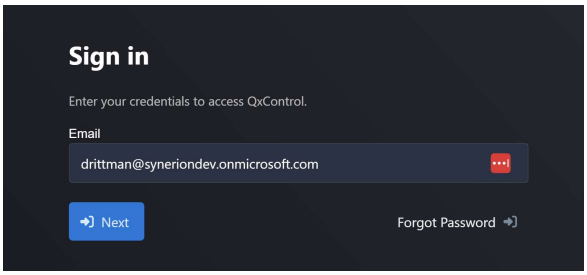
QxControl Setup Guide

Enterprise user management with Microsoft Entra

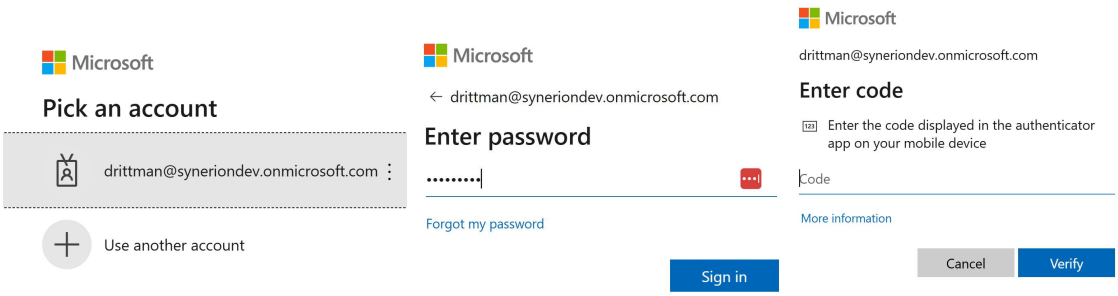
Integration with Microsoft Entra allows your organization to manage its application users and cardholders in QxControl via Entra. Users and Groups created and managed in Entra can be synchronized to QxControl, and identity management is governed by Entra, so the password management and authentication schemes used by other facets of your organization apply to QxControl as well.

Once configured following the steps in this document, your organization's QxControl users will follow a simple login flow:

1. Enter their Entra user principal name at the QxControl prompt

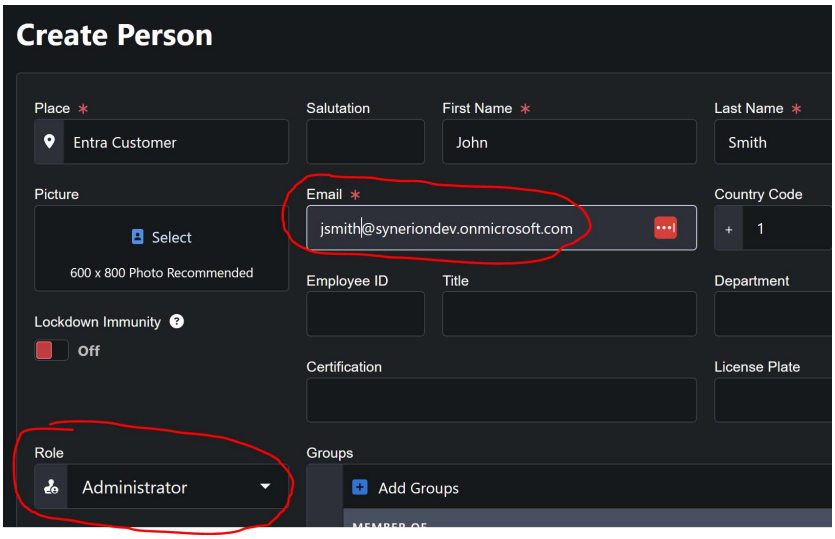


2. If they are already logged in to Entra, they will immediately enter QxControl; otherwise, they will follow the normal Entra login sequence, including 2FA if your organization requires it.

