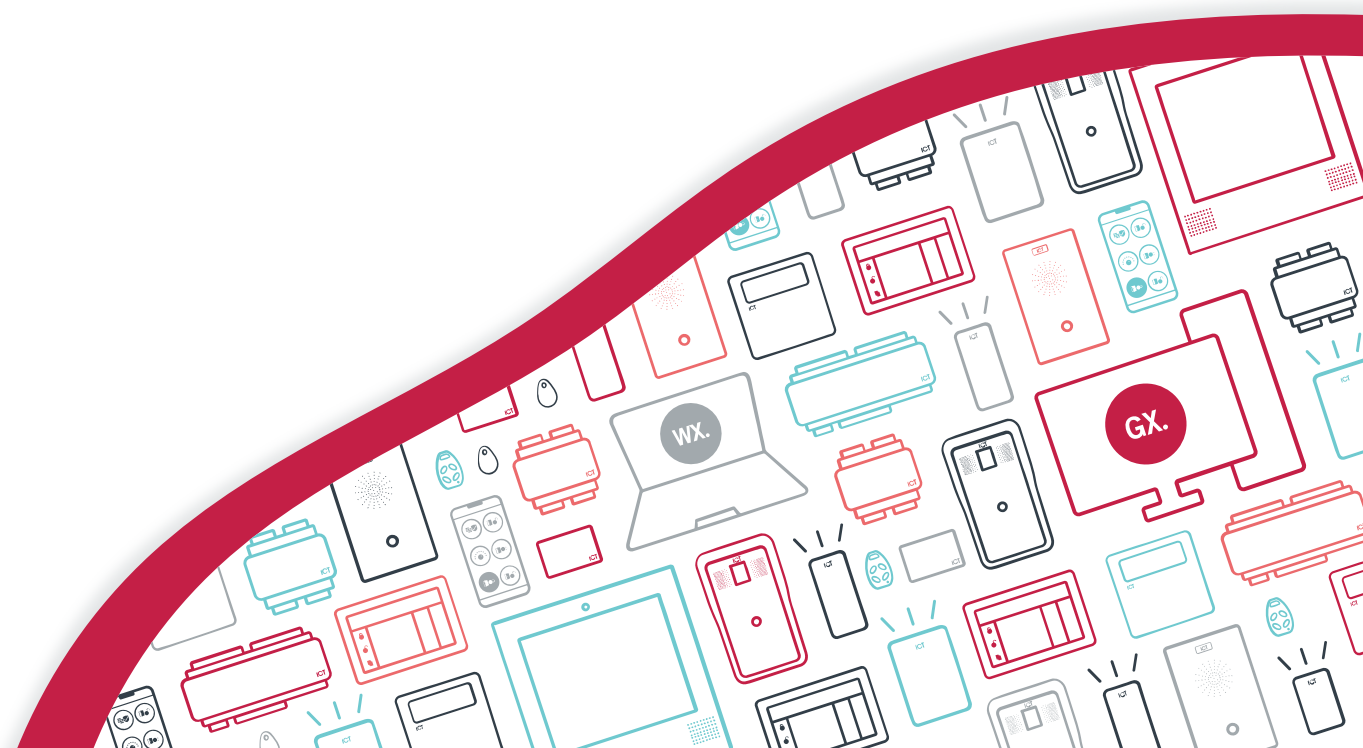
PRT-MOB-IF

Protege Mobile Credential Management Portal

User Guide



Last Published: 21-Sep-21 2:22 PM

Contents

Introduction

The Protege Mobile Credential Management Portal (https://wirelesscredentials.com) is a web portal for issuing and managing Protege GX and Protege WX mobile credentials.

This portal makes it easy for installers, building managers and security personnel to issue wireless credentials to staff, allowing them to access what they need with nothing more than their smartphone.

This document provides a guide to:

- Logging in to the mobile credential management portal
- Issuing credentials to users
- Revoking credentials
- Managing user credentials in Protege GX and Protege WX
- Assigning credentials to administrators
- Viewing credential profiles

Logging in to the Mobile Credential Portal

When you purchase mobile credentials from ICT, or when another administrator assigns credentials to you, you will receive an email notifying you that the credentials have been assigned to your portal account.

Browse to the portal by clicking the link in the email, or entering https://wirelesscredentials.com into a browser.

