Centralized Login FAQ

Document version: 1.9
Last modified: 11/12/2019

What is Centralized Login (CL)?

The CL is a new feature that will allow Dynamo users to access multiple Dynamo databases (or tenants) with one set of credentials. To facilitate this, Dynamo users will no longer be managed in the context of a single tenant/client. A user exists in the Dynamo realm and can be granted access to one or many tenants across Dynamo's infrastructure. Although individual tenants are still responsible for controlling entitlements and granting individual users access to tenant(s), end users will be the sole master of their own accounts going forward.

Why is Dynamo making this change?

Over the years, Dynamo's clients and the use cases have grown considerably. In addition, Dynamo's product offering has grown substantially, making a centralized authentication system an absolute requirement rather than a "nice-to-have".

The CL allows us to offer an efficient method for both end users and companies to utilize a modern and robust authentication system. For end users it means one set of credentials, less confusion when logging across multiple Dynamo portal tenants, and the ability to have more independence when updating their authentication preferences.

What does this mean for Dynamo users?

- All Dynamo users will now have only one profile across all of Dynamo's product offerings associated with a unique email address.
- The users themselves will administer their own credentials, and client administrators will not be able to update or create a password.
- In addition to passwords, two-factor settings will be managed through a single location.
- All Dynamo system emails will now be sent to the username email, and not to the email listed under the underlying contact.
- Users without real email addresses for their user name will not receive important email notifications such as password reset, updates to their account access, etc.

Administrators will still be able to activate/deactivate (grant/revoke access) users within a tenant. Additionally, user passwords will be active for 365 days before Dynamo prompts users for a new password. A shorter password expiration period can be configured per tenant, user group, or individual user.

When a user who has multiple Dynamo accounts with the same username/email logs in for the first time once the Centralized Login is in place, the passwords across all those tenants will be synchronized and "collapsed" into the password the user just used to log in with.

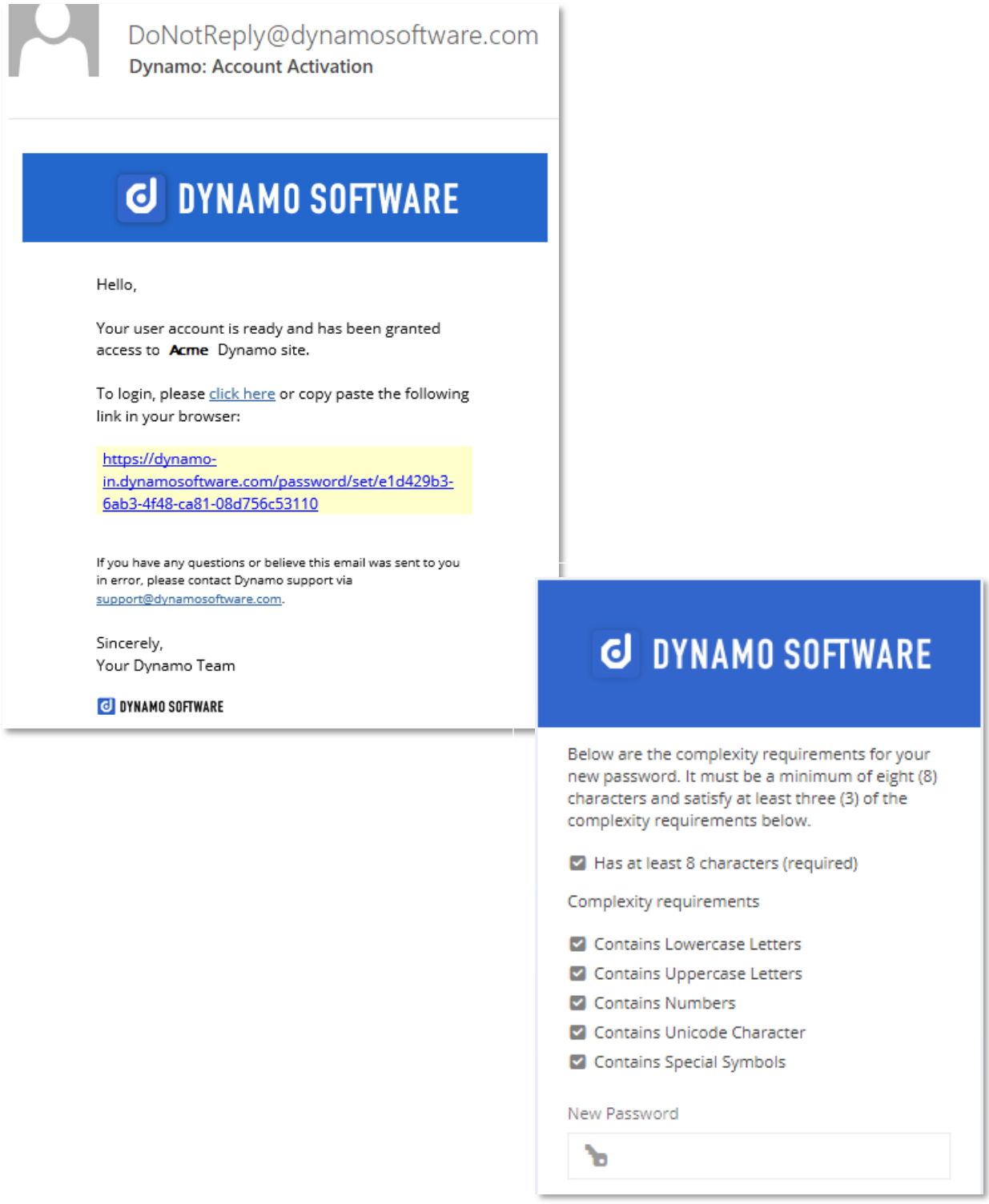
How does Dynamo manage user passwords?