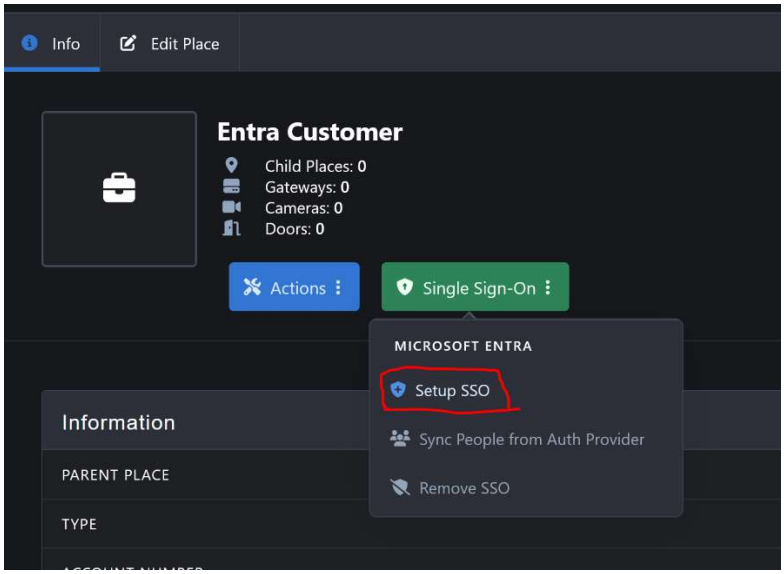


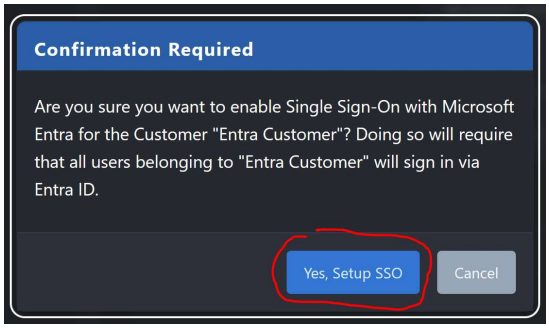
Integrator Steps

1. Have your integrator create a user at your customer place
    - Set Role to Adminstrator
    - Set Email to your Microsoft Entra User Principal Name



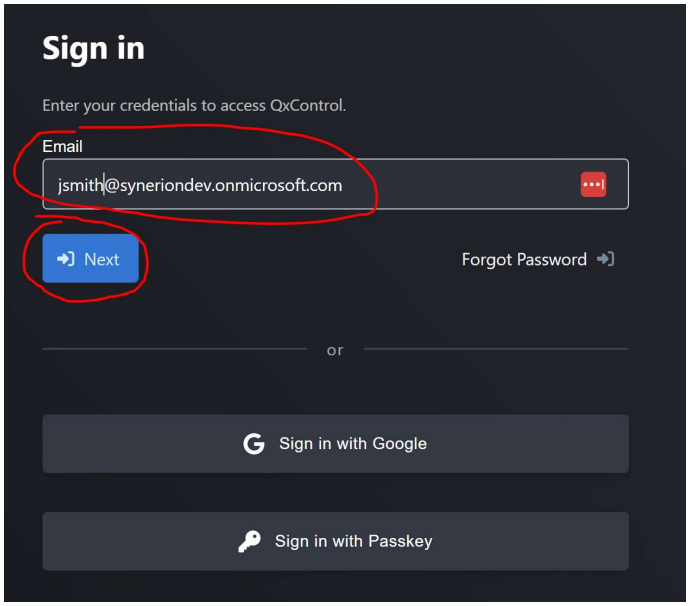
2. Have your integrator select “Setup SSO” on the Single Sign On menu at your customer place and accept the confirmation



