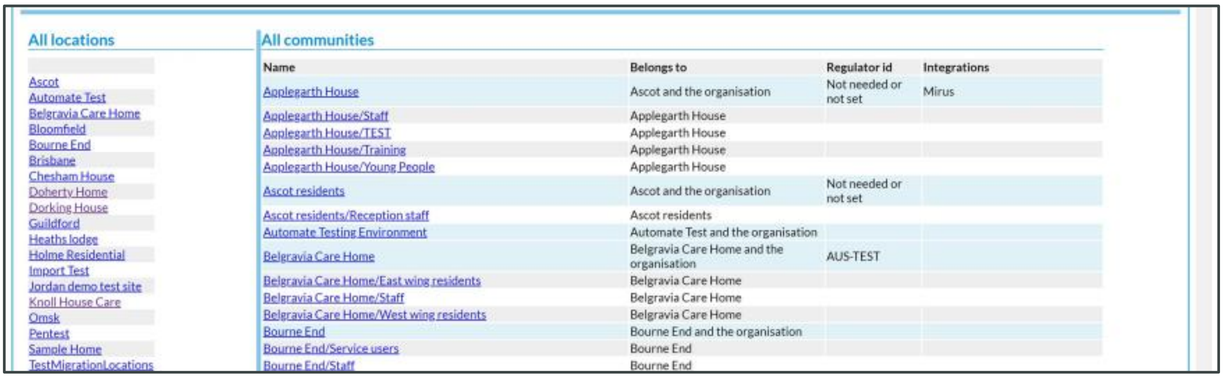
Maintain the permitted IP addresses dynamically using the Care app and location tags

The list of IP addresses can be automatically maintained, by enabling location tags to verify the network when a worker logs in to the Care app on their device, at an approved location.

For more information on NFC, please see **Appendix 1** at the bottom of this document.

Before enabling the new **Use dynamic IP whitelist for Monitor** setting, you must first start registering Location Tags on a device. These Location Tags will ensure the IP addresses for the location are added to the dynamic IP whitelist and validates the login to Monitor. To add the Location tags, the user registering the tags will need to ensure they are a **Manager** at the location the tags are being written against.

To check this, go to the **Admin** menu**,** click **Organisation details,** select the main community for that Location and click **Add person** against the **Manager** section.

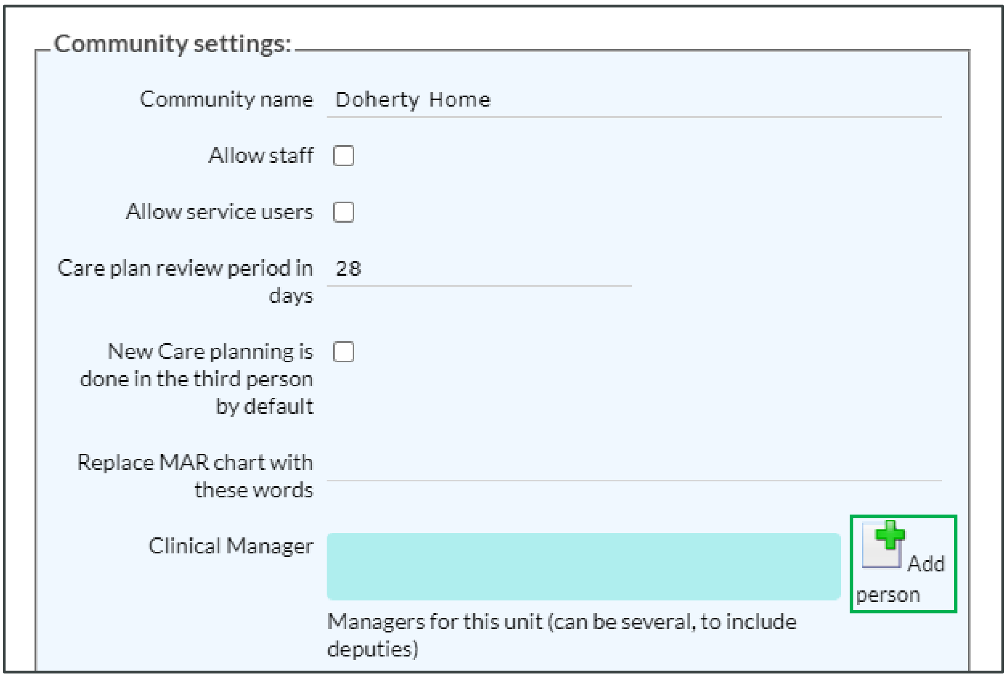


All locations

Ascot
Automate Test
Belgravia Care Home
Bloomfield
Bourne End
Brisbane
Chesham House
Doherty Home
Dorking House
Guildford
Heaths lodge
Holme Residential
Import Test
Jordan demo test site
Knoll House Care
Omsk
Pentest
Sample Home
TestMigrationLocations

