Admin Center – User Guide

Contents

About This Document

The Admin Center User Guide is designed to provide guidance for initial setup and use of the Admin Center application by Tyler Technologies, Inc. clients. The content in this document is organized to progressively introduce the Admin Center for a typical client situation in which Tyler implementation teams have installed and configured products with defaults. It is recommended to consume the document in the presented order of sections:

- *Overview* – provides a high-level overview of the Admin Center
- *Getting started with Admin Center* – Accessing the Admin Center
- *Managing security* – Configuring/customizing your Tyler Identity Workforce instance
- *Organization setup* – Setting up your organization details and preferences
- *Using the Admin Center* – On-going administrative activities, including managing employee and non-employee back-office users, workspaces, access to participating Tyler applications, and accessing product administration applications.
- *Getting support* – Options for getting support

This document does not cover content related to using specific Tyler products. Reach out to your product support team if you need assistance locating documentation for a particular product or solution.

Intended Audience

The audience for this content is client Information Technology (IT) or systems administrators, and other roles that are responsible for some or all the activities listed above. Some functionality like federations and network security may require specialized knowledge in those domains. This document does not cover evaluating, preparing, or configuring any technology or resource managed within your organization from which information is solicited in the Admin Center.

Email address domain whitelisting

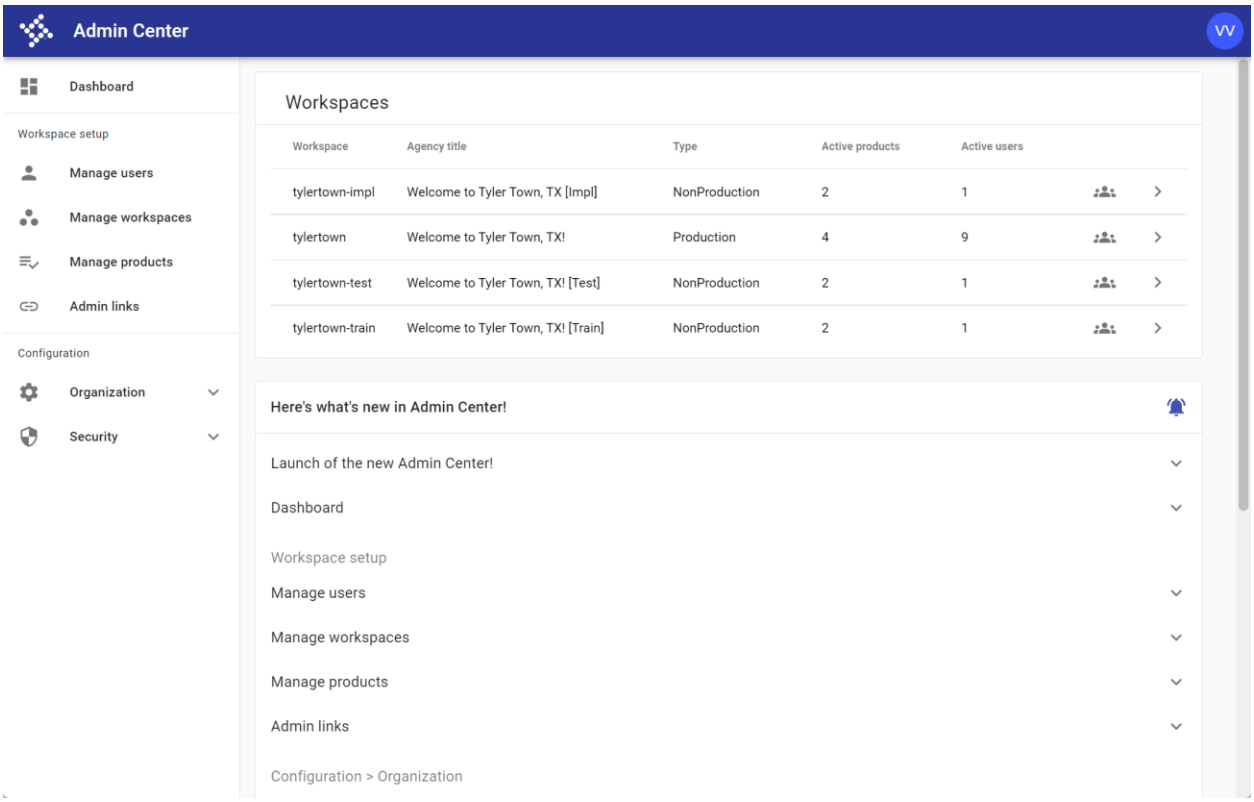
If your organization uses enterprise spam blocking solutions, whitelist the email address domains **okta.com** and **tylerportico.com** to allow invitation and other emails to pass through.

Content note

The screenshots and content in this guide are intended to only approximate your actual experience. Since we update the Admin Center frequently, there may be differences between the content in this document (including screenshots, and options available) and current state of the application.

Overview

The Admin Center is a centralized administrative tool to manage Tyler Identity Workforce and participating Tyler solutions and serves as a starting point for administrative tasks typically performed by client IT administrators.



Dashboard

The Dashboard is the page that you are first taken to upon sign-in. It presents a list of *workspaces* that have been setup for you and a notification area for the latest in the Admin Center.

Workspace

A workspace is an independent instance (copy) of your Tyler solution(s). Typically, you are provisioned a production instance, and one or more non-production instances.

What's new in Admin Center

The what's new in Admin Center is where you can see the latest updates to the Admin Center. The is organized by the same sections and sub-sections as seen in the overall Admin Center for consistency.

Workspace setup

This section deals with the management of Workspaces. Users of an organization can be added and assigned to workspaces, and then provided access to specific applications within those workspaces. Additionally, Tyler products that have been enabled on each workspace and the various applications under each can be seen and accessed (subject to you having access to them).

Only participating Tyler products and applications are available for management using the Admin Center currently. Please reach out to your product support to inquire if a product is available for administration and access through the Admin Center.

Manage users

This sub-section allows you to add new users or import users in bulk into the Tyler Identity Workforce solution. For non-federated users, this section can also be used to provide end user support (resend password emails, etc.). You can also inquire or set what access rights a user has or promote specific users as site administrators to grant them access to the Admin Center.

Manage workspaces

This sub-section lets you administer workspaces provisioned for your organization, including workspace settings. Some of these can also be managed globally at an organizational level for ease of maintenance (see *Configuration > Organization* below for more information). You can also create User groups to define application access which can then be assigned to users.

Manage products

This sub-section allows you to see all products and applications licensed to each workspace, including statistics of applications available for back-office (Workforce) and public facing (Community) and serve as a launch point for the applications.

Admin links

This sub-section allows you to access product administration applications that you have access to through *User groups* setup under *Manage workspaces*.

Configuration

This section is used to maintain organization wide configuration settings.

Organization

This sub-section is used to maintain core organization information and preferences like contact information, branding preferences, common organizational links, and approved domains for adding user email addresses.

Security

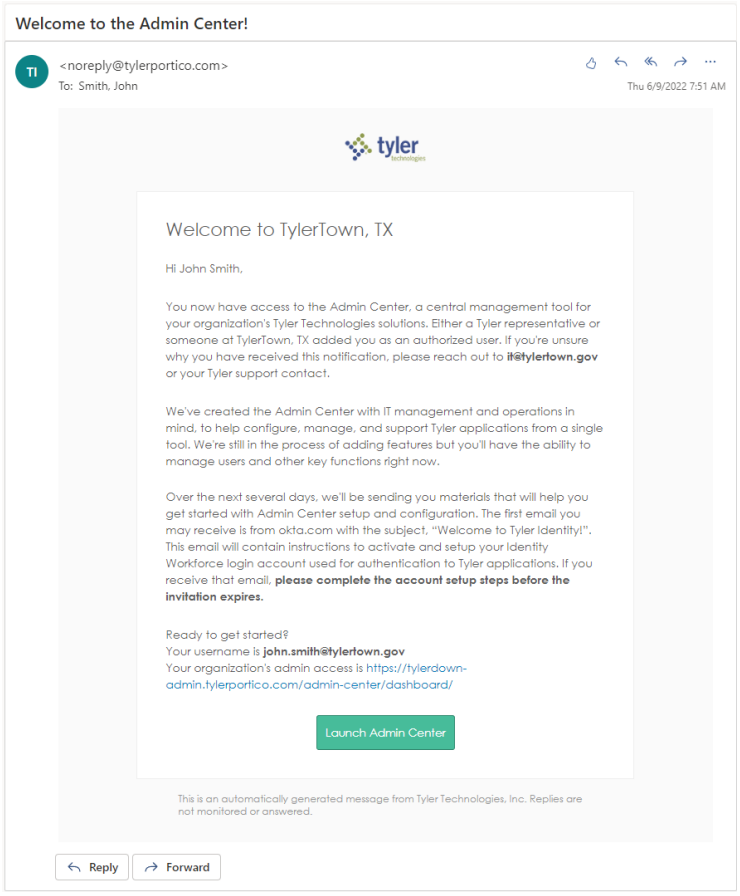
This sub-section is primarily used to maintain the configuration of the Tyler Identity Workforce solution. Depending on the licensing tier, you may be presented with different configuration options for password policy, etc.

Getting started with Admin Center

Getting Access

Initial access to the Admin Center for your organization will be provided by Tyler implementers as an email invitation. The email invitation will contain a link to the Admin Center and any additional instructions you may need to follow to set up your initial account. *We recommend you bookmark the URL in the invitation for quicker navigation in the future.*

The link to the Admin Center is of the construct:
https://<<your customer identifier>>-admin.tylerportico.com/admin-center/dashboard



Contact your Tyler implementation or support representative if you haven't received any invitation email.

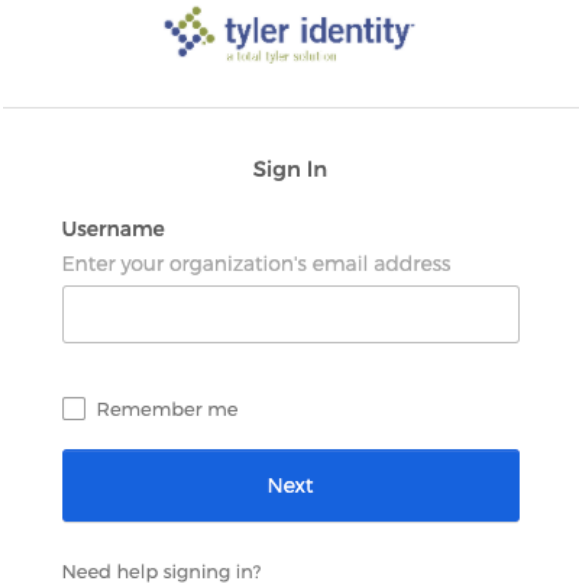
You may also receive additional emails to activate your account, set a password and enable Multi-Factor Authentication (MFA).

Navigating to the Admin Center

Click on the link provided in your invitation mail, your bookmark of the same link, or navigate to *https://<<<your client identifier>>>-admin.tylerportico.com/admin-center/dashboard*, replacing *<<<your client identifier>>>* with the specific identifier assigned for your organization.

Enter your Tyler Identity Workforce email address

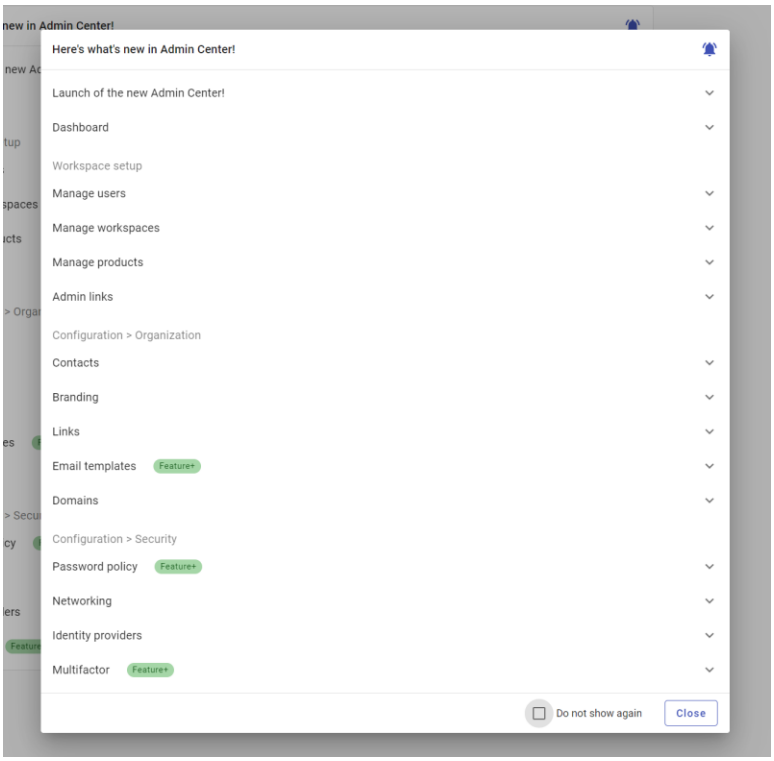
Enter your Tyler Identity Workforce credentials as prompted. This is the same email address as the one in which you received your invitation email. If your organization has already been federated, then you may see additional login screens managed by your organization after the initial email address screen.



