



**KSIS CLOUD DISTRICT TECHNICAL  
REFERENCE**

01/27/2020

**Table of Contents**

Introduction ..... 3

Update History ..... 3

Network ..... 3

Workstation/Browser Configuration ..... 3

Internet Content Management (Lightspeed) ..... 3

New Integration with KETS Active Directory using via Office365 using SAML ..... 4

    Benefits of AD Integration ..... 4

    Frequently Asked Questions ..... 4

    Planning Considerations ..... 5

    Implementation Process and Recommendations ..... 6

New Integration with KETS Active Directory via G Suite for Education using SAML ..... 8

    Benefits of AD Integration ..... 8

    Frequently Asked Questions ..... 8

    Planning Considerations ..... 9

    Implementation Process and Recommendations ..... 10

Campus Data Extract Utility ..... 11

    SMB Delivery Mode ..... 11

    Secure FTP Delivery Modes ..... 12

FRAM Eligibility Import Wizard Scheduled Imports ..... 12

    SMB Protocol ..... 12

    Secure FTP Protocol ..... 13

Email Messenger SMTP Relay Configuration ..... 13

## **Introduction**

This document describes the integration of the Kentucky Student Information System, using the Infinite Campus Private Cloud, with other KETS components. It is directed at technology staff who must support district users of KSIS and the integration of other systems with KSIS. This document is a supplement to Infinite Campus-provided documentation.

## **Update History**

6 March 2017 – Initial Release

10 May 2017 – Describe New LDAP Authentication configuration

15 March 2018 – removed information about earlier (now retired) version of LDAP configuration; added warning about SMB (Windows File Sharing) version support

1 October 2019 – removed section “New Integration with KETS Active Directory using LDAP” and added sections “New Integration with KETS Active Directory via Office365 using SAML” and “Integration with KETS Active Directory via G Suite for Education using SAML”

27 January 2020 – Added a point (#2) In both of the “Integration with KETS Active Directory ...” sections, under Planning Considerations (pages 5 and 9)

27 January 2021 - Updated Secure FTP Protocol section under FRAM Eligibility Import Wizard Scheduled Imports

## **Network**

By design, the vast majority of Campus-related network traffic to/from district-connected devices will pass through the KETS wide area network (KEN) and its public Internet connection. A small amount of traffic will travel through a VPN (Virtual Private Network) connection between KEN and Infinite Campus' datacenter.

## **Workstation/Browser Configuration**

No KETS-specific workstation/browser configuration should be necessary. Search Campus Community for “Supported Platforms” and “Recommended Browser Settings”.

## **Internet Content Management (Lightspeed)**

No Campus-specific configuration should be required on the Lightspeed-based KETS Internet Content Management system.

# Integration with KETS Active Directory via Office365 using SAML

General information about this integration feature is available in the Campus Community; search for “SAML Management.” Campus and Microsoft have jointly developed [documentation](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/infinitecampus-tutorial) (<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/infinitecampus-tutorial>) specific to Office 365 and Azure Active Directory, and Microsoft has also published more [general information](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on) (<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>) about integrating applications with Office 365 and Azure Active Directory.

## ***Benefits of AD Integration***

1. Users will be able to use their Active Directory/Office365 username (district email address) and password to log into Infinite Campus (via the Office365 login page) and do not need to remember a separate Infinite Campus password or manually keep two passwords in sync.
2. Users who already log into Office365 through a browser will not have to re-enter a password at all.
3. Infinite Campus access will effectively be subject to the same password policies as AD passwords with no additional management effort.
4. There is no need for users to periodically change their Infinite Campus password.
5. Administrators can disable a user’s access to Infinite Campus (as well as Active Directory and Office365) with one step for users set up to use this authentication.

## ***Frequently Asked Questions***

1. Does AD/Office365 Integration using SAML affect Parent/Student (Web) Portal Access?

Yes. If a district chooses to migrate students to AD/Office365 integration, those students will need to use their AD credentials to log into the Student Portal. District Staff who use the Parent Portal will need to use their AD credentials. Parents who do not have AD accounts will NOT use AD credentials and will continue to log in with their existing credentials.