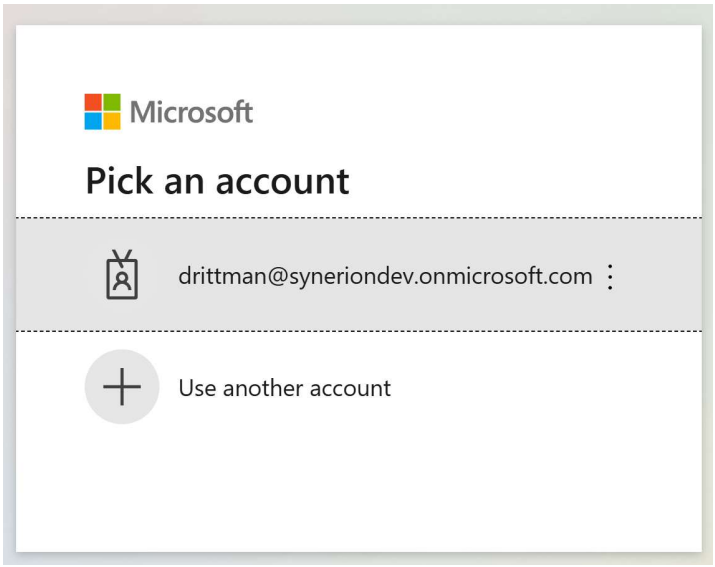


Customer Steps

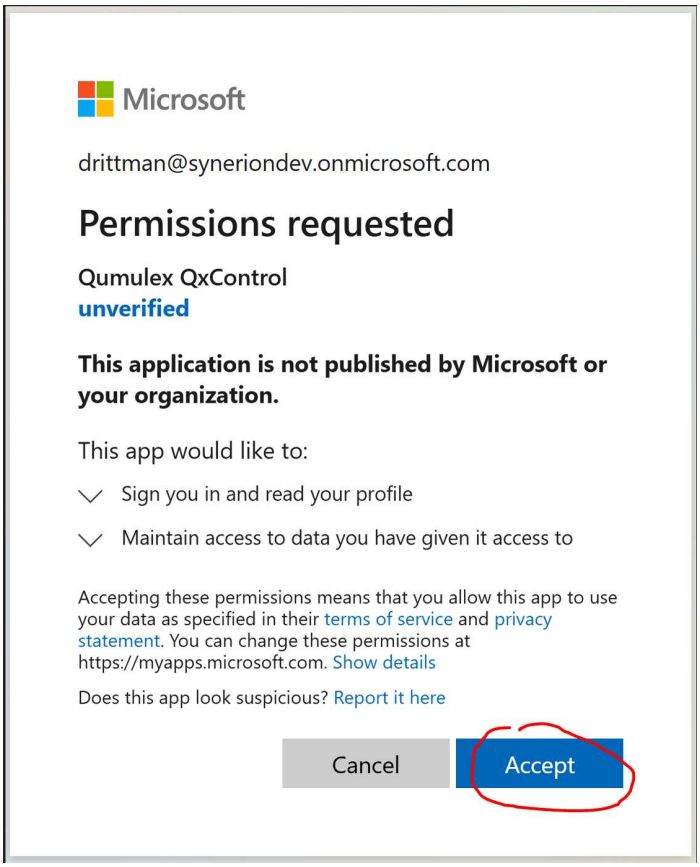
1. Browse to https://app.qumulex.io
2. Enter your Entra User Principal Name in the email field
3. Press “Next”



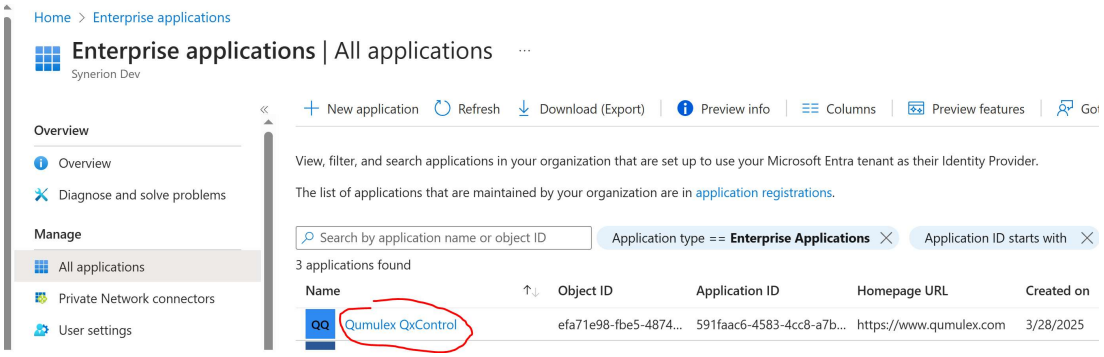
4. If you are not logged in to Microsoft Entra, you’ll be taken to the Entra login page