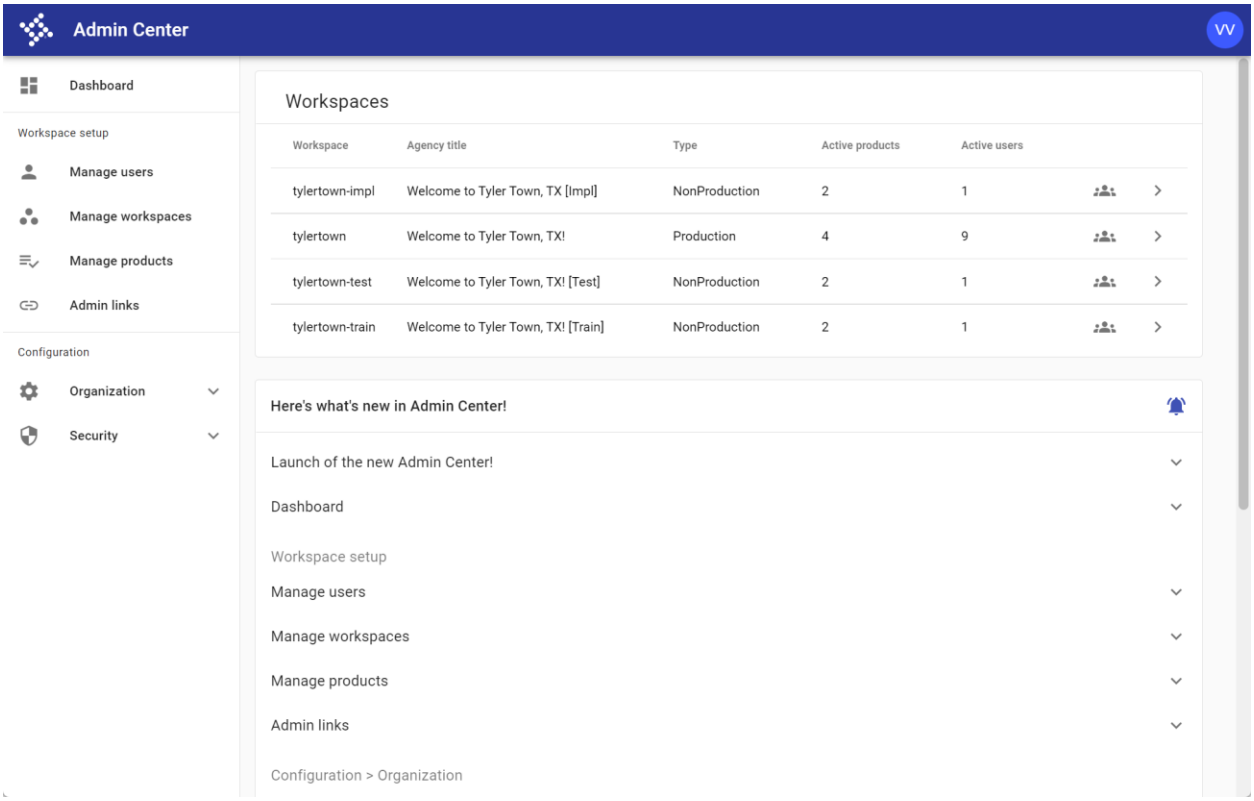
Contact your Tyler implementation or support representative if you are not sure which email address you are supposed to use with the Admin Center.

Complete sign-in and access the Admin Center dashboard

Upon sign-in, you may be presented with a "What's new in Admin Center!" dialog that you can close using the *Close* button. If you do not wish to see this again as a separate dialog, you can check the box against *Do not show again* before clicking the *Close* button. The content on the dialog is also presented in the *Dashboard* for future review.



You will then land on the Dashboard and see any Workspaces setup for your organization and a notification area announcing the latest updates to the Admin Center for the various sections.



Managing security

This section allows you to configure the Tyler Identity Workforce solution provisioned for your organization.

Tyler Identity Workforce (TID-W)

Tyler Identity Workforce (TID-W), used for back-office applications and managed by your organization, is distinct from the Tyler Identity Community (TID-C) solution, which is used for Community (public) applications. This document is applicable only to the Tyler Identity Workforce instance assigned to your organization, though some options like branding preferences may affect Tyler Identity Community in a limited way. Tyler Identity Workforce has multiple tiers of subscription and some of the functionality presented in this document is only available to clients with advanced tiers.

Tyler Identity Workforce supports two different types of workforce users: **Local Identity Users**, that are managed by the Tyler Identity Workforce solution, and **Federated Users**, when authentication to Tyler solutions is delegated to your organizational identity provider (IDP), and therefore are managed by your organization. At the Tyler Identity Workforce Core product tier, you can:

- Mix Local Identity Users and Federated Users
- Federate to a core IDP such as Azure Active Director (AD), Google Identity (Enterprise), Active Directory Federated Service (ADFS), and Okta.
- Sync a local Active Directory using the Okta AD Agent to Tyler Identity Workforce

Admin Center allows you to administer Local Identity Users and manage Federations. There are additional options to manage users and personalization at the Tyler Identity Workforce Advanced tier and higher.

To learn more about Tyler Identity Workforce Advance tier or using the Okta AD Agent, reach out to your Tyler Sales and Support contacts respectively.

Local Identity vs. Federated Users – Benefits and Disadvantages

Local Identity Users can be setup out-of-the-box and are ready to use right away. They are particularly useful when some of your back-office users are not part of your organization and therefore do not have an organization provisioned email address, or otherwise part of your organizational authentication systems. Some disadvantages of Local Identity Users are that you may have to manage them separately from the rest of your organization using the Admin Center should they lose their passwords, to resend activation emails, etc., and it exposes multiple security concerns, like users openly saving multiple passwords to different systems on their desks or PCs, and the need to remove their permissions in multiple systems when their engagement with your organization ends.

Federated Users on the other hand requires Federation be setup which requires an internet facing identity provider managed by your organization. Once setup, however, Federated Users enjoy Single Sign-On (SSO) experience without having to remember multiple passwords, and the organization's IT can simply disable an employee's ability to authenticate centrally without having to immediately disable their access and permissions on multiple systems when their engagement with the organization ends. Given the vastly superior security benefits of Federation, Tyler strongly recommends that you federate your organization's IDP when possible. You can, in parallel, use Local Identity for those users who are

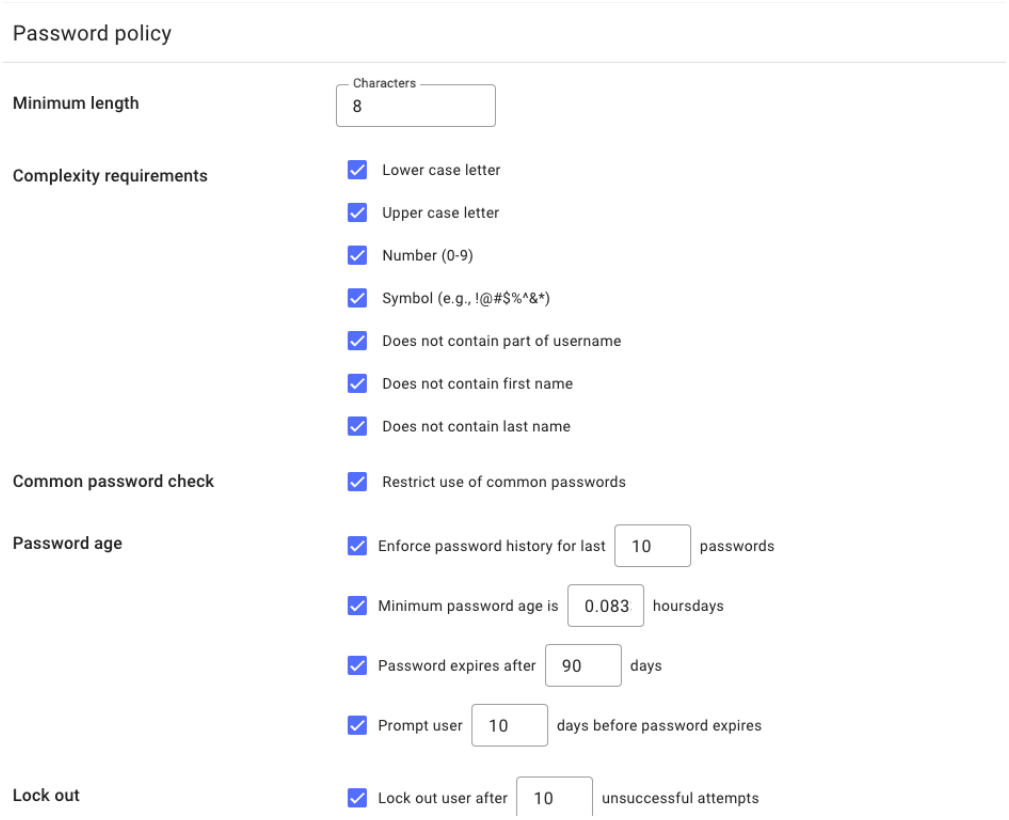
not part of your organization's IDP as identified through their non-organizational domain in their email address.

Local Identity Users

If you are planning to support Local Users, review the default settings on your Tyler Identity Workforce tenant.

Password Policy

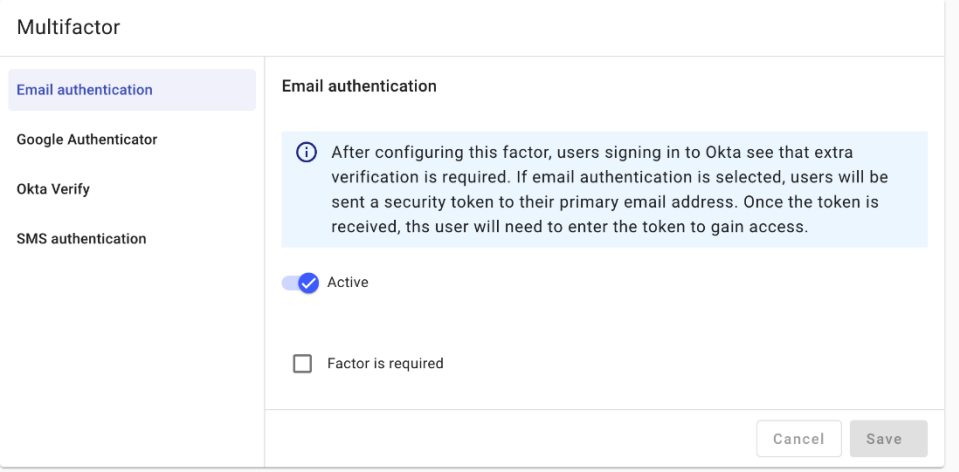
The default settings on your Tyler Identity Workforce are designed to meet Criminal Justice Information Services (CJIS) baseline requirements. Navigate to *Identity configuration > Password policy* and review the defaults. Modify the values to your organization's preferences.



Multifactor authentication (MFA)

Multifactor authentication is highly recommended for Local Users. Navigate to *Identity configuration > Multifactor* and select from one of the available options. Under any of the options, click on the *Inactive* toggle to allow for the specific method of MFA for your Tyler Identity Workforce users and fill out any additional options as appropriate. Email authentication-based MFA is included in the Tyler Identity Workforce Core tier.

Google Authenticator, Okta Verify, and SMS authentication are only available with higher tiers of Tyler Identity Workforce solution.



Federated Users

Federation is the delegation of user or application authentication to an external identity provider (IDP) typically managed by your organization. Federation involves an initial setup that requires the following as a minimum:

- Dedicated email address domain(s) for your organization
- An internet-accessible supported Identity provider (IDP) like ADFS, Azure, Google Cloud Identity, Okta, Rapid Identity, etc.
- Technical knowledge to generate necessary client credentials in your IDP
- Use the Admin Center to enter the client credentials against your email address domain(s)

Federation works by redirecting users on the Tyler Identity Workforce sign-in screens to your organizational IDP based on the domain on the entered email address. Multiple federations can be setup for different domains, but there can only be one federation IDP per domain.

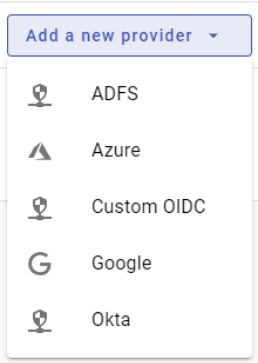
Federation involves two specific activities to completed before it is active:

1. Creating or registering a client on your organization's IDP to identify Tyler Identity Workforce as a broker or consumer of the IDP. This step will provide some details (which can differ considerably based on the type of IDP involved) that you will use towards the next step.
2. Use the information collected above to register the IDP using the Admin Center under the *Identity Providers* section.

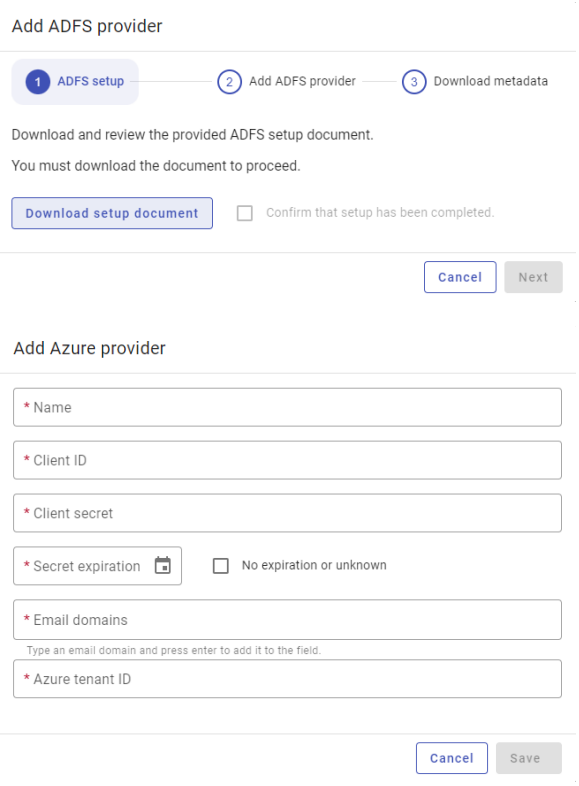
It is beyond the scope of this document to assist you with the first step of creating or registering a client on your organization's IDP. Please reach out to your IDP's support team to understand how to complete this process. Some details might be available here under Okta's documentation: https://developer.okta.com/docs/guides/identity-providers/#enterprise-identity-providers (*Enterprise Identity Providers* section)

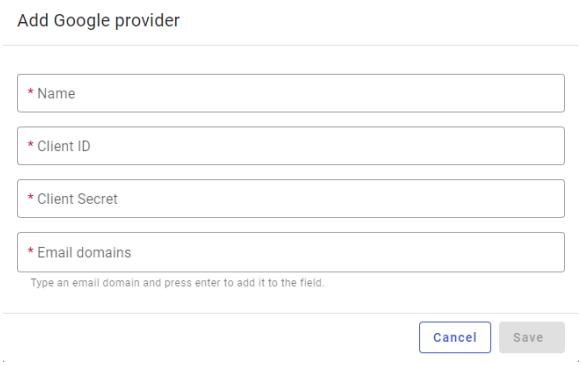
Identity providers

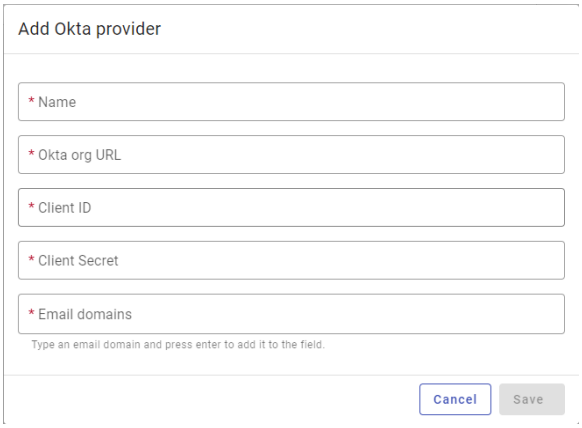
Navigate to *Security > Identity Providers*. Click on *Add a new provider* to see a list of available options. The Tyler Identity Workforce Core solution supports ADFS, Azure (*Enterprise solution, non-social, IDP*), Google (*Enterprise solution, non-social, IDP*), and Okta as IDP providers.



