TDS users provisioning, authorisation and authentication

- Intro
- Types of supported environments
    - From a network point of view
    - From AD/ADFS authentication integration point of view
    - From users origin point of view
    - From users origin combination point of view
- Provisioning capabilities
    - General provisioning capabilities
    - Provisioning capabilities flow diagrams
        - Invitations and sign-up flow
        - CSV import flow
    - Provisioning capabilities suitable for various types of environments
    - Authentication capabilities
    - Authorisation capabilities

Intro

TDS has multiple ways of users authentication, authorisation and provisioning. Possibilities depend on a combination of customer requirements and TDS capabilities.

Types of supported environments

From a network point of view

- public cloud
    - common TDS
    - dedicated TDS
- private cloud
    - dedicated TDS

From AD/ADFS authentication integration point of view

- AD/ADFS disabled
    - everyone has TDS account and is authenticated only using TDS LDAP credentials
- AD/ADFS enabled
    - everyone has TDS account and can be authenticated using TDS LDAP credentials
    - everyone has TDS account and can be authenticated using company AD/ADFS credentials

From users origin point of view

Two users categories are distinguished:

- AD users - users with AD account (usually employees, but very often also subcontractors)
    - can use AD or/and ADFS if enabled
    - can use TDS LDAP credentials
- non AD users - users without AD account (usually subcontractors)
    - cannot use AD nor ADFS
    - must use TDS LDAP credentials

From users origin combination point of view

When both AD users and non AD users are present in TDS, we are talking about a hybrid environment:

- standard TDS
  - either AD/ADFS is enabled AND all users are AD users
  - or AD/ADFS is disabled (TDS does not care whether users have or do not have AD accounts as there is no integration)
- hybrid TDS
  - AD/ADFS is enabled AND some non AD users are present

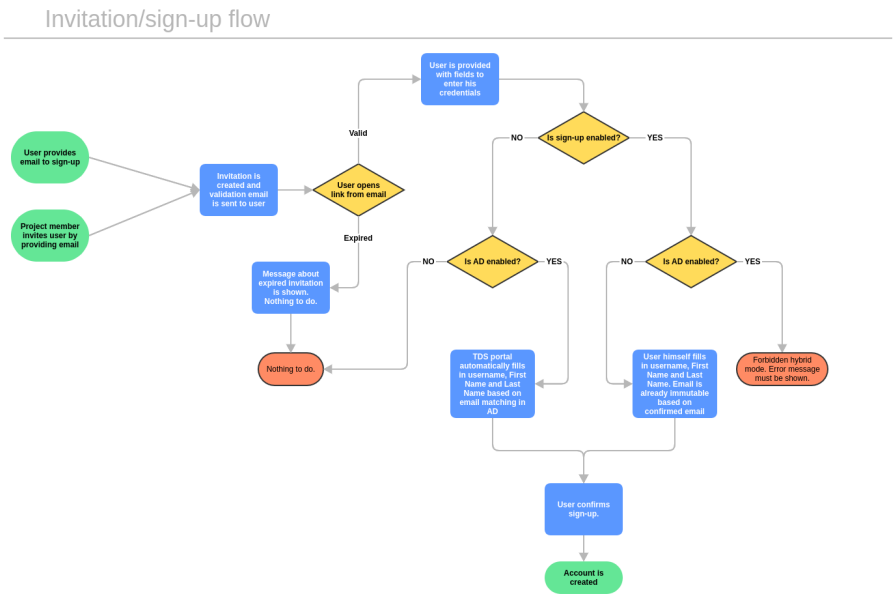
Provisioning capabilities

General provisioning capabilities

- invitations
  - colleagues or leaders can send invitations to people not present in platform, invited users must validate their email address, then they can enter their credentials or their credentials are read from AD if present
- sign-up
  - users can create accounts by themselves - first, they must validate their email address, then they can enter their credentials or their credentials are read from AD if present
  - recommended for
    - for a platform with AD users only without any externals (currently or in future)
    - for the platform without AD connection
  - it is NOT recommended
    - in hybrid environments when AD users and NON AD users should be working in the platform as users without AD account can create usernames as they wish and that can lead to conflict with current or potential future AD users leading to security issue
- CSV import
  - currently, requests must be raised via standard support channels as this functionality is available for TDS support ONLY (we are working on the possibility to provide this to customer area admins and owners)
  - recommended for
    - hybrid environments when AD users and NON AD users should be working in the platform - it gives customer key users (customer area admins/owners) full control over users that are joining the platform