Password management is restricted to Dynamo users only. Dynamo administrators are no longer able to see or modify user passwords. Newly created users automatically receive emails with instructions on how to activate their Dynamo accounts and configure their passwords.

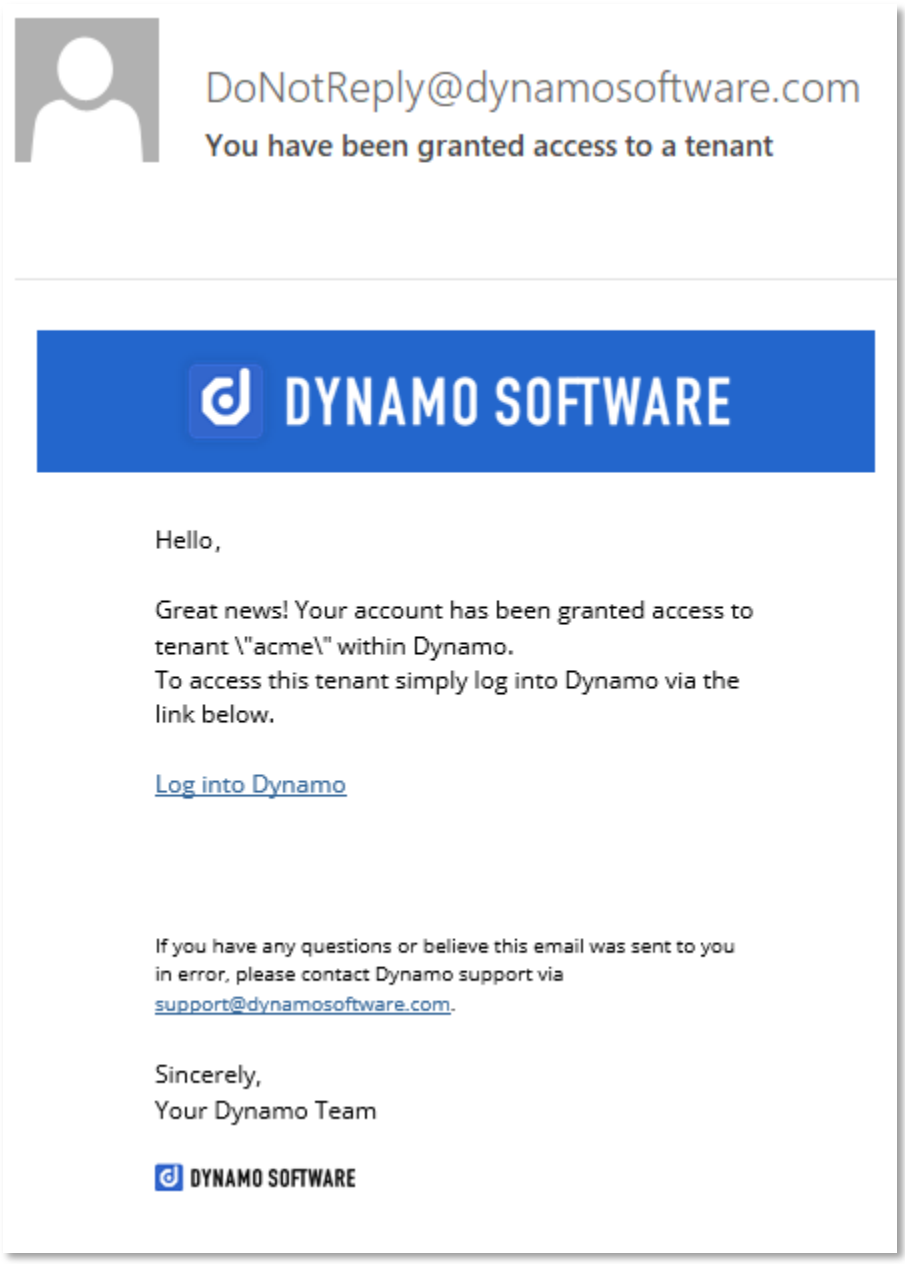
Please, note that since users will be automatically redirected to the CL login page, previously saved passwords will not auto-fill. It is highly recommended that users change or double check their passwords so when the CL rolls out, they remember what their current password is. They can also view their Dynamo saved passwords in their browser settings (for more information, visit https://blog.dashlane.com/view-delete-saved-passwords/).

Users can reset their passwords using the "Forgot password" link on the main login page. Users with invalid email addresses will still be able to log in, however, they will not be able to reset their passwords as the "Reset password" link is delivered to the email address/username of the user. Instead, they will have to request password resets from Dynamo Support, via the Dynamo administrator/Power User of their tenant. To avoid this process, Dynamo administrators are encouraged to change all invalid usernames to real emails before Centralized Login goes live.