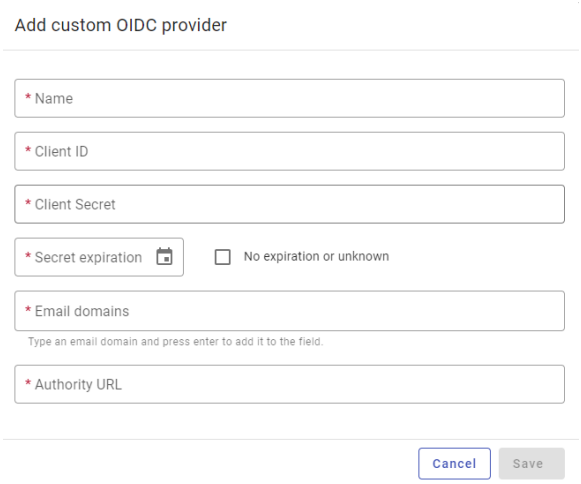
Select the option that matches your internet facing IDP. Each option presents a different set of instructions or data required to be entered. Please work with your IDP support to complete these steps successfully. If setup correctly, you can attempt to login again into the Admin Center (*tip: use an incognito or private browser window and access the Admin Center link to test federation*) and ensure that the login screen is redirected to your organizational IDP after you enter your email address in the *Username* field on the first sign-in screen.





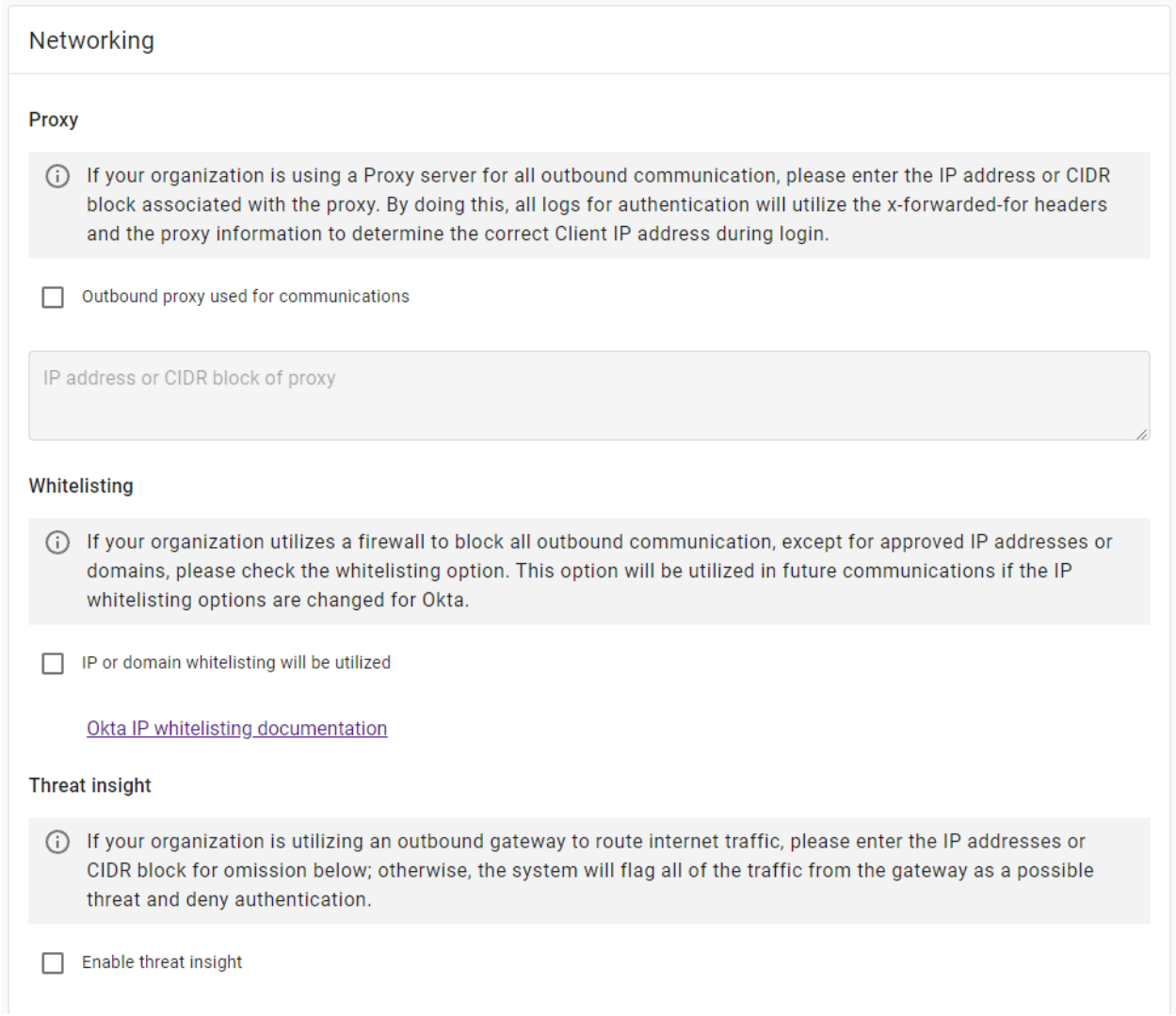


Custom OIDC shown below is only available in higher Tyler Identity Workforce tiers. If you do not see Custom OIDC as an option under the provider's list and are interested in this functionality, reach out to your Tyler sales representative to discuss subscribing to a higher tier of Tyler Identity Workforce solution.



Networking

The networking section controls how Tyler Identity Workforce interacts with your organization's network setup and trust it as an authorized source of network traffic. This affects all interactions, including user and application authentication attempts.



Proxy

If your organization uses a proxy server for outbound network traffic, check the *Outbound proxy used for communications* option and specify the IP address or CIDR block of the proxy server so that Tyler Identity Workforce can process the network traffic header information correctly for maintaining authenticated sessions.

Whitelist

If your organization uses IP whitelisting for outbound communications, then you can configure the firewall using the details under *Okta IP whitelisting documentation*. By checking the *IP or domain whitelisting will be utilized* box, the Identity support contact (see *Organization setup > Contact information* further down the document) will be alerted to any future updates to the whitelist.

Threat Insight

If your organization uses an outbound gateway to process all traffic from your network to the internet, specify the IP address or CIDR block of the internet gateway. Without this information, your gateway

could potentially be identified as a malicious (denial-of-service attack) source due to the volume of traffic originating from a single source and blocked from accessing the Tyler Identity Workforce solution.

Organization setup

We recommend that you use the following steps below to perform the initial setup. Click Save to save changes where applicable after making modifications.

Prerequisites

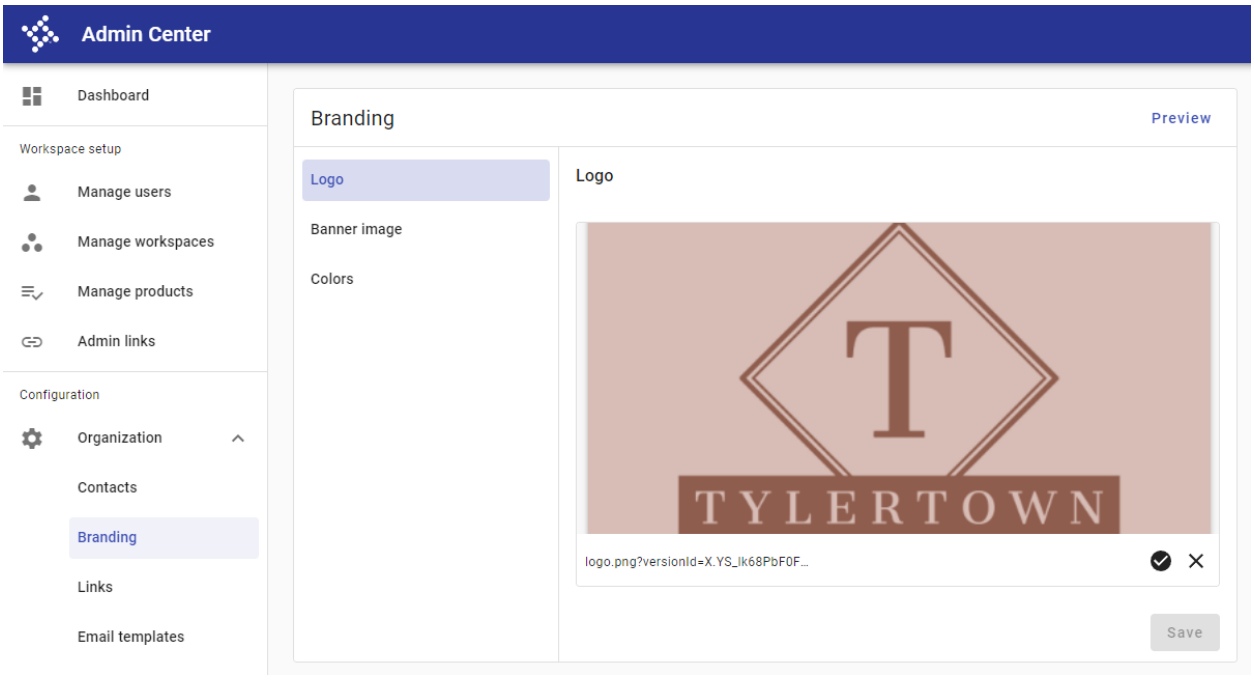
We recommend that you have your organization logo (under 500kB, square form factor, PNG format) and banner image (under 500KB, 960 pixels wide, landscape form factor, PNG format) available before you proceed.

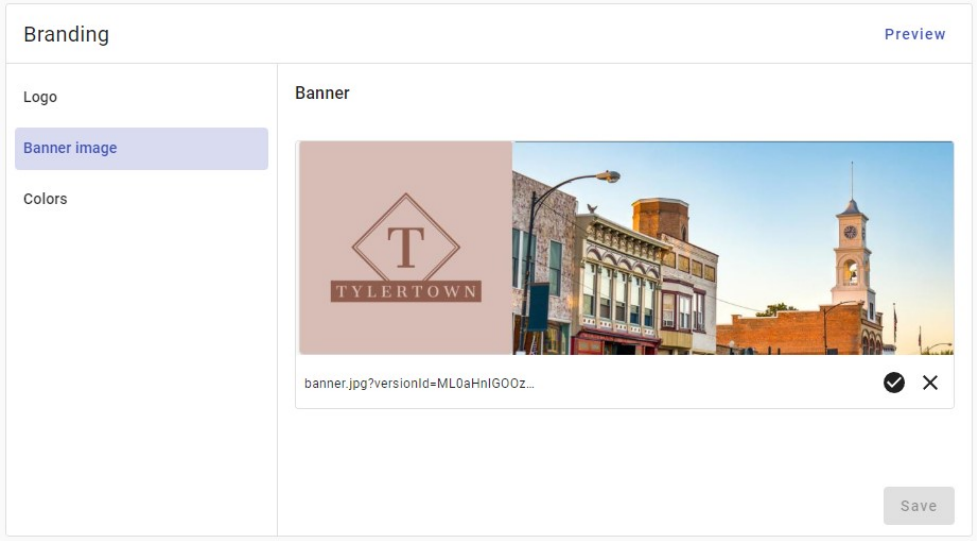
We recommend that you identify the appropriate employee to be used as a business contact for Tyler solutions.

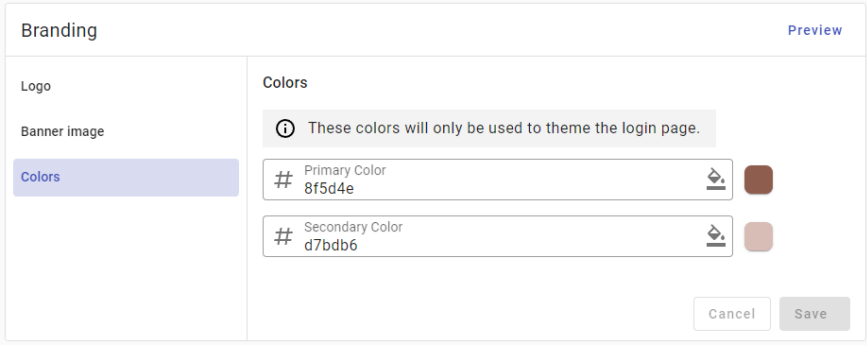
Branding

Navigate to *Organization > Branding*. Under *Logo*, *Banner image*, and *Colors*, upload your Logo, Banner image, and set the Tyler Identity Workforce login page theme colors.

