

Restricting access to Monitor & Care App based on IP Address

Monitor and the Care App are applications that by default can be accessed over the internet from anywhere, including mobile data networks, therefore Organisations may wish to restrict to networks within their control.

A couple of options available to do this and keep both Monitor and the Care app secure, is to specify the permitted list of the organisation's IP addresses that Monitor or Care App access is allowed from.

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.

If any of 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

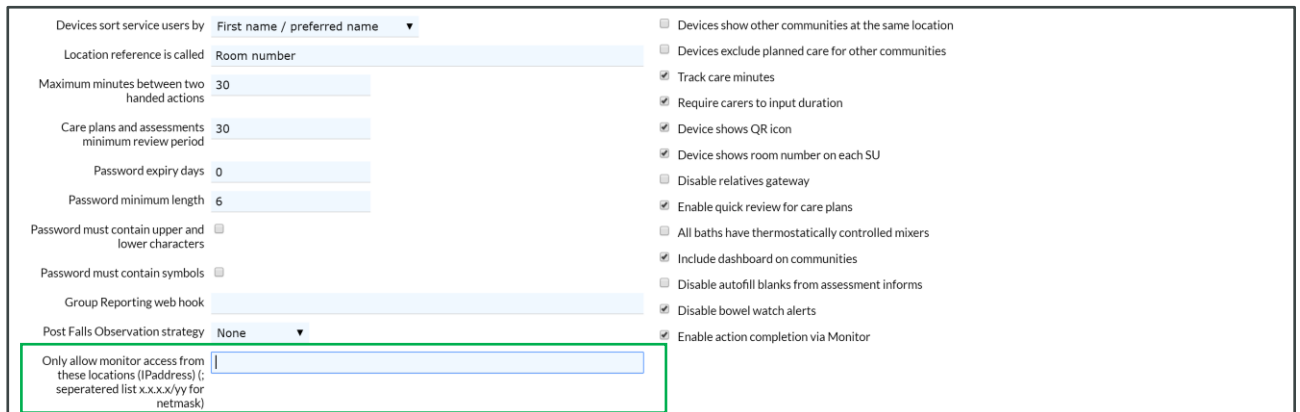
- ☒ View limited information about service users
- ☒ View service users information including reports, charts and processes
- ☒ Change care delivery information and manage service users
- ☒ Change assessments and care plans and manage service users
- ☒ Change activity delivery information and manage 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 be enabled before the IP Whitelist settings are turned on, to make sure there are users who can access Monitor at all times.

Specify the list of IP addresses that Monitor access is allowed from

This option 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.

To enable this option, go to the **Admin** menu, click **Organisation details**, and select the **Customisation** link. From within the Organisation customisation, there is the option to **Only allow monitor access from these locations (IP addresses)**.



Devices sort service users by: First name / preferred name ▼

Location reference is called: Room number

Maximum minutes between two handed actions: 30

Care plans and assessments minimum review period: 30

Password expiry days: 0

Password minimum length: 6

Password must contain upper and lower characters: ☐

Password must contain symbols: ☐

Group Reporting web hook:

Post Falls Observation strategy: None ▼

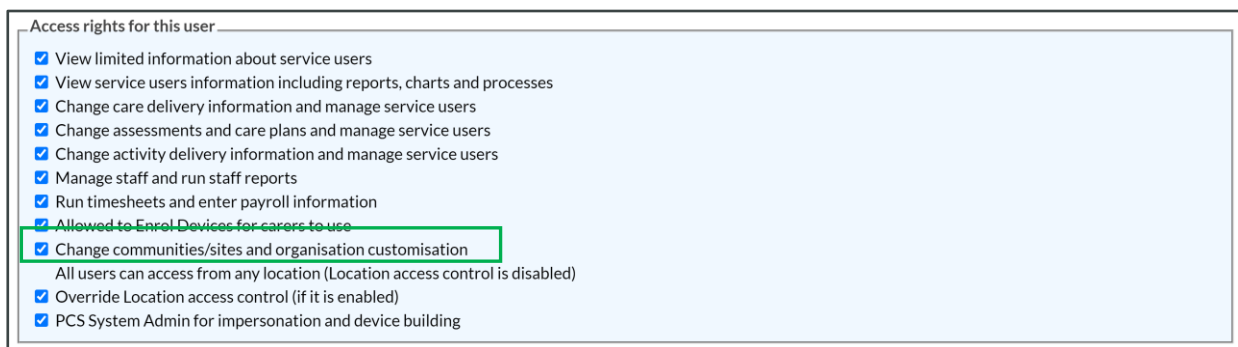
Only allow monitor access from these locations (IP address) ('; seperated list x.x.x.x/yy for netmask):

