

## Set up MFA with SafeNet Trusted Access from Thales

Last Modified on 04.17.26

To set up the Multi-Factor Authentication (MFA) with SafeNet Trusted Access you need to configure Microsoft Active Directory or Microsoft Entra ID (Azure AD) in Application Workspace and Thales. Application Workspace and Thales need to be connected through the same identity environment to work.

### Create an application in STA Access Management

1. In the STA Access Management console, select the **Applications** tab.
2. Click the **Add Application** or **+** button.
3. Select the *Generic Template*.

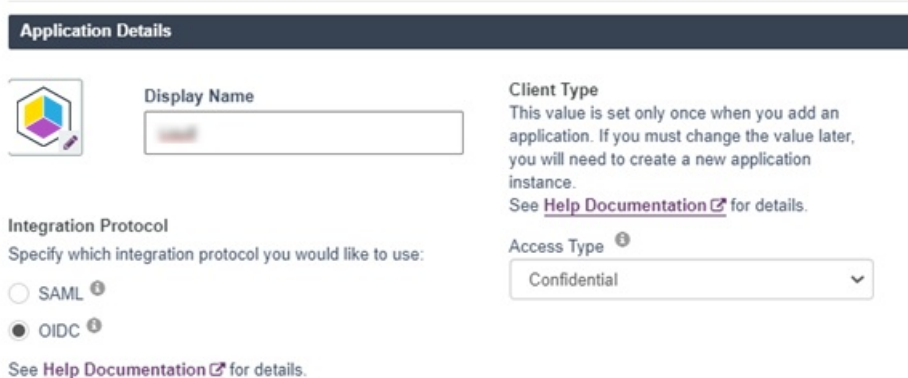
#### Add Application

Select an application to add



4. In the **Application Details** screen that opens, configure the following:
  - In the **Display Name** field add a name.
  - In the **Integration Protocol** section select *OIDC*.
  - For **Access Type** select *Confidential*.

#### Add Application



5. Click **Add** in the bottom right. The application details panel opens with the **Configure** tab displayed.
  - In **Step 01: Generic Template Setup** click **Next Step**.
  - In **Step 2: STA Setup** configure the following:

**ALLOWED FLOW TYPE** *Authorization code flow and implicit flow*

**SERVICE LOGIN URL** `https://workspace.recastsoftware.com`

**VALID REDIRECT URL** `https://workspace.recastsoftware.com/api/auth/token/end`

# Recast

USERINFO SIGNATURE ALGORITHM *RSA-SHA256*

REQUEST SIGNATURE ALGORITHM *RSA-SHA256*

In the **User Identity Claims** section, in the **Name** field insert an email (note that it is case sensitive) and in the **Value** field select *UPN*

## STA Setup

See [Help Documentation](#) for details.

ALLOWED FLOW TYPE

Authorization code flow and Implicit flow

SERVICE LOGIN URL

http://localhost:3000

VALID REDIRECT URL

http://localhost:3000/callback

USERINFO SIGNATURE ALGORITHM

RSA-SHA256

REQUEST SIGNATURE ALGORITHM

RSA-SHA256

## User Identity Claims

	NAME	VALUE	ADDITIONAL INFORMATION
	upn	UPN	

[Add Claim](#)

7. Click **Save Configuration**.



For more information about configuring a custom OIDC application, see [STA documentation](#).

## Create a policy in STA Access Management to grant users access to the application

1. In the STA Access Management console, select the **Policies** tab and then click the + (Add policy) icon.
2. In the **Create Policy** window displayed, configure the following:
  - In the **New Policy** field, enter a name for the new policy.
  - In the **New Policy Description** field, enter a description for the new policy.
  - Under the **Scope** section:
    - for **Users** select **All Users**.
    - for **Applications** select **Any of these Applications** and then enter the application you just created.
  - Under the **Decision** section:
    - for **Access attempts are** select **Granted**.
    - for **Authentication methods** select **Password, Once per session, Allow Integrated Windows Authentication (Kerberos), OTP, Every access attempt**.

3. Click **Save** to save your changes.

You are done configuring SafeNet Trusted Access.

For more information about adding a policy, see [STA documentation](#).

## Application Workspace

1. In Application Workspace, navigate to the relevant identity source that needs to utilize MFA for authenticating.
2. Open it and go to the **Authentication** screen.
3. Enable the *Federated* option and click **Edit**.
4. In the **Edit authentication dialog** box that opens configure the following:

Liquit Name	STA Value*	Default Value
Protocol		OAuth 2.0
Client ID	Client ID	
Client secret	Client Secret	
Redirect URI		https://workspace.recastsoftware.com/api/auth/token/end
Token URI	Token end-point URL	
Authorization URI	Authorization end-point URL	
Logout URI	Logout end-point URL	
Claim attribute		upn

\* These values are provided from the application in the STA management console.

For more information about SafeNet Trusted Access, see [SafeNet Trusted Access documentation](#) or [Thales Customer](#)

# Recast

Support Portal.

---