BUILD AND RUN
BUSINESS APPLICATIONS,
POWERED BY YOUR
IMAGINATION

K2 & AUTHENTICATION WITH MULTIPLE IDENTITY PROVIDERS

1/13/2016

This whitepaper explains how to configure K2 authentication when using multiple Identify Providers.

K2 & AUTHENTICATION WITH MULTIPLE IDENTITY PROVIDERS

When integrating K2 into an environment with multiple Identity Providers (IdPs), you must be aware of the technical aspects of introducing this complexity into your environment and how it impacts K2 functionality, especially for end-users. This includes environments where K2 is integrated with SharePoint hybrid environments (although multiple IdP scenarios are also possible without any SharePoint integration).

> Note: For more information on Identity Providers and Authentication in the K2 platform, please refer to the Authentication and Authorization in K2 series of whitepapers.

K2 works with SharePoint and non-SharePoint configurations that include multiple IdPs. In SharePoint, this is called a hybrid configuration, since it uses both an on-premises Active Directory (AD) provider for some users, and an online Azure AD (AAD) provider for other users. Sometimes these users are the same actual identity, but technically they are two separate identities. It is important to understand how K2 works with SharePoint hybrid configurations, and what impact hybrid configuration has on K2-SharePoint integration.

It is also important to understand what functions are not enabled by configuring multiple IdPs, such as presenting a unified K2 task list to a user which spans all of that user's identities from multiple IdPs.

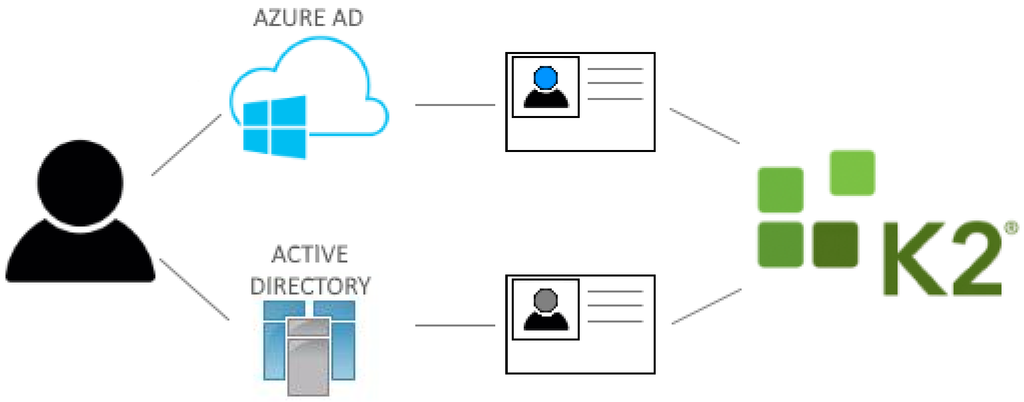
This document attempts to illustrate the issues and considerations to be aware of when:

- Integrating K2 blackpearl with a SharePoint hybrid configuration
- Integrating K2 blackpearl into an environment where multiple identity providers are present
- Integrating K2 Appit with on-premises line of business systems
- For K2 blackpearl, converting the primary K2 (AD) label to a different label, such as K2ADFS, and needing to maintain historical data, workflow definitions and active workflow instances.
- End-users need to interact with their K2 task lists and forms, and their identity information is not located in a single IdP.

EXAMPLE SCENARIO AND ILLUSTRATION

You have K2 for SharePoint solutions on SharePoint Online and SharePoint 2013 on-premises, as well as SmartForms-based applications that do not integrate with SharePoint. All users authenticate against the K2 label using their domain name when using the on-premises or non-SharePoint applications. However, when they log in to SharePoint Online and access a SmartForm, they are authenticated in K2 against the AAD label using their UPN (e-mail address) as the identifier.
In other words, if Bob logs in to his PC and browses to a SmartForm, Bob is authenticated as **K2:DOMAIN\Bob**. However, if Bob has not opened a SmartForm, and then he logs in to SharePoint Online and browses to a SmartForms page, he is authenticated as **AAD:bob@domain.com**.

