Protege Mobile Solution

Sales Enablement Kit

Protege Mobile Solution **Overview**

ICT's mobile solution complements your existing access control system by enabling secure access via an Android or iOS device.

Protege Mobile Solution **Components**

There are 3 key components to the mobile solution:

ICT tSec readers: with Bluetooth (BLE) support and optional NFC support for Android

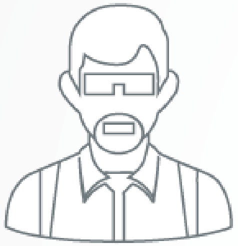
Protege Mobile App: free to download from the Apple Store (iOS) or Google Play (Android)

Mobile Credentials: virtual credentials that provide card-free access via Android and iOS devices

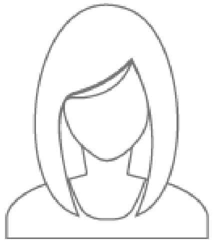
There are also 2 new tools for integrators encompassing everything necessary to deploy a mobile solution for small, medium or enterprise-sized organizations:

- **Reader Configuration App**: configures Bluetooth readers to work with mobile credentials that use an open site code
- **Mobile Credential Management Portal**: that allows you to manage, assign and issue credentials to your customers

Protege Mobile Solution **Overview**



As an **integrator**, Mobile Credentials eliminate the time spent handling physical access cards, and with everything managed online, there’s no shipping so customers can access them immediately. Multiple credentials can be stored on a single device – which is great for those managing multiple sites.



As an **end user**, Mobile Credentials provide the flexibility and added convenience of card-free access from a mobile device. No more issues with lost or forgotten cards and tags. Simply present your smartphone within range of the reader to gain entry. Customize the read range, and you don’t even need to take your phone out of your pocket.

Protege Mobile Solution **Key Benefits**

✓ **Added Efficiency:** Mobile credentials provide a simple, more cost-effective approach to managing access credentials, and eliminates the time and effort involved with handling, printing, distributing and disposing of physical access cards. Ordering, issuing, and management of credentials is all done online, with the credential emailed directly to the end user's mobile device. **Smart.**

✓ **Added security:** Credentials are stored securely on the mobile device, with access authenticated using a secure cloud based server and 256-bit encryption. Given that most people carry their smartphone everywhere, just as they do their car-keys and wallet, mobile credentials are much less likely to be lost or misplaced, and they are usually protected with a passcode or biometric security. **Secure.**

✓ **Added convenience:** Compared to traditional cards and tags, mobile credentials offer a more convenient end user experience by enabling a smartphone or other mobile device to securely unlock doors and enter buildings. With most (if not all) people carrying a smartphone with them every day, it eliminates the need for physical cards, meaning lost and forgotten cards become a thing of the past. **Convenient.**

Protege Mobile Solution Open vs Managed Credentials

Open Credentials

Allow you to specify **any** facility/site code.

Open credentials provide an additional layer of encryption that locks the readers to the credential profile used. This provides an extra level of security by ensuring the credentials can only ever be used on that site.