5. You will have to grant permission to **Qumulex QxControl** to access fields in your Entra tenant

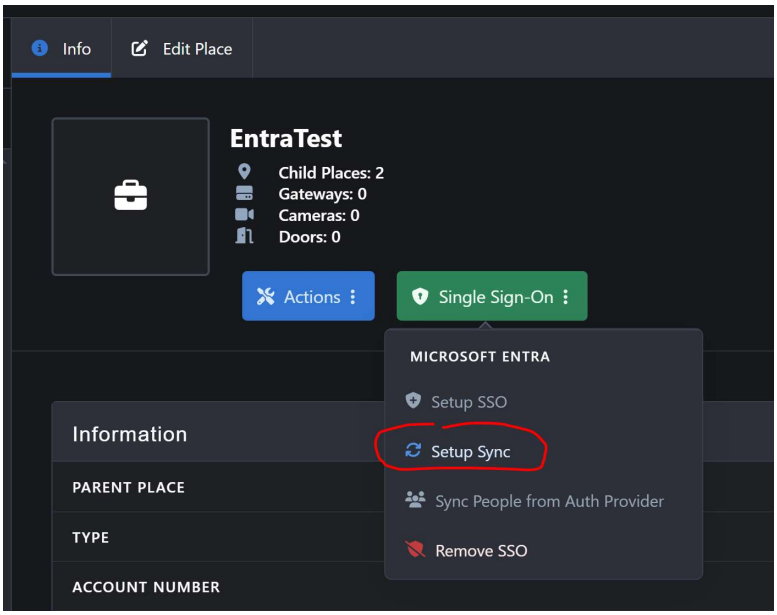


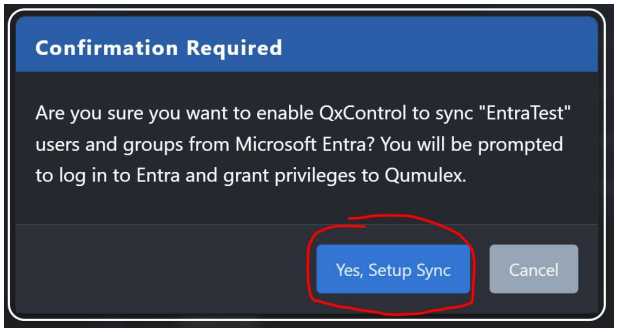
6. Once complete, you will see **Qumulex QxControl** as an Enterprise Application within your Entra tenant



   - At this point, you will be logged in to QxControl.
   - You, and each new application user who signs in, will have to accept the End User Terms Agreement within QxControl.
7. If you want to synchronize the Users and Groups within your Entra tenant into QxControl, navigate to the top of your Place hierarchy

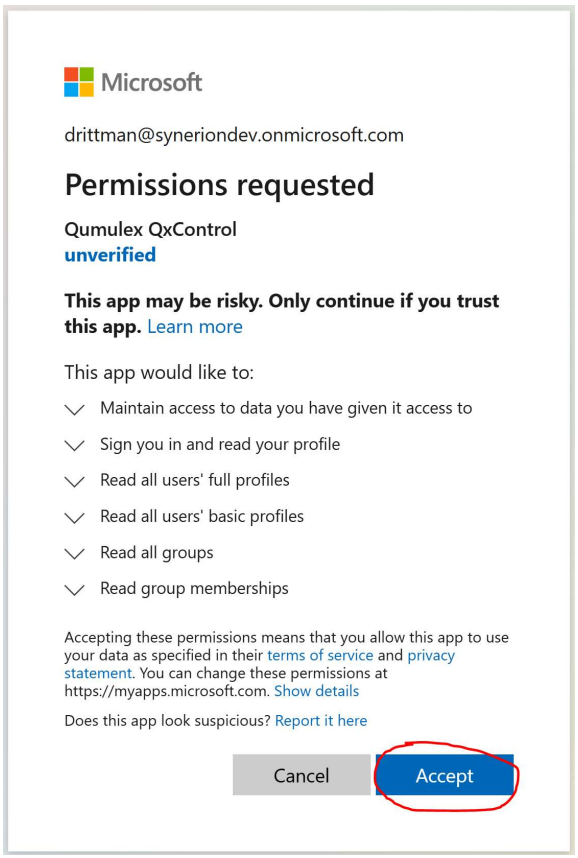
8. Select “Setup Sync” from the Single Sign On menu and accept the confirmation