All communities

Name	Belongs to	Regulator id	Integrations
Applegarth House	Ascot and the organisation	Not needed or not set	Mirus
Applegarth House/Staff	Applegarth House		
Applegarth House/TEST	Applegarth House		
Applegarth House/Training	Applegarth House		
Applegarth House/Young People	Applegarth House		
Ascot residents	Ascot and the organisation	Not needed or not set	
Ascot residents/Reception staff	Ascot residents		
Automate Testing Environment	Automate Test and the organisation		
Belgravia Care Home	Belgravia Care Home and the organisation	AUS-TEST	
Belgravia Care Home/East wing residents	Belgravia Care Home		
Belgravia Care Home/Staff	Belgravia Care Home		
Belgravia Care Home/West wing residents	Belgravia Care Home		
Bourne End	Bourne End and the organisation		
Bourne End/Service users	Bourne End		
Bourne End/Staff	Bourne End		



Community settings:

Community name Doherty Home

Allow staff □

Allow service users □

Care plan review period in days 28

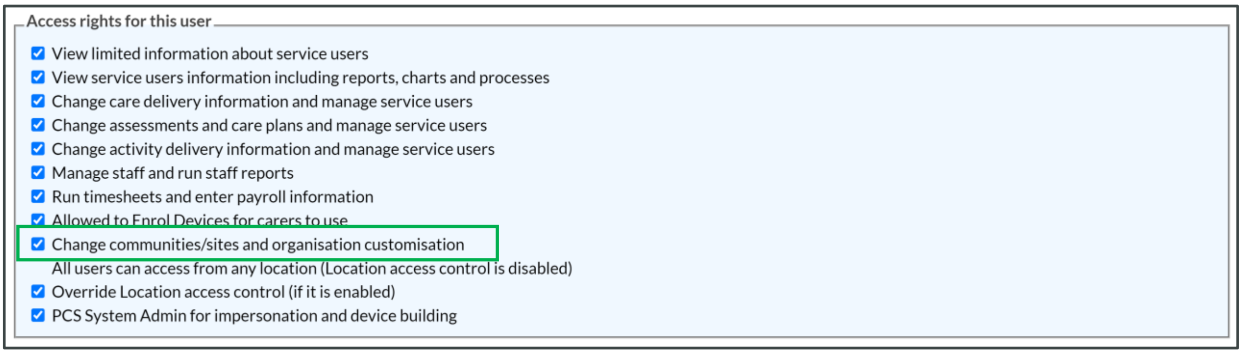
New Care planning is done in the third person by default □

Replace MAR chart with these words

Clinical Manager

Managers for this unit (can be several, to include deputies)

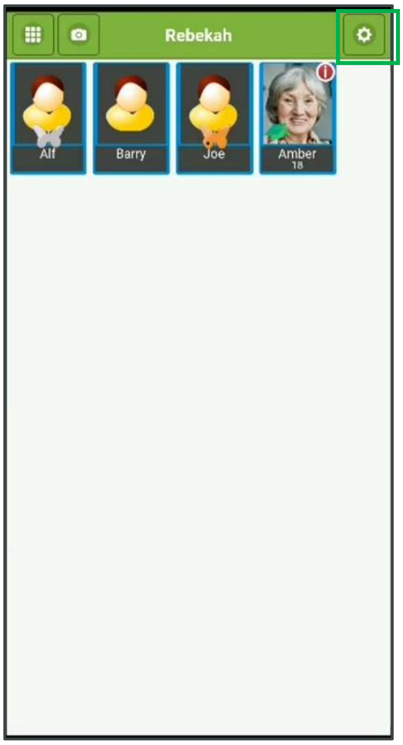
Note: In order view the **Organisation details** page, you must have the **change communities and organisation customisation** Access rights enabled on your Worker file.