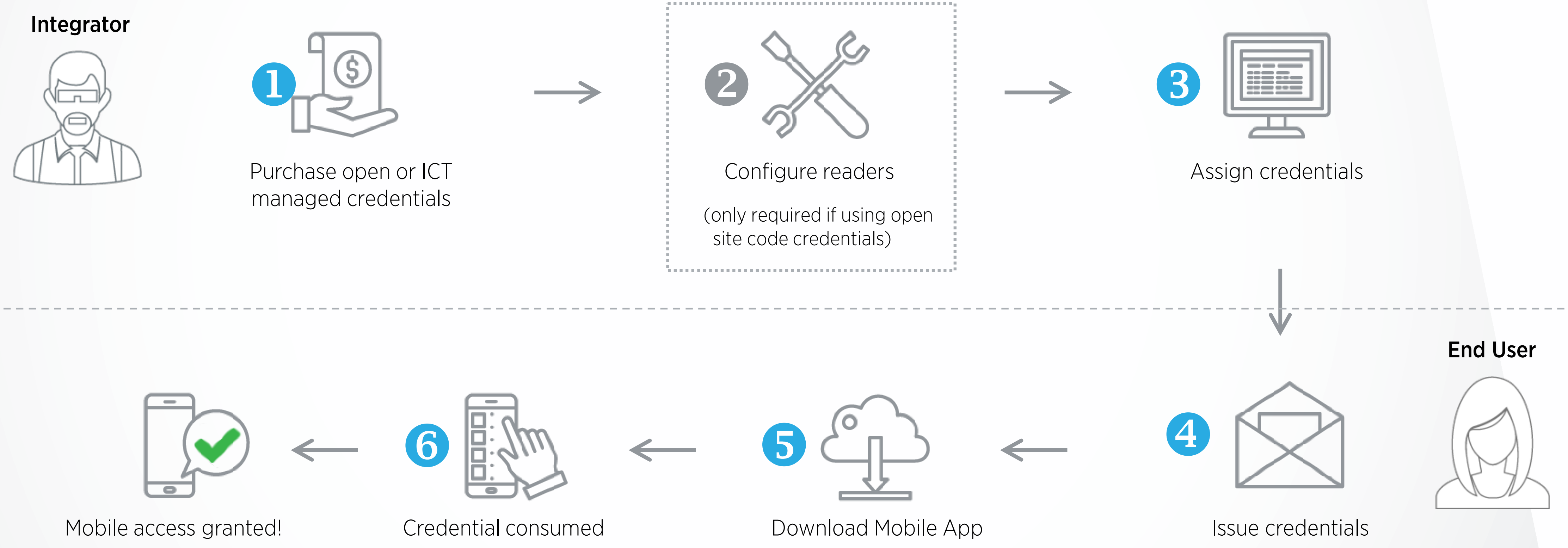
ICT Managed Credentials

Facility/site codes are managed by ICT.

Every site is registered with its own globally unique credential profile, and every credential recorded in our secure database. This ensures that duplicate credentials are never created.

ICT

Protege Mobile Solution The Implementation Process



Integrator

1 Purchase open or ICT managed credentials

2 Configure readers

(only required if using open site code credentials)

3 Assign credentials

End User

4 Issue credentials

5 Download Mobile App

6 Credential consumed

Mobile access granted!

Protege Mobile Solution **The Implementation Process**

1

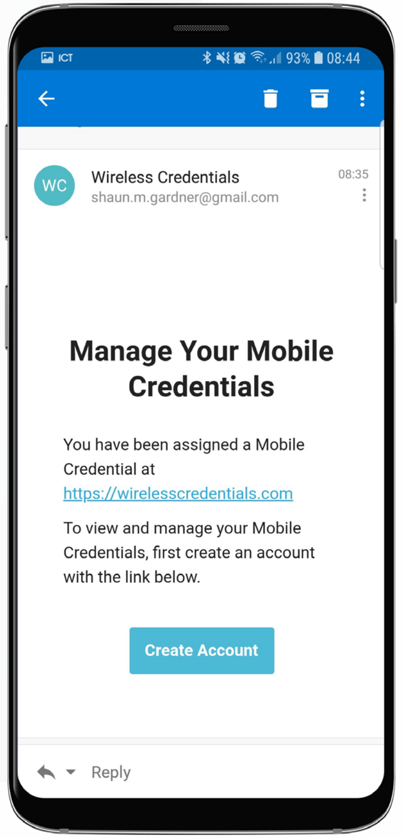
Purchase credentials

Mobile credentials are purchased through your normal distributor or system integrator, just like regular cards and tags – but without the added logistics of handling, printing, and shipping.

Use the order code PRX-MCR, and supply:

- The site name
- Number of credentials required
- Required site code (if using open credentials)
- Email address/es of those who will be managing the credentials

Ordering and management is all done online, so there's no delay in processing. Purchased credentials are loaded into your Mobile Credential Management Portal, ready for you to assign or issue to your customers.



Wireless Credentials
shaun.m.gardner@gmail.com

Manage Your Mobile Credentials

You have been assigned a Mobile Credential at https://wirelesscredentials.com

To view and manage your Mobile Credentials, first create an account with the link below.