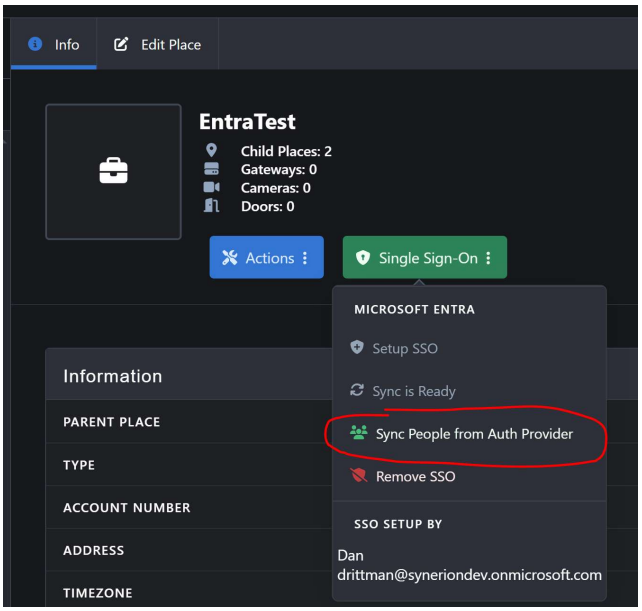


9. Again, if you are not logged in to Entra, you will be taken to the login page

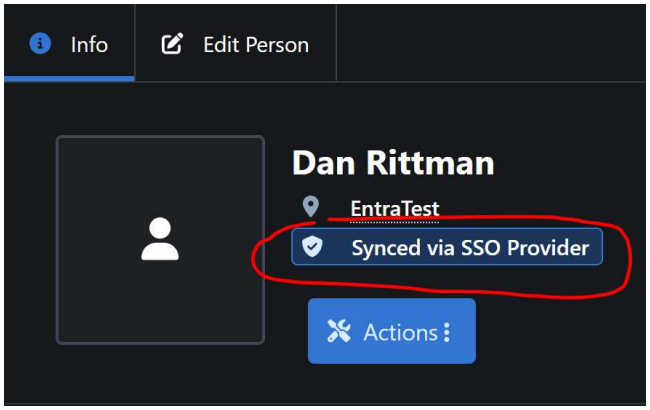
10. Once logged in to Entra, you will have to grant additional permissions to **Qumulex QxControl** within your Entra tenant allowing it access to your users and groups.



11. After granting those permissions, you are able to sync QxControl with Entra by selecting the “Sync People and Groups” menu from the top of your Place hierarchy.



12. All of the users and groups within your Microsoft Entra tenant will be created within QxControl
    - Users and Groups will be created at the top Place in your QxControl hierarchy with an indication that they were created via the sync



    - As you build out a hierarchy within QxControl, you may move the People and Groups to Places lower in your hierarchy
    - The sync process creates People with no Role (meaning they cannot log in to the QxControl application) and no credentials (meaning they cannot access any doors).
    - You may edit People within QxControl to give them a Role and/or Credentials
    - If a user is ***deleted in Entra***, the Person with the matching User Principal Name will not be deleted, but their Role will be set to “None” and all their credentials will be set to “Expired” so they can neither log in to QxControl nor access any doors with their credentials.
    - If a group is ***deleted in Entra***, that Group will be deleted from QxControl. This may affect doors which People in that Group were able to access.

Entra Custom Security Attributes (Role, Credential & Group sync)

The Entra sync brings users and their Entra group membership into qx automatically — no attributes required. It can **also** sync a person's **role**, **credentials** (e.g. card numbers), and additional qx groups when those values are provided as Entra custom security attributes.

Groups therefore come from two sources that combine:

1. **Entra group membership** — every group the user is a member of in Entra is mirrored into QxControl as a group, and the person is added to it. This is automatic.
2. **The groupID attribute** — QxControl group ids listed on the user, added on top of the groups from source 1. Use this to put someone in a QxControl group that has no Entra equivalent.

These are **additive**, not either/or: a person in the Entra group "Facilities" who also carries a groupID value ends up in both QxControl groups.

This doc covers the one-time Entra setup an administrator does to enable that.