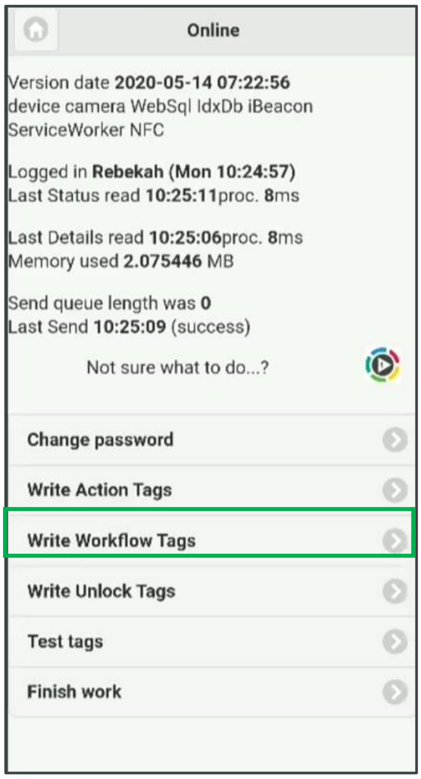
Access rights for this user

- ☑ View limited information about service users
- ☑ View service users information including reports, charts and processes
- ☑ Change care delivery information and manage service users
- ☑ Change assessments and care plans and manage service users
- ☑ Change activity delivery information and manage service users
- ☑ Manage staff and run staff reports
- ☑ Run timesheets and enter payroll information
- ☑ Allowed to Enrol Devices for carers to use
- ☑ Change communities/sites and organisation customisation
- All users can access from any location (Location access control is disabled)
- ☑ Override Location access control (if it is enabled)
- ☑ PCS System Admin for impersonation and device building

Once the user is set as a **Manager,** login into the Care app and click on the settings icon at the top right-hand side of the screen.



Within the Care app settings, click on **Write Workflow Tags**, which will enable you to write the new Location tags.



Online

Version date **2020-05-14 07:22:56**
device camera WebSql IdxDb iBeacon
ServiceWorker NFC

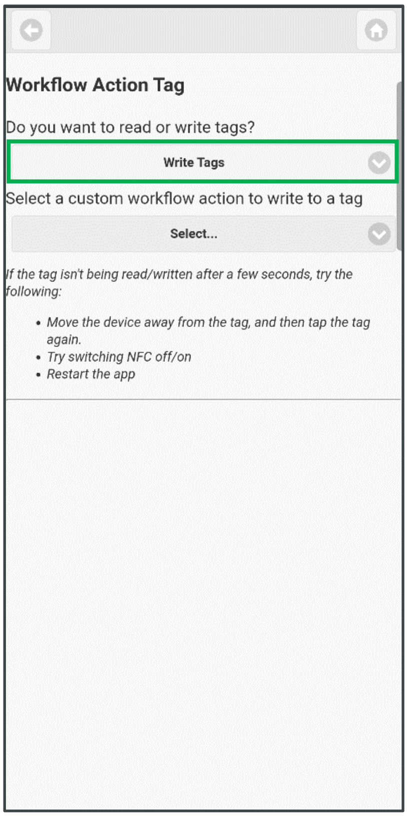
Logged in **Rebekah (Mon 10:24:57)**
Last Status read **10:25:11**proc. **8**ms

Last Details read **10:25:06**proc. **8**ms
Memory used **2.075446** MB

Send queue length was **0**
Last Send **10:25:09** (success)

Not sure what to do...?

To write a Location Tag, ensure the **Do you want to read or write tags?** drop-down is set to **Write Tags**. Then on the **Select a custom workflow action to write a tag** drop-down, there are three available options, select the **Location Unlock** option to write a Location tag.



Workflow Action Tag

Do you want to read or write tags?

