OFFICE OF EDUCATION TECHNOLOGY

DIVISION OF SCHOOL DATA SERVICES

Technical Guide

Active Directory/Infinite Campus Integration in the KETS Environment

Version 1.4
January 19, 2017

Contents

Introduction 3
Benefits of AD Integration 3
Frequently Asked Questions 3
Planning Considerations 4
Configuration Recommendations 5
Migration Options 6
Scripted Migration Options 6
Support 7
Tools 7

Introduction

This document contains KDE recommendations for districts that are implementing the Active Directory integration feature of Infinite Campus. More information about this integration feature is available in the Campus document *LDAP Authentication* on Campus Community. This document is not intended to replace the Campus document mentioned but rather supplements it with Kentucky-specific information.

Benefits of AD Integration

- Users do not need to remember a second IC password or manually keep two passwords in sync.
- IC passwords will effectively be subject to the same password policies as AD passwords with no additional management effort.
- Passwords are stored securely and there is no need for users to periodically change their IC password.
- Administrators can disable a user's access to AD/Email and IC with one step for users set up to use LDAP authentication.

Frequently Asked Questions

1. **Does AD Integration affect Parent/Student Portal Access?**

   Yes. If a district chooses to migrate students to AD 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 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.

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

   Yes, but only using the Account Editor screen, not using the Account Settings screen.

4. **Will AD Integration 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.

Planning Considerations

1) When implementing AD integration, it is ESSENTIAL to create or retain an administrative-level Infinite Campus user that is NOT linked with Active Directory. In case of an AD connectivity issue, this account may be the only one that can be used to adjust the Infinite Campus configuration.
2) After switching to AD integration, consider removing the "Account Settings" Tool Right from most groups so that users do not try to change their passwords (which will not be effective) or change their LDAP connections.
3) The Campus *LDAP Authentication* document mentions the possible need to make firewall adjustments; no adjustments should be required in the KETS environment.
4) Be cautious about deleting and recreating an AD account that is linked to an Infinite Campus account; depending on the order of events you may be required to recreate the Infinite Campus account after recreating the AD account.
5) Even though users can log into Windows using multiple forms of their username (such as logon/SAMAccountName, User Principal Name, and primary SMTP address), they will only be able to log into Infinite Campus using the attribute specified in the Campus LDAP configuration screen.
6) If there is ever a need to remove AD integration, you must ensure that each user has an appropriate password set on their Campus user before disconnecting the user from Active Directory.
7) You may implement AD integration for students (for access to the Parent/Student Portal) as well as for district staff users.
8) In a Disaster Recovery scenario in which Campus is temporarily hosting the district's installation, AD integration will be disabled. Infinite Campus Hosting will set a unique password on each Campus user and provide a list of all usernames and passwords to the district contact for distribution to users.
9) Per Microsoft Licensing Product Use Rights (July 2011), you are expected to have User or Device CALs suitable for Windows Server 2008 access in place for all users who will be using AD credentials for access to Campus.
10) 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); Infinite Campus considers this a bug and in some future version this field will no longer have any effect.
11) 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* (available at www.education.ky.gov) describes options for requiring stronger AD passwords.
12) Every character that appears on a standard Windows keyboard can be used in an AD password for an account that is integrated with Infinite Campus. Other characters (such as symbols generated with the Alt key) have not been tested.
13) Campus will lock out a user account after 5 failed login attempts even if the user account is integrated with AD. When this happens an administrator will have to unlock the Campus user account in addition to unlocking the AD account. Consider whether you wish to reduce the AD threshold for failed login attempts to a smaller value than 5 in order to help prevent this. Infinite Campus considers this a bug and in some future version the Campus system will not lock out Campus user accounts for AD-integrated users.
14) The password for the Bind User (an AD account used by Campus for Active Directory lookups in certain situations) is stored in plain text within the Campus database. Infinite Campus will modify the product to store this password securely in a future version.
15) Campus has placed code in their login page that blocks the browser from remembering the username, such that every time a user wants to log into Campus, they have to type all of the username and password.

16) If an AD-integrated user's username is changed in Active Directory, the user will need to log into Infinite Campus one more time using the prior username in order for Campus to properly update the link; after that one time the new AD username must be used for Campus login.

Configuration Recommendations

These recommendations apply specifically to the one-time system-wide configuration described in section "Configuring Campus for LDAP Authentication" of the Campus document *LDAP Authentication*.