2. Does AD/Office365 Integration using SAML work in the mobile app?

Yes, BUT ONLY in the Campus Student and Campus Parent mobile apps released in late 2018. The older version of the app, named “Infinite Campus Mobile Portal”, will NOT allow authentication via AD/Office365.

3. Does LDAP integration have to be configured along with AD/Office365 integration using SAML?

No. Note that, as of 9 August 2019, some Campus documentation still indicates that LDAP configuration is required for mobile app functionality, but this is no longer true.

4. Does AD Integration affect an administrator's ability to "Login as User" within Infinite Campus?

No, "Login as User" continues to work as before even if the user has been migrated to AD integration.

5. Can a user be switched back to a Campus-specific username once they have been configured for AD integration?

Yes.

6. Will AD/Office365 Integration using SAML and Campus Password Reset functionality conflict with each other?

No, but users will only be able to use the Campus Password Reset functionality if their Campus account is NOT integrated with Active Directory. A district can choose to have some users integrated with Active Directory and others using Campus passwords and Campus Password Reset functionality.

7. Will AD/Office365 Integration with Campus using SAML allow users to access the Infinite Campus Data Analysis Portal (Tableau) without a separate login?

No, but the username and password will be the same for both systems (Infinite Campus itself and the Infinite Campus Data Analysis Portal).

## ***Planning Considerations***

1. When implementing AD/Office365 integration using SAML, it is ESSENTIAL to create or retain an administrative-level Infinite Campus user that is NOT linked with Active Directory. In case of a connectivity or configuration issue, this account may be the only one that can be used to adjust the Infinite Campus configuration.
2. The public key certificates used as part of the SAML configuration will eventually expire. Users with a Campus Product Security Role of "Student Information System (SIS)" will receive advance notice of these expirations and will need to take action at that time to ensure continued functionality. Review the Campus documentation for the LDAPS Certificate Management tool for more information about these notifications.

3. If using the Campus Food Service solution, be aware that the Food Service Point of Sale software does NOT support AD/Office365 integration using SAML; users who need to log in through the Point of Sale software will need standard Campus accounts.
4. If there is ever a need to remove AD/Office365 integration using SAML, you must ensure that each user has an appropriate password set on their Campus user before disconnecting the user from Active Directory.
5. You may implement AD/Office365 integration using SAML for students (for access to the Parent/Student Portal and Student mobile app) as well as for district staff users.
6. The “Expires Date” field on the User Account screen will still be effective for a user that has migrated to AD (though it only affect the ability to log into Campus).
7. Consider whether you want to start requiring stronger AD passwords as part of the migration. Section 3.1.5 of the [KETS Active Directory Operations Guide](https://education.ky.gov) (available at <https://education.ky.gov>) describes options for requiring stronger AD passwords.
8. Azure Active Directory has the capability to allow or prevent access to an integrated application (such as Infinite Campus, once integrated) on a per-user or per-group basis; or to allow any authenticated user access and rely entirely on Campus’s authorization functionality (no different than before integration). You can choose either approach.

## Implementation Process and Recommendations

Implementation is done in two major steps:

- Configuration of Infinite Campus SAML functionality: this is a one-time activity using System Administration functionality in Campus, and related administration functionality within Office365 (Azure Active Directory), as described in [Microsoft’s documentation](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/infinitecampus-tutorial) ( <https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/infinitecampus-tutorial>). Specific recommendations:
  - Within the “Configure Azure AD single sign-on” section, Step 4 requires several URLs; use the server name (such as <https://kyede3.infinitecampus.org>) of your existing Campus login page as the base for the URL, and in place of the <DISTRICTNAME> placeholder, use the district name value that is followed by .jsp on your login page. For example, if your existing Campus login page is <https://kyede3.infinitecampus.org/campus/clark.jsp>, then the “Sign-on URL” should be <https://kyede3.infinitecampus.org/campus/SSO/clark/SIS>.
  - As part of configuring Campus SSO Service Provider Configuration, you will need to choose a name for the button that will appear on the login page to initiate login through AD/Office365. This button will appear IN

ADDITION TO the standard Campus username and Password fields, so consider how to label the button to best help your users make the right choice.