Protege Mobile Solution The Implementation Process

2

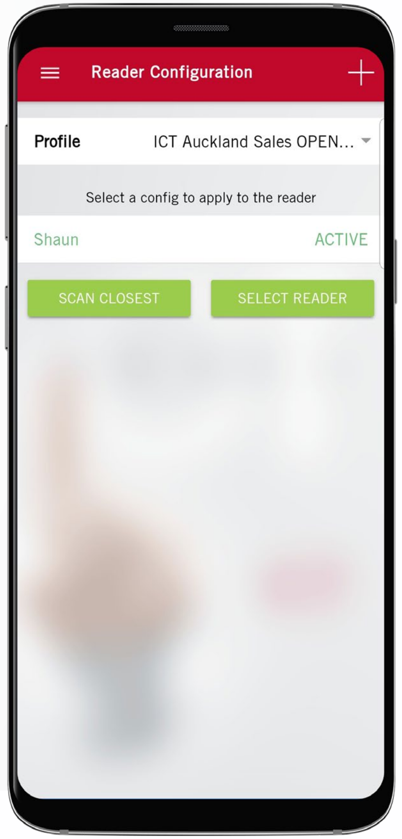
Configure readers

Only required if using open site code credentials.

Each customer site that uses open credentials will have a unique credential profile.

Use the Reader Configuration App to view the profiles assigned to the site and deploy these to the readers. This locks the credentials to the readers, ensuring they can only ever be used on that site.

- Log in to the app using your online portal details
- Select the profile to load
- Power up the reader
- Choose to **Scan Closest** or **Select Reader** within 2 mins to deploy the credential profile to the reader.



Profile ICT Auckland Sales OPEN...

Select a config to apply to the reader

Shaun ACTIVE

Reader Configuration
Profile
ICT Auckland Sales OPEN...
Select a config to apply to the reader
Shaun
ACTIVE
STOP SCAN
SELECT READER
Configuration of _R56F3F3C3 successful
ICT
EMERGENCY DOOR RELEASE

Protege Mobile Solution **The Implementation Process**

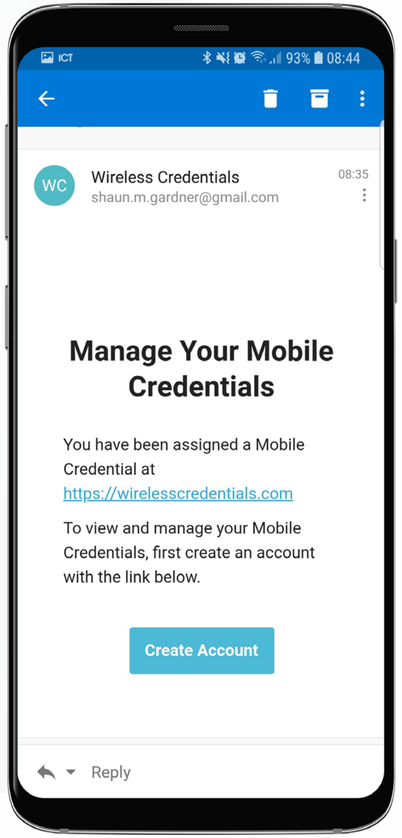
3

Assign credentials

Once the credentials are loaded into your Mobile Credential Management Portal, you can then **assign** credentials to other staff members or security personnel on site, who can then issue the credentials to end users for their mobile device(s).

Assigning a credential, sends an invitation to that operator to access the portal, where they can then log in to on-assign or issue those credentials as required.

Credentials can be on-assigned as many times as needed until they are issued. Once issued, they can be reissued to another email address, provided they have not been consumed, but they cannot be assigned again.



Wireless Credentials
shaun.m.gardner@gmail.com

Manage Your Mobile Credentials

You have been assigned a Mobile Credential at https://wirelesscredentials.com

To view and manage your Mobile Credentials, first create an account with the link below.