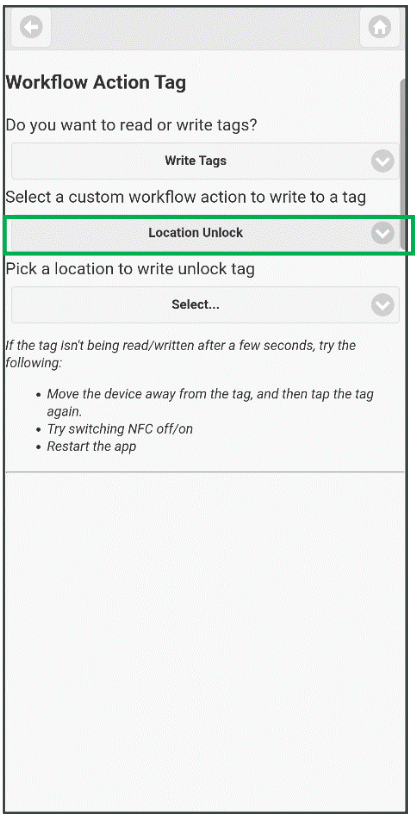
Write Tags

Select a custom workflow action to write to a tag

Select...

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*



Workflow Action Tag

Do you want to read or write tags?

Write Tags

Select a custom workflow action to write to a tag

Location Unlock

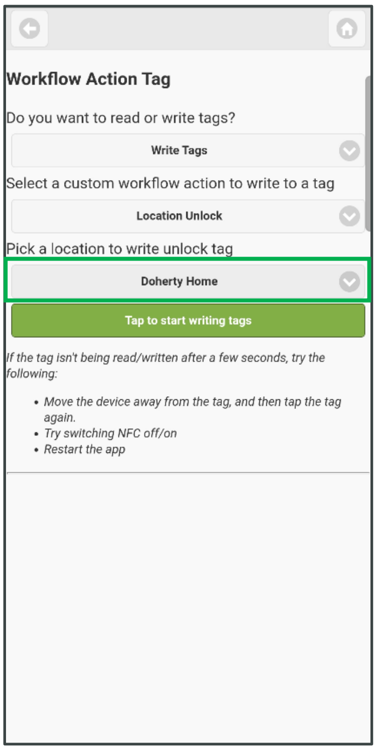
Pick a location to write unlock tag

Select...

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*

When the **Location Unlock** option has been selected, an additional drop-down will be visible called **Pick a location to write unlock tag;** select the location you wish to write the tags to.



Workflow Action Tag

Do you want to read or write tags?

Write Tags

Select a custom workflow action to write to a tag

Location Unlock

Pick a location to write unlock tag

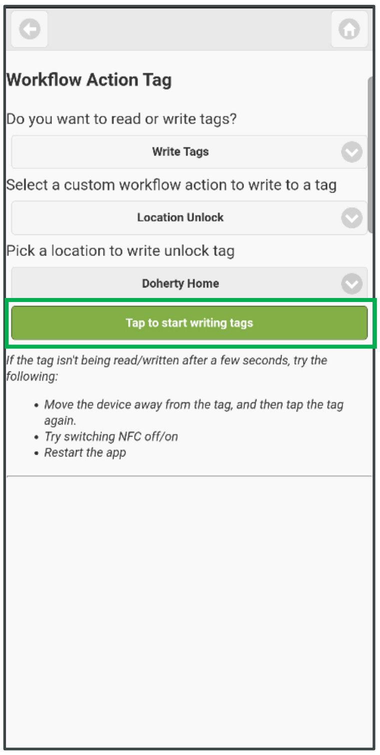
Doherty Home

Tap to start writing tags

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*

Once the location is selected, the option to start writing tags will be visible.



Workflow Action Tag

Do you want to read or write tags?

Write Tags

Select a custom workflow action to write to a tag

Location Unlock

Pick a location to write unlock tag

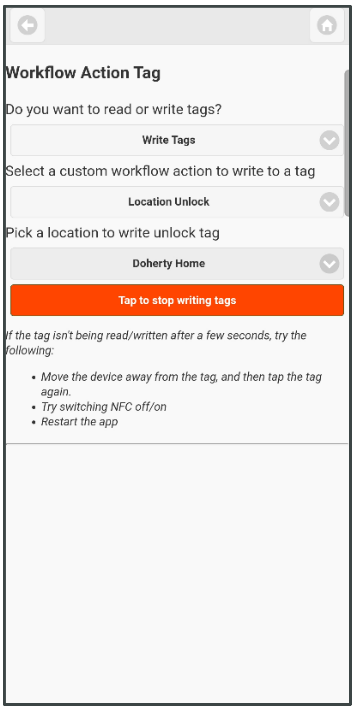
Doherty Home

Tap to start writing tags

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*

Location tags are not worker specific and therefore several Location Tags can be written at Once, to do this tap on the green button which displays **Tap to start writing tags**, which will then change to a red **Tap to stop writing tags** button. From here, hold the NFC tag against the mobile device until **Tap to stop writing tags (1 processed)** is displayed. You can remain in Write mode and continue to write additional tags if required (the processed number will increment each time the process is successful).