What the sync reads

The sync looks for a single attribute set named **Qumulex** with these attributes:

Attribute	Type	Maps to in qx
roleID	String (single value)	The person's role — a **role id** (built-in or custom, see below), matched exactly. The role must be a built-in role or one at/under the customer's place. An unmatched id is ignored.
credentials	String (multiple values)	One or more access cards for the person. Use siteCode-cardNumber. A value with no - in it (e.g. 1234) is stored as -1234 — card number 1234 with no site code — which is the same thing QxControl stores when you add a card by hand and leave Site Code blank.
groupID	String (multiple values)	One or more group ids that add the person to qx groups directly (on top of any groups synced from their Entra group membership). Each group must be at/under the customer's place, matched exactly. An unmatched id is ignored. Removing an id removes the person from that group on the next sync.
excludeFromSync	Boolean (single value)	When true, the person is soft-deleted in qx — they act as deleted while their record is kept for history — **and all of their credentials are disabled, both their synced and their manual credentials**. Set back

Attribute	Type	Maps to in qx
		to false (or unset) to restore them (synced credentials re-sync on the next run; disabled manual credentials are not automatically restored).

roleID accepts a role id — matched exactly:

- A built-in role id:
  - administrator
  - poweruser
  - manage_people
  - live
  - live_and_search
  - live_and_search_no_people
- **or** a custom role id — the last segment of the role's URL in QxControl, e.g. https://app.qumulex.io/qx/roles/1SoAExCV0M7 → 1SoAExCV0M7.

groupID accepts group ids — matched exactly:

- A group id is the last segment of the group's URL in QxControl, e.g. https://app.qumulex.io/qx/groups/0ACLosU00Kb → 0ACLosU00Kb.
- The group must be at/under the customer's place; an id for another customer's group (or one that does not exist) is ignored.

Notes:

- The set and attribute names are **case-sensitive** and must be exactly Qumulex, roleID, credentials, groupID, and excludeFromSync.
- credentials is **multi-valued**, so a person can carry more than one card.
- groupID is **multi-valued**, so a person can be added to more than one group. Groups it assigns are added alongside the groups synced from the person's Entra group membership; removing an id removes the person from that group on the next sync.
- **Entra is authoritative for group membership.** Each sync sets a synced person's QxControl groups to exactly the combination of their Entra groups plus their groupID

values. A group a QxControl administrator adds them to by hand is removed on the next sync — to make a group assignment stick, set it in Entra (either by adding them to the Entra group or by adding the QxControl group id to groupID).

- **Card format:** use siteCode-cardNumber (e.g. 100-1234) — site code 100, card number 1234. A value with no - in it (e.g. 1234) is stored as -1234: card number 1234 with an empty site code. That is the same value QxControl writes when you add a card by hand and leave Site Code blank, so a card set here and a card typed into QxControl behave identically at the door. A value that already contains a - is stored exactly as entered. A value of just - is never synced, because QxControl keeps it for PIN-only credentials.
- **Card values that need correcting:** each value should be two numbers joined by a - (e.g. 0-123). Any other value is still synced as described above, and the account is listed under Single Sign-on Error in QxControl until the value is corrected.
- **One account per card value:** a value on more than one account is given to only one of them, and the accounts are listed under Single Sign-on Error in QxControl until the value is on just one.
- **Entra wins over a lost or revoked card.** A card marked lost or revoked in QxControl is made active again at the next sync while credentials still lists it. Remove the value in Entra to stop it; once it is no longer listed, the card stays lost or revoked.
- **One email, several people:** QxControl keeps one live person per email in your organization, and that person is managed by the account. A deleted one is restored only when none is live, and then only the one deleted most recently, in the place it was in.
- All attributes are optional per user.
    - Leave roleID unset to leave the person's qx role untouched (a role the sync previously set is cleared from QxControl when roleID is removed in Entra).
    - Credentials created by Entra sync are issued valid for 50 years. A card removed from credentials is set to expired (reason: "disabled from entra sync") and kept in history. A card issued by hand in QxControl is left alone while the account is enabled and not excluded, unless credentials lists the same value; when the account is disabled, deleted or excluded it is expired too.

Step 1 — Ensure the person setting up Entra has the correct role

By default **Global Administrator and Privileged Role Administrator cannot read or create custom security attributes.** Custom security attributes use their own dedicated directory roles, which must be assigned explicitly:

Role	Needed to…
Attribute Definition Administrator	Create the attribute set and attributes (Steps 2–3).
Attribute Assignment Administrator	Assign roleID / credentials / groupID values to users (Step 4).
Attribute Assignment Reader	Read the values. Assign to the **user who connects the qx sync** (Step 5).

Assign these under Entra → Roles & administrators. Search for "Attribute" to find them. You can assign a role to yourself if you are a Global Administrator.