- Configuring individual Campus users: each Campus user account for which this integration is desired must be configured to 1) specify use of SAML, and 2) set the username equal to the user's district email address (AD UserPrincipalName). Specific recommendations:
  - Setting user to use SAML:
    - Individual users can be switched to use SAML using the standard user account editor.
    - The Campus User Account Type Wizard can be used to mass-convert all or subsets of user accounts to use AD/Office365 integration using SAML. This wizard is documented on Campus Community.
    - The Campus Account Security Preferences tool, which has functionality to automatically create user accounts when students are enrolled or staff are given an active district assignment, can be configured to set the newly created users to use SAML. This tool is documented on Campus Community.
  - Setting username to user's district email address:
    - Individual users' usernames can be updated to their district email addresses using the standard user account editor.
    - Mass update of existing Campus user accounts to have district email address as the username (assuming these email addresses are already configured within Census) can be done by a district person with ODBC access to the district's Campus database and SQL skills.
    - Mass update of existing Campus user accounts to have district email address as the username (assuming these email addresses are already configured within Census) can be done by Campus Technical Services. KDE will cover the cost for Campus to do this task; contact Campus Support and request the Match Username to Email Address service. Campus Technical Services will work with your staff to update the needed subset of users.

# Integration with KETS Active Directory via G Suite for Education using SAML

This functionality is intended for districts that have implemented G Suite Password Sync (GSPS) or Google Cloud Directory Sync (GCDS) to synchronize AD users to G Suite.

General information about this integration feature, and specific guidance for integration with G Suite, is available in the Campus Community; search for “SAML Management.”

## ***Benefits of AD Integration***

1. Users will be able to use their Active Directory/G Suite username (district email address) and password to log into Infinite Campus (via the G Suite login page) and do not need to remember a separate Infinite Campus password or manually keep two passwords in sync.
2. Users who already log into G Suite through a browser will not have to re-enter a password at all.
3. Infinite Campus access will effectively be subject to the same password policies as AD passwords with no additional management effort.
4. There is no need for users to periodically change their Infinite Campus password.
5. Administrators can disable a user’s access to Infinite Campus (as well as Active Directory and G Suite) with one step for users set up to use this authentication.

## ***Frequently Asked Questions***

1. Does AD/G Suite Integration using SAML affect Parent/Student (Web) Portal Access?

Yes. If a district chooses to migrate students to AD/G Suite integration, those students will need to use their AD credentials to log into the Student Portal. District Staff who use the Parent Portal will need to use their AD credentials. Parents who do not have AD accounts will NOT use AD credentials and will continue to log in with their existing credentials.

2. Does AD/G Suite Integration using SAML work in the mobile app?

Yes, BUT ONLY in the Campus Student and Campus Parent mobile apps released in late 2018. The older version of the app, named “Infinite Campus Mobile Portal”, will NOT allow authentication via AD/G Suite.

3. Does LDAP integration have to be configured along with AD/G Suite integration using SAML?

No. Note that, as of 9 August 2019, some Campus documentation still indicates that LDAP configuration is required for mobile app functionality, but this is no longer true.



4. Does AD Integration affect an administrator's ability to "Login as User" within Infinite Campus?

No, "Login as User" continues to work as before even if the user has been migrated to AD integration.

5. Can a user be switched back to a Campus-specific username once they have been configured for AD integration?

Yes.