Workflow Action Tag

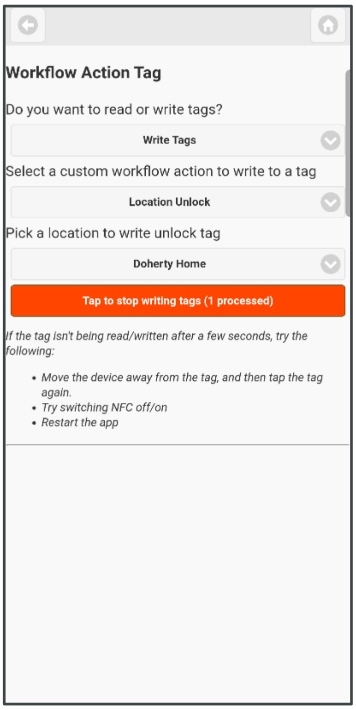
Do you want to read or write tags?

Select a custom workflow action to write to a tag

Pick a location to write unlock tag

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*



Workflow Action Tag

Do you want to read or write tags?

Select a custom workflow action to write to a tag

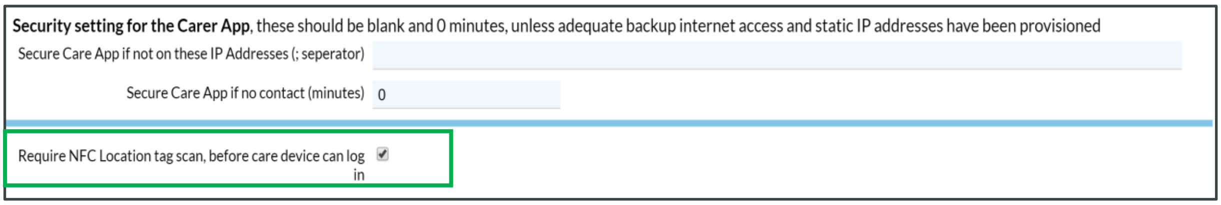
Pick a location to write unlock tag

If the tag isn't being read/written after a few seconds, try the following:

- *Move the device away from the tag, and then tap the tag again.*
- *Try switching NFC off/on*
- *Restart the app*

Once the Location tag has been written tap the **Tap to stop writing tags** button again to come out of Write mode; log out of the Care app and go back to the login screen.

To use the location tags when logging in to the Care app, you must then enable the Location tag setting, by going to the **Admin** menu, click **Organisation details,** select the location you have registered the tags against and check **Require NFC Location tag scan, before care device can log in.**



Security setting for the Carer App, these should be blank and 0 minutes, unless adequate backup internet access and static IP addresses have been provisioned

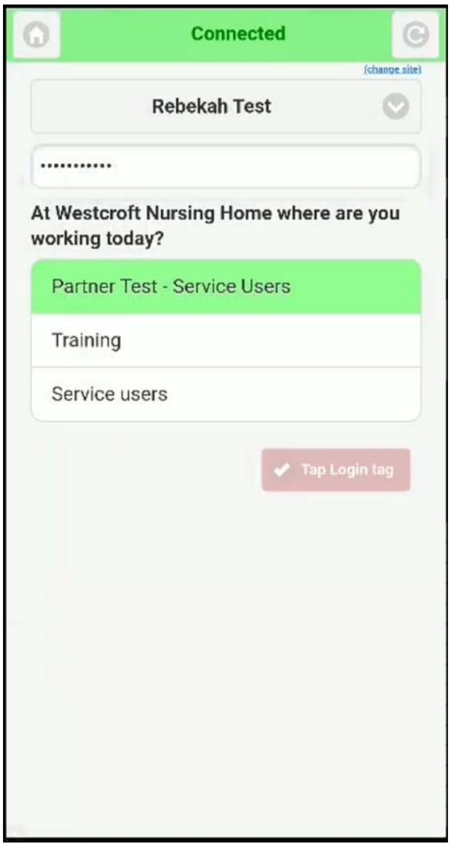
Secure Care App if not on these IP Addresses (; seperator)

Secure Care App if no contact (minutes) 0

Require NFC Location tag scan, before care device can log in ☑

With the new Location tag configured and the setting enabled the login workflow to the Care app will appear slightly different. Before being able to login, you will need to tap the Location tag against the device, after selecting your name and entering your password.

