SynQ Prox Web App

Reseller/Dealer Guide

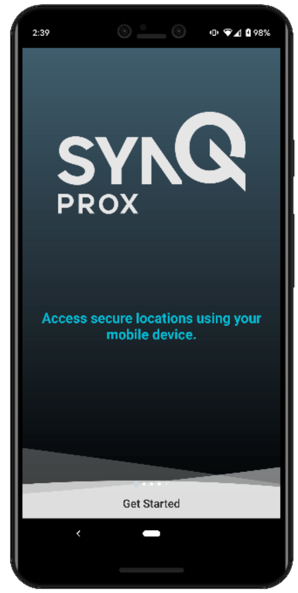
November 2020

Table of Contents

What is SynQ Prox?

SynQ Prox is an access control solution that allows individuals to access a secured area using an Android or iOS smart device.

The SynQ Prox Web Portal is where site administrators can manage users and assign mobile credentials.



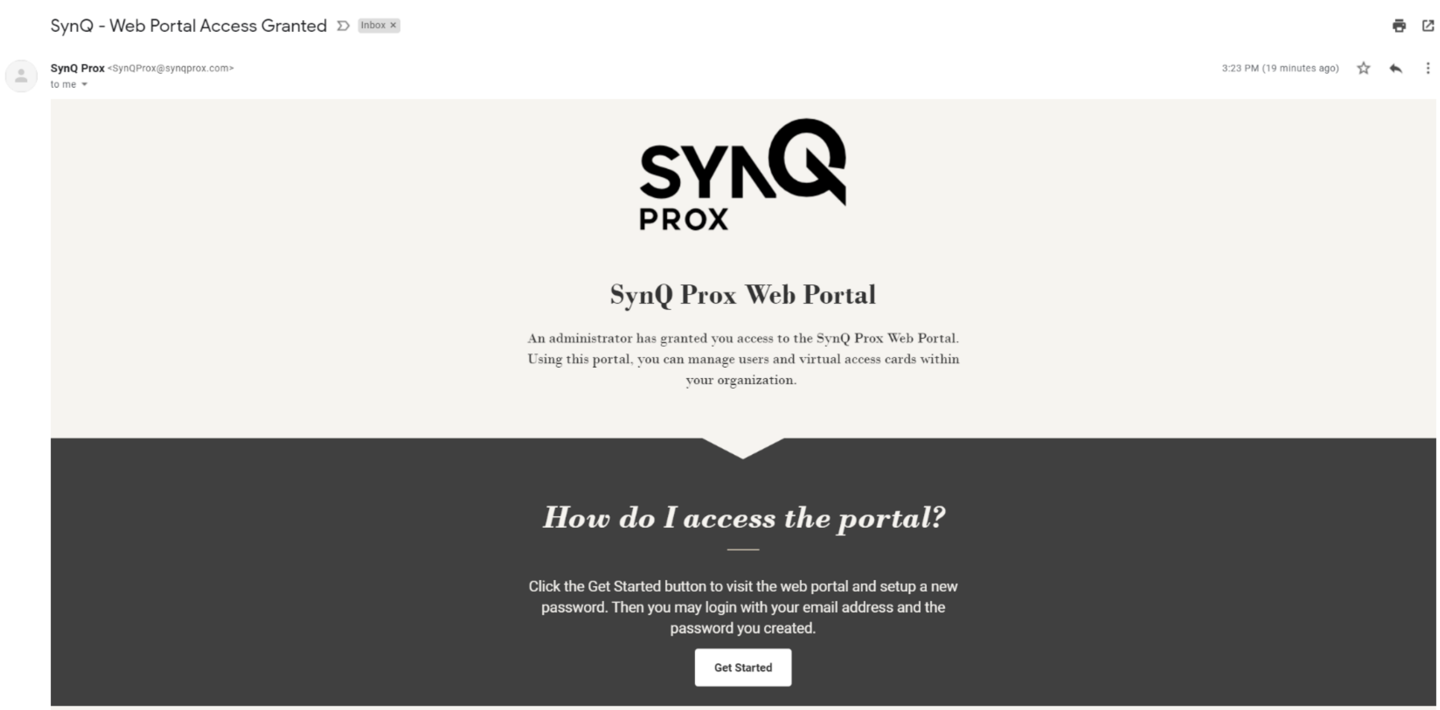
Get Started

1. You must be invited to use the SynQ Web Portal by an administrator. The web portal can be found at app.synqprox.com.

   Note: If you are using Internet Explorer, some features may not function properly. Please consider using a different browser such as Google Chrome, Mozilla Firefox, Microsoft Edge, etc.