The activation link (below) redirects users to Dynamo's Centralized Login password selection page. When a user selects a password, their password will automatically synchronize across all Dynamo tenants that share the same username. To ensure your data is secure, Dynamo will now enforce high password complexity per image below.


DoNotReply@dynamosoftware.com
Dynamo: Account Activation
DYNAMO SOFTWARE
Hello,
Your user account is ready and has been granted access to Acme Dynamo site.
To login, please click here or copy paste the following link in your browser:
https://dynamo-in.dynamosoftware.com/password/set/e1d429b3-6ab3-4f48-ca81-08d756c53110
If you have any questions or believe this email was sent to you in error, please contact Dynamo support via support@dynamosoftware.com.
Sincerely,
Your Dynamo Team
DYNAMO SOFTWARE
DYNAMO SOFTWARE
Below are the complexity requirements for your new password. It must be a minimum of eight (8) characters and satisfy at least three (3) of the complexity requirements below.
Has at least 8 characters (required)
Complexity requirements
Contains Lowercase Letters
Contains Uppercase Letters
Contains Numbers
Contains Unicode Character
Contains Special Symbols
New Password

If a Dynamo user is granted access to a new Dynamo tenant, the password configuration process is skipped and Dynamo automatically sends an email informing the user about that. After logging in to Dynamo, the user is able to select the desired tenant as described above.