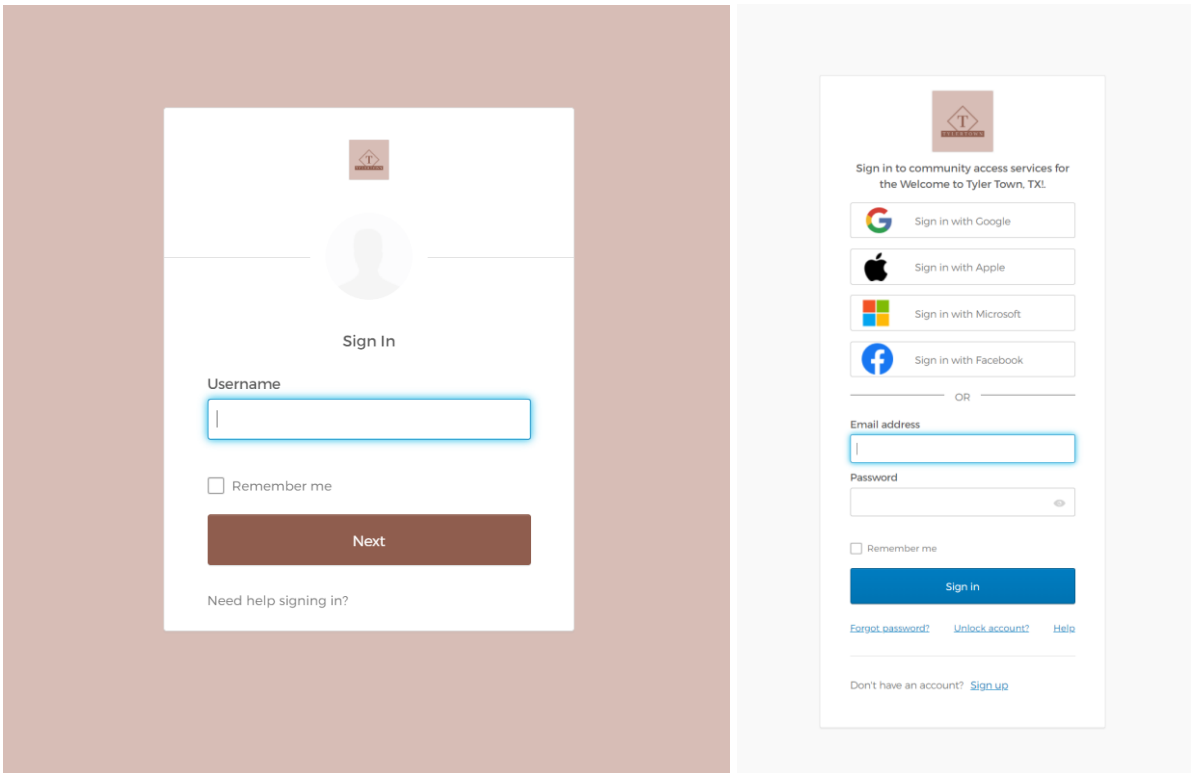
You may need to trim or change the aspect ratio of your banner image to get the desired display.





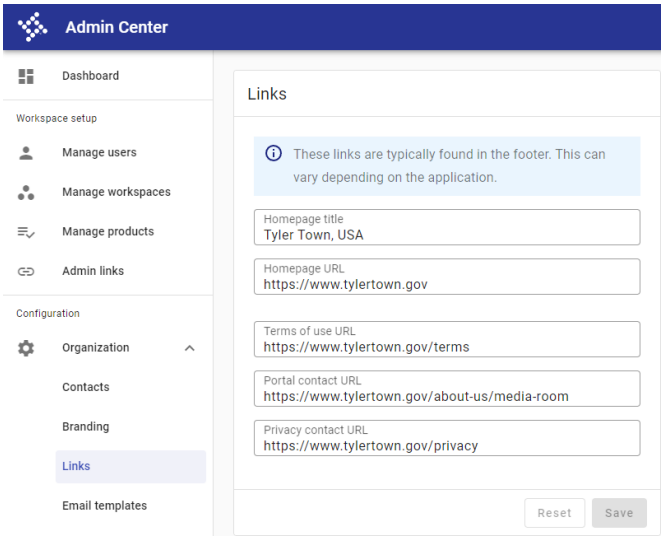


The Logo and Colors are used in the Tyler Identity Workforce solution (left image below), while only the Logo is used for Tyler Community access (right image below).



Links

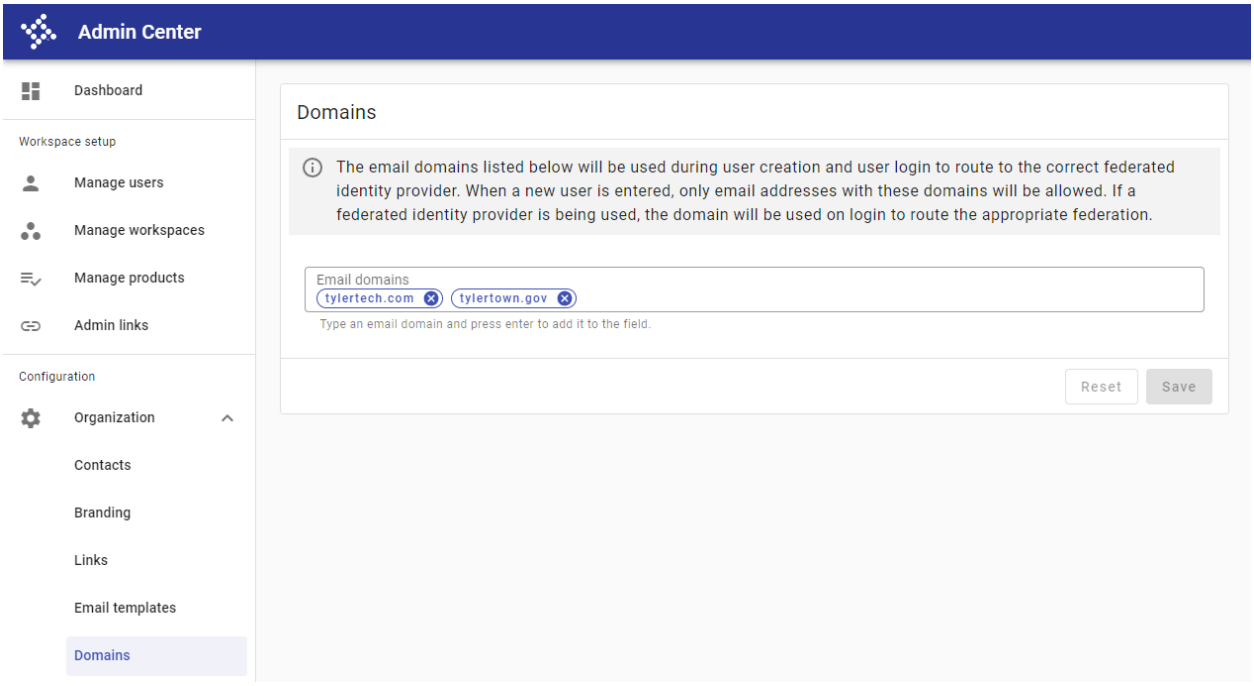
Navigate to *Organization* > *Links*. Set any links available for your organization as applicable.



Domains

Domains allows you to specify the email address domains that you wish to allow for your organization's users. Only email addresses containing these domains will be allowed to be added as users to your organization using the Admin Center. Enter the domain value alone without any @ and press Enter to add the domain.

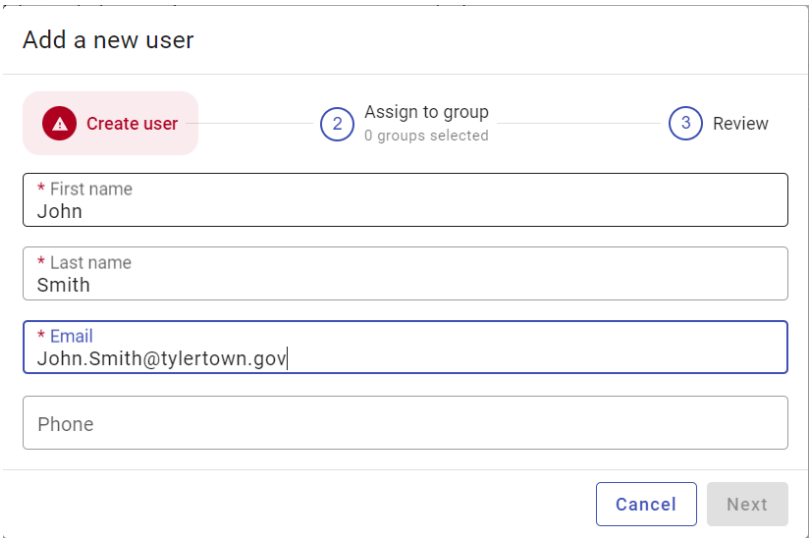
We recommend that you add 'tylertech.com' as an allowed domain to provide access to Tyler Support in the future.

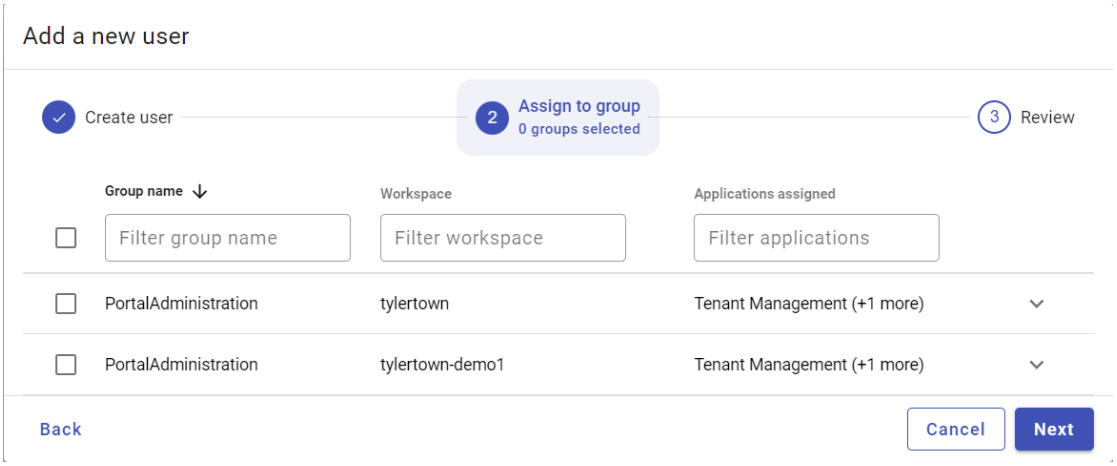


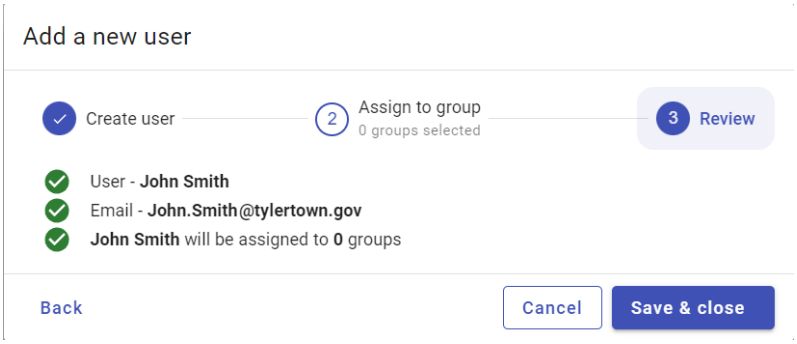
Adding contact information users

Before you can set the organizational contact information, they must be first added add users to the Tyler Identity Workforce solution. These contacts may receive alerts and notifications from the Admin Center and/or Tyler support personnel. We recommend the Business, Technical, and Identity support contacts are different people. Additionally, for Technical and Identity support contact, we suggest using an email alias encompassing multiple administrators instead of an individual contacts to account for employee attrition and non-availability.

Navigate to *Workspace setup > Manage users*. Click *+ Add user*. To add the Business contact, fill out the *First name*, *Last name*, and *Email* fields appropriately and click *Next*. You can skip assign to group at this time and click *Next*. Finally, click *Save & close* to save the new user. Repeat these steps for the Technical and Identity Contact (or alias as appropriate).