If the Location tag has been successfully recognised, the red **tap login tag** button will change to **Start work** and you will be able to login as normal.



Connected

(change site)

Rebekah Test

•••••••••••

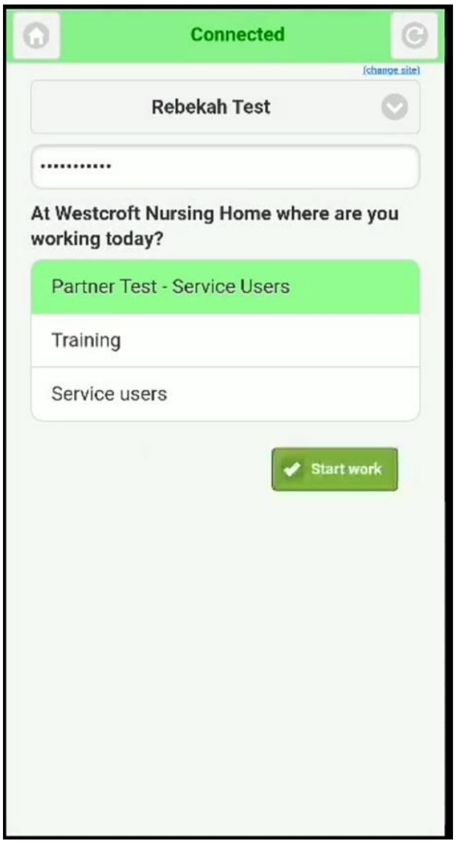
At Westcroft Nursing Home where are you working today?

Partner Test - Service Users

Training

Service users

✓ Tap Login tag



Connected

(change site)

Rebekah Test

•••••••••••

At Westcroft Nursing Home where are you working today?

Partner Test - Service Users

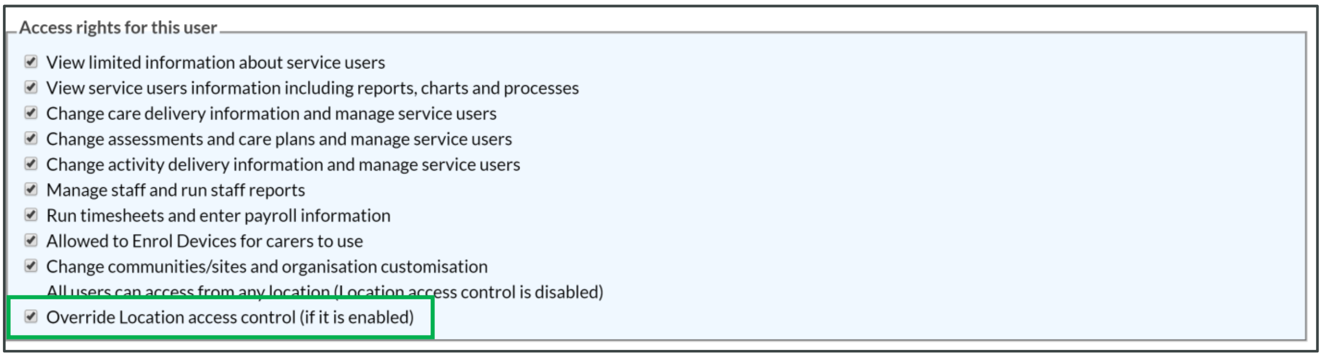
Training

Service users

✓ Start work

Now the Location tags have been written, it is recommended to wait two to three days before turning on the dynamic IP whitelist function. This is to ensure that once the dynamic IP whitelist setting is enabled, the Location's IP addresses logged in the whitelist are validated as being obtained from the Care App using the Location Tags and are therefore secure.

It is possible to override the IP address restrictions at a worker record level, by enabling the **Override Location access control** setting. This will ensure that the worker can log on from their device without the requirement of being on the whitelist.

