**Enterprise Policy Management Website/UI**

The system admin should first set the authenticators allowed for different grades and then set the authenticator/(s) to be used from the allowed list for each app provided by the organization.

1. ***Home Page***

Cancel

Login

Password

Username

The first page of Enterprise Management Policy website/Tool.

The sysadmin/normal employee will login here. If a system

admin logs in, he will be taken to a new page wherein he will be

presented with a menu kind of page either to set authenticators

to be allowed for each grade or to set authenticators to be used

for each app provided by the organization, out of the allowed list

of authenticators for each grades. The page is as described

below in section 1.1):

***1.1) Menu Page for System Admin***

[***Logout***](https://login.microsoftonline.com/login.srf?client-request-id=e8b25e91-184f-444e-9771-312398e323fe)

Hello <System Admin Name>!

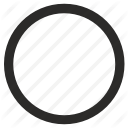
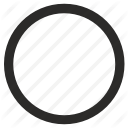
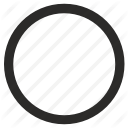
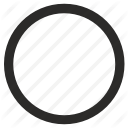
\*\*\*\*\*\*\* Maybe Show some details of his like his designation, grade, employee id and stuff. All this will be static data \*\*\*\*\*\*\*\*

**Allow Authenticators for different apps for each employee grades**

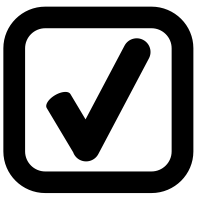
**Set Authenticators for employee grades**

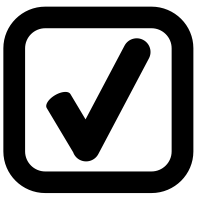
The above page will have two buttons. When the system admin clicks on button “**Set Authenticators for employee grades**”, he will be taken to a new page which will allow him to set different authenticators for each employee grade. The page will be as shown below in section 1.1 a)

***1.1 a) Add Authenticators allowed for employee grades Page***

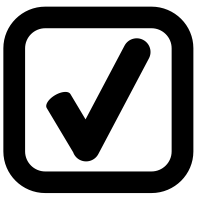
Grades: 3.x  5.x  7.x  9.x  13.x 

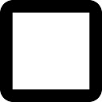
Authenticators allowed:

 No Authentication

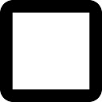
 Pin-code

Fingerprint verification

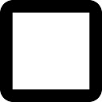


 Face recognition

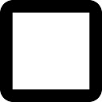
Voice recognition



Eye/Retina verification



Heartbeat verification



**BACK**

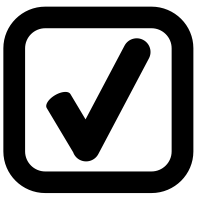
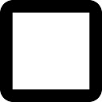
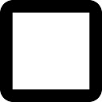
**SUBMIT**

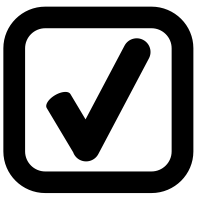
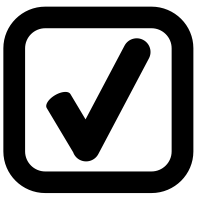
The above page will allow system admin to set authenticators to be allowed for different set of grades of employees. For example, system admin may decide to allow ***pin code*** and ***fingerprint*** authenticators only for ***3.x employees*** and he may allow ***pin code, fingerprint*** and ***face/voice recognition*** authenticators for ***5.x employees***, and so on). Every time the system admin selects a grade and list of authenticators for that grade and then clicks on Submit button, the data gets stored in a DB table called “**gradePolicies**”. [*Please refer Database document to know more about this table*]. The Back button will take the admin to the previous menu page.

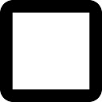
Next, if the system admin clicks on button “**Allow Authenticators for different apps for each employee grades**” from the menu page, he will be taken to a new page which will allow him to set which authenticators each grade of employees will use for each app the organization provides, out of the allowed authenticator list for each grade. The page will be as shown below in section 1.1 b):

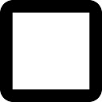
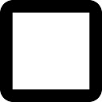
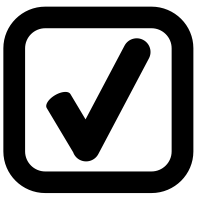
***1.1 b) Allow Authenticators for different apps for each employee grades Page (Example of 3.x employee is shown below)***

Employee Grade: Cafeteria Menu App Attendance App Salary App

 No Authentication  No Authentication  No Authentication

Pin - code  Pin - code  Pin - code



 Fingerprint  Fingerprint  Fingerprint

3. X

5. X

7. X

9. X

13. X

**Go Back**

**Add Policy**

The above page allows the system admin to select which all authenticators each employee grade can use for each app provided by the organization. The list of authenticators that is shown for each grade will be only those authenticators that were set by the system admin in section 1.1a). So if a new authenticator is to be shown in the above page, the same has to be set first by the system admin for that employee grade as described in the section 1.1a). Whenever the system admin selects the authenticators allowed to be used for each app and clicks on “Add Policy” button, the details will be stored in another DB table called “**appPolicies**” [*Please refer Database document to know more about this table*]. The “Go Back” button will take the system admin back to the menu page.

This way the system admin can log into this website anytime and edit the authenticators for each employee grade and also edit the list of allowed authenticators to be used for all apps provided by the org. Finally on the menu page, the user will have a link called as “Logout”, which will log him out of this policy maker website.

Now back to the home page, if a normal employee logs into the website with his credentials, he will be taken to the below page which will show him below details as shown in section 1.2)

***1.2) Policies for user.***

[***Logout***](https://login.microsoftonline.com/login.srf?client-request-id=e8b25e91-184f-444e-9771-312398e323fe)

Hello <User name>!

\*\*\*\*\*\*\* Maybe Show some details of his like his designation, grade, employee id and stuff. All this will be static data \*\*\*\*\*\*\*\*

Authenticators allowed for your grade:

**1)** **No Authentication**

**2) Pin – Code Authenticator**

***Details:***

AAID: 4746#F816

Vendor ID: null,

Key IDs: null,

User Verification: 0,

Key Protection: 0,

Matcher Protection: 0,

Attachment Hint: 0,

Tc Display: 0,

Authentication Algorithms: null,

Assertion Schemes: null,

Attestation Types: null,

Authenticator Version: 0,

Extensions: null

Apps allowed to use this authenticator: Cafeteria Menu

**3) Fingerprint Authenticator**

***Details:***

AAID: 53EC#3801

Vendor ID: null,

Key IDs: null,

User Verification: 0,

Key Protection: 0,

Matcher Protection: 0,

Attachment Hint: 0,

Tc Display: 0,

Authentication Algorithms: null,

Assertion Schemes: null,

Attestation Types: null,

Authenticator Version: 0,

Extensions: null

Apps allowed to use this authenticator: Attendance App, Salary App

The above details will show the authenticators allowed for the employee grade along with the apps that are currently allowed to use any of those. We can decide on which of the above fields to show to the end user on UI (The fields that the user will understand. Not all above fields are required to be shown, I feel). The employee can view this details anytime by logging into this website, but he will not be allowed to edit any policies here. The system admin is the only person who is allowed to do that. Once the employee sees these details he can logout from the website by clicking on the “**Logout**” ink at the top right corner of the page, which will bring him back to home page with login option.