Protege Mobile Solution The Implementation Process

4

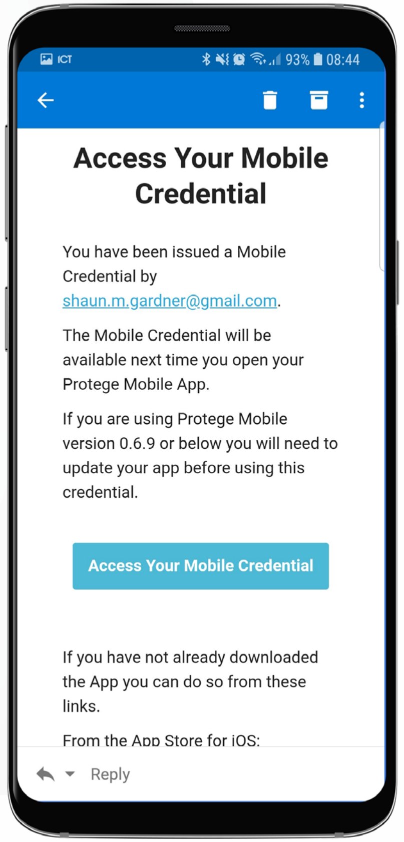
Issue credentials

Issuing a credential, sends an email to the end user with instructions for downloading the mobile app and accessing their credential.

When a credential is issued, it is allocated for use on the mobile device associated to the email used.

A credential can be issued once, but can then be reissued up until the point it is consumed. Once consumed, it cannot be reissued.

Once a credential is issued, the ability to assign it is blocked. You can only reissue it to another end user (as long as it is not yet consumed).



Access Your Mobile Credential

You have been issued a Mobile Credential by shaun.m.gardner@gmail.com.

The Mobile Credential will be available next time you open your Protege Mobile App.

If you are using Protege Mobile version 0.6.9 or below you will need to update your app before using this credential.

Access Your Mobile Credential

If you have not already downloaded the App you can do so from these links.

From the App Store for iOS:

Protege Mobile Solution **The Implementation Process**

5

Download Mobile App

The end user **downloads** the mobile app from the Apple Store (iOS) or Google Play (Android).

The app can be used on its own (by a building manager) to monitor and control the site, or with mobile credentials to provide card-free access.

Credentials are linked to the email account that is used to sign in to the mobile app. This means it’s important they use the same email address that the credential was issued to.

Protege Mobile Solution The Implementation Process

6

Credential consumed

When a valid connection is made, the credential is **consumed** and can be used to provide card-free access.

Once consumed, the credential can no longer be reissued.

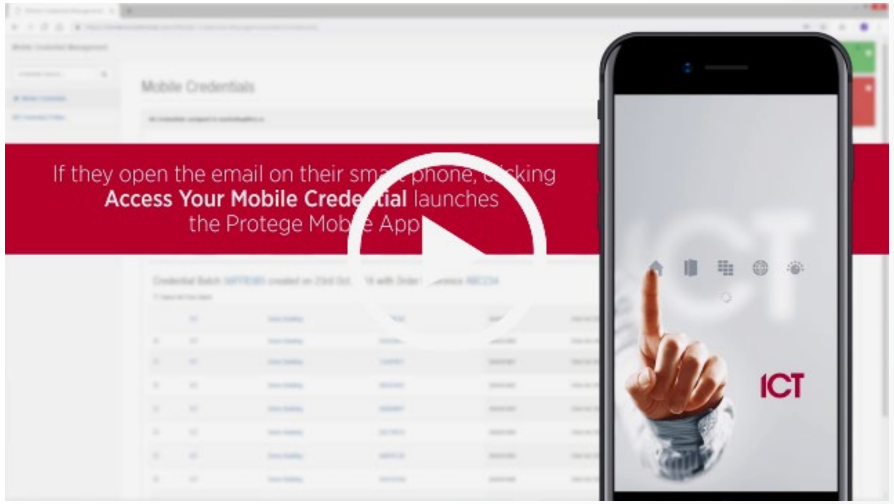
Protege Mobile Solution **Mobile Credential Management Portal**

Order Mobile Credentials from ICT just as you would order cards or tags.