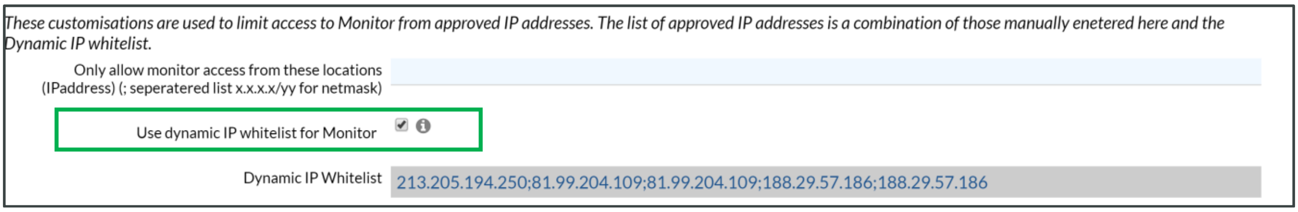


Access rights for this user

☑ View limited information about service users
☑ View service users information including reports, charts and processes
☑ Change care delivery information and manage service users
☑ Change assessments and care plans and manage service users
☑ Change activity delivery information and manage service users
☑ Manage staff and run staff reports
☑ Run timesheets and enter payroll information
☑ Allowed to Enrol Devices for carers to use
☑ Change communities/sites and organisation customisation
All users can access from any location (Location access control is disabled)
☑ Override Location access control (if it is enabled)

It is essential that Admin users and workers who need to access Monitor on the road have this setting enabled in their worker record, before enabling the **Use dynamic IP Whitelist for Monitor;** to make sure there are Users who can access Monitor at all times.

The new setting for Dynamic IP addresses can now be enabled, by going to the **Admin** menu, click **Organisation details,** click **Customisation** and tick **Use dynamic IP Whitelist for Monitor.**



These customisations are used to limit access to Monitor from approved IP addresses. The list of approved IP addresses is a combination of those manually enetered here and the Dynamic IP whitelist.

Only allow monitor access from these locations (IPaddress) (; seperatered list x.x.x.x/yy for netmask)

Use dynamic IP whitelist for Monitor ☑

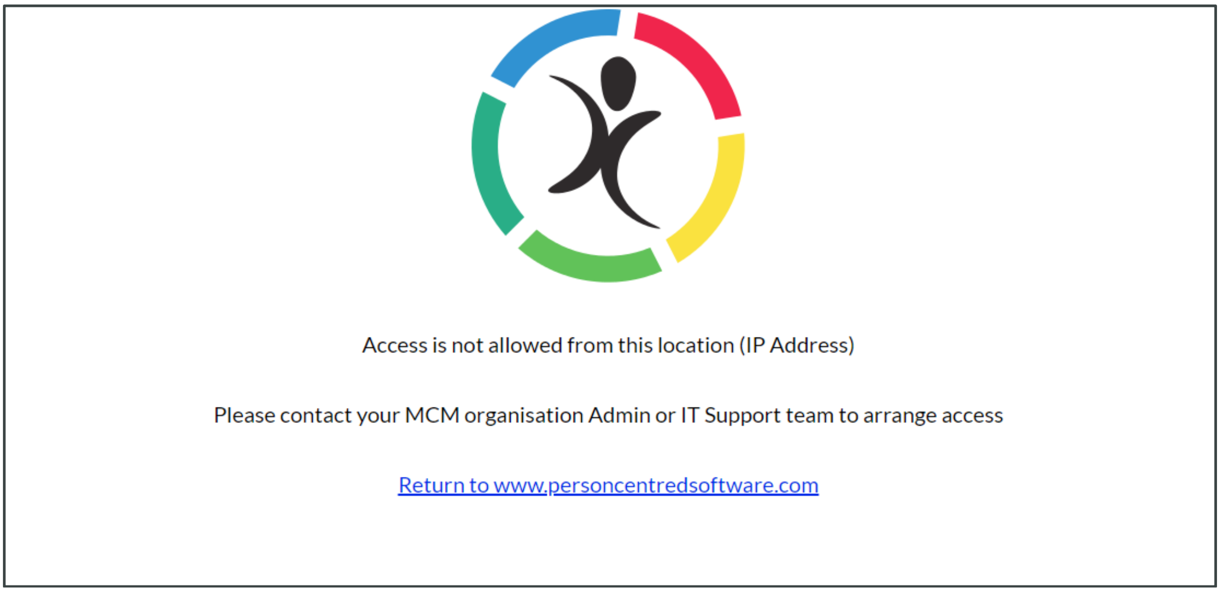
Dynamic IP Whitelist 213.205.194.250;81.99.204.109;81.99.204.109;188.29.57.186;188.29.57.186

When using the Location tag to login to the Care app, Monitor will register the dynamic IP from the worker’s device to that Location and will store the IP address in the **Dynamic IP Whitelist** field in Monitor. The IP addresses will only get written to the whitelist upon login, however people already on shift will still be able to continue to work, whilst the setup is being completed.