DoNotReply@dynamosoftware.com

You have been granted access to a tenant

DYNAMO SOFTWARE

Hello,

Great news! Your account has been granted access to tenant \"acme\" within Dynamo.
To access this tenant simply log into Dynamo via the link below.

Log into Dynamo

If you have any questions or believe this email was sent to you in error, please contact Dynamo support via support@dynamosoftware.com.

Sincerely,
Your Dynamo Team

DYNAMO SOFTWARE

What happens if a user has different passwords within different Dynamo tenants?

If a user currently uses different passwords within different Dynamo tenants, Centralized Login will authenticate the user. He/she will be notified that their password will be synchronized across all tenants.

Can new user accounts be activated via activation code and security question?

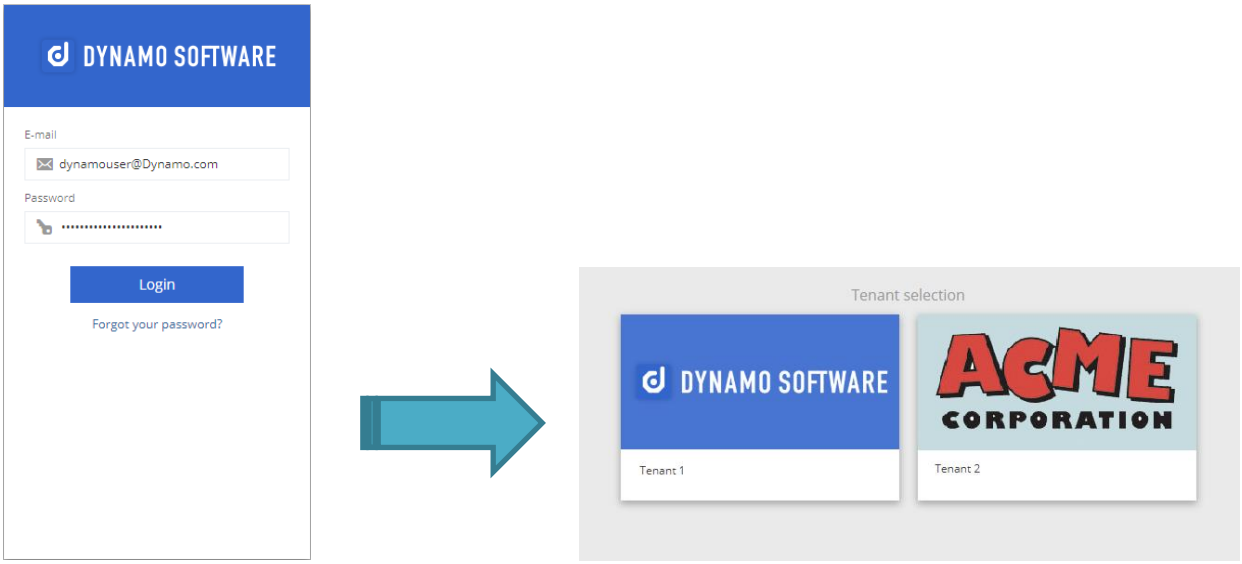
Dynamo no longer supports the contact security question functionality for activating users. The **Security question** and **Security answer** fields are removed from the Contact entity. Dynamo administrators are no longer able to unlock or reset passwords. This process is entirely managed by the end user.

So how would the login work?

Very similar to the way it works today. In fact, users who have only one account across the Dynamo ecosystem will not even notice the change.

Users are presented with a login form on which the username is entered. Dynamo will automatically determine if the user can log into tenants with username/password combinations, SSO providers, or a combination of the above, and present all available options to the user.

If there are multiple tenants for a given login (authentication) method, the user will be presented with a tenant selection after successful authentication.



