

USER SECURITY TRAINING

PM SESSION

WINNING WITH
CAMPUS



WEDNESDAY, JULY 29TH
TRAINER – DAVE GRAFF

OVERVIEW

Multifactor Authentication	Information about Multifactor Authentication, the options available for your district and how to set it up.	3
3 rd Party Vendors	Discussing 3 rd Party Vendors, how they get data from Campus, and gathering information about them.	8
EOY Data & Information Cleanup	Areas to check to make sure data is up to date and ready for the beginning of the next school year.	10



MULTIFACTOR AUTHENTICATION



User Management > Settings

By **January 1, 2027** Both Infinite Campus and META will be requiring that all District Staff users of Infinite Campus use a multi-factor authentication option when logging into the Campus Dashboard. Most Districts already have this in place. But those that don't will need to get it configured before that date.

Please note that this only affects staff users and does not affect Parent or Student Portal accounts.

MFA: Campus/Email Authentication

User Management > Settings

Enabling this option allows users to authenticate via a code sent to a security email address.

Step 1: Make sure that you have an SMTP Server or Campus MailGun Sever set up to send Campus emails (most districts should already have this configured) Communication > Messenger Settings > Email Settings

You can also test that it is working correctly by sending a test email on that page.

Step 2: Mark The Radio Button and set authentication frequency in: User Management > Settings > Login Security Settings

Troubleshooting: If a user reports that they are not receiving MFA emails, you will want to reset their security email. You can do so by clicking the 'Reset Account Settings' button in their user account information. Note: make sure they are using their district email address, as personal email may block emails from Campus or send them to junk mail.

Basic Settings	
*Default Sender Email Address	icdemo@icdemo.mg.infinitecampus.org
☒ Use Mailgun API	☐ Use SMTP Server
*Mailgun Domain	icdemo.mg.infinitecampus.org
Advanced Settings	
Minutes Between Retries	10
Max Errors Before Cancel	1
Throttle Email Messages	emails per second (leave blank to not throttle)
Email Attachment Settings	
Allow Email Attachments	☒
Limit Email Attachment File Size	MB
Global Email Settings	
Use Sender's Email from Census as Reply To Email Address	☐
Allow Custom Reply To Email Address	☒
Allow Custom Sender Display Name	☐
Test Email Settings Configuration	
Send Test Email	test@example.com

Multi-Factor Authentication Options	
☐ Do not require a verification code to log in.	
☒ Require Email-Based Multi-Factor Authentication Code.	
<i>- This option requires email messenger to be configured in order to function.</i>	
Require authentication frequency	Each New Device
Require MFA for SAML logins	No

Reset Account Settings

MFA: Time Based MFA with 3rd Party App

User Management > Settings

Enabling this option allows users to authenticate via any 3rd party authentication app on their phone or device.

Step 1: Mark The Radio Button and set authentication frequency in:
User Management > Settings > Login Security Settings

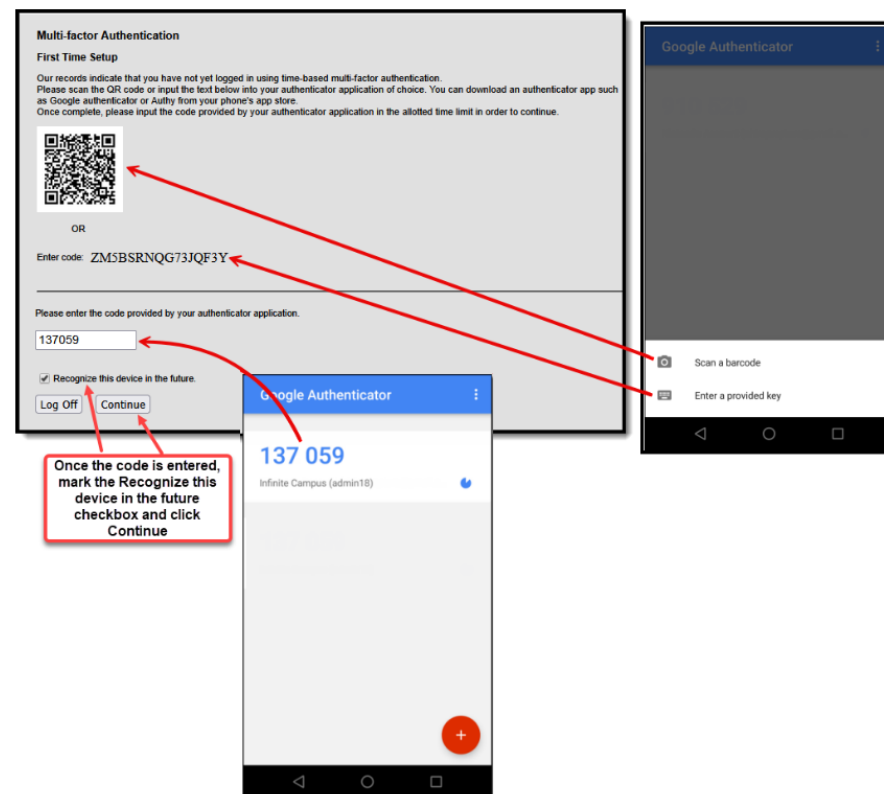
☒ Require Time-Based Multi-Factor Authentication from a Third Party App.
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exist, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Require authentication frequency: Each New Device ▼