The custom domain (domain.com) is in place because DirSync is used to sync all domain accounts to Azure AD, and the way in which a user logs in determines which user they are authenticated as. (More specifically, the way in which they log in determines which IdP is used to authenticate that user). Furthermore, when a person authenticates against different IdPs, that person is not considered the same user according to K2, because their user identities are from two different locations (stores), and therefore they have two different, unique identities.



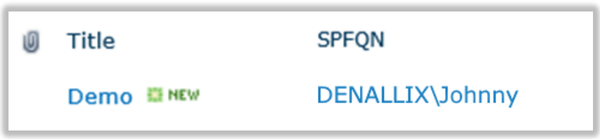
The user's unique identities, stored in two separate repositories, means that the K2 server does not see the unique identities as related to a single identity.

This behavior is not unique to K2. Other systems such as SharePoint treat these users as different identities as well. As an example, if you were to switch a SharePoint on-premises server from using Active Directory to using Azure AD as its primary authentication method, you would notice that all of your previous rights and membership (based on the identities stored in AD) would not apply to the Azure AD users. You would need to grant all Azure AD users access to the SharePoint sites, essentially recreating the AD rights but with Azure AD users.

Illustrating Different Identities in SharePoint

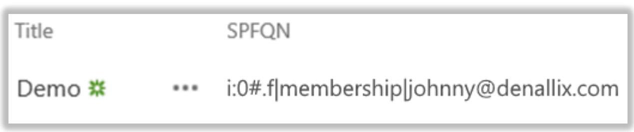
Although SharePoint does a good job of masking who your identity is and tries to make it seamless between on-prem and online, you can easily demonstrate the differences by creating two lists, one on your local on-prem SharePoint site and one in SharePoint Online. Add the **Account** field to the newly-created list and then create an item in each list.

In the on-prem server you'll see the domain name as you would log in to your computer on the corporate network.



Title	SPFQN
Demo NEW	DENALLIX\Johnny

In SharePoint Online, you'll see that your identity is different, and looks more like an e-mail address.



Title		SPFQN
Demo	•••	i:0#.f|membership|johnny@denallix.com

This scenario exists when SharePoint is not setup in hybrid mode and there is no mechanism in place for syncing accounts between AD and Azure AD.

The sequence of steps below illustrates the impact on K2 worklists and SmartForms when multiple identity providers are used, using a typical SharePoint hybrid scenario:

1. A user navigates to a non-SharePoint SmartForm, such as a SmartForm with the worklist control, and is authenticated as K2:<domain>\<user>, such as K2:DENALLIX\Johnny, and the cookie is kept in memory.
2. The user is assigned as the destination user in a SharePoint Online workflow as AAD:<email address>, such as AAD:johnny@denallix.com
3. The user receives a task e-mail from the SharePoint Online workflow with a link to open the task.
4. The user clicks on the link and when the SmartForm page loads, it recognizes that this user has an authentication cookie already saved and uses these credentials to open that page.
5. The user is authenticated as K2:DENALLIX\Johnny because the cookie was created like this the first time when the original worklist SmartForm was opened in step 1.
6. K2 throws an error stating that K2:DENALLIX\Johnny is not allowed to open this worklist item. This is because the user's FQN does not match who was assigned the task (AAD:johnny@denallix.com).
   To temporarily workaround this problem, the user closes all browsers and then deletes all cookies. They click again on the link in the task e-mail. This prompts them to log into Office 365 and, once they do, the SmartForm page is displayed without the error in Step 6.

Note

An alternative to closing all browsers and deleting cookies is to open a private browsing mode, such as Incognito in Chrome, or Private in Safari, Firefox or IE.

