Starting with KICS 2.4.0, Directory Authentication and Federated Services are now available.

Authentication Methods

How Local Authentication Works

Local Authentication is our traditional KICS authentication method. Each user is supplied an account within the KICS account manager. A User authenticates to KICS with their username and password and the local account table is checked for an existing account. When an account is found, roles are checked to determine the permissions available for the user.

Local authentication doesn't currently support User Registration; however it allows users to reset their password if forgotten.

How Directory Authentication Works.

Directory Authentication allows KICS to authenticate using a company's corporate directory. The types of authentication methods available are LDAP and SAML. With LDAP, KICS supplies a login screen where a user logs in with their directory username and password. With SAML, the user is redirected to the company's authentication server and then directed back to KICS. SAML supports Single Sign-On if the user has already authenticated with the company's authentication server.
When a user authenticates, the authentication server supplies the following properties about the user:

- Account Name
- Account Serial Number
- Email Address
- First Name
- Last Name
- Group Membership

KICS uniquely identifies directory accounts by the Account Serial Number (see mapping process below). If an account is not found, a new account is created automatically for the user. If an account IS found, the account is updated with the supplied properties.

The local roles are checked to supply permissions to the user.

If the user is a member of any directory groups and those groups are configured within KICS, the directory groups will also supply permissions to the user.

Account Mapping Process.

Directory Authentication uses Account Serial Numbers to keep track of the user accounts. This allows the user to maintain the same account regardless of a name, email or position change. Accounts that are associated with an Account Serial are called Linked Accounts and accounts without a Serial are called Unlinked Accounts.

When a User authenticates or an Account Sync occurs:

- KICS searches the Linked Accounts for an account matching the Serial Number
- If an account cannot be found, KICS searches unlinked accounts for an account with the identical account name.
- If an account is still not found, KICS searches unlinked accounts for an account with an identical email
- If an account is still not found, a new linked account is created with the Serial Number

During the mapping process, KICS Account's properties are updated with the supplied Account Information.

LDAP

LDAP can supply Directory Authentication and Account Management within KICS.

When LDAP authentication is used, KICS supplies the account login page and passes the account credentials to the LDAP authentication server for verification. The LDAP server returns the authenticated account's properties back to KICS.

LDAP can also supply Account Management and be used alongside other Authentication Methods. This means LDAP can be used for account lookups for creating Linked Accounts within the Account Manger, as well as a nightly directory sync to automatically add / update KICS accounts.

LDAP requirements:

- For LDAP to work, KICS will require communication to an LDAP server.
- An LDAP service account is also required to allow KICS to perform account lookups and directory syncs.
- A Base DN will need to be configured to constrain KICS to a specific Organization Unit for User and Group lookups (if no filtering is required, the root DN can also be used).
- If you are identifying users by their UserPrincipalName (user@domain), you can also supply a list of domain names to simplify the login process for the end user.

SAML / ADFS / Federated Services.

With SAML, a user is redirected to a company's authentication server for sign-in. When the user authenticates, the SAML server provides an authentication token to KICS. This token provides the account properties (Account Name, Group Membership, First Name, Last Name, Email, Account Serial), which KICS uses to lookup / map / create a Linked account for the user.

SAML Requirements

- HTTPS / SSL needs to be enabled for the KICS site
- A Service Provider Certificate (SP) needs to be generated within KICS
- An Identity Provider Certificate (IDP) needs to be provided from the federation server and installed within KICS.
- The authentication URLs (login/logout) for the federation server need to be configured.

- A relaying Party trust needs to be configured on the Federation Server for KICS (note: Specific attributes are required for KICS to authenticate a user, therefore it's recommended to configure the trust using the KICS metadata url)

Setting up KICS for SAML

Please refer to the **KICS - SAML, ADFS Federated Services Setup** technical document for setup instructions.