You will be presented with a login screen:

- The Protege mobile credential management portal uses the same login account as the Protege apps. If you already have an account on the **Protege Mobile App** or the **Protege Config App**, enter the same username and password to log in to the mobile credential portal.

  This is **not** the same account that you would use to log in to the ICT website, Protege GX or Protege WX.

- If you do not yet have a Protege mobile account, click **Create an Account**. Enter your email address and a new, secure password (repeating it to confirm). Click **Create Account**.

  If you have already been assigned mobile credentials, ensure that you create your account using the same email address as the one that the credentials have been assigned to.

- If you have forgotten the password for your mobile account, click **Forgot Password?**, enter your email address and click **Send Reset Link** to receive an email inviting you to reset your password.
- After you have logged in, you can reset your password at any time by navigating to **Your Account** in the sidebar and entering a new password.

Managing Mobile Credentials for Users

When you log in, you will be presented with the **Mobile Credentials** page. This displays all of your available mobile credentials; allowing you to view details, issue credentials or reassign them. Mobile credentials are organized by batch, allowing you to separate credentials that were assigned to you at different times.

Each mobile credential displays the following details:

- **Company**: The company to which the credential is assigned.
- **Credential Profile**: The sub-category of credentials within that company. This corresponds to a particular range of facility/site codes.
- **Credential Token**: A unique code for each mobile credential.
- **Credential**: The facility and card number for the credential. These must be assigned to the user as a card number in Protege GX or Protege WX (see page 8) before it will be recognized by the security system.
- **Batch Token**: A unique code for each batch of credentials.
- **Created**: Date that the mobile credential was first created.
- **Issued**: Date that the mobile credential was issued to a user.
- **Consumed**: Whether the mobile credential has been consumed (i.e. activated by the user) or not.

To view more information about each credential, including a full event log, click the **Credential Token** code.

Issuing Credentials

To issue a credential to a Protege GX or Protege WX user:

1. On the **Mobile Credentials** page, locate a credential with the correct credential profile (i.e. site) for that user.
2. Click **Issue Credential**.
3. Enter the email address of the user.
4. Click **Issue**.

The user will receive an email informing them that they have been issued a mobile credential and providing instructions for how to activate it.

Once the user activates it this consumes the credential, and it will be displayed as unavailable in the web portal.

For more information on using the Protege Mobile App, see the Protege Mobile App User Guide.

Note that the credential must be assigned to a user in Protege GX or Protege WX before it will be recognized by the security system (see page 8).

Reissuing Credentials

If a credential has been issued to a user but not yet consumed (i.e. activated in the mobile app), it can be reissued to another email address. This is especially useful when an incorrect email address has been entered, preventing the user from accessing their credential, or when user requirements change.

1. Locate the credential to be reissued on the **Mobile Credentials** page.
   - Ensure that the **Show Issued Credentials** option is checked.
   - You can use the **Search** field to easily locate a particular credential.
2. Click **Reissue Credential**.
3. Enter a new **Email Address**. Enter **Notes** to indicate why the credential has been reissued.
4. Click **Reissue**.

The new user will receive a credential issue notification email as normal.

Once a credential has been consumed, it cannot be reissued to another user.

Revoking Credentials

Once a credential has been assigned to and consumed by a user, it can still be revoked if no longer required.

Revoking a credential in the mobile credential portal is equivalent to cutting up an access card; it will no longer be available to assign to any user. If a user misplaces their mobile device, it is better to temporarily disable the credential in Protege, rather than revoke the credential.

To revoke a credential:

1. Locate the relevant credential on the **Mobile Credentials** page.
   - Ensure that the **Show Consumed Credentials** option is checked.
   - You can use the **Search** field to easily locate a particular credential.
2. Click on the **Credential Token** code to open the Credential Details page.
3. Click the **Revoke Credential** button.
4. Enter a note to explain why the credential is being revoked. Click **Revoke**.

The credential will be removed from the user's mobile app account

Note: The user will not receive an email notifying them of this.

Limiting the Number of Devices per Credential

By default, a mobile credential can be installed on an unlimited number of devices. This is convenient for end users, but can also create a security risk as some users might give their mobile app logins to unauthorized parties to grant them access. To mitigate this risk, you can limit the maximum number of devices that each credential can be installed on.

This feature is only available with Protege Mobile App versions 1.0.6 or higher.