2. Upon invitation, you will receive an email from SynQ Prox – follow the "Get Started" link in the email to set your password and login.

   Be sure to check your spam folder if you are unable to find the email.

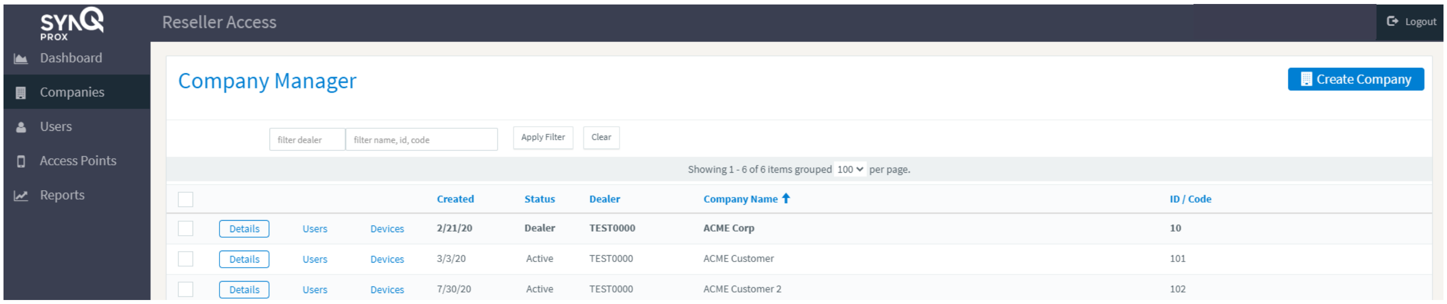


3. Upon login, you will see the Welcome screen. Use the menu items on the left to navigate the web portal.

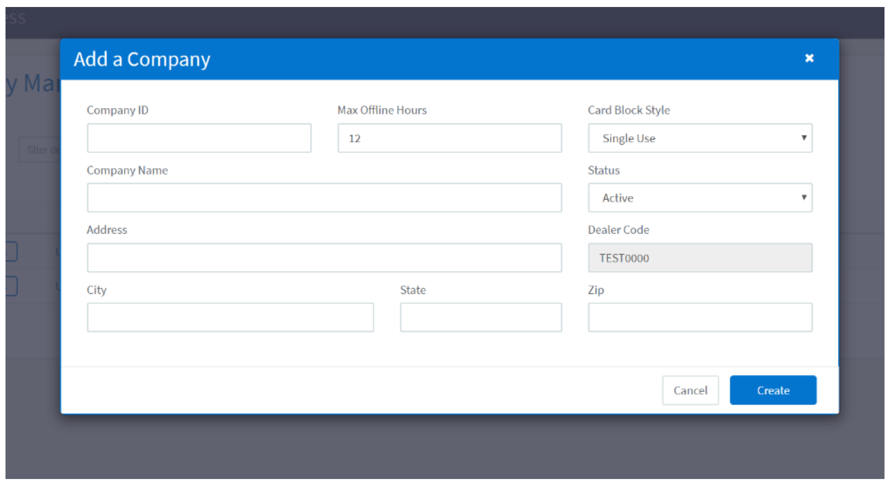
Create a Company

As a reseller, you can add your customers to the web portal under the “Companies” screen.