Provisioning capabilities flow diagrams

Invitations and sign-up flow



CSV import flow

Steps:

- Customer key users send a ticket to TDS support in CSV format

```
username,email,FirstName,LastName
```

- TDS support team imports users to the portal

- Customer end-users with eligible project admin/owner permissions can manage users accesses via TDS portal. Key users that have area admins /owners roles can manage every project in the area.

Provisioning capabilities suitable for various types of environments

- public cloud
  - common TDS - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
    - ✅ invitations
    - ✅ sign-up
    - ✅ CSV import
  - dedicated TDS
    - ADFS disabled - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
      - ✅ invitations
      - ✅ sign-up
      - ✅ CSV import
    - ADFS enabled - only CSV import is available due to security-related limitations to avoid usernames collision and similar. It does not matter whether users have or do not have AD account, in the public cloud we would not be able to control users that are invited or signed-up, thus we would not be able to prevent security issues caused by potential users accounts collisions
      - ❌ invitations
      - ❌ sign-up
      - ✅ CSV import
- private cloud
  - dedicated TDS
    - both AD + ADFS disabled - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
      - ✅ invitations
      - ✅ sign-up
      - ✅ CSV import
    - AD enabled (ADFS does not matter) AND only AD users are present - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is AD integration which TDS invitations or signup functionality use to read username+email+FirstName+LastName (NOT password!)
      - ✅ invitations
      - ✅ sign-up
      - ✅ CSV import
    - AD enabled (ADFS does not matter) AND some non AD users are present - only CSV import is available due to security-related limitations to avoid usernames collision and similar
      - ❌ invitations
      - ❌ sign-up
      - ✅ CSV import

Authentication capabilities

- public cloud
  - common TDS
    - ✅ TDS
    - ❌ ~~ADFS~~
    - ❌ ~~AD~~
  - dedicated TDS
    - ✅ TDS
    - ✅ ADFS
    - ❌ ~~AD~~
- private cloud
  - dedicated TDS
    - ✅ TDS
    - ✅ ADFS
    - ✅ AD

Authorisation capabilities

These depend on agreed service delivery mode and on the capability of the application to provide non-system administrator permissions.

- TDS integrated services
  - AD groups NOT available - there is NO centralised authorisation or provisioning solution available
  - TDS project-oriented users and roles management using portal
    - Portal and application roles
    - Roles, Invitation, Add/Remove Users
- TDS standalone services (only Bitbucket, Confluence or Jira)
  - TDS provides infrastructure
  - TDS maintains application

        - No TDS integration in the application
        - Customer key users maintain application (when non-system administrator permissions are available)
        - TDS provides assistance with integrations to AD/ADFS or other platforms, so, for example, AD groups and users sync is possible as there is no interference with TDS
        - AD/ADFS integration possibilities and costs depend mainly on network setup:
            - Bitbucket, Confluence or Jira can reach AD directly
                - AD sync is available using built-in AD functionality
            - Bitbucket, Confluence or Jira cannot reach AD directly
                - Atlassian Crowd
                    - Requires on-premise server
                    - Requires firewall opening 443/tcp from internet to Atlassian Crowd server
                    - License costs involved - https://www.atlassian.com/software/crowd/pricing
                    - It provides sync users and groups from AD through Crowd into Bitbucket, Confluence or Jira
                    - TDS SSO cannot be used
                - Script workaround
                    - Requires on-premise server
                    - Needs to be maintained for new versions
                    - Slow - it is just script, has quite significant overhead for various API calls
                    - Requires continuous updates manual CSV/EXCEL sheet mapping between projects, roles and AD groups intended for sync every time project or groups is created or removed
                        - total number of mappings is the number of projects X number of roles(constant 4) X number of AD groups necessary to be assigned to each project and role
                        - With example 10 projects and 5 AD groups it might be 10 x 4 x 5 = 200 mappings/lines
                - IDM used by some customers
                    - calling application APIs
                    - calling TDS APIs (expected to come at the beginning of Q3 2020)

- Intro
- Types of supported environments
    - From a network point of view
    - From AD/ADFS authentication integration point of view
    - From users origin point of view
    - From users origin combination point of view
- Provisioning capabilities
    - General provisioning capabilities
    - Provisioning capabilities flow diagrams
        - Invitations and sign-up flow
        - CSV import flow
    - Provisioning capabilities suitable for various types of environments
    - Authentication capabilities
    - Authorisation capabilities

Intro

TDS has multiple ways of users authentication, authorisation and provisioning. Possibilities depend on a combination of customer requirements and TDS capabilities.