They’ll be loaded into your Mobile Credential Management Portal

You can then **assign** credentials to other staff members or security personnel on site, who can then **issue** the credentials to end users for their mobile device(s).

- **Assign**: grant rights to access in the portal
- **Issue**: Allocate for use on a mobile device(s)



If they open the email on their smartphone, clicking **Access Your Mobile Credential** launches the Protege Mobile App

Protege Mobile Solution **Bluetooth vs NFC**

Communication between the mobile device and reader can use either Bluetooth (BLE) or NFC.

Bluetooth uses the 2.4 GHz radio frequency which allows for a longer read range than NFC.

- Supports both Android and iOS devices
- Short and long read distance (configurable)
  - Proximity unlock up to 0.5m (1.6ft)
  - Shake to unlock up to 5m (16.4ft)

NFC operates at the same 13.56 MHz frequency as smart cards.

- Supports Android devices
- Short read distance (up to 60mm)
- Slightly shorter transaction time than Bluetooth

There is no significant difference in battery consumption between the two communication methods.

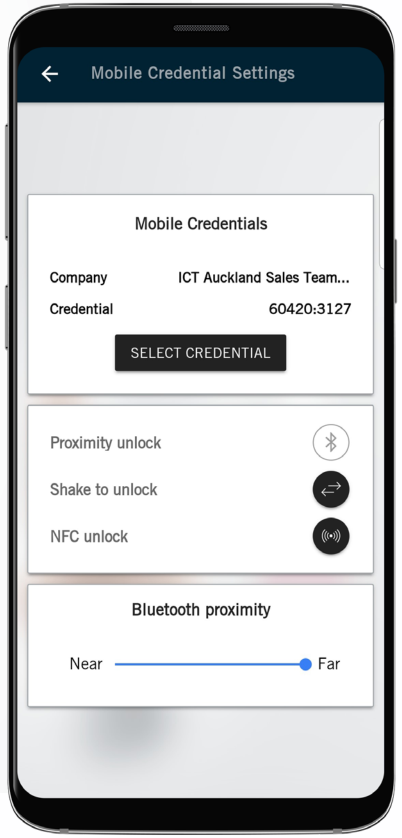
Protege Mobile Solution **Shake to Unlock vs Proximity Unlock**

Proximity Unlock behaves very much like a physical credential - by unlocking the door when the phone comes within range of the reader. Depending on the read range selected (using the Near / Far slider), this may require the user to physically present the phone at the reader or it may operate in a more passive mode that simply requires the user to be near the door.

Shake to Unlock requires the conscious action of holding the phone and shaking it within range of the reader. This can be useful when the door is in constant range and would otherwise continue to unlock.

Use the **Bluetooth Proximity** slider to set the range field of your device from Near to Far. Setting a longer read distance is ideal for garages, warehouses, or for installations where the reader is on the inside of the door. It can also help those living with a disability where presenting a standard access card is problematic.

Note that the read distance may vary due to environmental factors (including the surface the reader is mounted on) and the hardware and software of the mobile device.



Mobile Credential Settings

Mobile Credentials

Company ICT Auckland Sales Team...

Credential 60420:3127

Proximity unlock

Shake to unlock

NFC unlock

Bluetooth proximity

Protege Mobile Solution Frequently Asked Questions

Will existing credentials (that were issued during the beta) continue to work?

Yes. Credentials that were provided during beta will continue to work, but new credentials need to be purchased - just like regular cards and tags.

Will mobile credentials work on third party readers?

No. Mobile credentials will only work on ICT's Bluetooth enabled tSec readers.

Will mobile credentials work on third party systems?

Yes, but only when the system uses ICT's Bluetooth enabled tSec readers.

Do mobile credentials need an internet connection?

Yes. A valid internet connection is required at all times as the credentials are uniquely encrypted by the server to ensure end to end security and can be challenged/revalidated at any time.

How do I order credentials?

Credentials are purchased through your normal distributor or system integrator.

Can I purchase credentials in bulk, then on-assign them in smaller batches as required?

Yes. In the same way that you can order batches of cards or tags, you can order a batch of credentials then on-assign these as required using the Mobile Credential Management Portal.