1. Navigate to the “Companies” page on the menu on the left side of the screen.
2. Click “Create Company”



4. Enter the company’s details (unique company ID, name, address etc.)



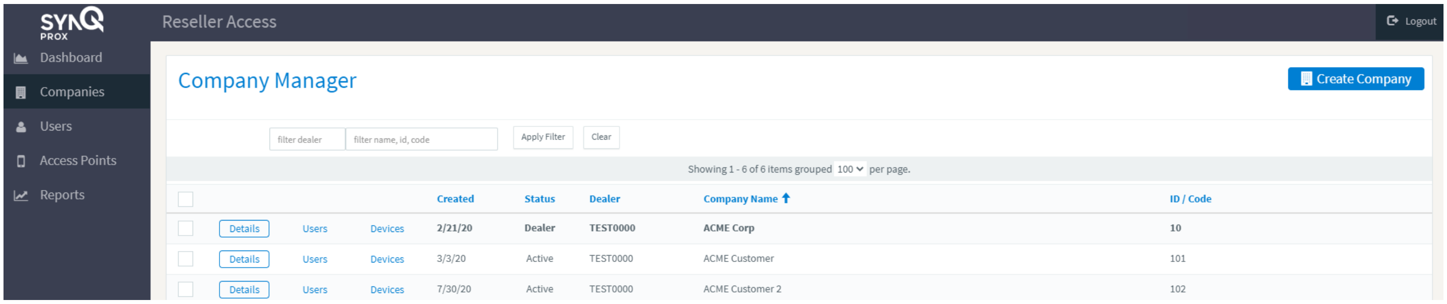
5. Set “Max Offline Hours”
   a. This sets the limit that an end user’s mobile device can be offline or without a data connection. For example, if Max Offline Hours is set to 12 and an end user has their mobile device on airplane mode for 12 hours or hasn’t used the app for 12 hours, the user will be required to connect to the network to ensure they have valid credentials.

6. Set “Card Block Style”
   a. This determines whether the companies virtual credentials will be “Single Use” or “Perpetual.” Single use cards will not be recycled when a user’s card is deleted. Perpetual cards may be reused by other users once a user’s card has been deleted.
   b. Note, please contact us to upgrade / change Card Block style.

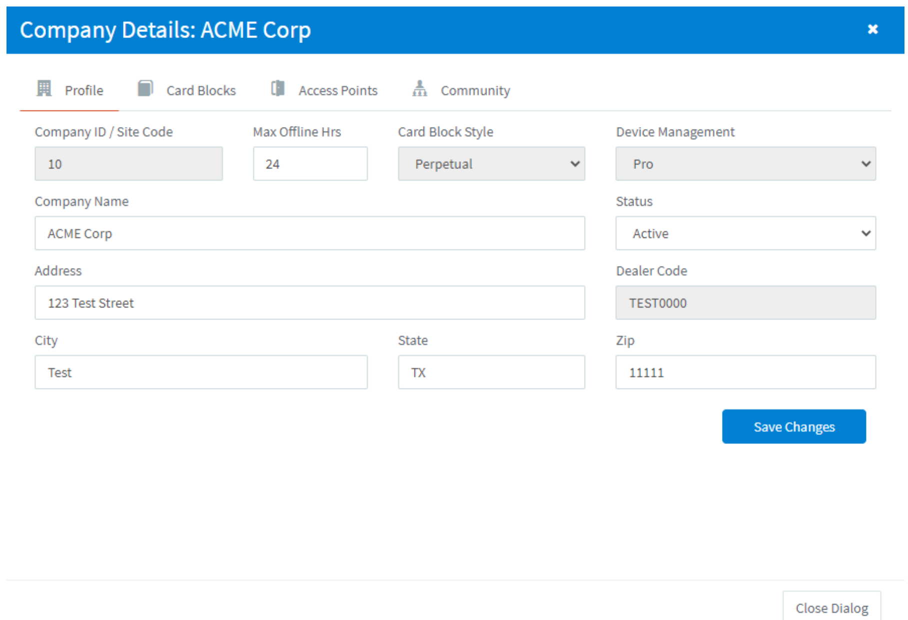
7. Set “Status” to “Active” to activate the new company.
   a. Note, a company may be deactivated in the future by visiting its “Details” screen.