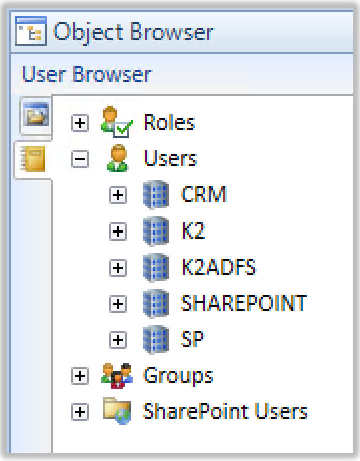
USER INFORMATION IN K2

The first item to familiarize yourself with is how K2 handles identities. Using what's known as a User Manager, K2 associates each user based on where their user information is stored, and prepends a label to that user's login name, forming what's called a Fully Qualified Name (FQN). Think of this as your K2 label if you have AD, and the SQL, AAD, SP and K2ADFS labels if you've already configured K2 to use a different User Manager or if you’ve added the K2 for SharePoint app to your SharePoint Online sites.
For example:

- A typical AD user's FQN: **K2:DENALLIX\Johnny**
- A typical AAD user's FQN: **AAD:johnny@denallix.com**

For a complete discussion of this topic see Introduction to User Managers in the Installation and Configuration Guide. For an example of an environment where multiple user managers are used, take a look at the following User Browser. This environment has five different user managers in use:

- CRM
- K2
- K2ADFS
- SHAREPOINT
- SP



It's important to understand that each of these user managers stores user information, and while a user's actual identity might be the same across multiple labels, to K2 each of these users are distinct users and there is no mechanism to treat two or more users across different labels as the same K2 user. ***This is true for K2 as well as SharePoint and most other line of business systems – a user's unique identity cannot be shared or equated with another, unique identity.*** What makes a unique K2 identity is the label and the user's login name from the IdP, such as K2:DENALLIX\Johnny or AAD:johnny@denallix.com.

Note

It is important to understand the implications of having multiple user identities for a single, actual user, present in multiple IdPs. Because K2 and other systems must store the unique identity of a user, changing that user's unique identity (or needing to equate it with another, unique identity) has fundamental challenges associated with historical data, workflow definitions, and running workflow instances.

ASSIGNING WORK TO SOMEONE

When you use the Context Browser in K2 Studio or the K2 Designer for SharePoint to assign work to someone, such as adding them as a destination user on a workflow task, you must choose a user that is known to the K2 system. If K2 has not been configured to resolve users from a particular user identity store, then you cannot assign those users any work.

When using a SharePoint group as a destination user e.g. to assign work to anybody contained in that group, the SP object is used by other user managers, such as the K2 label, to resolve users in the group. However, if a user in that group is not known by K2, they will not be able to get work assigned to them.

HOW YOU AUTHENTICATE WITH K2

When you browse to a SmartForm directly, and you're on your company's network that is based on Windows Active Directory, your credentials are automatically passed to K2 via a Kerberos token. This verifies your identity and registers you as a user with a K2 label. If you browse to the K2 Designer you'll see that K2 knows your identity.

If you hover over your username you'll see your FQN in a tooltip. In this case, the tooltip says **K2:DENALLIX\Johnny**. If Johnny had signed in with his AAD credentials, the tooltip would be **AAD:johnny@denallix.com**, but would still look the same from simply glancing at his name in the upper right corner of the K2 Designer.

If you are browsing a SharePoint site (on-prem or online), and you open a K2 form or integrate a list or library with the K2 Application, your identity is passed to K2. Your username is matched against a known user manager in K2. If you're not known to K2, you may see errors such as the following:

- `Error: You do not have permission to open this form.`
- `Error: You must be a member of the Solution Designers group to design applications.`

Many times this means that although SharePoint knows who you are, K2 does not. You might check your various permissions if you think K2 should know who you are, but if the permissions appear to be OK, you are most likely dealing with a problem of the identity only being configured for SharePoint and not K2. In the SharePoint 2013 and SharePoint Online architecture, any third-party app such as K2 must directly trust all identity providers used by SharePoint.

You may see a different error, namely
`The user "K2ADFS:johnny@denallix.com" cannot be found in SharePoint.`

If you see this error, it means that you have multiple identity providers configured across multiple SharePoint farms, and your workflow has most likely assigned a task to a user that doesn't exist on, or have permissions to browse, a particular site.