6. Will AD/G Suite Integration using SAML and Campus Password Reset functionality conflict with each other?

No, but users will only be able to use the Campus Password Reset functionality if their Campus account is NOT integrated with Active Directory. A district can choose to have some users integrated with Active Directory and others using Campus passwords and Campus Password Reset functionality.

7. Will AD/G Suite Integration with Campus using SAML allow users to access the Infinite Campus Data Analysis Portal (Tableau) without a separate login?

No, but the username and password will be the same for both systems (Infinite Campus itself and the Infinite Campus Data Analysis Portal).

## Planning Considerations

1. When implementing AD/G Suite integration using SAML, it is ESSENTIAL to create or retain an administrative-level Infinite Campus user that is NOT linked with Active Directory. In case of a connectivity or configuration issue, this account may be the only one that can be used to adjust the Infinite Campus configuration.
2. The public key certificates used as part of the SAML configuration will eventually expire. Users with a Campus Product Security Role of "Student Information System (SIS)" will receive advance notice of these expirations and will need to take action at that time to ensure continued functionality. Review the Campus documentation for the LDAPS Certificate Management tool for more information about these notifications.
3. If using the Campus Food Service solution, be aware that the Food Service Point of Sale software does NOT support AD/G Suite integration using SAML; users who need to log in through the Point of Sale software will need standard Campus accounts.
4. If there is ever a need to remove AD/G Suite integration using SAML, you must ensure that each user has an appropriate password set on their Campus user before disconnecting the user from Active Directory.

5. You may implement AD/G Suite integration using SAML for students (for access to the Parent/Student Portal and Student mobile app) as well as for district staff users.
6. The “Expires Date” field on the User Account screen will still be effective for a user that has migrated to AD (though it only affect the ability to log into Campus).
7. Consider whether you want to start requiring stronger AD passwords as part of the migration. Section 3.1.5 of the [KETS Active Directory Operations Guide](https://education.ky.gov) (available at <https://education.ky.gov> ) describes options for requiring stronger AD passwords.

## Implementation Process and Recommendations

Implementation is done in two major steps:

- Configuration of Infinite Campus SAML functionality: this is a one-time activity using System Administration functionality in Campus, and related administration functionality within G Suite, as described in Campus’s documentation (search for “SAML Management” in Campus Community). Specific recommendations:
  - As part of configuring Campus SSO Service Provider Configuration, you will need to choose a name for the button that will appear on the login page to initiate login through AD/G Suite. This button will appear IN ADDITION TO the standard Campus username and Password fields, so consider how to label the button to best help your users make the right choice.
- Configuring individual Campus users: each Campus user account for which this integration is desired must be configured to 1) specify use of SAML, and 2) set the username equal to the user’s district email address (AD UserPrincipalName). Specific recommendations:
  - Setting user to use SAML:
    - Individual users can be switched to use SAML using the standard user account editor.
    - The Campus User Account Type Wizard can be used to mass-convert all or subsets of user accounts to use AD/G Suite integration using SAML. This wizard is documented on Campus Community.
    - The Campus Account Security Preferences tool, which has functionality to automatically create user accounts when students are enrolled or staff are given an active district assignment, can be configured to set the newly created users to use SAML. This tool is documented on Campus Community.

- Setting username to user's district email address:
  - Individual users' usernames can be updated to their district email addresses using the standard user account editor.
  - Mass update of existing Campus user accounts to have district email address as the username (assuming these email addresses are already configured within Census) can be done by a district person with ODBC access to the district's Campus database and SQL skills.
  - Mass update of existing Campus user accounts to have district email address as the username (assuming these email addresses are already configured within Census) can be done by Campus Technical Services. KDE will cover the cost for Campus to do this task; contact Campus Support and request the Match Username to Email Address service. Campus Technical Services will work with your staff to update the needed subset of users.

## Campus Data Extract Utility

Detailed documentation of the Campus Data Extract Utility is available in Campus Community; search for "Data Extract Utility (Custom Development)".