Company Management

The Company Management screen is where all of the companies you have created are listed.



1. To edit a company, click “Details” to the left of the company.
2. You may edit the company details, including deactivating the company by setting its status to “Disabled”.
3. The CARD Blocks tab at the top of the window shows the details of each card block provided to the company.



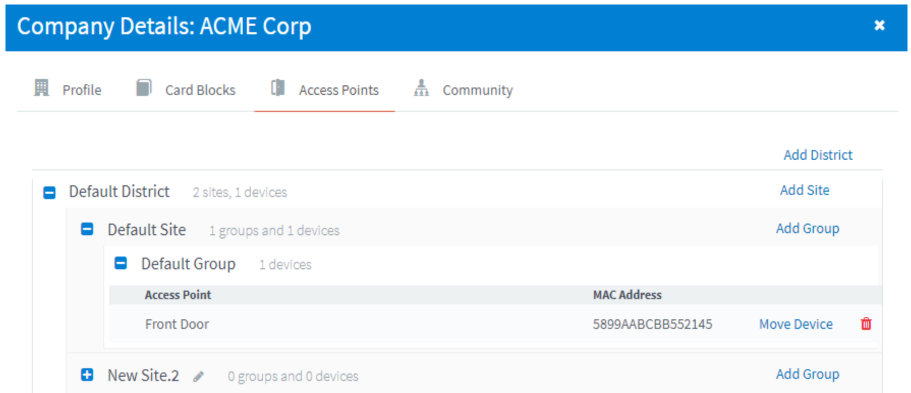
Access Points Management

The Access Points Management screen is where registered access points can be managed. Note, only standard and pro plans have the access point management feature enabled.

1. Click on the “Access Points” tab.

2. Click “Add District”, “Add Site”, and “Add Group” to create levels for managing your access points. Note, Districts and Sites are only available for pro plans.

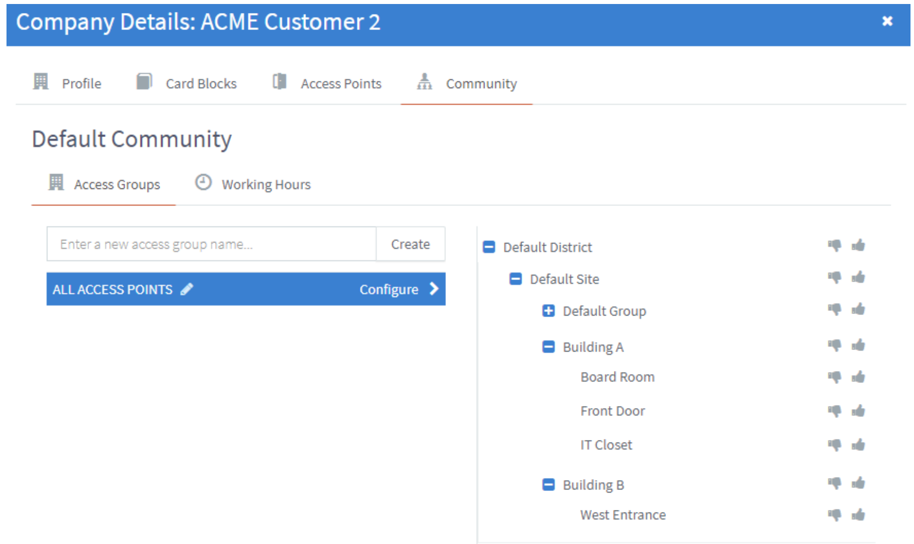
3. Once you have registered your access points from the mobile app, they will appear in the Default Group. Click “Move Device” to move the access point to another group.