If the Custom security attributes blade shows **"Add attribute set" greyed out**, you are missing the **Attribute Definition Administrator** role — that is the cause, not a licensing issue.

Assigning the role to yourself

You must be a **Global Administrator** (or Privileged Role Administrator) to assign directory roles. To unblock the greyed-out **Add attribute set** button, assign yourself **Attribute Definition Administrator**:

1. Go to Entra → Roles & administrators.
2. In the search box, type **Attribute**.
3. Click **Attribute Definition Administrator**.
4. Click **+ Add assignments**.
5. **Select members** → pick your own user → **Select**.
6. Leave it **Active** (not Eligible) so it applies immediately, set the assignment type/duration as your org requires, then **Assign**.
7. **Sign out and back in** (or refresh) — directory role changes only apply to a new token. The **Add attribute set** button will then be active.

Repeat the same steps for **Attribute Assignment Administrator** (so you can set values on users in Step 4) and **Attribute Assignment Reader** for the user who connects the qx sync (Step 5).

PIM tenants: if your tenant uses Privileged Identity Management and you only see an **Eligible** option, you must also **activate** the role from **My roles** after assigning it before it takes effect.

Step 2 — Create the attribute set

1. Go to Entra → Custom security attributes.
2. Click **+ Add attribute set**.
3. **Attribute set name:** Qumulex
4. Set a max number of attributes (e.g. 25) and **Add**.

Step 3 — Add the attributes

Open the Qumulex set and add four attributes:

1. **+ Add attribute**
    - **Attribute name:** roleID
    - **Data type:** String
    - **Allow multiple values assigned:** No
    - **Only allow predefined values:** No (or Yes if you want to restrict to a fixed list of role ids)
2. **+ Add attribute**
    - **Attribute name:** credentials
    - **Data type:** String
    - **Allow multiple values assigned: Yes** (a person can have more than one card)
3. **+ Add attribute**
    - **Attribute name:** groupID
    - **Data type:** String

- **Allow multiple values assigned: Yes** (a person can be added to more than one group)

4. **+ Add attribute**
    - **Attribute name:** excludeFromSync
    - **Data type:** Boolean
    - **Allow multiple values assigned:** No

Step 4 — Assign values to users

For each user that should sync a role, credentials, groups, and/or excludeFromSync state:

1. Go to Entra → Users, open the user.
2. Open **Custom security attributes** → **Add assignment**.
3. Select the **Qumulex** set, choose the desired attribute(s), and enter the value(s). Do not populate attribute(s) for a user if they are not needed.
    - **roleID** → a role id, matched exactly: a built-in role id (e.g. administrator, manage_people) or a custom role id copied from the URL in QxControl when viewing the Role Info page, e.g. 1SoAExCV0M7 from https://app.qumulex.io/qx/roles/1SoAExCV0M7.
    - **credentials** → one or more card values. Use siteCode-cardNumber (e.g. 100-1234) to set a site code; a value without a - (e.g. 1234) is stored as -1234 — that card number with no site code.
    - **groupID** → one or more group id values to add the person to those QxControl groups, in addition to any groups from their Entra group membership. These should be copied from the URL in QxControl when viewing the Group Info page, e.g. 0ACLosU00Kb from https://app.qumulex.io/qx/groups/0ACLosU00Kb.
    - **excludeFromSync** → true to soft-delete the person in qx and disable their credentials (both synced and manual), false (or unset) to keep them active.
4. Save.

Step 5 — Let the sync read them

The QxControl Entra app requests the CustomSecAttributeAssignment.Read.All Microsoft Graph permission as part of the sync consent. The sync reads attributes **as the user who connected it** (a delegated flow), so:

1. Grant admin consent for that permission when prompted during the Entra sync setup
2. If you have previously configured Entra sync in QxControl, you will have to re-sync to consent to the new permission being requested. You can do that from the Single Sign On menu on the Places page. Note: This can not be done by the integrator. It must be done by a user from the customer.



3. Assign the **Attribute Assignment Reader** role (from Step 1) to the user whose account connects the QxControl sync, so Entra will return the attribute values.

Without the Attribute Assignment Reader role on that user, Entra silently omits customSecurityAttributes and roles/credentials/groupID will not sync (users and Entra group membership still sync normally).