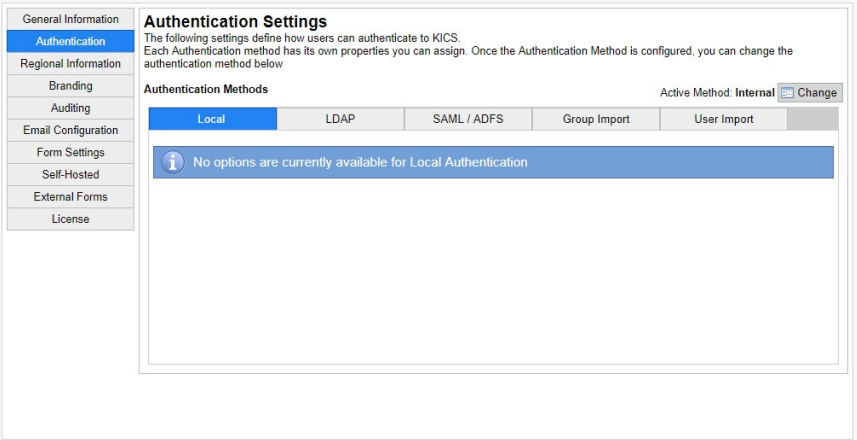
NOTE: Federated Services solely provides user authentication. It does not offer account management. Therefore SAML can only be used to authenticate users and create user accounts as they sign on.

To create directory accounts, LDAP needs to be configured, OR a manual import of directory accounts and groups needs to be performed (found on the Settings > Authentication pages).

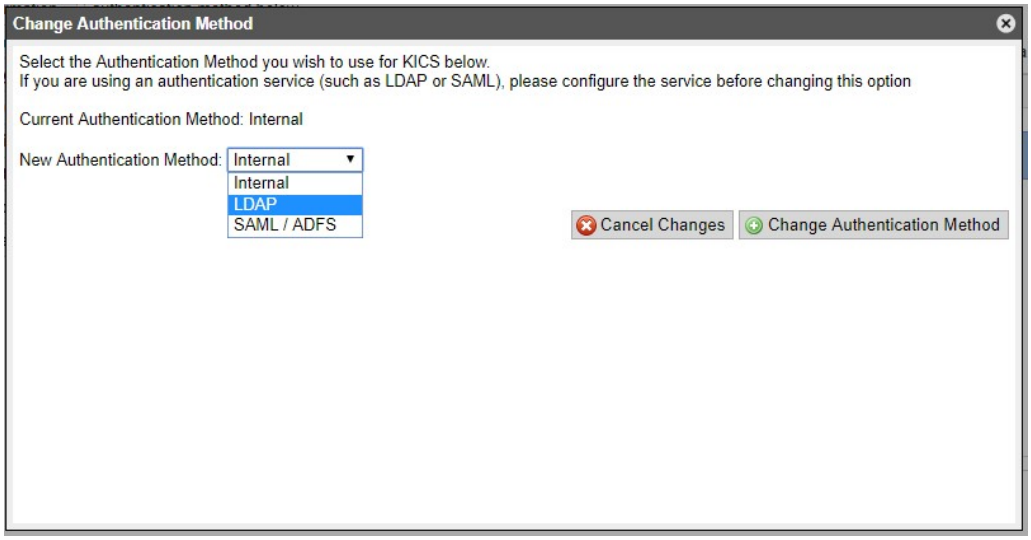
Configuring the Authentication Method KICS uses

Once you have configured LDAP or SAML/ADFS, you need to configure KICS to use the appropriate authentication method.

Under **KICS Administration > System Settings**, select **Authentication**



Beside the Active Method status, click **Change**



The **Change Authentication Method** dialog appears.

Select the new authentication method you wish to use and click **Change Authentication Method**.

NOTE: When you select a new authentication method, KICS may inform you of the authentication changes and how this will impact your system.

Once the Authentication Method is changed, the User Manager, Role Manager and login pages will update to reflect the new authentication method.

Impacts of switching between Local and Directory Authentication

The default install of KICS supplies local authentication. When local authentication is switched to directory authentication, the following changes occur:

Existing Local Accounts become 'unlinked accounts' because they are not assigned a serial # to a corresponding directory account.

These accounts need to be manually linked to a directory account (within the Account Manager), OR they will become automatically mapped to a directory account when user authenticates, or an 'Account Sync' occurs, (as long as the account name and email matches a directory account).

If you switch from directory authentication to local authentication, users can log in with their existing account name. Existing directory accounts won't have a configured password. Therefore you will need to assign a password within the Account Manager, or allow the user to reset their password from the login page.

Roles and Groups

Local Roles

Local roles are our traditional KICS roles. Each role can be configured for template permissions and special access to KICS. These roles are assigned to accounts.

Directory Groups

Directory groups operate the same as Local Roles, with the exception that group membership is determined by the directory server and not KICS. When a user authenticates, their account's group membership is checked against the directory groups configured on the server.

A directory account can be member of both local roles and directory groups.

Parklane Emergency Access

An administrator could potentially lock themselves out of KICS if the authentication settings are not configured properly, OR the KICS Admin account is mapped to an incorrect account.