Note: If the NFC tag is damaged or lost, simply login to Monitor and turn off the Location tag setting and the Care App can be accessed again.

Any dynamic IP address which have been added to the whitelist will expire after 3 days; this is for data security reasons to ensure any unused devices, or staff leavers cannot access the Care app.

If a user attempts to access Monitor from a device which is not listed in the whitelist, the following message will be displayed.



Access is not allowed from this location (IP Address)

Please contact your MCM organisation Admin or IT Support team to arrange access

Return to www.personcentredsoftware.com

It will be possible to use the Dynamic IP whitelist alongside the two other IP whitelist options if required.

- The **Only allow monitor access from these locations** setting ensures that a specific location such as Head Office will always authenticate. This setting enables an internal IT team to manually set a list of IP addresses, which ensures that only devices on the specified whitelisted IP addresses can access Monitor.

- The **Secure Care App if not on these IP Addresses** setting will make sure only devices within the Organisation’s network, will be able to access the Care App. If this setting is used in conjunction with the Dynamic IP whitelist, devices will use the Care App static

IP setting to determine whether the Care App can be accessed and login will not be overwritten by the Dynamic IP whitelist.

Note: if you wish to know more about the other whitelist options available, please contact client success

Information Governance

Information governance is a key part to any digital solution being implemented in a care setting. Access to information at the point of care is essential to providing the best possible care to the people you support, but as information held on devices is sensitive, protecting this data from access by unauthorised people is equally as important.

The Dynamic IP Whitelist feature keeps information secure and provides evidence of meeting IG requirements, such as the CQC's KLOE Well-Led 2.8

KLOEs	Description
W2.8	How does the service assure itself that it has robust arrangements (including appropriate internal and external validation) to ensure the security, availability, sharing and integrity of confidential data, and records and data management systems, in line with data security standards? Are lessons learned when there are data security breaches?

Appendix 1

What is NFC?

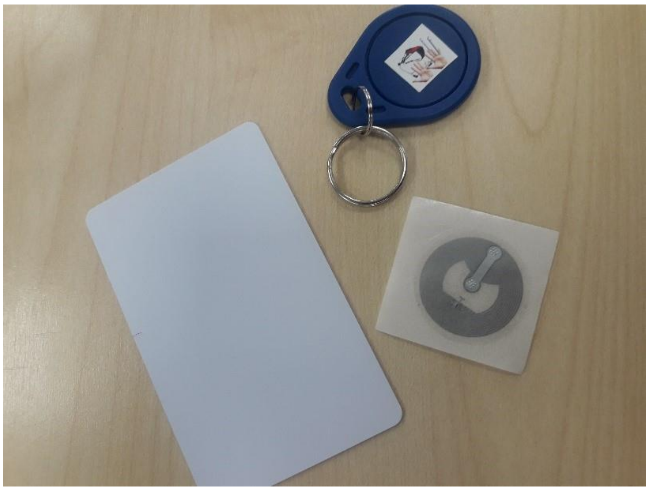
NFC stands for “Near Field Communication” and is the same technology that contactless payments use on your bank card or phone.

MCM uses NFC technology to read and write tags that are programmed for use with the Dynamic IP Whitelist feature.

What you’ll need?

- Android devices that support the use of NFC
- Choose the type of NFC tags that meet your needs
- Programme the tags as “Location tags”
- Each person working on shift will need to scan the tag when logging on to the Care App

What types of tags are there?



There are a range of tags available from amazon or other retailers online, and much will depend on what use cases you plan to implement as to the form of tag you decide to use. For instance, some come as stickers, some tags can be painted over, some CANT be used on metal services, some come with tamper proof measures that destroy the tag if removed, key-fobs, cards and even wearable ones.

IMPORTANT: The main requirement of the tags for use with MCM devices is that they are to **NTAG216** specification.