Preparing for Tyler Identity Integration

Tyler Employee Self Service will utilize your local active directory. In preparation for implementing this easier to use and more secure employee self service portal, please read this document.

About Tyler Identity

As a part of Tyler’s continuing efforts to ensure our products are secure and resilient in today’s complex application environments, Tyler Employee Self Service will be implemented using Tyler Identity, a cloud-native identity service built on Okta, a leading provider of identity services and access management.

Tyler Identity seamlessly integrates with Azure AD, ADFS, and G Suite.

Tyler Identity also supports modern multi-factor authentication (MFA), if it is enabled on your identity provider. We strongly recommend the use of MFA, as it substantially reduces the risk of security breaches. It is also #1 in Microsoft’s top 10 ways to secure your business data.

Note that as Tyler continues to migrate our product to a web interface, Tyler ID can also integrate with iVisions.

Benefits of Tyler ID

- **Security**: Organizational access controls Tyler application access.
- **Employees** are registered with Tyler Identity when they first sign in.
- Any changes to employee status are immediately enforced at sign-in.
- **Customer-defined security policies**: You define the security model applicable to your authentication provider.
- **Reduced overhead**: No additional user store to maintain.

Requirements

- A compatible identity provider (Azure AD, ADFS, Google Identity)
- The identity provider needs to be publicly available. If using ADFS, a Web Application Proxy is needed.

Information needed by Tyler ID

The information needed to integrate Tyler ID with your local Active Directory varies depending on your integration solution.

Please go to https://check.tylertech.com for requirements. Login info is your email address, and the password is Tyler.
Handling Users not in Active Directory

Tyler ESS authenticates using Tyler ID. Tyler strongly recommends maintaining all users, including temporary employees such as substitutes within your Active Directory. While users can be added directly to the Tyler ID user store, it is a manual process and those users will have to be maintained by someone at the District.

Limitations for Manual Setup

- The account username must be a personal email address.

- Someone at the District will have to add the users one by one in the user management app in the Tyler Cloud Platform.

- The user added will become part of one large user database. That means the user may exist already if they have been setup with another District. HR or IT would still add the user. If the user is new, they will receive an email with login instructions. If they’ve been setup prior, they will not receive an email and will simply login with the credentials they’ve used in the past. Note that the user can be setup within multiple districts and link themselves to their respective employee at each district.

- If the user is deleted, they are only removed from being linked to your site. The user is not removed from the Tyler ID user store since they could be registered as a user at another site/location.

- The temporary employee will need to be instructed on how to log in. If they are currently or ever have been employed by another site that uses Tyler ESS, they should use the same credentials to log into TESS that they use at the other school.

- Upon termination of employment, HR admins need to inactivate the employee within Infinite Visions in order to restrict access to the active Employee portal.