Types of supported environments

From a network point of view

- public cloud
    - common TDS
    - dedicated TDS
- private cloud
    - dedicated TDS

From AD/ADFS authentication integration point of view

- AD/ADFS disabled
  - everyone has TDS account and is authenticated only using TDS LDAP credentials
- AD/ADFS enabled
  - everyone has TDS account and can be authenticated using TDS LDAP credentials
  - everyone has TDS account and can be authenticated using company AD/ADFS credentials

From users origin point of view

Two users categories are distinguished:

- AD users - users with AD account (usually employees, but very often also subcontractors)
  - can use AD or/and ADFS if enabled
  - can use TDS LDAP credentials
- non AD users - users without AD account (usually subcontractors)
  - cannot use AD nor ADFS
  - must use TDS LDAP credentials

From users origin combination point of view

When both AD users and non AD users are present in TDS, we are talking about a hybrid environment:

- standard TDS
  - either AD/ADFS is enabled AND all users are AD users
  - or AD/ADFS is disabled (TDS does not care whether users have or do not have AD accounts as there is no integration)
- hybrid TDS
  - AD/ADFS is enabled AND some non AD users are present

Provisioning capabilities

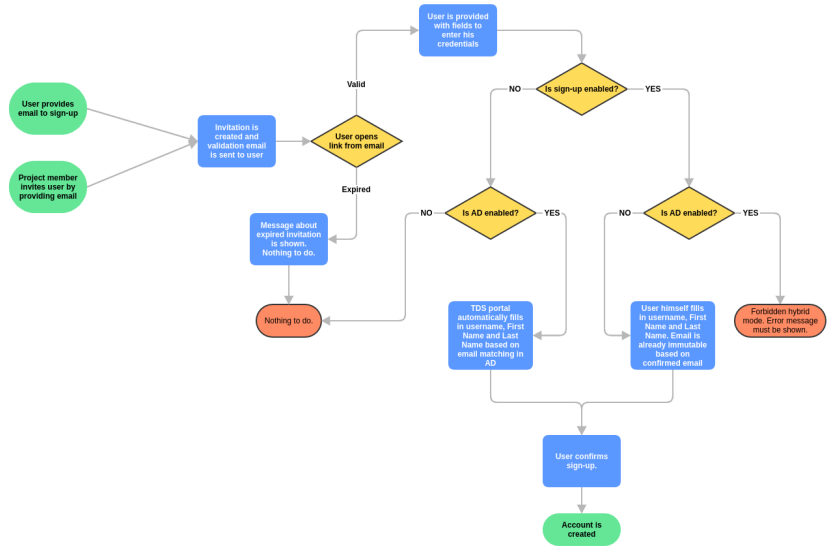
General provisioning capabilities

- invitations
  - colleagues or leaders can send invitations to people not present in platform, invited users must validate their email address, then they can enter their credentials or their credentials are read from AD if present
- sign-up
  - users can create accounts by themselves - first, they must validate their email address, then they can enter their credentials or their credentials are read from AD if present
  - recommended for
    - for a platform with AD users only without any externals (currently or in future)
    - for the platform without AD connection
  - it is NOT recommended
    - in hybrid environments when AD users and NON AD users should be working in the platform as users without AD account can create usernames as they wish and that can lead to conflict with current or potential future AD users leading to security issue
- CSV import
  - currently, requests must be raised via standard support channels as this functionality is available for TDS support ONLY (we are working on the possibility to provide this to customer area admins and owners)
  - recommended for
    - hybrid environments when AD users and NON AD users should be working in the platform - it gives customer key users (customer area admins/owners) full control over users that are joining the platform

Provisioning capabilities flow diagrams

Invitations and sign-up flow

Invitation/sign-up flow



CSV import flow

Steps:

- Customer key users send a ticket to TDS support in CSV format

```
username,email,FirstName,LastName
```

- TDS support team imports users to the portal
- Customer end-users with eligible project admin/owner permissions can manage users accesses via TDS portal. Key users that have area admins /owners roles can manage every project in the area.