Require MFA for SAML logins: Yes ▼

Step 2: When the user next logs in, they will receive a QR code to scan (or a text code to enter) using their authentication application.

Troubleshooting: If a user needs to reset which authentication app they are using. You will need to reset their User account security settings. You can do so by clicking the 'Reset Account Settings' button in their user account information.



MFA: Single Sign On SSO/SAML

User Management > Settings

Enabling this option allows users to authenticate via a District determined SSO/SAML application.

The district will need to generate of upload service provider certificate information to Campus as well as set up login preferences for the SSO service they are using. Depending on the service the setup can vary.

Full Campus instructions can be found at the link below:

<https://kb.infinitecampus.com/help/saml---sso-service-provider-configuration>

MFA: LDAP Authentication

User Management > Settings

Enabling this option allows users to be linked to the District's local LDAP server and linked to their local accounts.

Setup involves entering your server information including DN and filtering information. Note that users will need to have the same username as on your LDAP server to be able to use this method. Full instructions on setting up LDAP Authentication in Campus can be found at the link below:

<https://kb.infinitecampus.com/help/ldap-configuration>

3rd PARTY VENDORS



What is a 3rd Party Vendor?

A 3rd Party Vendor is any company that the District has contracted with that either pulls data into Campus or pushes data into Campus. Some Examples of vendors include SameGoal, Transfinder, Clever, Schoollinks, etc.

Vendors typically have 3 options for pulling Campus Data

Data Extract [System Settings > Data Utilities > Data Extract Utilities](#)

Data is pulled using an AdHoc or a SQL script and is sent via SFTP to the vendor's server.

OneRoster API [Instruction > Settings > Digital Learning Applications Configuration](#)

Groups of data are accessible via a pre-configured API connection. How much data and what data is available is determined by whether the vendor is a Campus partner. Non-partners have limited data access using this method.

Database Connection

We do NOT recommend this method of pulling data. As giving a 3rd party company a database connection allows them access to ALL data on your Campus server. This could represent a FERPA or HIPA violation during a security audit.

3rd Party Vendors: Vendor Audit

Since Districts deal with 3rd party vendor contracts on their own, it is sometimes hard to tell which districts are still using what vendors. We would like to go through and disable any SFTP extracts, Oneroster connections or database accounts that are no longer in use.

We are asking that each district take the time to fill out the following spreadsheet. This will let us know what vendors they are currently using and what connections they use to pull data from Campus. Please note that we will not be disabling any processes without contacting districts first to make sure they are no longer in use.

Vendor Information Spreadsheet
(Please Fill out and Return)

<https://bit.ly/meta3rdpartyvendor>

Once completed, please return to: infinitecampushelp@metasolutions.net

EOY DATA & INFORMATION CLEANUP



School & District Information Updates

Make sure that the following information is up to date and accurate for the new school year:

School Information: Principal Name & Email, Phone Number, Address, URL of Building Website

School & District Settings > School > School Information

District Information: Phone Number, Address, URL of District Website.

School & District Settings > District > District Information

Check Old Staff Accounts

Make sure that the user accounts of any staff that left within the last year have been disabled, this is typically done on the staff's end date, but it is important to double-check for security purposes.