☐ Devices show other communities at the same location
☐ Devices exclude planned care for other communities
☒ Track care minutes
☒ Require carers to input duration
☒ Device shows QR icon
☒ Device shows room number on each SU
☐ Disable relatives gateway
☒ Enable quick review for care plans
☐ All baths have thermostatically controlled mixers
☒ Include dashboard on communities
☐ Disable autofill blanks from assessment informs
☒ Disable bowel watch alerts
☒ Enable action completion via Monitor

The external IP address for each location you wish to restrict access to, should be added here. Only the IP addresses added in this field, will then be able to access Monitor on a device within the Organisation's network. The list of IP addresses will need to be maintained manually to ensure any new locations are included in the list.

If you do not have an internal IT Team or individual who can manually manage your IP addresses, but still wish to have the option to restrict access to Monitor to your network, then please see the Dynamic IP Whitelist feature documentation.

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

Restricting Care App access from whitelisted IP addresses

In addition to restricting access to Monitor, it is also possible to restrict access to the Care App by including a list of whitelisted IP address to ensure the Care App cannot be accessed outside of the Organisation's allowed networks.

To use this feature, go to **Admin**, click **Organisation details**, select the location you wish to enable this feature against and enter the IP Addresses in the **Secure Care App if not on these IP Addresses** field.

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 (; separator)	
Secure Care App if no contact (minutes)	0
Require NFC Location tag scan, before care device can log in <input checked="" type="checkbox"/>	

Only the IP addresses added in this field, will be able to access the Care App on a device within the Organisation's network. The list of IP addresses will need to be maintained manually to ensure any new locations are included in the list.

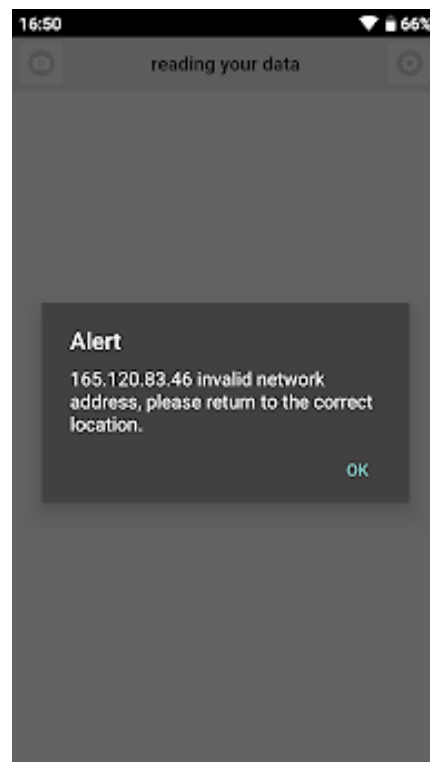
Note: Please ensure you have sufficient wifi coverage and static IP addresses at the Location before using this feature. As previously mentioned, mobile devices generate a different IP address each login, which can cause problems if on a 4G network and not using the organisation's network.

There is also a secondary option within this page to **Secure Care App if no contact (minutes)**.

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 (; separator)	
Secure Care App if no contact (minutes)	0
Require NFC Location tag scan, before care device can log in <input checked="" type="checkbox"/>	

This ensures that if there is an area at the location which does not have an internet connection, the Care App can be used for the number of minutes specified. Once past that time, the Care App will display a blank screen on the Resident page until a connection can be re-established.

If the mobile device is taken outside of the confines of the Organisation's network (e.g. accidentally taken home), users will be able to connect to the Care App from any network connection. Therefore, to prevent this happening, using the **Secure Care App if not on these IP Addresses** setting limits access to your data from authorised networks only.



Once the device has reconnected with the server either through the Organisation's whitelisted IP Address or establishing an internet connection, the device will establish a connection and the carer can continue to use the Care App.

If this setting is used in conjunction with the Dynamic IP whitelist (see the Dynamic IP Whitelist documentation), the Care App will use the Care App static IP setting to determine whether the Care App can be used and access will not be overwritten by the Dynamic IP whitelist.

Note: These features can also be used together with the NFC Location Tags.

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 and on computers is sensitive, protecting this data from access by unauthorised people is equally as important.

The security and audit features keep information secure and provides evidence of meeting IG requirements, such as the following CQC KLOEs.

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?