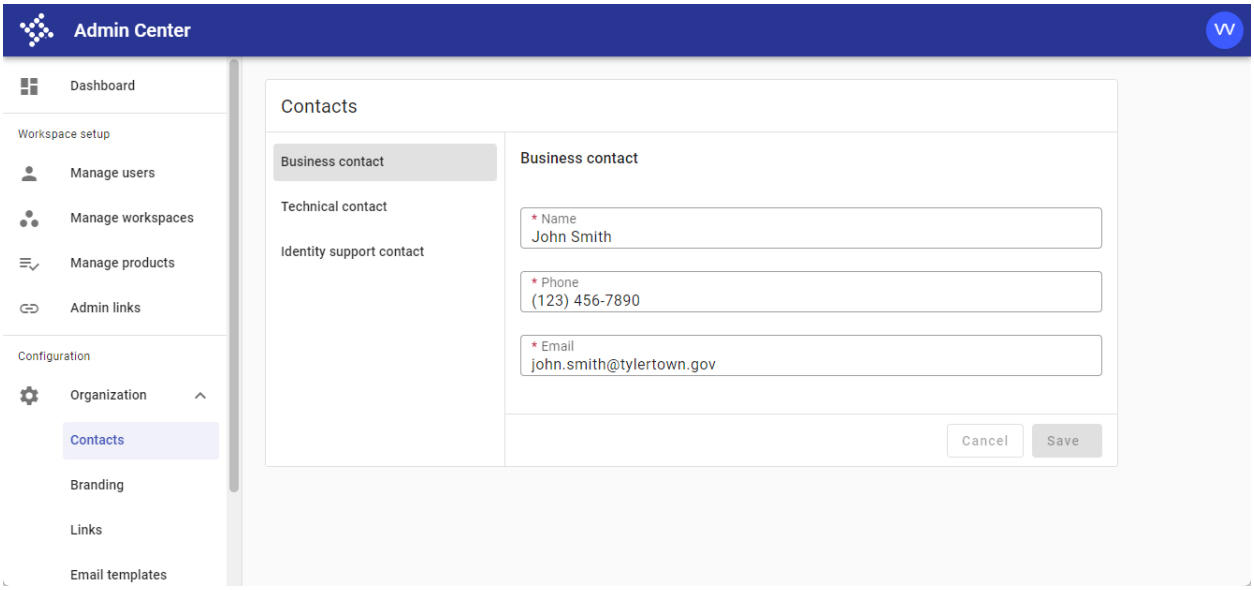


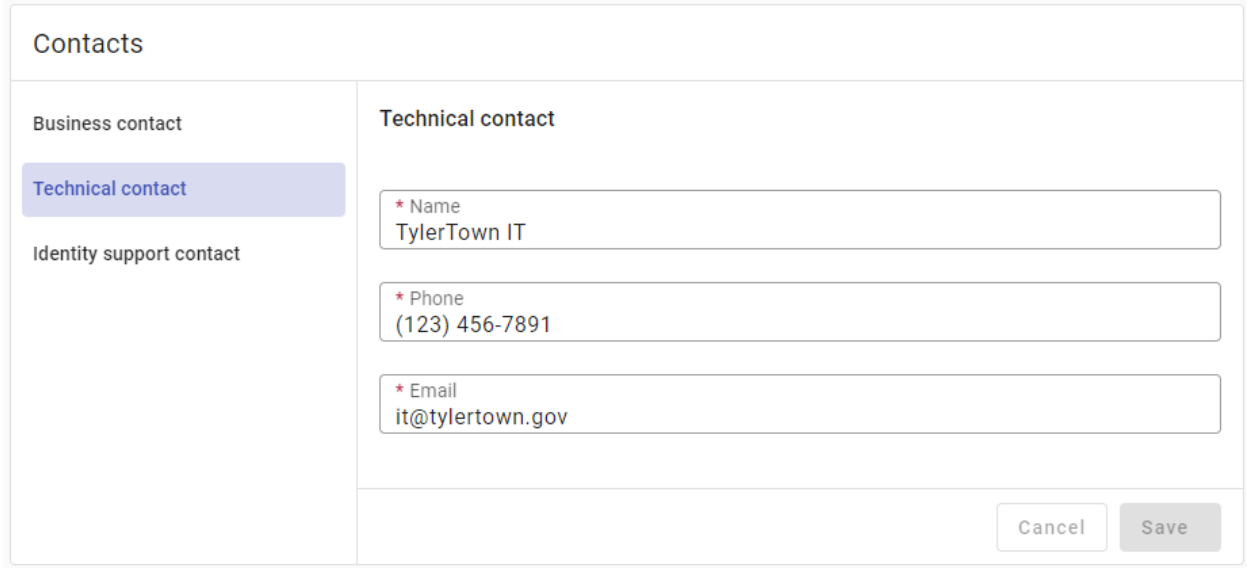


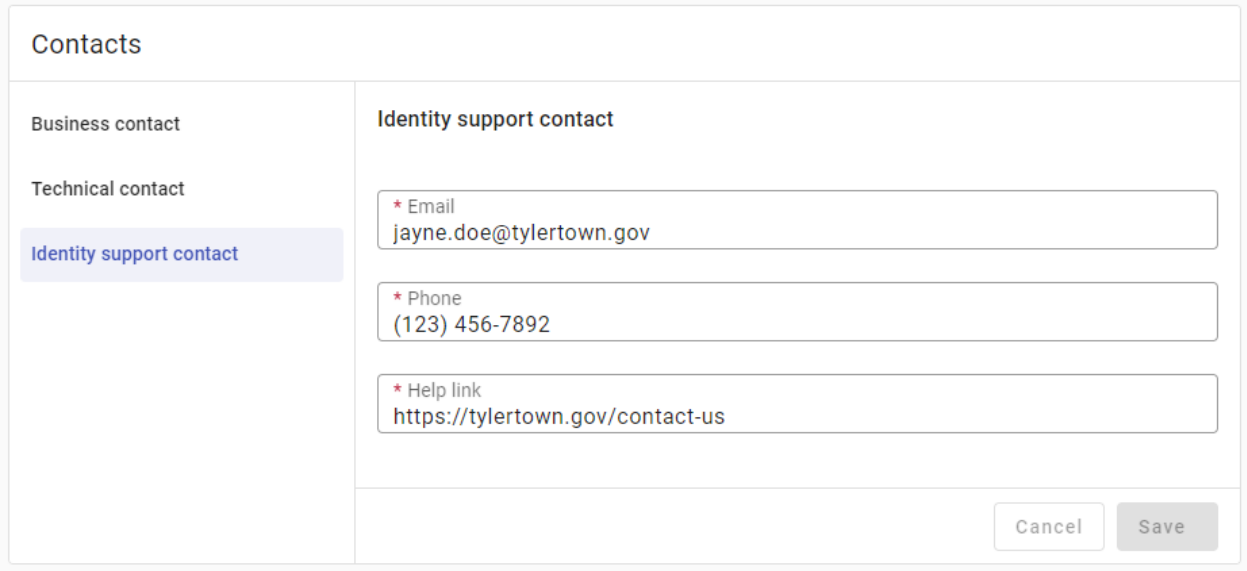


Contact information

Navigate to *Organization > Contacts*. Add or modify the Business, Technical and Identity support contacts.



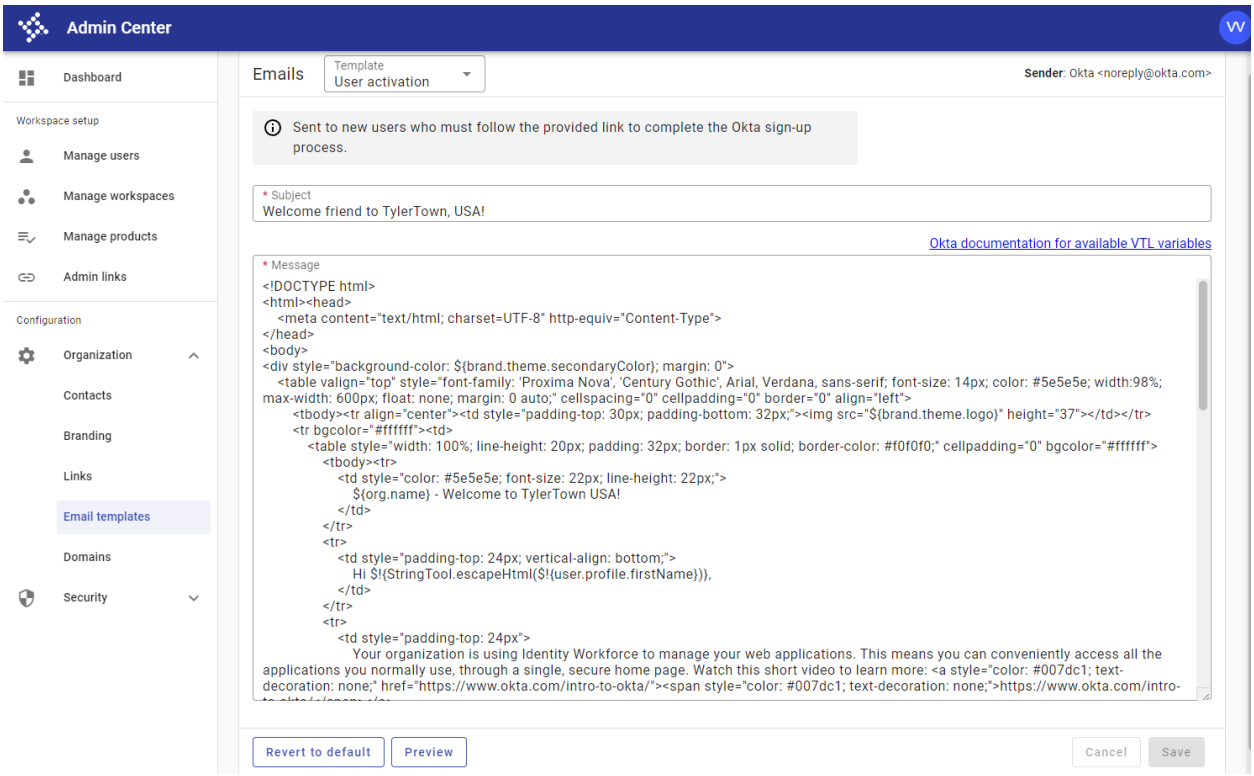




Email templates

Email templates is only available with higher Tyler Identity Workforce tiers. If you do not see Email templates as an option in the Admin Center > Organizations and are interested in this functionality, reach out to your Tyler sales representative to discuss subscribing to a higher tier of Tyler Identity Workforce solution.

You can customize the email templates used to send email communications to back-office users. The templates use standard html markdown with the ability to use embedded dynamic variables using the Velocity Templating Language (VTL).



Navigate to *Organization > Email templates*. To select the template to be modified, click the *Template* drop-down at the top of the page and select from one of the options below:

- User activation
- Forgot password
- Forgot password denied
- Password reset by admin
- AD user activation
- AD forgot password denied
- AD forgot password
- LDAP user activation
- LDAP forgot password
- LDAP forgot password denied

Some email templates only apply to Local Identity Users, while others are only for Federated Users (AD or LDAP based setup). For more details, see: https://developer.okta.com/docs/guides/custom-email/main/#use-customizable-email-templates

To understand what VTL variables can be used in the template click on *Okta documentation for available VTL variables* above the template editor.

Using the Admin Center

This section covers performing administrative activities using the Admin Center. Some activities covered under this section only applies to participating Tyler solutions.

Manage Users

This section deals with managing Local Identity Users and Federated Users on the Tyler Identity Workforce solution. Different management options may be presented depending on the type of user.

Users of community applications (Vendor access, Resident access, etc.) utilize the Tyler Identity Community solution and are therefore not managed by the Admin Center. Only their corresponding administrative applications (Vendor access administration, Resident access administration, etc.) with back-office users performing these administrative functions are expected to be included in the Admin Center.

Some applications may not require routine back-office users to be added and granted access to it first. Please check with your Tyler product documentation or support to find out if this required for the solution.

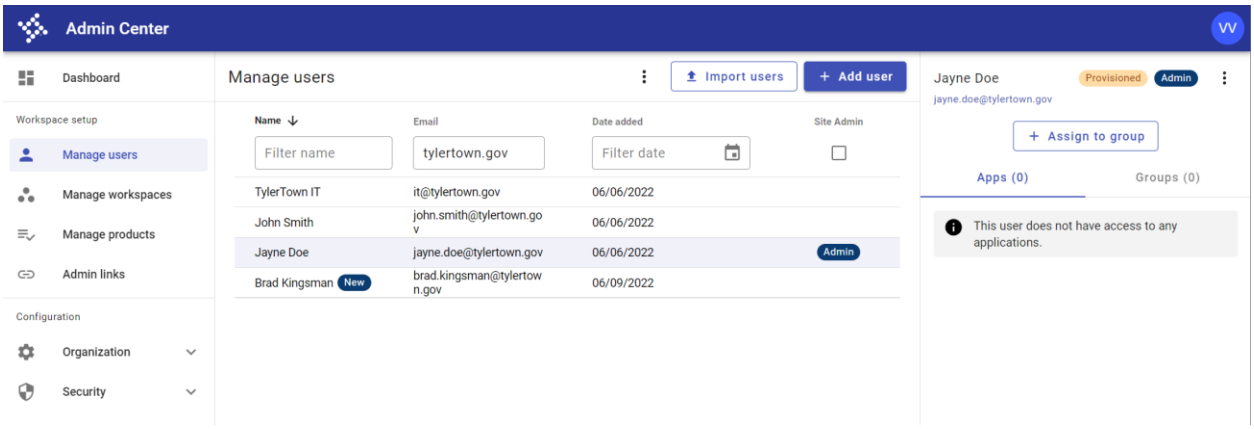
Prerequisites

Ensure that every email address domain from which your back-office users can originate from are added under *Configuration > Organization > Domains* as demonstrated under *Organization setup* discussed earlier in this document. This additional setup requirement ensures that users from non-approved domains are not accidentally added as users. You many need to add social media email address domains

(gmail.com, outlook.com, hotmail.com, yahoo.com, etc.) if you expect non-employee Local Identity Users to be accessing enterprise applications (e.g. Employee Access).

Overview

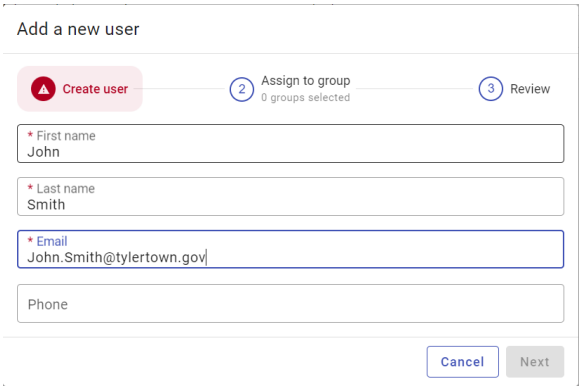
You can see a list of current users in the main section and their status in the details section to the right. To add back-office users to allow for Single Sign-On (SSO) experience across participating Tyler solutions, you can use the *Add user* option for adding a small number of users or *Import users* for bulk user addition. You can use any of the filters to narrow down the list of users you want to see under *Manage users*. Additionally, you will see an *Admin* label against users who have been promoted as Site Admin on Tyler Identity Workforce which grants them access to the Admin Center, and *New* label against users just recently added. You can also assign a user to a group or see what groups they are already added to (See *Managing workspaces* later in this document for more details on *User groups*).



Adding a single user

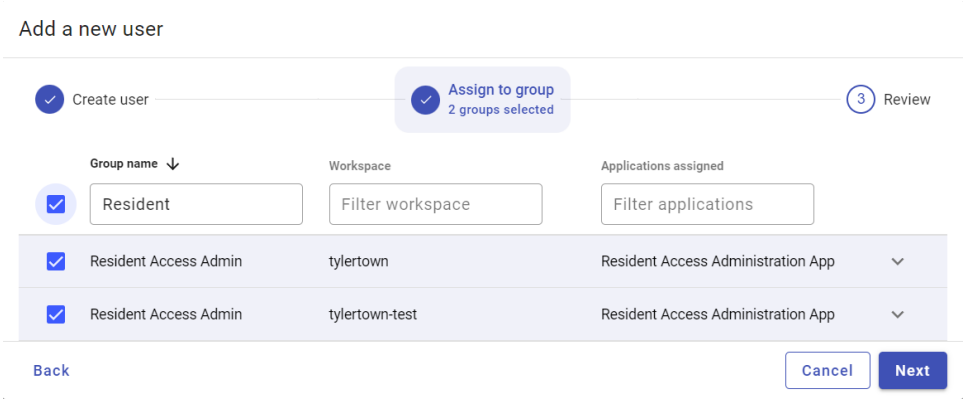
To add a single user or a small number of users, click on *+ Add user*.