Access Groups and Working Hours

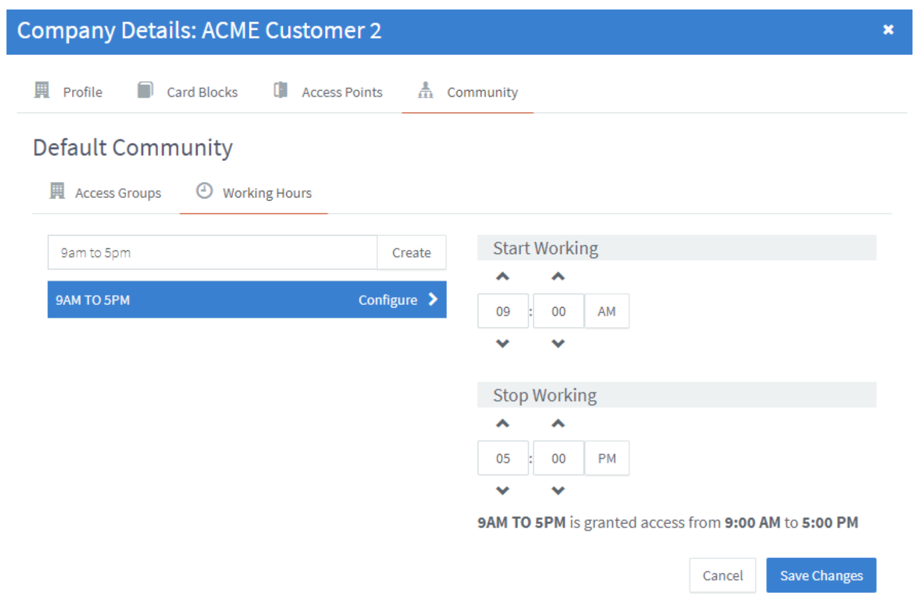
Access Groups let you define a set of access point permissions you can apply to any user with a click.

1. Click on the Community tab within the Company Details dialog.
2. Click “Access Groups”, enter a new access group name, and then click “Create”.
3. Select the access points that should be a part of the access group.
4. Access Groups can be applied in the user dialog.



Working Hours let you define a global set of times that your registered access points are available. Note, 24 hour access is the default.

1. Click on the Community tab within the Company Details dialog.
2. Click “Working Hours”, enter a new working hours name, and then click “Create”.
3. Change the start and stop hours in the dialog on the right.
4. Working Hours are in the local time zone of the access point so 9AM to 5PM represents this time anywhere in the world.
5. Access Groups can be applied in the user dialog.