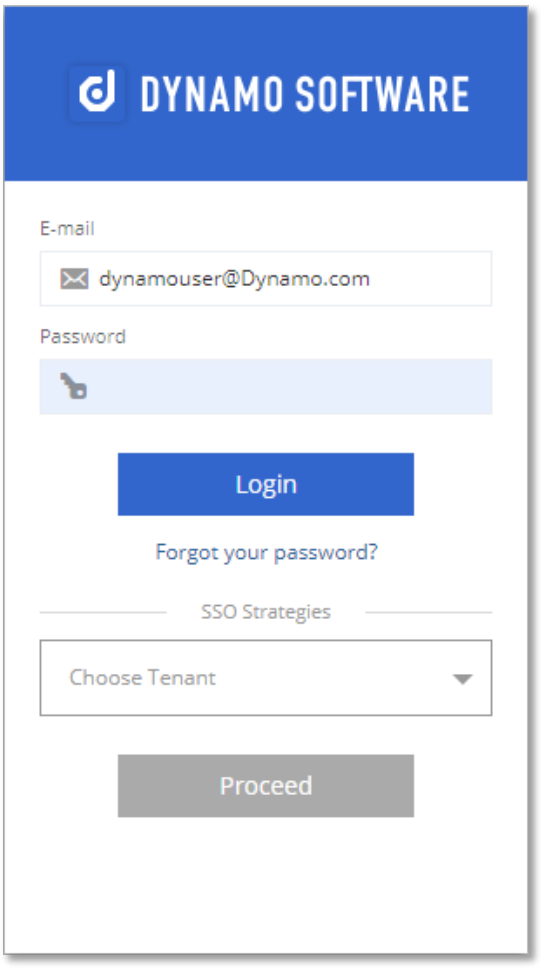
What about tenant-specific authentication methods, such as SSO providers?

SSO providers will continue to function as they have up to this point in addition to (if applicable) Dynamo's standard username/password login.

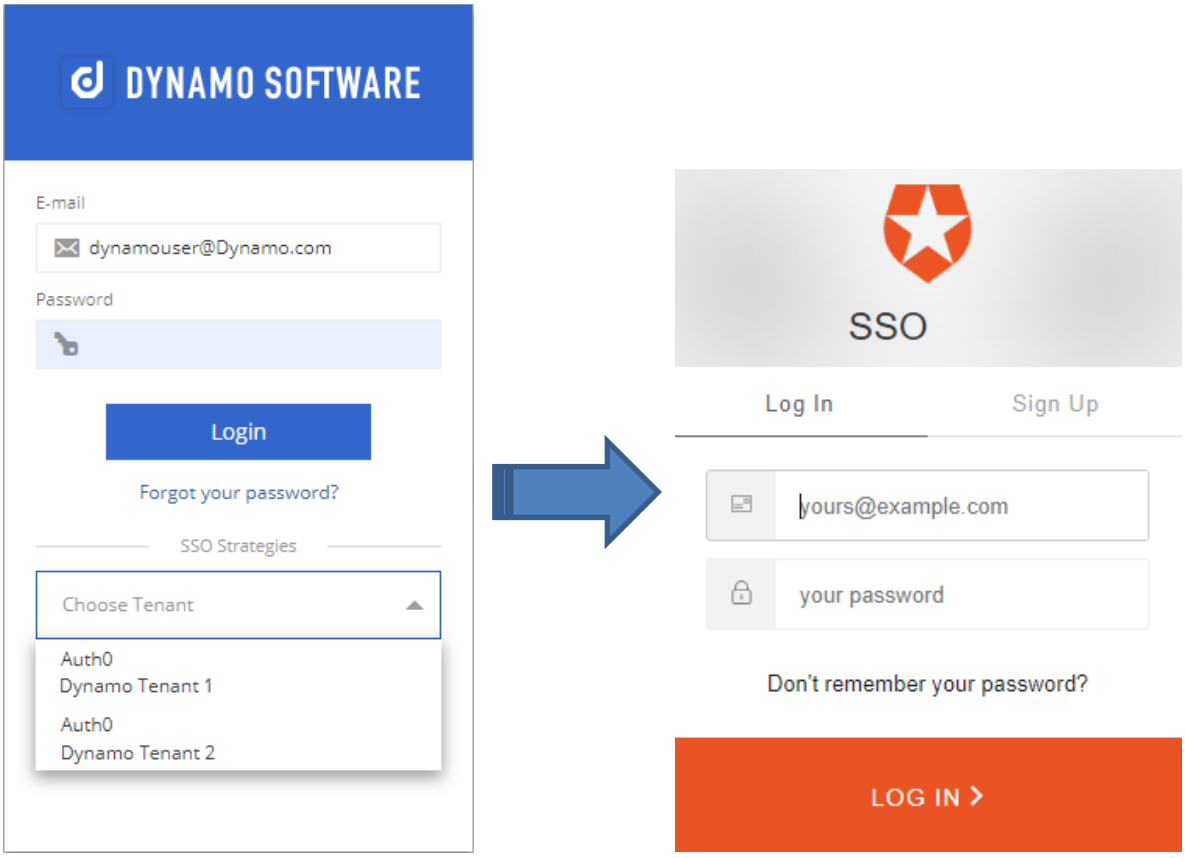
We are introducing the context of a "client domain", which will allow clients to group multiple tenants into a single client domain thus propagating SSO identity providers across all grouped tenants, allowing for a single SSO strategy across all tenants for a given client. For more information about single sign-on (SSO) in Dynamo, please visit our product's help section.

