LINQ Connect

Multi-Factor Authentication

DISTRICTS INFORMATION

Launching Multi-Factor Authentication at Your School

LINQ Connect now offers multi-factor authentication to users. Multifactor authentication, often called MFA, is a security process requiring users to provide two or more verification methods to gain access to an online account. As more services move online, there's an ever present risk of bad actors interfering or taking control of our data with some research showing as much as 30% of school districts have experienced some sort of cyber attack in the last few years. At LINQ, we continue to invest in ensuring that the products and features we provide to districts help them face these challenges head on.

How it works

We will make MFA an available option to everyone, both on the district side and the parent user side. There will be different authentication factors offered initially:

1. SMS/Text: six-digit code will be sent via text message to the phone number provided
2. Phone/Voice: a six-digit code will be communicated through a phone call to the number provided
3. Google Authenticator: QR code will be provided that can be scanned using Google Authenticator or another authentication app

Users will be required to reauthenticate after each session expires. Session expiry is currently set to 24 hours. That said, there will be an option to “remember this device” which will extend that period to 30 days if the user selects that option.

District Functionality

Districts will have the ability to turn MFA on or off for the parent users within their district. If a district chooses to enable MFA, this means that any parent who has a child linked to their account from that district will be required to set up a secondary factor to authenticate their account.

If a district chooses to disable MFA after it has already been enabled/required, parents with children linked to their account from that district will no longer be required to set up a secondary authentication factor for their account. In this situation, we will not perform any further action on the parent's secondary authentication; however, the ability for them to self-select out of MFA will be available. In other words, because the district is no longer requiring it, that doesn’t mean we’ll deactivate it for the parent who already has it on.

Districts will not have any control over which factors are offered to a parent. This will be a standard offering controlled by the LINQ Connect team. In the near term, districts also will not be able to reset a

parent's authentication should there be an issue (e.g. parent had authentications set up to a phone, but then got a new phone number). These issues will need to be resolved by our support team for now.

Should a district choose to require MFA, it is strongly recommended that you send communication to LINQ Connect users in advance to help them understand that their login experience will change and why. We have provided a sample email.

Parent Functionality

Parents will have the option to enable MFA for themselves from their profile settings within LINQ Connect. If a parent chooses to enable MFA, they will be prompted to log out and upon logging back in, they will be required to set their secondary authentication factor.

If a parent has a student linked to their account and that student is enrolled in a district where MFA is required, the parent will not have the option to deselect MFA from their settings. The option will be greyed out with messaging that MFA is required by their district. If a parent has multiple students in their account from different districts, if at least one of those districts requires MFA, it will be mandated for their account. Should a district choose to disable MFA (therefore removing it as a requirement), the option to set MFA on the parent side within LINQ Connect will become active and the parent can choose whether they'd like to continue using it or disable it.

Whether a parent is linking a child for the first time or they already have a child linked when the district enables MFA as a requirement, they will have the same experience:

- Upon next login, parent will be prompted to set up MFA
- If parent does not set up MFA, they cannot re-enter their account