User Management > User Account Management > User Account

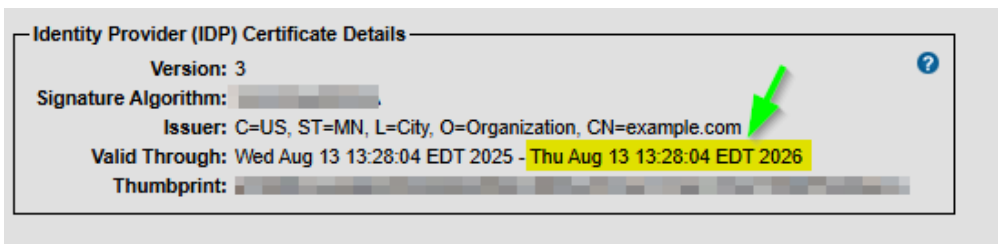
A screenshot of the 'User Credentials' form in a web application. The form has a light gray header with the title 'User Credentials'. Below the header, there are two dropdown menus: 'Homepage' with 'Campus Tools' selected, and 'Authentication Type' with 'Local Campus Authentication ...' selected. Below these is a text input field for 'Username *' containing 'OldStaffMember'. There is an unchecked checkbox for 'Force Password Change'. Below that is a date input field for 'Account Expiration Date' with the placeholder 'month/day/year' and a calendar icon. At the bottom, there is a checked checkbox for 'Disable Account', which is highlighted by a green arrow pointing to it from the right.

EOY DATA & INFORMATION CLEANUP

SSO/SAML Certificate Dates

If your district uses SAML/SSO for Multifactor authentication, you will want to check the date that your IP security certificate is valid, you may need to submit a new one if it is set to expire soon. Our suggestion is that if it is set to expire before the end of the 1st term, you should go ahead and renew it, so you aren't surprised by it expiring and making it so that users cannot log in.

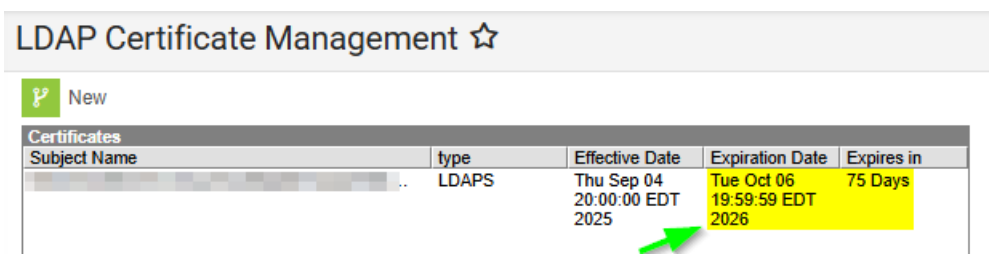
User Management > Settings > SAML – SSO Service Provider Configuration



LDAP Certificate Dates

If your district uses LDAP for user authentication, you will want to check the date that your security certificate is valid, you may need to submit a new one if it is set to expire soon. Our suggestion is that if it is set to expire before the end of the 1st term, you should go ahead and renew it, so you aren't surprised by it expiring and making it so that users cannot log in.

User Management > Settings > LDAP Certificate Management



META Admin User Accounts

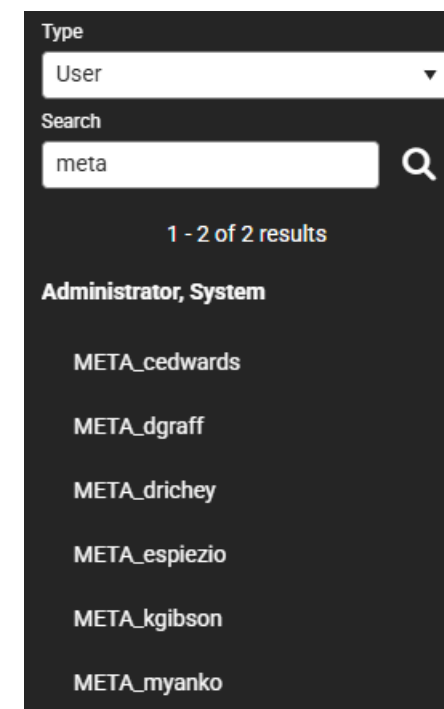
As part of our yearly security audit at META, it was decided that we needed to change the way that META's admin accounts were handled on Campus district instances.

Previously, all META staff used the same account, which in most cases was not named as a META user, only 'admin'

Going forward we have set up individual admin accounts for each staff member. These accounts all have a META_ prefix and follow a naming convention to make it easier to identify the user.

These accounts are only accessible by our trained Campus support staff.

The accounts have already been set up and nothing additional is needed on the District side.



WINNING WITH CAMPUS



Please help us help you, by filling out a training survey.

www.metasolutions.net/campussurvey

Need More Info? Get More!

META IC Support: infinitecampushelp@metasolutions.net

META IC Training Videos & Docs: metasolutions.net/campustraining

META IC Website: metasolutions.net/infinitecampus

THANK YOU!