What happens if the login uses SSO service?

If the login requires SSO, the user will see a SSO section on the login form.



To log in to Dynamo, the user needs to enter his/her email address as username for authentication, and then select the desired tenant from the dropdown with available SSO strategies, and click the Proceed button. This action will redirect the user to the respective SSO provider login page. After a successful authentication with the identity provider, the user will then be automatically redirected to Dynamo.



What happens if a user logs in via SSO on one tenant, but not on another?

SSO identity providers are tenant-wide, not user-specific. However, specific login methods can be enforced for single users via the *Allowed login services* setting, which is configured per user. When a user enters their email address on the login page, Dynamo determines which tenants they can access, and what login methods are available to them (both tenant- and user-specific), and presents the user with all relevant login options.

For example, a user may have access to Tenant A and Tenant B, both of which have SSO strategies configured. In this case, there are two possibilities:

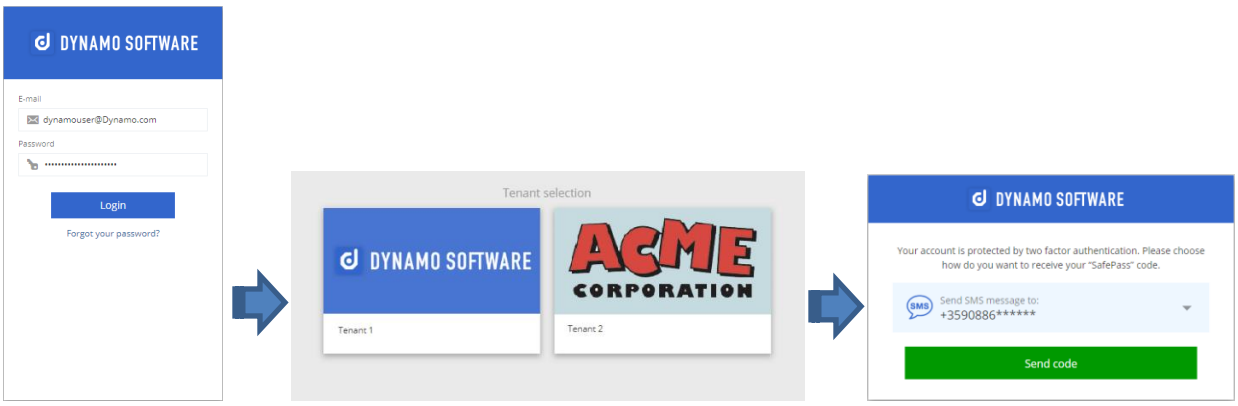
- If no specific login services are allowed for the user on either of the tenants, when they login, they will see password login and SSO providers configured for Tenant A and Tenant B.
- If allowed login services are specified for the user on one of the tenants, e.g. there is 'local' under Tenant B, meaning only password logins are permitted on that tenant, when the user logs in, they will see password login and the SSO providers from Tenant A only (since Tenant B only allows password logins).