How do I allow additional operators to assign and issue credentials through the portal?

New operators will be sent an invitation to the portal when they are assigned credentials. They can then log in to on-assign or issue these credentials as required.

Protege Mobile Solution **Frequently Asked Questions**

Can my end user administer their own credentials?

Yes but only provided you assign (and don’t issue) the credentials to the end user. They will then get an invite where they can issue them.

How many times can a credential be assigned?

Credentials can be on-assigned as many times as needed until they are issued. Once issued, they can be reissued to another email address, provided they have not been consumed.

How many times can a credential be issued?

It can be issued once, but can then be reissued up until the point it is consumed. Once consumed, it cannot be reissued.

How/when is a mobile credential consumed?

When a valid connection with the app is made and the credential is downloaded.

I issued a credential to the wrong email address, can I reissue it?

Yes, as long as the credential has not been consumed, it can be reissued.

I issued a credential when I meant to assign it, can I change this?

No. Once a credential is issued, the ability to assign it is blocked. You can only reissue it to another end user (as long as it is not yet consumed).

Can a mobile credential be transferred to a new device?

Yes. Credentials are linked to the email account used to sign in to the mobile app. Simply install the app on the new device, and login using the same account.

Protege Mobile Solution **Frequently Asked Questions**

What if I uninstall the Mobile App or factory-reset my device?

Credentials are linked to the email account used to sign in to the mobile app. Simply reinstall the app, and login again.

What is a credential profile?

A credential profile contains information about the type of credentials that can be created within that credential profile and the company that owns those credentials. A credential profile generally relates to a site or place where those credentials can be used.

As an integrator, can I create my own credential profiles?

No. Profiles are created and administered by ICT. When ordering credentials, you can request a specific profile, but keep in mind that the name used will be visible to any organizations you then assign credentials to.

How do I revoke a credential once issued?

Select the credential token to view details, then click the Revoke Credential button.

If a credential has been issued can it be revoked so that a user doesn't use it on another system?

Yes. When the credential is revoked this removes it from the end user's mobile application and it ceases to exist. Much the same way as if you cut a physical card in half.

What do you do when someone leaves/moves out?

This will depend on who has been assigned the credential and how they want to manage it. At a minimum the user record in the access control system will be updated/disabled/deleted. Whether the credential is revoked is entirely the credential manager's decision.

Protege Mobile Solution **Frequently Asked Questions**

What happens when there are multiple readers in range of the mobile device?

Each reader will open. In this case, we recommend adjusting the Bluetooth Proximity slider (position it closer to near)

Can an integrator or building manager reassign the issuance of mobile credentials to company managers and still keep track of the number of credentials issued by company managers? Including those that have been assigned to other managers?

Yes, the system is hierarchical so you have full visibility down the chain of assignment but not upwards.

Let's look at an example:

- Integrator Ian assigns 100 credentials to Building Manager Bob.
- Bob then assigns 50 of these credentials to Company Manager Chris and 50 to Company Manager Craig.
- Chris issues these to various staff, as does Craig.

In this scenario:

- Ian can see all credentials assigned to Bob, Chris, and Craig, and those that Chris and Craig have issued.
- Bob can see all credentials assigned to Chris and Craig, and those that Chris and Craig have issued, but he cannot see those that are assigned to Ian.
- Chris only sees those that are assigned to him or that he has issued. He cannot see those that are assigned to Ian, Bob, or Craig.

Is there an event log to show which operator assigned or issued a credential?

Yes. Click on the credential token to view details.

Is there a CSV user import tool for sites with a large number of users and need to issue large quantities of credentials?

Not at this stage but it is being considered for a future release.

Protege Mobile Solution More Information

▶ View Supporting Videos

[Configure the Protege Mobile App]

[Navigating the Protege Mobile App]

[Using the Protege Mobile App]

[Using the Mobile Credential Management Portal]

Contact ICT

Phone toll free:

New Zealand	0800 428 111
Australia	1800 428 111
USA/Canada	1855 428 9111

Email:

sales@ict.co

support@ict.co