How you access K2 or a K2-based item such as your worklist, determines what you're able to get to and see. For example, your worklist lists all the work assigned to the identity that you are currently logged in to SharePoint with. If you have two logins for SharePoint, and you're working with multiple K2 apps across multiple SharePoint sites, there is no way currently to see a consolidated list of tasks. The workaround is to have the K2 Worklist app part in each SharePoint environment where you expect to get assigned tasks.

FAQS

Here are a list of some frequently asked questions about authentication when using multiple identity providers.

1. WHAT CONFIGURATION IS SUPPORTED TODAY?

So how do end-users work with K2 when there are multiple IdPs in the environment, and what doesn't work?

Multiple IdPs (and their default labels) would be systems like AD (K2), Azure AD (AAD), AD FS (K2ADFS), SQL (K2SQLUM) and SharePoint (SP).

Any combination of these IdPs, excluding SharePoint in most cases, require your end-users to be aware of which identity they are logging into their task list with and how to switch identities when necessary.

2. WHY CAN'T I HAVE A UNIFIED TASK LIST?

Perhaps what you desire is a unified task list that has all of your K2 tasks related to SharePoint on-premises, SharePoint Online and even non-SharePoint related tasks. This amounts to Single Sign-On (SSO), which K2 supports but only for configuring service instance authentication.

SSO for your task list is not currently possible today because each IdP issues what it believes to be a unique user's complete information. A better way to think about it would be like wanting your Facebook and Linked In messages to be in the same shared inbox. This is not possible because it is two completely different systems in the background.

3. HOW DO OKTA, PING AND OTHER SERVICES SOLVE THIS PROBLEM?

SSO solutions, like Okta, Ping and others, essentially log you in to the appropriate system at the appropriate time. Your identities in those systems does not become shared or the same. SSO systems do not solve the problem of having multiple, unique identities, but rather allow end-users to more easily manage their different identities so they don't have to remember multiple login names and passwords. But these systems do not provide data consolidation capabilities that would allow K2 to be unaware that multiple identities are present.

4. WHAT HAPPENS WHEN I MOVE FROM SHAREPOINT ON-PREMISES TO SHAREPOINT ONLINE?

If you are moving functionality to Office 365 you may find yourself in this position: you have created new users on Office 365 that map to current users, and you have not synced your AD users to Azure Active Directory.

K2 supports users from multiple directories, and can interoperate between SharePoint on-premises and SharePoint Online. However, this scenario means that you have duplicated users in two different directories (AD and AAD), but there are scenarios where separate and distinct users have access to the online properties. Where there are effectively the same users in both directories, K2 does not equate the AD users with the AAD users but rather treats them a separate and distinct users.

Having separate users means that there cannot be a unified worklist and that, when designing workflows, your destination users must be chosen from the correct label depending on the business rules. For example, if a client event step in your workflow requires that online users take action on the workflow, such as reviewing, approving or rejecting the request, if you choose users from the AD label (typically K2), then the workflow participants coming in from SharePoint Online may not be able to see the task on their worklist or open the task.

One workaround, as a temporary measure to facilitate the move from SharePoint on-premises to SharePoint Online, would be to use the K2 management tooling to redirect tasks from AD user accounts to AAD User accounts for any existing tasks.