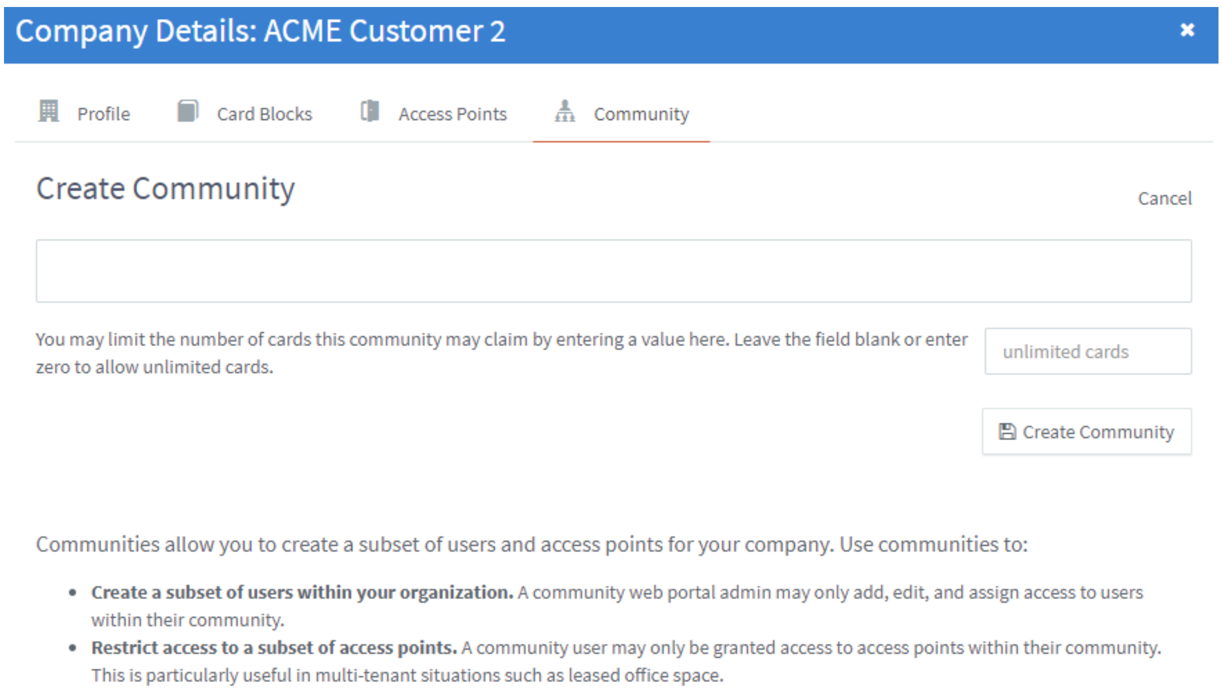


Community Management (Pro Plan Only)

Communities allow you to create a subset of users and access points for your company. Use communities to:

- Create a subset of users within your organization. A community web portal admin may only add, edit, and assign access to users within their community.
- Restrict access to a subset of access points. A community user may only be granted access to access points within their community. This is particularly useful in multi-tenant situations such as leased office space.

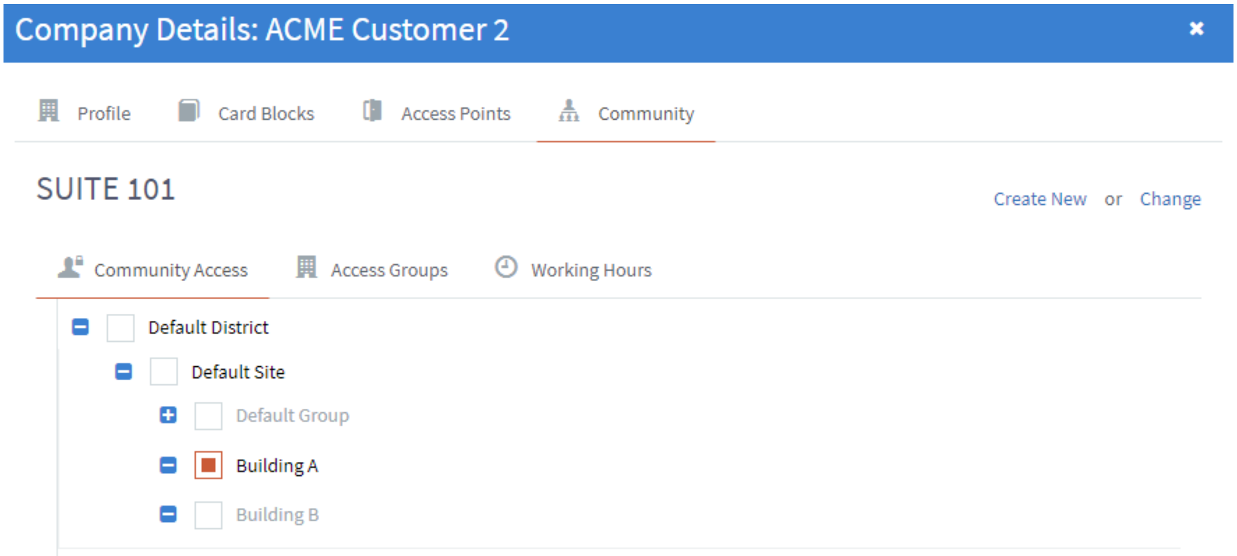
1. To create a community, click “Create New” in the Community tab of the Company Details Screen.



2. Enter the name of the Community in the top box.

3. Enter the number of virtual cards that the community may issue. Note, the community’s cards will come from the parent company’s card block (i.e. each card issued in the community will reduce the total number available of the parent company. Cards will be the same Wiegand format of the parent card block).