On the first tab *Create user*, enter the *First name*, *Last name*, and *Email* address of the user. If you enter an email address with a domain that wasn't previously added to the *Configuration > Organization > Domains* list, you will be prevented from adding the user. Optionally enter *Phone* information and then click *Next*.

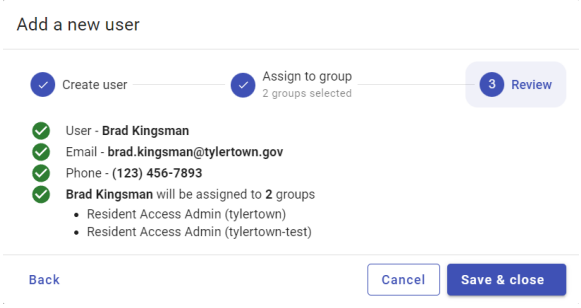


On the *Assign to group* tab, filter to existing groups that you wish to add the user to (see *Managing workspaces* section of this document to learn more about *User groups*). You can choose not to assign

the user to any groups at this time and do this step later. After selecting any groups, click *Next* to go to the *Review* tab.



On the Review tab, confirm all the details for the new user and click Save & close to add the user to Tyler Identity Workforce. Depending on whether the user is a *Local Identity User* or a *Federated User* and the organizational preferences setup for email templates, the user may get emails sent to them potentially with instructions to complete the rest of their account setup like activation, setting a password and multi-factor authentication.

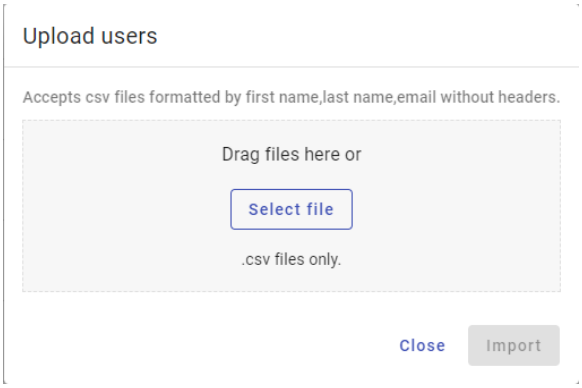


Importing users in bulk

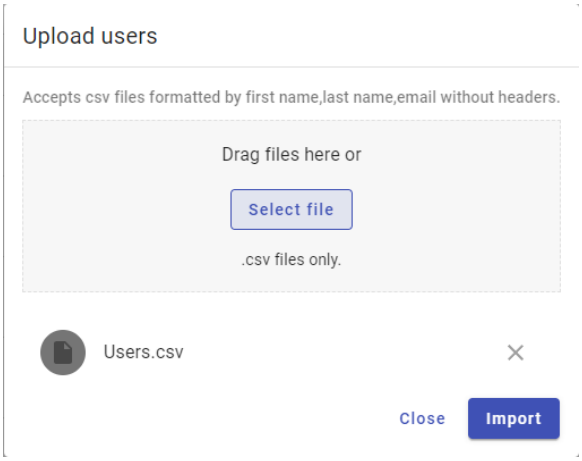
Importing users in bulk is useful when you have more than a handful of users to add, which can quickly become tedious using the *Add user* option. A key distinction between this method and *Add user* is that the latter lets you pre-assign *User groups* when creating the user. Importing users, therefore, requires a separate step to assign imported users to groups if desired.

You must first prepare a Comma Separated Variables (CSV) text file using the construct first *name,lastname,email* without any heading row, spaces between the values, and with one user record per line. It is always a good idea to encapsulate these values within double quotes to avoid issues processing special characters in the names. A sample CSV file would look like this:

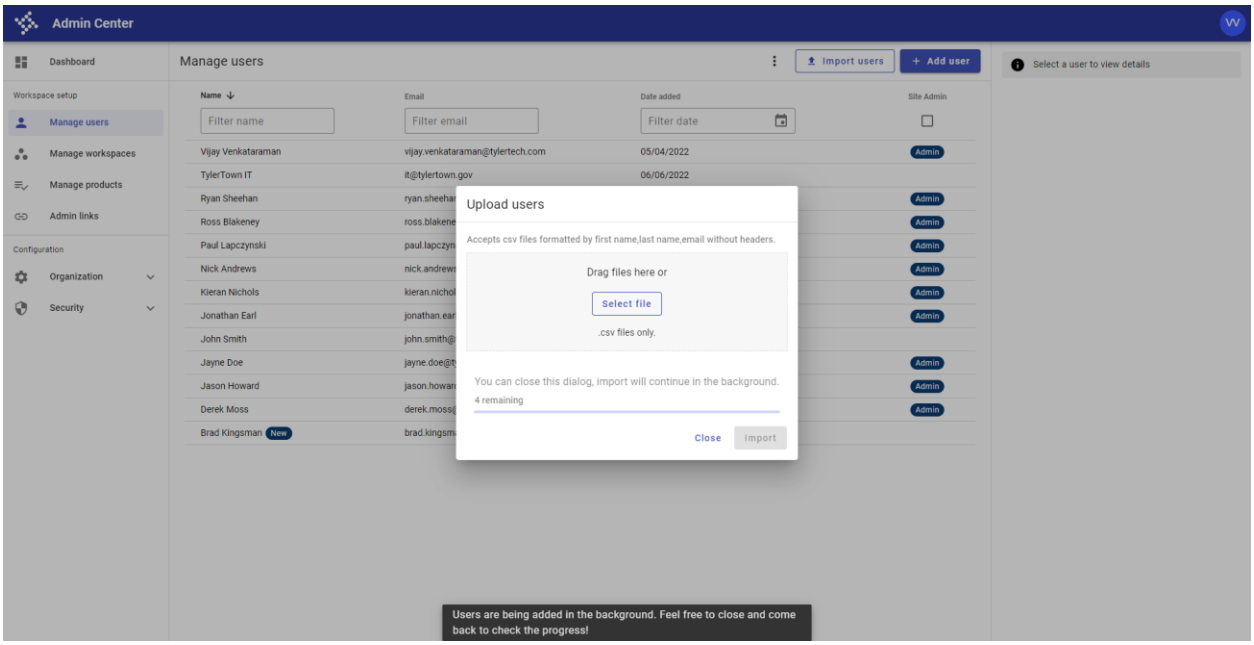
Once the file has been prepared, click on *Import users*. On the *Upload users* dialog, click on *Select file* or drag-drop the CSV file you created above on the gray area on the dialog.



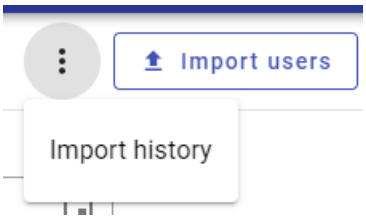
If the file was successfully selected, you should see that reflected on the *Upload users* dialog. Click *Import* to continue.



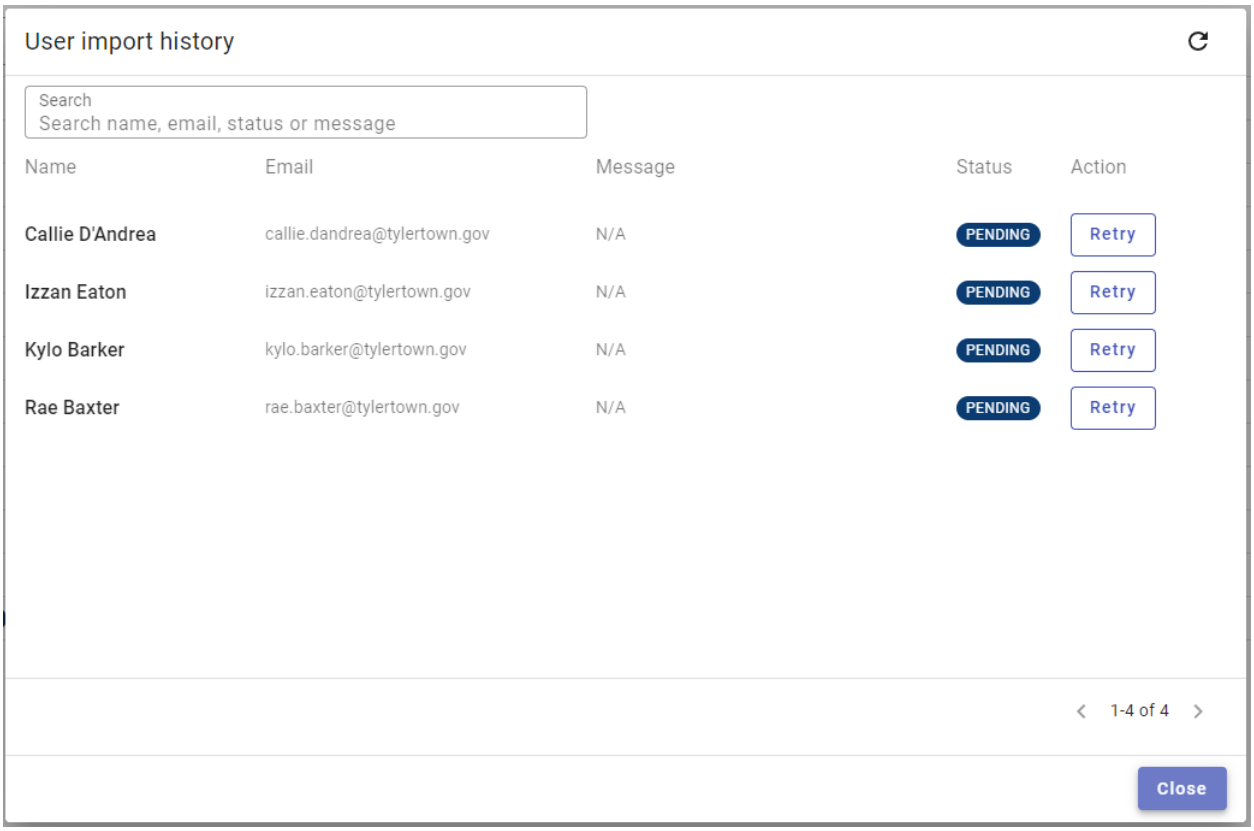
If the import is successful, users will be added in the background. Click the *Close* button



To see the current status of the user imports, click on the 3-dot menu next to the Import users option and select Import history.

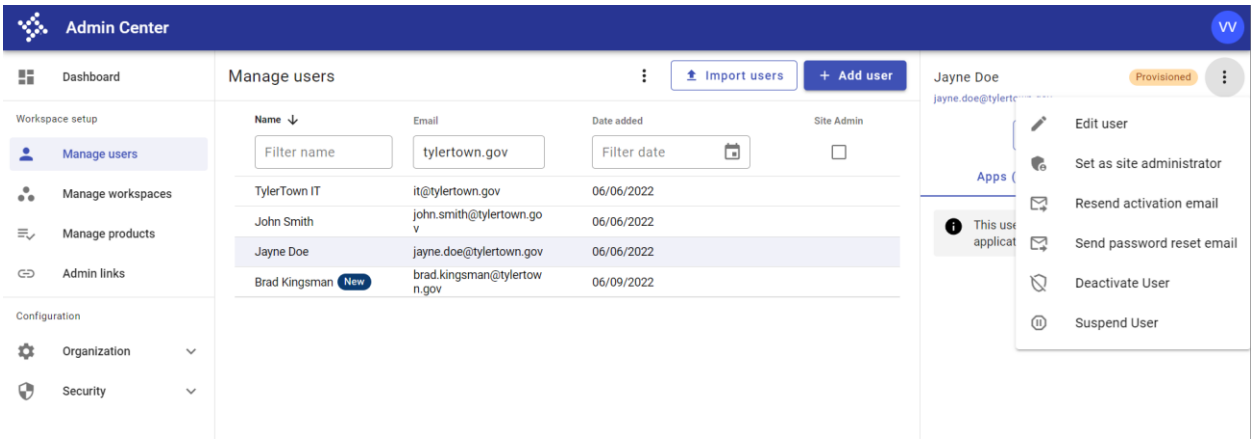


The status of the users (which will vary depending on the type of user) will be listed along with an option to *Retry* will be available should there be temporary glitches in the import process. Click Close to return to the main screen.



Promoting a user as Site Administrator and other user actions

On the main screen, select the user you wish to promote as a Site Admin, click on the 3-dot menu at the top of the user's details and select *Set as site administrator*. This menu option also allows you to edit the user's details, resend activation email, send password reset email, deactivate or suspend the user. You can also delete a previously deactivated user or reactivate them again using the same menu whose options change based on the status and the type of user.



Manage workspaces

A workspace (previously called a 'portal') in the context of the Admin Center is an instance of a Tyler Solution used for a particular purpose. You are typically provisioned a production workspace along with

one or more non-production workspace with the solutions that you have licensed or subscribed to. Each workspace can have independent product configurations suitable for the workspace's intended purpose.

Some settings on workspaces can be maintained either at your organizational configuration settings or be overridden and maintained separately at the workspace level.

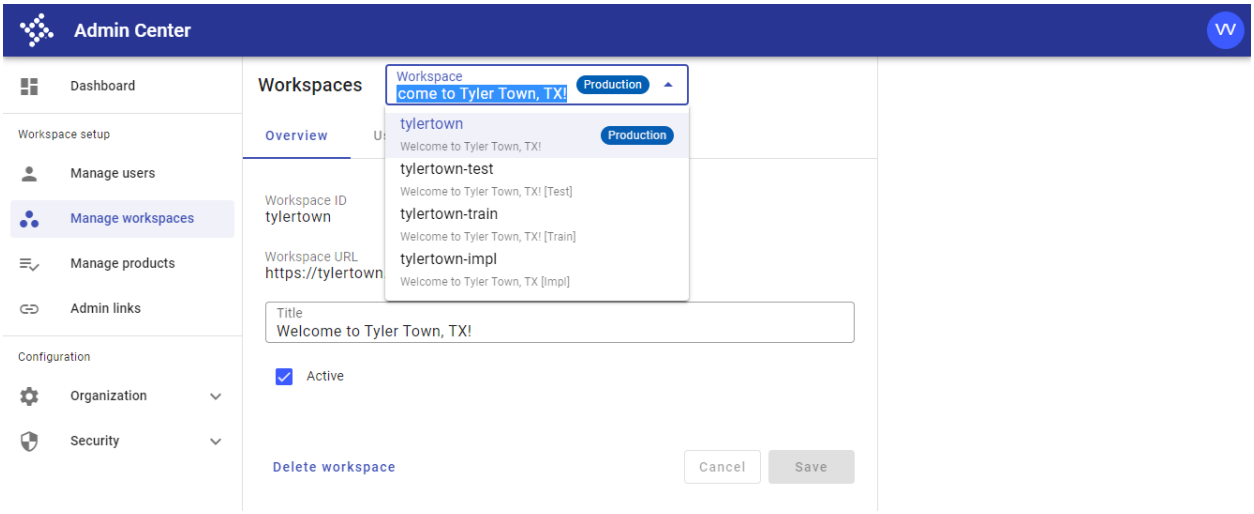
Prerequisites

All the workspaces that you need for your organization must have been provisioned by Tyler implementation teams prior to your use of the Admin Center. You are not able to provision a new workspace through the Admin Center interface currently.