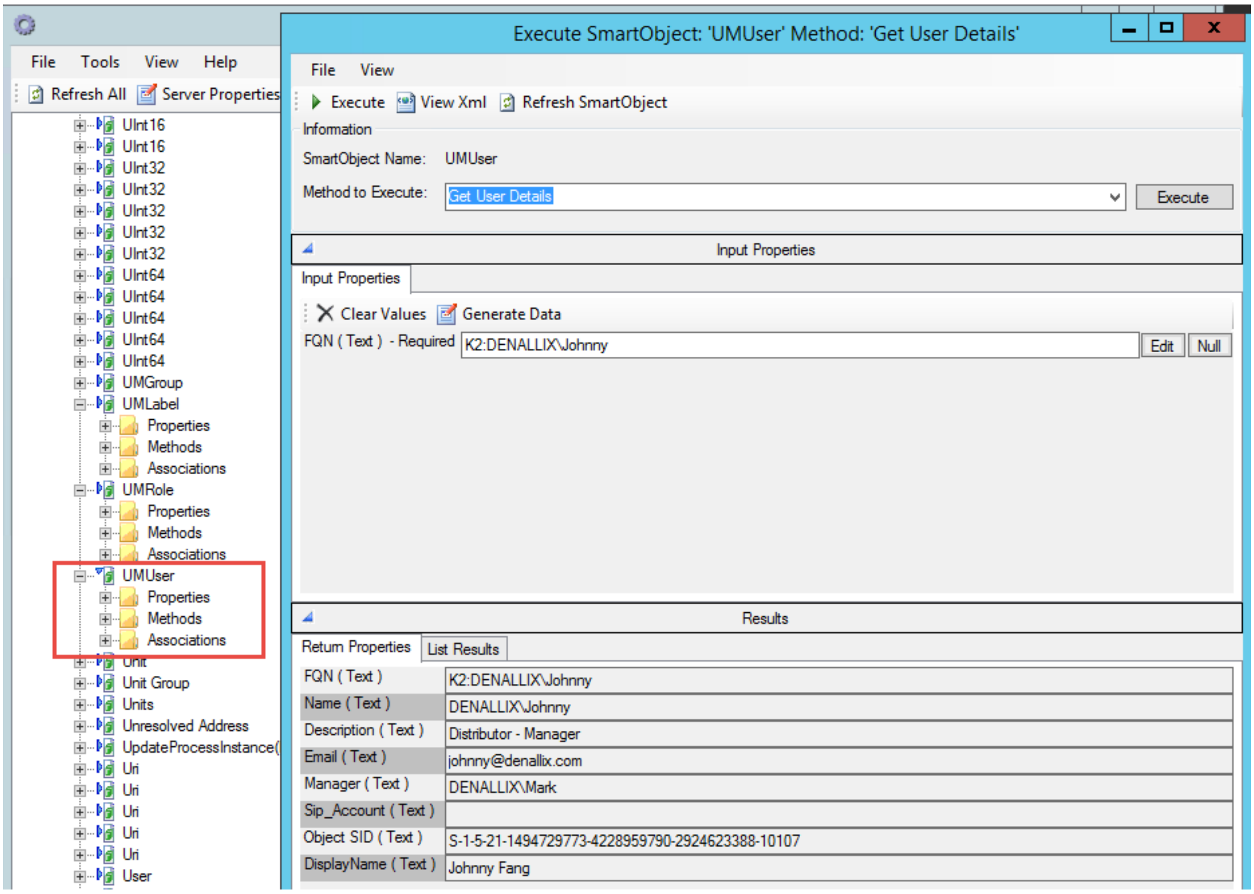
Another workaround (although this would only work when there is only one slot for a user task), is to assign all of the same user’s identities (e.g. K2:domain\bob and AAD:bob@domain.com) as destinations for the task. This way, the user can successfully open the workflow task regardless of which account was used to authenticate in K2.

5. HOW CAN I TEST USER RESOLUTION?

You can use direct SmartObject calls using the SmartObject Services Tester Tool to ensure that users are resolved correctly and as expected. You can find the following SmartObjects under the **All SmartObjects** category in the tester tool:

- UMLabel
- UMGroup
- UMRole
- UMUser

These SmartObjects are part of the User Role Manager service and represent how K2 manages to resolve users across all registered labels. If you are unsure how a user's information is being resolved, use this to test a known FQN.



RECOMMENDATIONS

K2 recommends that you establish your identity store strategy before building, deploying and starting K2 solutions. Changing your identity strategy after you've had K2 in place for a while will affect your reports and possibly other purposes for which you're using data captured by K2 processes.

If you have concerns about how K2 works with multiple IdPs, you can log a Support Ticket or contact K2 Remote Services in order to discuss your strategy moving forward. For more information see http://help.k2.com/customer-support

CONCLUSION

Handling the SharePoint Hybrid scenario, and any other scenario that requires K2 to handle users from multiple identity providers (IdPs), results in some challenges and behaviors in K2 that may not be desired. If you can plan your identity strategy before deploying K2 solutions, you can avoid some issues that cause identity problems when moving to a new identity provider when running and completed process instances are present.