4. Click “Create Community”.

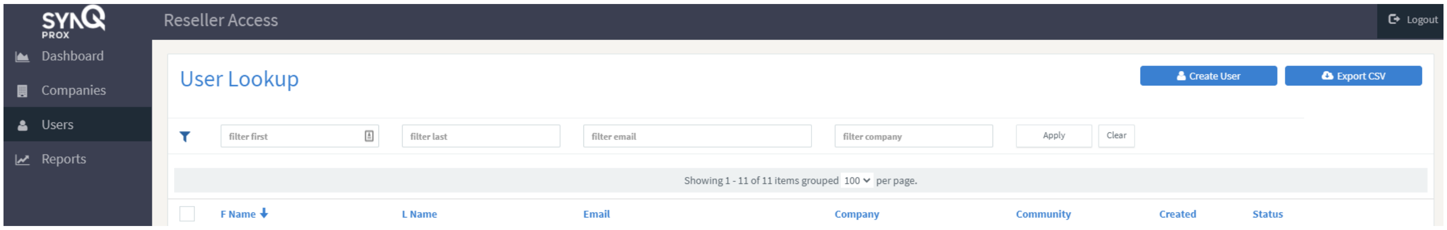


5. Select the Districts, Sites, and / or Groups that the Community will have access to. This may be edited at any time.

6. Create Access Groups and Working Hours as detailed above.

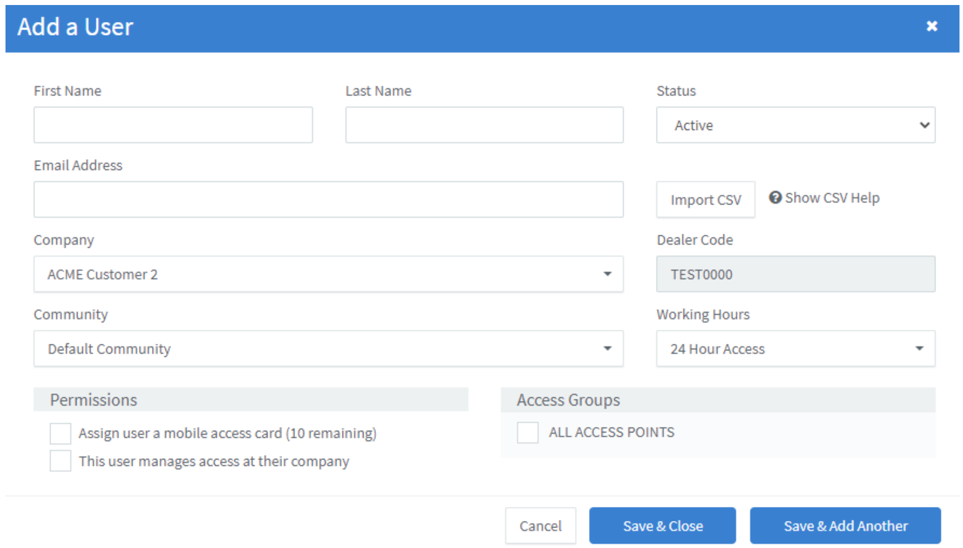
7. Click “Change” in the top right of the screen to switch the community you are editing.

Create a User



1. To create a new user, click “Users” on the left menu bar.

2. Click the “Create User” button in the top right corner of the screen.



3. Enter the user’s name and email address.

4. Select the user’s company.

5. Select the user’s community (if applicable).

6. Click “Assign user a mobile access card” if you would like to assign this user a mobile access card.

7. If the user manages access at their company and needs portal access, select “This user manages access at their company.”