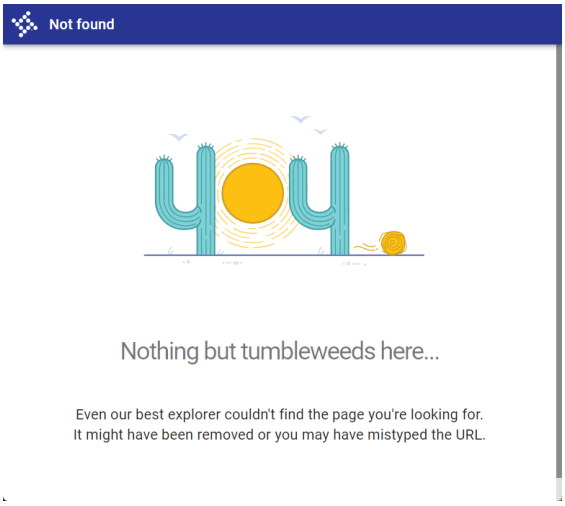
If you are not seeing a workspace that you expect to be present, reach out to your Tyler product support for assistance.

Overview

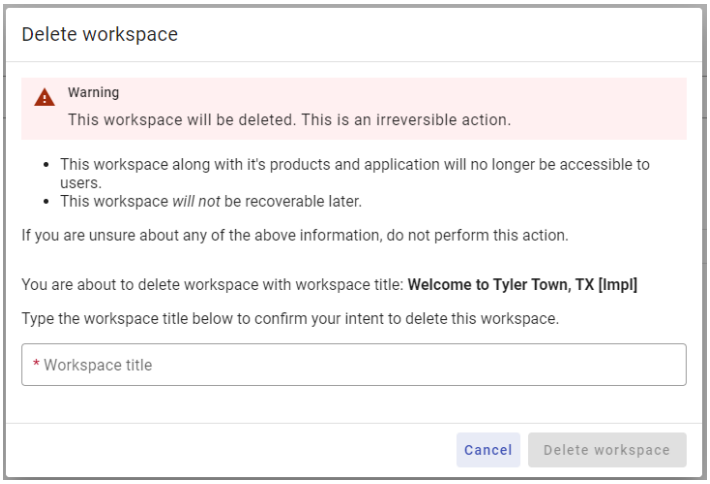
You can view a list of available workspaces by selecting the drop-down menu at the top. Production workspaces have a *Production* label distinguishing it from other workspaces. Underneath the selection are tabs with information related to the selected workspace. Under the *Overview* tab, you can some information related to the workspace, can update the agency *Title* of the specific workspace, and select whether you want to activate or deactivate the entire workspace using the 'Active' checkbox. Finally, you can use *Delete workspace* to permanently delete the workspace.



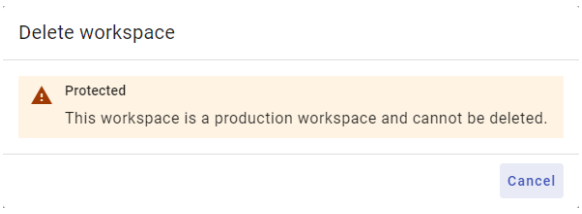
Deactivating a workspace will result in end users seeing a HTML 404 error message.



Clicking the 'Delete workspace' and completing the instructions will result in the workspace being removed.



There are limitations to deleting workspaces – first being that *Production* workspaces cannot be deleted to prevent accidents. Secondly, you may not be able to delete certain non-production workspaces in which you have legacy back-office solutions installed.



Please reach out to your product support if you need to remove a workspace that is restricted from deletion.

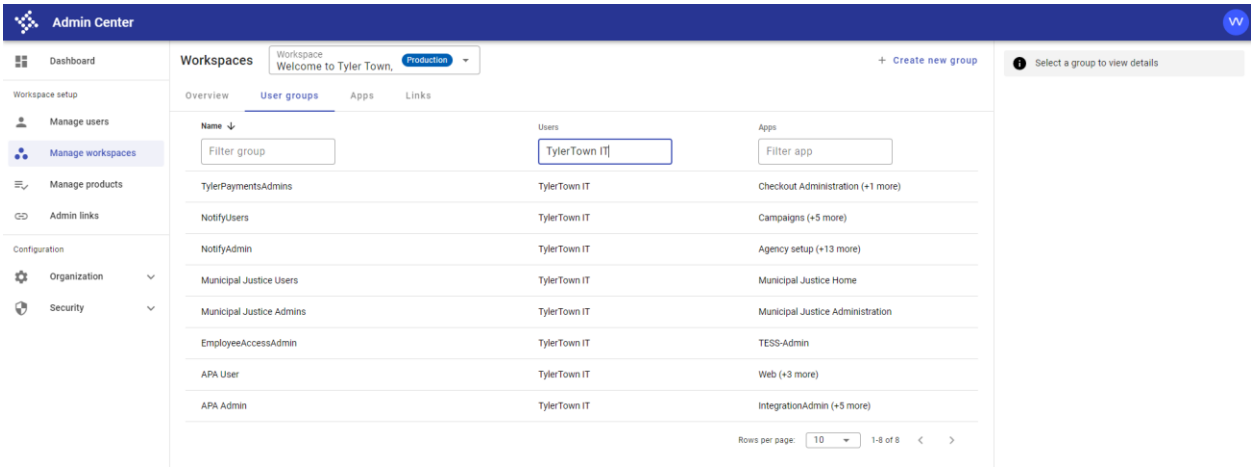
User groups

User groups are workspace level functionality that is used to grant access to select participating Tyler applications. A *User group* definition contains a list of applications that it provides access to, and then

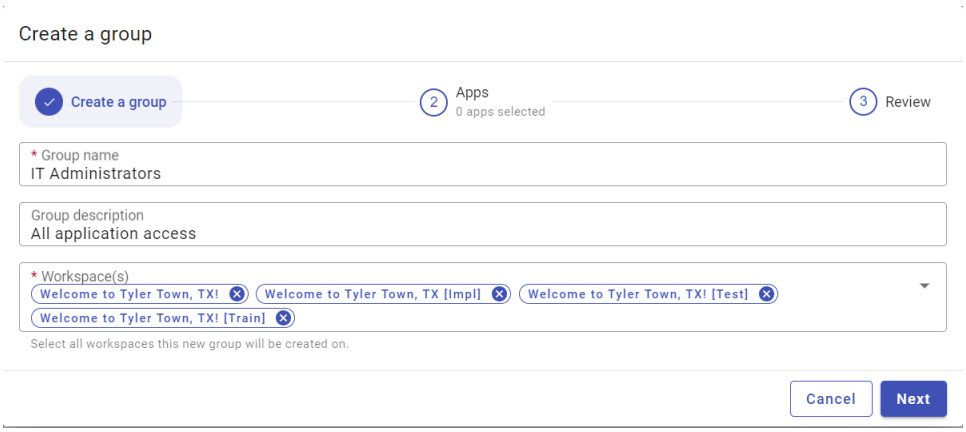
can be assigned to one or more users. Typically, newer cloud applications are available for access control which may include newer cloud applications in hybrid solutions where a newer cloud interface extends a back-office solution built on older technologies.

Any user belonging to one or more User groups with a set of applications defined in each of them will be granted access to all the applications across all the groups assigned to the user. Access control simply allows an application to be accessed or not by a user. It is not related to any fine-grained authorization within applications like the ability to view only or be able to edit specific fields which are managed within each application.

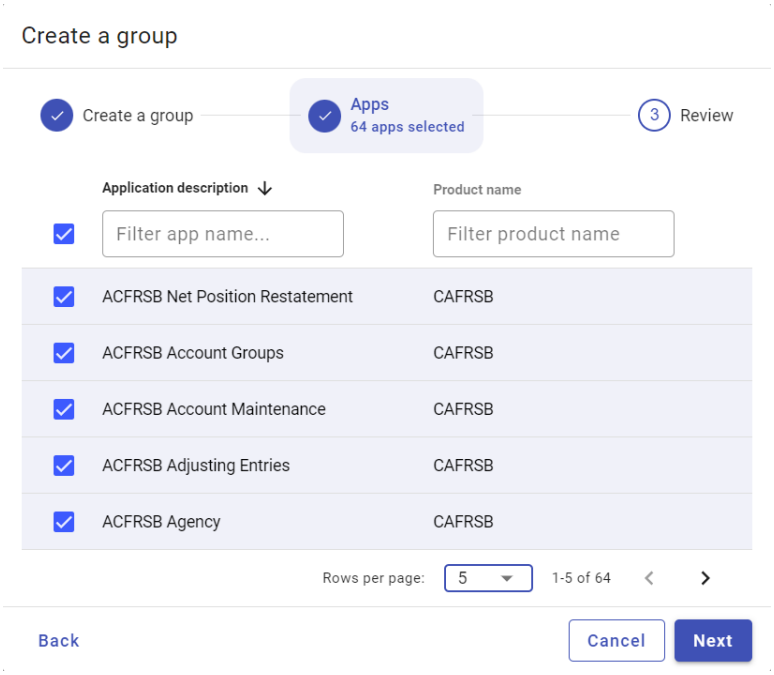
You may see a set of pre-created default *User groups*, but you can choose to create new user groups or replace existing ones. A User group can be limited to applications related to a single product or solution or can include applications across products to fit your needs. For example, you might create a User group for Resident Access administration containing just the application for Resident Access administration and assigning it to department heads for Resident services to manage the solution. You may choose to create another group with all applications in it and assign it your organizations IT administrators or staff so that they are able to access everything for providing support.



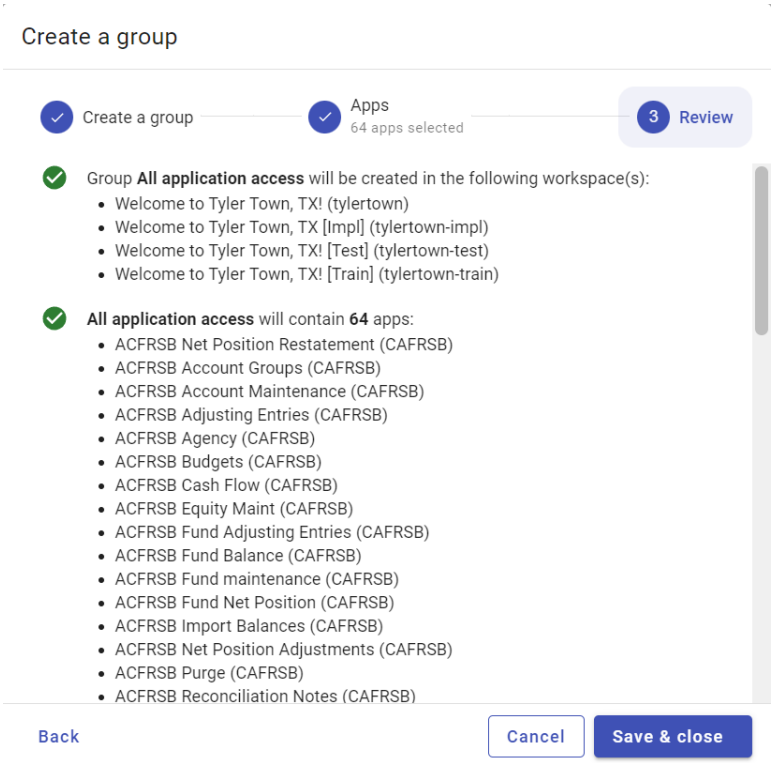
To create a new *User group*, click on the *+ Create new group*. Enter a meaningful but short *Group name*, and then a more detailed *Group description*. Finally, select one or more workspaces to which you would like the group to be available in. Click *Next* to move to the next tab.



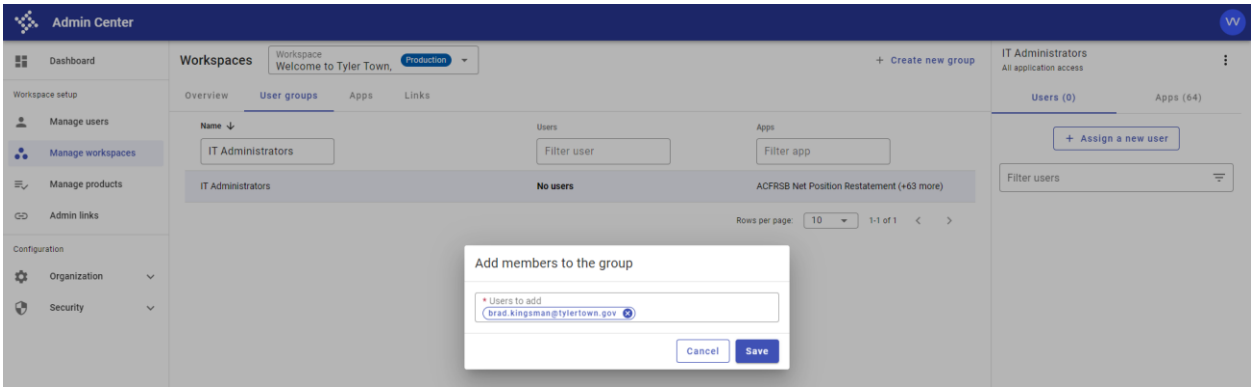
Select one or more applications in the list. You can filter by an application name, or the product it belongs to. You can also increase the number of rows of application you can see at the bottom and use the quick select against the filters to select all records in the current view. You can select records across multiple pages of applications without losing your selection. Click *Next* when you are done selecting your preferred applications.