We have implemented a maintenance page to 'override' the authentication settings and grant admin access to KICS. This request requires communication with Parklane Support.

NOTE: When the Emergency Access page is used, an email alert is sent to the admin's account informing them of the authentication bypass.

Methods to create Directory Accounts

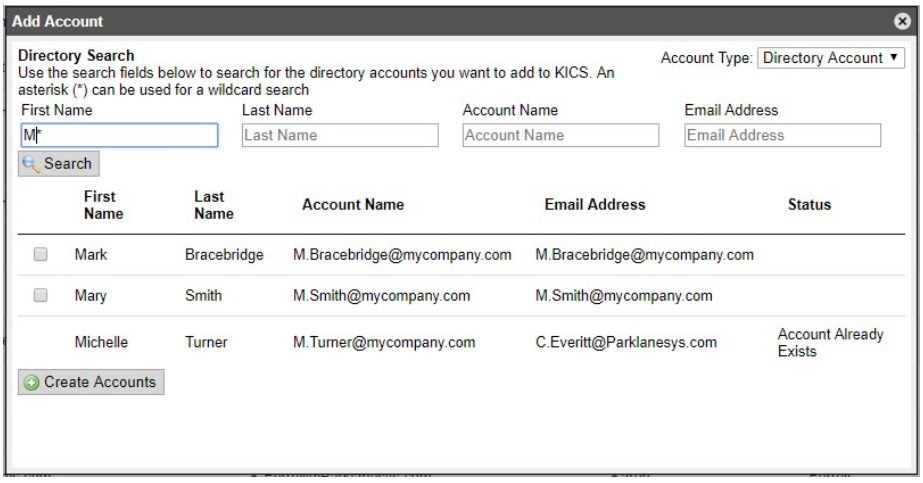
Sign On (LDAP, SAML)

When a user logs into KICS, the accounts table is searched for their directory account. If an account is not found, KICS maps an unlinked account (if found with a matching account name / email), or automatically generates a new account for the user.

Add User (LDAP)

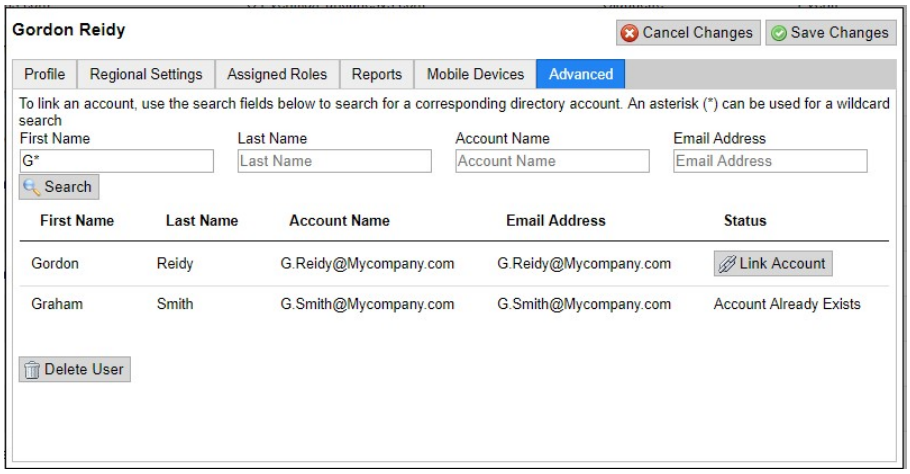
In the Account Manager, selecting Add User will allow you to search the directory server for accounts. KICS will inform you of accounts already added, as well as let you select multiple accounts at once to add.

When you add a user, KICS performs the mapping process to determine if there are any unlinked accounts that match the new account information. If not, new accounts are created.



Link user to Directory Account (LDAP)

If you want to map a specific directory account to a user, you can use the 'Link' option in the User profile settings. This will allow you to search the directory server and link the account the KICS user. This is handy if you want to re-assign the top-level KICS admin to another account.



Account Sync (LDAP)

If you have a large user base, Account Sync can keep your linked accounts and directory groups up-to-date.

Once a night, KICS will query the Directory Server for a list of accounts. KICS will use this information to update existing accounts (account name, email, firstname, lastname), as well as automatically create new accounts if the option as enabled.

Note: Before the account sync can occur, a dry run needs to be performed and verified to make sure the sync doesn't cause an unexpected result.