8. If the user is a technician or installer at your company, select “This user is a technician.” **This will enable the user to access the installation features in the mobile app to change settings in the device.**

9. Change Working Hours if applicable.

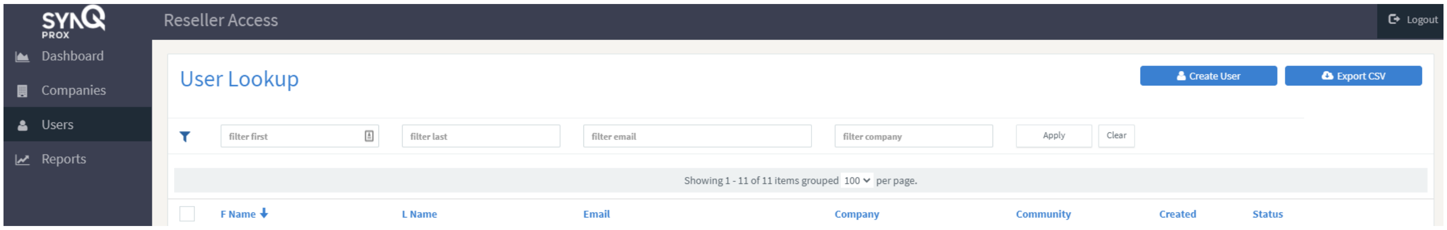
10. Assign access groups to the user if applicable.

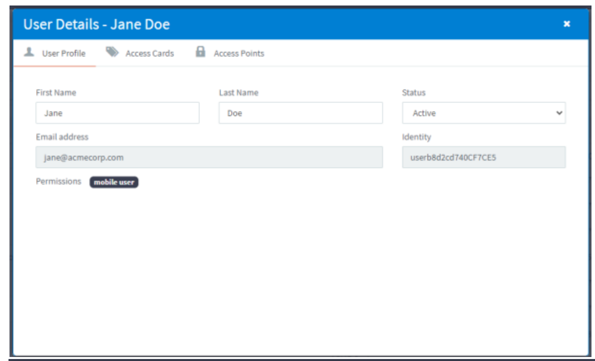
11. To import a list of users at one time, select “Import CSV” and upload a CSV with the appropriate formatting. The CSV should be formatted first name, last name, and email address with each new user on a separate row. See picture below:

	A	B	C	D
1	John	Doe	john@acmecorp.com	
2	Jane	Doe	jane@acmecorp.com	
3	Bob	Doe	bob@acmecorp.com	
4				
5				
6				

User Management

All users are listed under the "Users" screen.



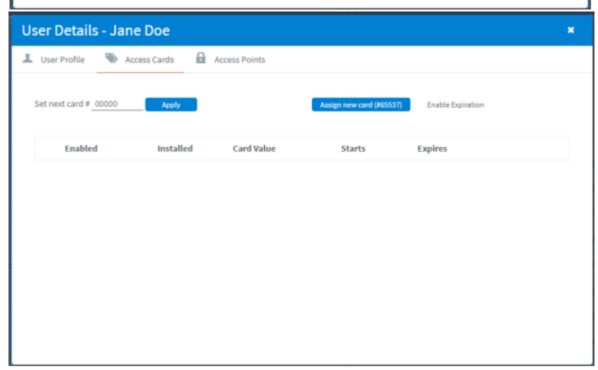


1. To edit a user, click "Details" to the right of the user.

2. To assign a virtual card to a user, click on the "Access Cards" tab at the top of the screen, select "Assign new card (######)."

    a. The card number to be assigned is shown to the right of "Assign new card" – if you wish to change the card number, enter the new number in "Set next card #" and click "Apply".

    b. If you wish to set a start and end date for the card, click on "Enable Expiration" and choose the appropriate start and end date. Note, the card will only be valid between the start and end dates. Once expired, a new card will need to be assigned to the user to function.



3. Cards that have been assigned to the user will be shown. If the card is enabled, it will show a green check. If the user has successfully retrieved their card on their mobile device, it will show a green check mark under "Installed".

    Note: if the user needs the card on a different mobile device (lost device, new device, etc.), the card must be reset in the web portal and claimed again.

    Note: if the user needs cards on multiple devices, they must be assigned an additional card for each device.

4. If your organization has Access Point Management enabled (standard and pro plans), user access to specific access points can be set on the "Access Group" tab.

    a. Access can be granted or denied at an access point, group, site, or district level. Click the thumbs up to grant access or the thumbs down to prohibit access.

    Note: access points will be visible on the mobile device to those who have been granted access.