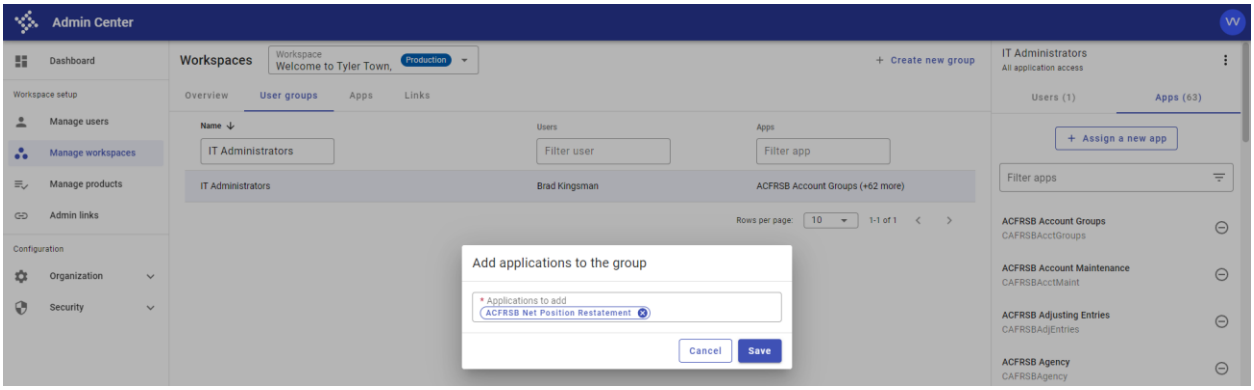
Review the details of the group you are about to create and confirm that it is accurate. Then click *Save & close* to create the group.



After creating the group, it typically has no users assigned to it. To assign it to one or more users, use the *+ Assign a new user* option under the *Users* tab in the group details pane to the right of the screen.

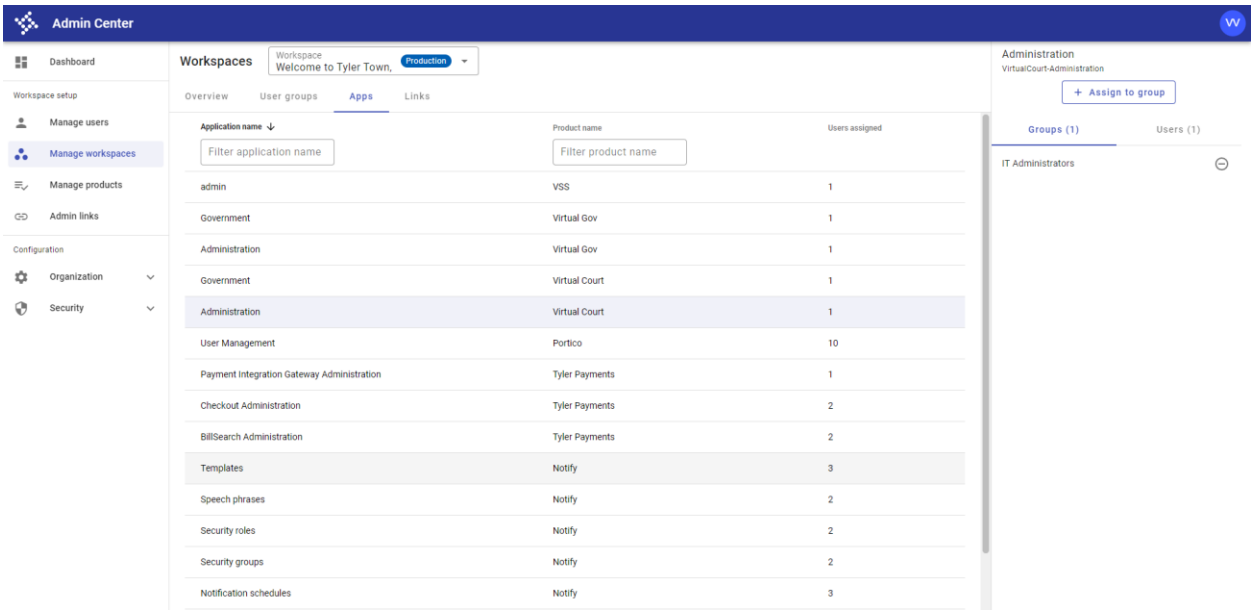


To update an existing group more applications, use the *+ Assign a new app* under the *Apps* tab in the group details pane to the right of the screen.

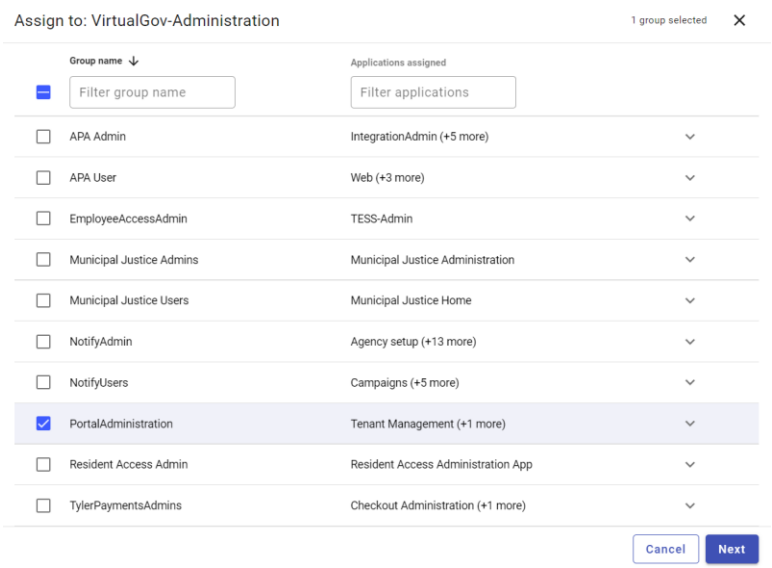


Apps

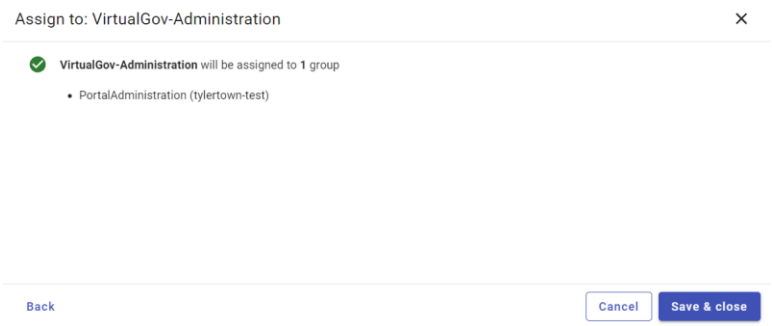
The *Apps* tab lists the Products and Applications associated with the products that have been enabled for your organization.



Clicking on any of these applications gives you the ability to add to add the selected application to one or more groups analogous to the ability to add one or more applications to a *User group* detailed under the *User groups* section. After selecting an application, click on *+ Assign to group* and select one or more groups in the list and click *Next*.

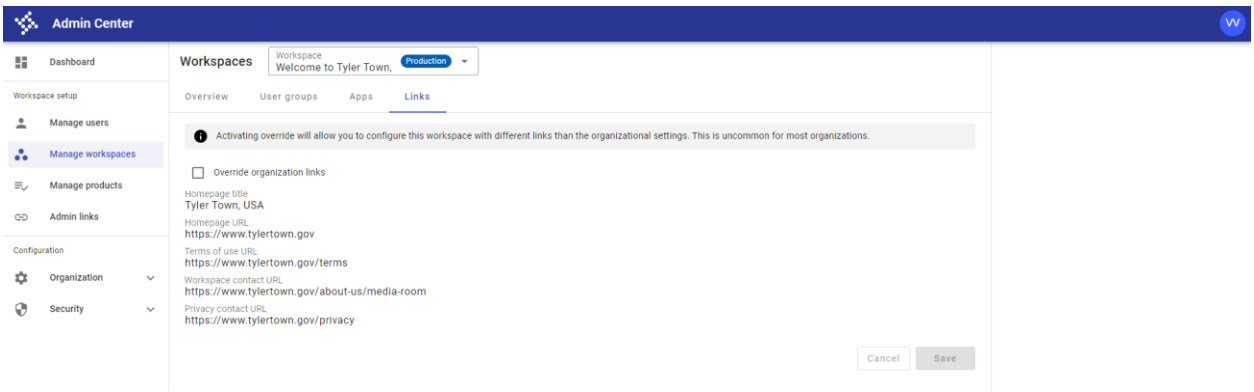


Review the groups to which you have selected to have this application included and click on *Save & close* to complete the assignment.



Links

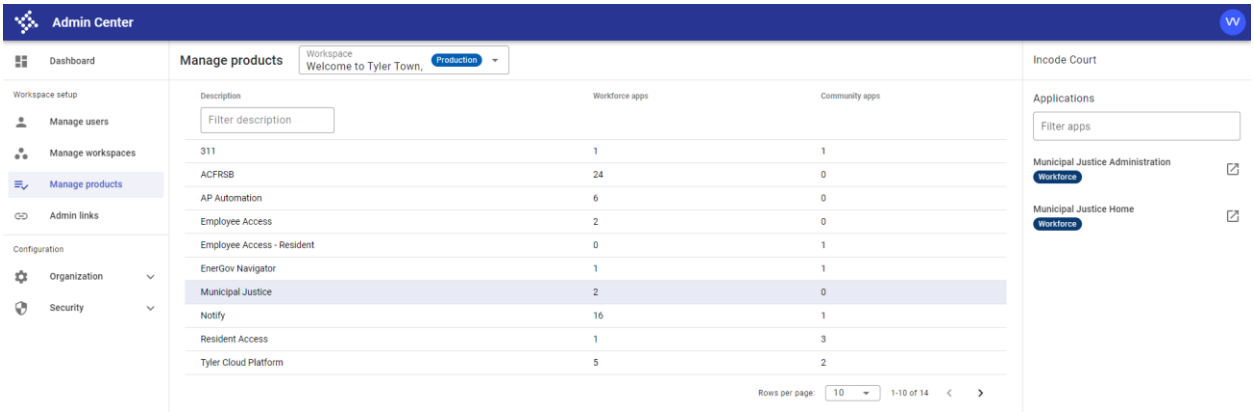
The links tab allows you have different settings per workspace that is different from any organization level links setup under *Configuration > Organization > Links*. To override, check the 'Override organization links' and set values specific to the selected workspace. Unless required, it is recommended that this information be maintained at an organizational level for ease of maintenance.



Manage products

The *Manage products* section provides a listing of various products licensed to your organization, and the number of Workforce (back-office) and Community (resident/public) applications associated with each product. Select any product in the list and a list of applications associated with them is presented in the detail section on the right pane. Access to those applications is controlled through *User groups* and so you must be associated with one or more groups before you can use any of the applications.

This document does not cover content related to using specific Tyler products. Reach out to your product support team if you need assistance locating documentation for a particular product or solution.

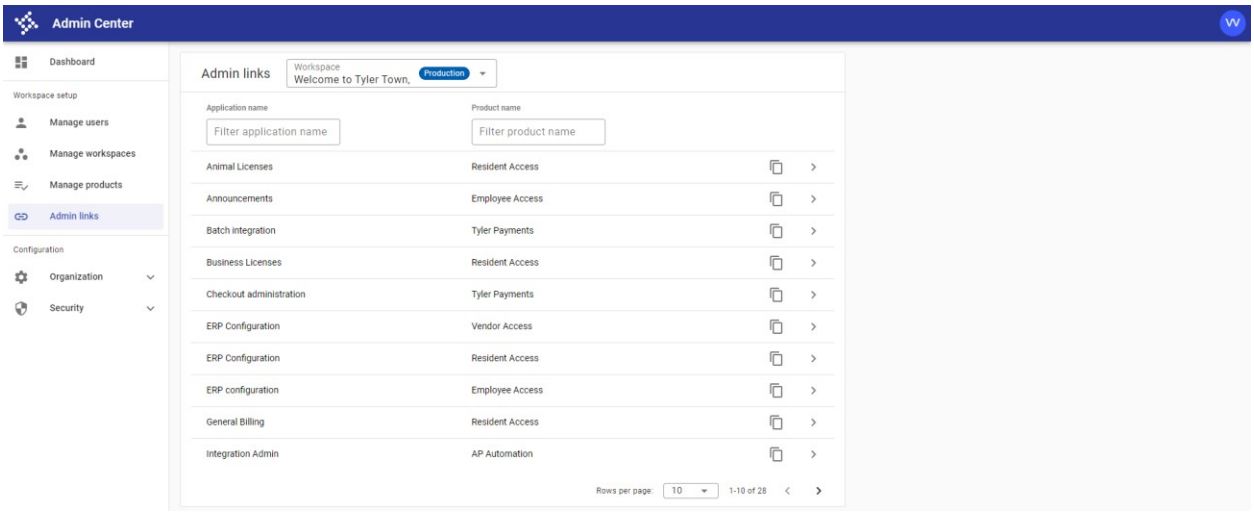


Admin links

Admin links is more focused version of Manage products section providing application links specifically to administrative apps (vs. all applications under Manage products). Therefore, it is typically used to as the launch point for product administration. As stated earlier, access to any of the administrative apps requires you to be part of one or more User groups that contains the administrative app and so you will only see entries on this page reflecting actual access rights. A blank list typically indicates no access to any administrative applications.

You can filter by Product name or Application name. Click on the copy icon to copy the URL of the application or the chevron (>) to actually navigate to the application directly in a new tab. When you are done administrating the application, simply close the tab associated with the product's administration to return back to the Admin Center.

This document does not cover content related to administering specific Tyler products. Reach out to your product support team if you need assistance locating administration documentation for a particular product or solution.



Getting support

To get assistance for any issues using the Admin Center, reach out to your Tyler product team for support:

- During implementation, Tyler's professional services team members you may be in touch with.
- Tyler Support Options: https://www.tylertech.com/client-support
  (select the Tyler product that you are primarily engaged with).