Provisioning capabilities suitable for various types of environments

- public cloud
  - common TDS - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
    - ✅ invitations
    - ✅ sign-up
    - ✅ CSV import
  - dedicated TDS
    - ADFS disabled - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
      - ✅ invitations
      - ✅ sign-up
      - ✅ CSV import
    - ADFS enabled - only CSV import is available due to security-related limitations to avoid usernames collision and similar. It does not matter whether users have or do not have AD account, in the public cloud we would not be able to control users that are invited or signed-up, thus we would not be able to prevent security issues caused by potential users accounts collisions
      - ❌ invitations
      - ❌ sign-up
      - ✅ CSV import
- private cloud
  - dedicated TDS
    - both AD + ADFS disabled - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is no ADFS nor AD integration. That means freedom in usernames, thus no security-related limitations are present (to avoid usernames collision and similar)
      - ✅ invitations
      - ✅ sign-up
      - ✅ CSV import
    - AD enabled (ADFS does not matter) AND only AD users are present - all provisioning options are available - invitations + signup + CSV import. This is thanks to the fact that there is AD integration which TDS invitations or signup functionality use to read username+email+FirstName+LastName (NOT password!)
      - ✅ invitations
      - ✅ sign-up

        - ✅ CSV import
    - AD enabled (ADFS does not matter) AND some non AD users are present - only CSV import is available due to security-related limitations to avoid usernames collision and similar
        - ❌ invitations
        - ❌ sign-up
        - ✅ CSV import

Authentication capabilities

- public cloud
    - common TDS
        - ✅ TDS
        - ❌ ~~ADFS~~
        - ❌ ~~AD~~
    - dedicated TDS
        - ✅ TDS
        - ✅ ADFS
        - ❌ ~~AD~~
- private cloud
    - dedicated TDS
        - ✅ TDS
        - ✅ ADFS
        - ✅ AD

Authorisation capabilities

These depend on agreed service delivery mode and on the capability of the application to provide non-system administrator permissions.

- TDS integrated services
    - AD groups NOT available - there is NO centralised authorisation or provisioning solution available
    - TDS project-oriented users and roles management using portal
        - Portal and application roles
        - Roles, Invitation, Add/Remove Users
- TDS standalone services (only Bitbucket, Confluence or Jira)
    - TDS provides infrastructure
    - TDS maintains application
    - No TDS integration in the application
    - Customer key users maintain application (when non-system administrator permissions are available)
    - TDS provides assistance with integrations to AD/ADFS or other platforms, so, for example, AD groups and users sync is possible as there is no interference with TDS
    - AD/ADFS integration possibilities and costs depend mainly on network setup:
        - Bitbucket, Confluence or Jira can reach AD directly
            - AD sync is available using built-in AD functionality
        - Bitbucket, Confluence or Jira cannot reach AD directly
            - Atlassian Crowd
                - Requires on-premise server
                - Requires firewall opening 443/tcp from internet to Atlassian Crowd server
                - License costs involved - https://www.atlassian.com/software/crowd/pricing
                - It provides sync users and groups from AD through Crowd into Bitbucket, Confluence or Jira
                - TDS SSO cannot be used
            - Script workaround
                - Requires on-premise server
                - Needs to be maintained for new versions
                - Slow - it is just script, has quite significant overhead for various API calls
                - Requires continuous updates manual CSV/EXCEL sheet mapping between projects, roles and AD groups intended for sync every time project or groups is created or removed
                    - total number of mappings is the number of projects X number of roles(constant 4) X number of AD groups necessary to be assigned to each project and role
                    - With example 10 projects and 5 AD groups it might be 10 x 4 x 5 = 200 mappings/lines
            - IDM used by some customers
                - calling application APIs
                - calling TDS APIs (expected to come in the beginning of Q3 2020)