1) Host priority	Locally Hosted Districts: Specify the district DC (Domain Controller) as Server 1 Host, GC (Global Catalog) as Server 2 Host, using fully-qualified domain names (for example, ed999addc1.kets.ketsds.net). Cloud Districts: Contact Campus Support through normal channels and request the surrogate (Network Address Translation, aka NAT) IP addresses that will allow your cloud-located installation to connect to your district's AD servers.
2) Port	Specify 636 for both servers to support SSL.
3) SSL	Check the box to specify SSL. The necessary certificates for LDAP communication over SSL are already in place on all KETS domain controllers.
4) Bind User	This AD account will be used by the Infinite Campus software to query Active Directory. This account does not need any AD permissions beyond the default granted to all AD accounts. This is a service account and should be configured to not expire password and to not require password change on first login. Object name: IC_Integration_Bind_User Object OU: _District Admins/Service Accounts
5) Bind Password	This account should be given a strong (long, complex) password since the password cannot be changed frequently.
6) Search Base	This identifies the level on the AD tree from which Infinite Campus will begin searches when attempting to match Campus users to AD users. The recommended value is DC=*districtname*,DC=ketsds,DC=net Where *districtname* is the district AD domain name.
7) Username Attribute	The recommended value is

	userPrincipalName so that users can log into Campus using their email address, just as they log into Office 365.

Migration Options

You have three options for the actual process of migrating users to Active Directory Authentication.

1) An administrator can edit each existing Campus user account. Further details are available in the Campus *LDAP Authentication* document.
2) Each user can edit their own Campus user account. Further details are available in the Campus *LDAP Authentication* document.
3) Scripted migration through Campus Support and Data Conversion groups. Further details are found below.

NOTE: The user's Microsoft Office 365 email address must be used as the Campus username if choosing the Scripted Migration Option.

Scripted Migration Options

KDE will pay for each district to use the scripted migration process to connect your Campus usernames to Active Directory accounts. If you wish to use the scripted process, you will need to follow these steps:

1) Retrieve the Staff and optionally the Student file from https://live.kyschools.us/ADIC. Any district user can access these files by logging in with their Office 365 username and password (note that depending on your browser you may have to authenticate several times). The three-digit district number is part of the filename. The data in these files is available to any district user by connecting to Active Directory but is assembled in these files for convenience. These files are updated nightly.
2) Review the files (which are in CSV [Comma Separated Values] format) using Excel or a text editor and remove the rows for any Campus users that should NOT be integrated with Active Directory. Rows whose email addresses cannot be found in Campus will be skipped by the migration process and listed in a provided report.
3) Verify that you have correct Office 365 email addresses attached to each Campus user to be integrated with Active Directory.
4) Decide if you are going to have the Data Conversion group migrate your Campus Sandbox installation first. A Sandbox migration can help you find any issues in your existing user accounts before performing a Production migration, but is not required.
5) Open a ticket with Campus Support, titling it "AD Authentication Migration for *districtname*", specifying preference for Sandbox migration or not, whether you're migrating Staff only or Staff and Students, and uploading the edited CSV files.
6) If you have requested a Sandbox migration, Campus Hosting will refresh your Sandbox and Campus Data Conversion will execute the migration in the Sandbox and provide a report of the

results through your Support Ticket. Review the results and make any appropriate changes in Infinite Campus and/or Active Directory.

7) Update your Campus Support ticket with at least three possible dates for your Production migration. Campus Data Conversion will respond and any further timing details will be settled through the Support ticket.
8) Communicate with your users regarding the upcoming change in login process and any changes to Active Directory password policies.
9) Complete the one-time system-wide configuration described in section "Configuring Campus for LDAP Authentication" of the Campus document *LDAP Authentication*, referencing the configuration recommendations listed above.
10) Shortly before your Production migration, download fresh versions of the Staff and (optionally) Student files, remove rows for any Campus users that should NOT be integrated with Active Directory, and upload them to your existing Support ticket.
11) Campus Data Conversion will execute the migration in Production and provide a report of the results through your Support ticket.
12) Provide any follow-up communication to your users.

Support

For Campus product functionality support, please contact Infinite Campus Support through the usual channels.

For questions about this document, issues with the Staff and Student files provided by KDE, or other support needs related to integration in the KETS environment, please contact the KETS Service Desk at KETSHelp@education.ky.gov.

Tools

KDE has created and pushed down to all districts a Campus ad-hoc filter named "User AD Integration Status" that can be used to identify which users have been integrated with Active Directory.