Note that if users, which are only able to log into a specific tenant (via a specific URL), access a login page with tenant-specific branding, all of the **tenant** login options are displayed, as the page does not know who the user is.

How do users log in with two-factor authentication (2FA)?

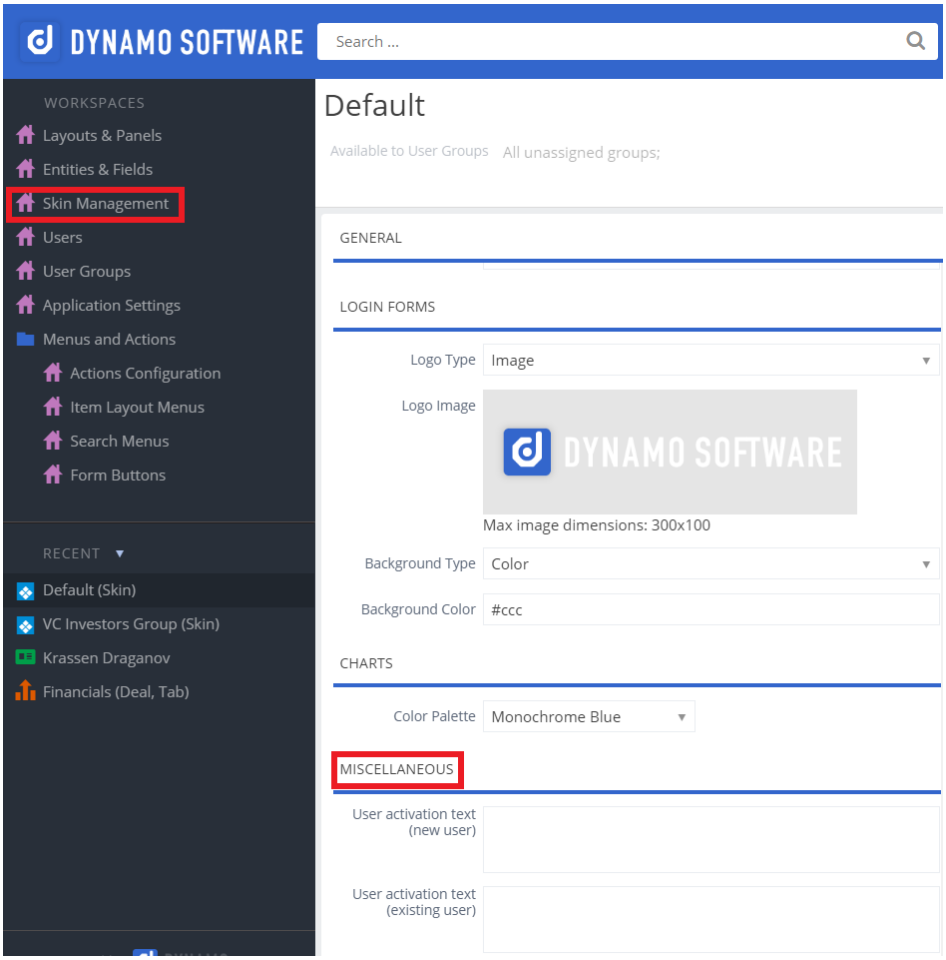
Two-factor authentication settings for each Dynamo user are automatically synchronized across every Dynamo tenant or slot in which the user exists. All authentication sources the user adds or modifies in any of his/her Dynamo tenants are then automatically synchronized with the rest of the Dynamo tenants to which the user has access. (e.g. If a user adds a 2FA requirement when logging into Dynamo, they will need to enter the 2FA code when logging in your tenant even if you have not mandated 2FA for your tenant)

After the user authenticates successfully with username and password, and selects the desired Dynamo tenant, he/she will be required to proceed with two-factor authentication depending on the configured 2FA settings.