Managing Devices for a Single Credential

1. Locate the relevant credential on the **Mobile Credentials** page.
   You can use the **Search** field to easily locate a particular credential.
2. Click on the **Credential Token** code to open the credential details page.
3. Set the **Device limit per Credential** to the maximum number of devices which can use this credential.

   The default setting is 0, which means that there is no limit on the number of devices for the credential.

When the user has consumed their credential on a device, you will see the device's platform, model and last used date listed on this page.

To remove a credential from one or more devices, check the boxes beside each required device and click **Remove Devices**. This is useful if the device is lost, stolen or replaced.

It is not possible for app users to remove their devices from the device limit. If they need to free up a device, they must talk to their administrator.

Managing Devices Using a Credential Profile

You can set a device limit for all of the credentials in a specific credential profile.

1. Navigate to **Credential Profiles** and select the required credential profile.
2. Set the **Device limit per Credential**.

   The default setting is 0, which means that there is no limit on the number of devices per credential.

3. Click **Update Credential Profile Details** to apply this device limit. All future credentials added to this credential profile will use this default device limit.
4. To apply this new limit to all existing credentials in the credential profile, click **Update all Credentials in this Profile**.

   If one or more credentials in this credential profile already has more devices than the new limit, you will see a warning popup. You must resolve this issue before you can apply the new limit.

Managing Credentials in Protege GX and Protege WX

Even though the mobile credential has been issued to an email address via the web portal, it still needs to be assigned to the corresponding user in Protege GX or Protege WX to allow them to use it to access the system.

Managing users in Protege GX or Protege WX requires the correct operator permissions. If these are not available, please contact your installer or system administrator.

To assign a credential to a user in Protege:

1. Identify the **Facility/Card Number** that you wish to assign. This will be in the **Credential** column on the **Mobile Credentials** page in the form of `FACILITYNUMBER:CARDNUMBER` (e.g. 1000:234).
2. Log in to Protege GX or Protege WX and navigate to **Users | Users**.
3. Select the user who has been issued this credential, or create a new user if necessary.
4. Enter the credential details into one of the **Facility/Card Number** fields.
   Eight fields are available to accommodate multiple credentials.
5. If you need to disable a user credential, check the **Disabled** checkbox beside that credential.
6. Click **Save**.

Once a mobile credential has been assigned in Protege, the user can use it to access any parts of the system that are allowed by their access levels, just like a normal access card.

Assigning Credentials to Administrators

As well as issuing credentials to users, you may need to assign batches of credentials to administrators (such as building managers or security personnel) for management.

1. On the **Mobile Credentials** page, select any number of credentials by clicking the checkboxes beside each row. Click **Select All** or enable the **Select All From Batch** option to bulk select credentials.
2. Return to the top of the page. Enter the email address into the **Assign Selected Credentials To** field.
3. Enter any relevant **Notes** into the field that opens.
4. Click **Assign**. The person will receive an email informing them that they have new credentials assigned. They can now issue or assign these credentials from their account as required.

Once credentials are assigned to another person they are no longer visible from your account. They can only be accessed by the account they are currently assigned to.

If credentials are assigned to a person who is no longer available or in the organization, and you are unable to access the account or reset the password, you will need to contact ICT Customer Services for assistance.

Reassigning Consumed Credentials

Once an issued credential has been consumed by a user, it may be necessary to assign it to a new administrator. For example, if an administrator has been removed from the system, their assigned credentials should be reassigned so that they can be managed and revoked by a different administrator.

Reassigning credentials can only be performed from the account they are currently assigned to.

1. You will need to log in to the account the credentials are assigned to.*
2. Select the credentials to be reassigned.
3. Enter the email address of the account to reassign to into the **Assign Selected Credentials To** field.
4. Click **Assign**.

* If you do not know the account password, you can use the **Forgot Password** function to reset the password.

This does require that you have access to the email address associated with the account. For this reason, it is recommended that any accounts that you assign credentials to for management are general company email accounts that you can access, and not personal email accounts.

If you are unable reset the password, you will need to contact ICT Customer Services for assistance.

Viewing Credential Profiles

The **Credential Profiles** page displays the various credential profiles which are used by your assigned credentials. Each credential profile represents a company and category of credentials within that company (such as a site and a particular range of card numbers).

Click on the **Credential Profile** column to view profile details, including the number of available and consumed credentials in the profile.

Click **View Credentials in this Credential Profile** to filter your assigned credentials by this profile.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.