### ***SMB Delivery Mode***

The SMB delivery mode causes the Campus servers to place the extract file on an in-district Windows file server using standard Windows file sharing (no additional software required). SMB will eventually be retired as an option for Kentucky cloud districts.

**NOTE:** The Campus application can only connect to Windows file servers using SMB Version 1 (SMBv1); recent versions of Windows Server 2016 disable SMBv1 by default, and Microsoft recommends disabling SMBv1 on all supported Windows versions, so specific configuration for the destination server may be required.

Use of SMB requires a surrogate (Network Address Translation) IP address which allows the Campus servers to connect to the district's Windows file server through a VPN connection between Campus and Kentucky (KEN). This surrogate IP address is entered in the Data Extract Utility interface only; the locally configured IP address of the Windows file server is NOT changed.

In order to request a surrogate IP address, contact Campus support through the usual channels and provide the locally configured IP address and name of the Windows file

server. Up to three surrogate IP addresses can be provided per district (including those used for Eligibility Import, discussed later).

### ***Secure FTP Delivery Modes***

The two secure FTP delivery modes (SFTP and FTPS) cause the Campus servers to place the extract file on a secure FTP site of the district's choosing. Both types of secure FTP require installing and configuring software on a server. Neither Campus nor KETS can provide assistance with procuring, installing, configuring, or operating secure FTP software. However, for secure FTP sites on a district-located server, the KETS Service Desk can assist with configuration changes to the KETS firewall and the allocation of a public IP address.

The Campus Cloud servers' public IP addresses (from which secure FTP connections will originate) will be from one or more of these ranges:

65.124.140.0/24

207.225.137.0/24

198.73.96.0/21

216.226.196.0/22

## **FRAM Eligibility Import Wizard Scheduled Imports**

Detailed documentation of the Campus FRAM Eligibility Import Wizard Scheduled Imports feature is available in Campus Community.

### ***SMB Protocol***

The SMB protocol causes the Campus servers to import the data file from an in-district Windows file server using standard Windows file sharing (no additional software required). SMB will eventually be retired as an option for Kentucky cloud districts.

**NOTE:** The Campus application can only connect to Windows file servers using SMB Version 1 (SMBv1); recent versions of Windows Server 2016 disable SMBv1 by default, and Microsoft recommends disabling SMBv1 on all supported Windows versions, so specific configuration for the destination server may be required.

Use of SMB requires a surrogate (Network Address Translation) IP address which allows the Campus servers to connect to the district's Windows file server through a VPN connection between Campus and Kentucky (KEN). This surrogate IP address is entered in the Scheduled Imports interface only; the locally configured IP address of the Windows file server is NOT changed.

In order to request a surrogate IP address, contact Campus support through the usual channels and provide the locally configured IP address and name of the Windows file

server. Up to three surrogate IP addresses can be provided per district (including those used for Data Extracts, discussed earlier).

### ***Secure FTP Protocol***

The two secure FTP delivery modes (SFTP and FTPS) cause the Campus servers to import the data file from a secure FTP site of the district's choosing. Both types of secure FTP require installing and configuring software on a server. Neither Campus nor KETS can provide assistance with procuring, installing, configuring, or operating secure FTP software. However, for secure FTP sites on a district-located server, the KETS Service Desk can assist with configuration changes to the KETS firewall and the allocation of a public IP address.

Note that the SFTP protocol is NOT supported by the Scheduled Imports feature.

The Campus Cloud servers' public IP addresses (from which secure FTP connections will originate) will be from one or more of these ranges:

65.124.140.0/24

207.225.137.0/24

198.73.96.0/21

216.226.196.0/22

### **Email Messenger SMTP Relay Configuration**

Detailed documentation of the Campus Email configuration is available in Campus Community; search for "Email Settings".

Campus provides an SMTP Relay that can be used as the "SMTP Host", though districts may choose to use another SMTP Relay instead.

If changing the SMTP Relay, contact the KETS Service Desk to have the district's SPF (Sender Policy Framework) DNS record updated appropriately.