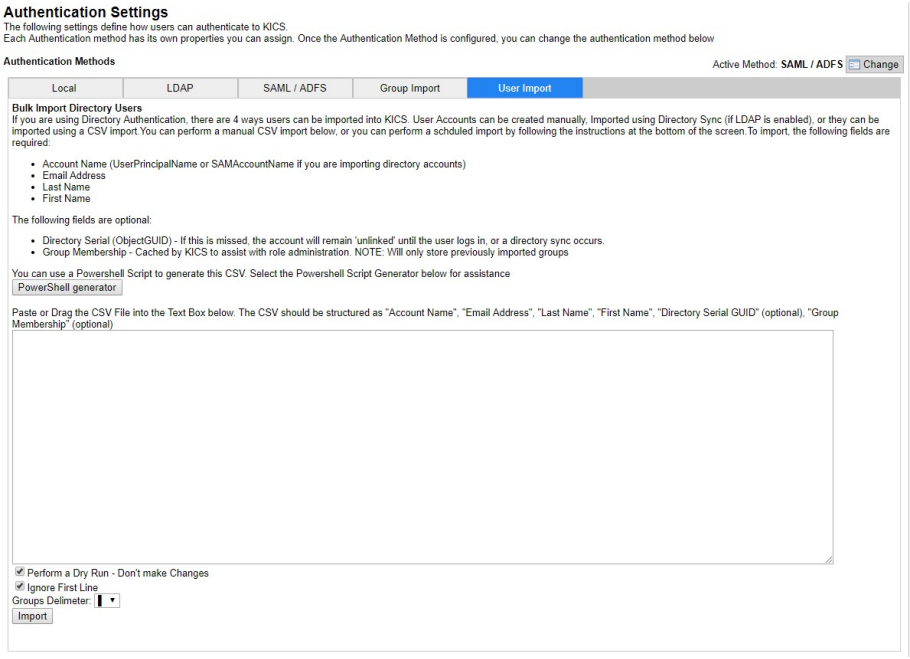
parklane SYSTEMS

Creating Unlinked Accounts (LDAP / SAML)

In situations where a directory server is not available, you can create unlinked accounts within the account manager to set up a user profile. Once a user (with the matching account name or email) signs in for the first time, their directory account will be mapped to the unlinked account.

Manual Import (LDAP, SAML)

In situations where a directory server is not available (such as hosted, or a SAML-Only deployment) you can import your accounts and directory groups using the Manual Sync option.



On the Settings -> Authentication Page, KICS has an option for a Group and User import. A powershell generator option is available to assist you in generating a CSV (using powershell) for the required account information.

Please Note: The powershell generator does not provide any user / group filtering, so you will be required to supply a DN to the powershell script if you wish to only have it query a specific OU.

With the import, new accounts will be mapped / added and existing accounts will be updated.

Deployment scenarios

Local Authentication

This is the traditional authentication used with KICS. Accounts are created within KICS and are assigned a password. Users use this Account & Password combination to log in. Privileges are decided solely based on the Roles the user is a member of.

Local Authentication does not allow for user registration (at this time), however it allows for Password Resets.

Local Authentication is suitable for organizations where only a small group of users need to log into KICS. Both Onsite and Hosted deployments of KICS support Local Authentication

LDAP Integration & Authentication

LDAP Authentication will be used by organizations where they wish to use their existing username / passwords but don't have a Federated Server. This will most likely be used by customers who have Active Directory and have KICS onsite. LDAP is possible for hosted customers, however it requires a site-to-site VPN between the customer and Parklane.

The other component to LDAP is the LDAP Integration of the User and Role Managers. This allows User Accounts to be searched, created and linked from the customer's directory server, as well as a sync process to keep user accounts up-to-date.

SAML Authentication with LDAP Integration

SAML Authentication with LDAP Integration is the most feature-rich deployment of KICS. Users will use SAML / Federated Services to authenticate with KICS, while the KICS Administrators can use the LDAP component to create / update and manage the associated user accounts from the customer's directory server.

This type of deployment is suitable for on-premise customers with a federation server. LDAP is possible for hosted customers, however it requires a site-to-site VPN between the customer and Parklane.

SAML Authentication

SAML Authentication can be used for organizations that want to authenticate with their Federated Server, but are unable to use LDAP services for account management. A SAML-Only authentication is mostly suited for our Hosted customers.

SAML Authentication allows the users to sign in with their federated server and pass the authentication details to KICS. This allows KICS to create or update a user record for the user during the sign-in process.

A SAML-Only deployment limits the ability of searching and adding directory accounts and roles. However, unlinked accounts can be created, OR a user / group list can be manually imported on the KICS Settings Page.