Can I modify the text templates of Dynamo account-related Emails?

Yes, clients will have the option to add a personalized paragraph to the text of the email templates for *New User Activation* and *Existing User Activation* email messages. The email templates can be configured in the New UI admin console by clicking on the *Skin Management* Workspace and scrolling down to the *Miscellaneous* section in the corresponding form. (Even clients who are on the Legacy UI can use the Admin Interface of the New UI to configure the Activation template messages. Please, check with your Account Manager or Dynamo support if you need help setting this up).



How this works

When clients configure the Activation template messages, Dynamo automatically checks if the user group has been set up with the necessary attributes and generates the respective information in the following sequence:

1. When there is a new skin assigned to the user group, and the fields which need to be exposed in the email template are populated (e.g. Tenant Name, User activation text, etc.), Dynamo extracts the tenant name and the user activation text from the *Miscellaneous* section of the respective skin, and displays these elements in the email template.
2. If the user group is a portal group with a legacy portal skin assigned to it, Dynamo takes the tenant name from the legacy portal skin, and displays it in the email template.
3. If the user group has a specific Tenant name, Dynamo displays the same name in the email template.
4. When no specific Tenant name is set for the group, Dynamo takes the Tenant name for the tenant-wide setting, and displays it in the email template.

Can user account-related emails be sent from a "real" email address?

No. Centralized Login-related system emails (emails regarding user account activation, resetting a forgotten password, and unlocking an account) are send from DoNotReply@dynamosoftware. The sender cannot be changed. All Dynamo users and portal users receive the same emails from the same sender.

What happens if I forget the password to my administrator account?

By default, administrator accounts have dummy emails, so make sure that you do not lose or forget your password. In case you forget your password, contact Dynamo support to restore it.

What happens if a client uses a custom login URL to log in to Dynamo?

Clients use custom login URLs mostly to provide access to their Portal users. Such clients will still be able to use their custom login URLs. When their users log in to Dynamo, they will be automatically routed to Centralized Login like any other Dynamo users using this functionality.

In addition, Centralized Login allows for "skinned" login pages. If portal users have already bookmarked a URL pointing to a login page with a custom skin, Centralize Login will not interfere with the customized login page. Centralized Login will automatically redirect users to an updated URL while keeping skin customizations.

How would this change affect the Investor Portal link that we currently have on our Public Web site?

Your Investor Portal links will not be affected by Centralized Login. When users click the Investor Portal link on your Public Web site, they will be automatically redirected to Centralized Login. Skin customizations on the login page will be preserved.

Will I lose the branding in my Investor Portal Login Page?

There will be no change to client branding within their Investor Portals – the current branding will carry over without the need for any further configuration.

Will Centralized Login affect how I share links to views and reports?

No. We have taken great care to ensure that Centralized Login will not affect client day-to-day activities. Clicking on a link to a view or report will redirect users to the Centralized Login Page if they are not already logged into the respective tenant.

Will our end user license agreement change as a result of the Centralized Login?

No. New users logging into Dynamo for the first time will go through the same login routine in respect to the license agreement as they go through today.

Will Centralized Login affect how users log into Dynamo Add-ins?

No. Users logging into the Excel, Outlook and other Dynamo Add-ins will go through the same login routine as they go through today, they might just see more tenant names in the "Select tenant" dropdown that shows if someone has access to multiple tenants.

Will Centralized Login affect how users log into Dynamo mobile applications?

No. Users logging into the mobile applications will go through the same login routine as they go through today.

We are a self-hosted client – how will we configure the Centralized login?

The Centralized Login will be rolled out across Dynamo cloud-hosted clients initially. Please, contact your Client Services Representative to coordinate the upgrade.