credenti
A Tecnics Company

Tecnics Tap and Go Authentication

TecTANGO for CyberArk Identity Users

v6.0.0

May 2024

Table of Contents

What is TecTANGO?

TecTANGO is a Windows credential provider that allows users to login to their desktop without passwords. Users can authenticate into their own or shared devices by simply tapping their smart card or proximity card on a reader. Additionally, PIN and Security Question can be added as additional security factors.

Supported Scenarios

TecTANGO supports an online and offline mode, with both being in a Standard and Kiosk mode. Tap In, Tap Out, and Tap Over are supported in these scenarios.

- Standard Mode:
    - Tap In - the user taps their card to the reader to enter into their personal session on the workstation
    - Tap Out - the user taps their card to the reader to leave their session on the workstation
    - Tap Over - if multiple users are logged into the same workstation they will be able to tap their card and be switched over to their respective session
- Kiosk Mode:
    - Tap In - the user taps their card to the reader to enter into a generic user's session on the workstation
    - Tap Out - the user taps their card to the reader to leave the generic user's session on the workstation
    - Optional Profile Selection feature - allows the user to choose whether they sign in under their own profile or the generic user profile on the TecTANGO login prompt

Supported Card Readers

- HID Omnikey - 5025
- HID Omnikey - 5427 CK
- HID Omnikey - 5422
- RFIDeas RDR 6082AKU- C16
- RFIDeas RDR 60D2- AKU - Keyboard
- RFIDeas RDR - 80081 AKU
- RFIDeas RDR 80581 AKU
- RFIDeas RDR - 80582 AKU
- RFIDeas RDR - 80532 BKU

Note: *A 60D2 reader and a 6082 reader will read the same card differently. This will pose an issue for the end user, as 60D2 on one workstation and 6082 on another workstation would authenticate the user on one workstation while asking for an enrollment on another workstation. Therefore, using only one type of reader in the organization is highly recommended. This also applies for HID Omnikey readers to RFID readers.*

Online Scenario

In an online scenario, the user's workstation or laptop is connected to the internet and can reach the CyberArk Identity cloud. The user should have their smart card/proximity card/security key with them. Security can be further enhanced by optionally adding Password, PIN, or Security Question as an additional factor.

Offline Scenario

In an Offline scenario, the user's workstation or laptop is not connected to the internet, or it is in airplane mode. In order to login to the workstation with TecTANGO while offline, the user must at least login once in online mode. Any additional MFA configured will work in offline mode as well.

Note: Card enrollment will not work in offline mode.

Prerequisites

- Windows 10/11 workstations with .NET Framework 4.7.2+. In order to use "Privacy Shield" feature, the .NET framework must be upgraded to 6.0.0+
- RFID badge or proximity card used for building access
- RFID reader connected to the workstation (various readers from HID and rfIDEAS are supported)
- If branding is desired:
    - Company logo in .bmp format and not more than 192px by 192x
    - Company logo in .bmp format and not more than 304px by 186px
- CyberArk Identity Tenant with active users
- If Kiosk Mode is desired:
    - A generic user with a generic password that can be shared is needed
    - This user does not need to be in CyberArk Identity
- Admin Access to CyberArk Identity Tenant to create OIDC app

Deployment Steps

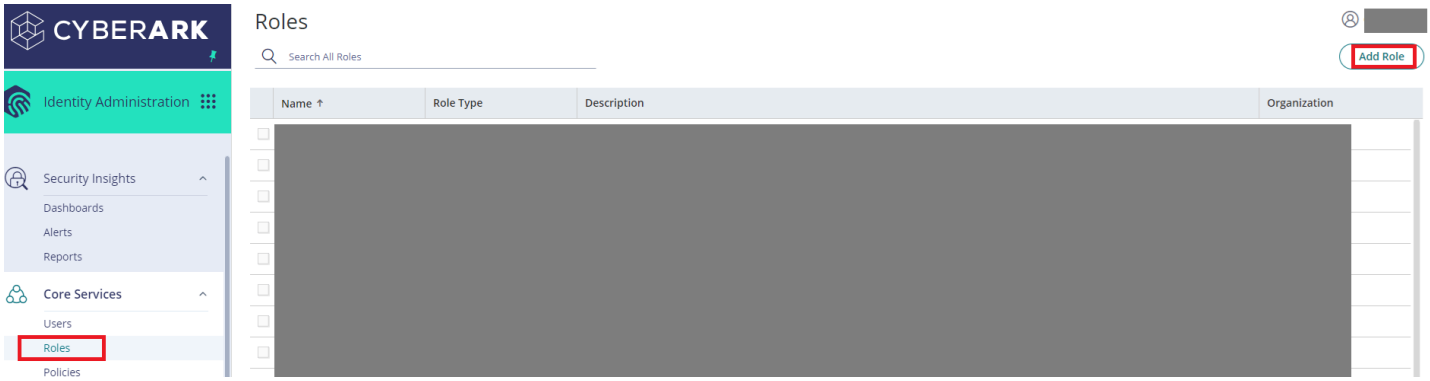
Deployment of TecTANGO involves the below steps:

1. CyberArk Identity Configuration
    a. Create a Role
    b. Create the OIDC Application
2. Credenti Portal Configuration
    a. Installer Configuration
    b. Set up Kiosk User (if applicable)
    c. Configure Mechanisms and Policies
    d. Add Domains
3. Workstation Configuration
    a. Install TecTANGO on the workstation

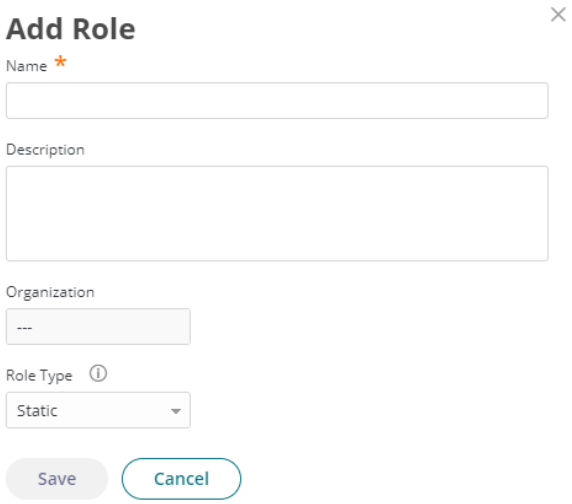
CyberArk Identity Configuration

Create Roles in CyberArk Identity Portal

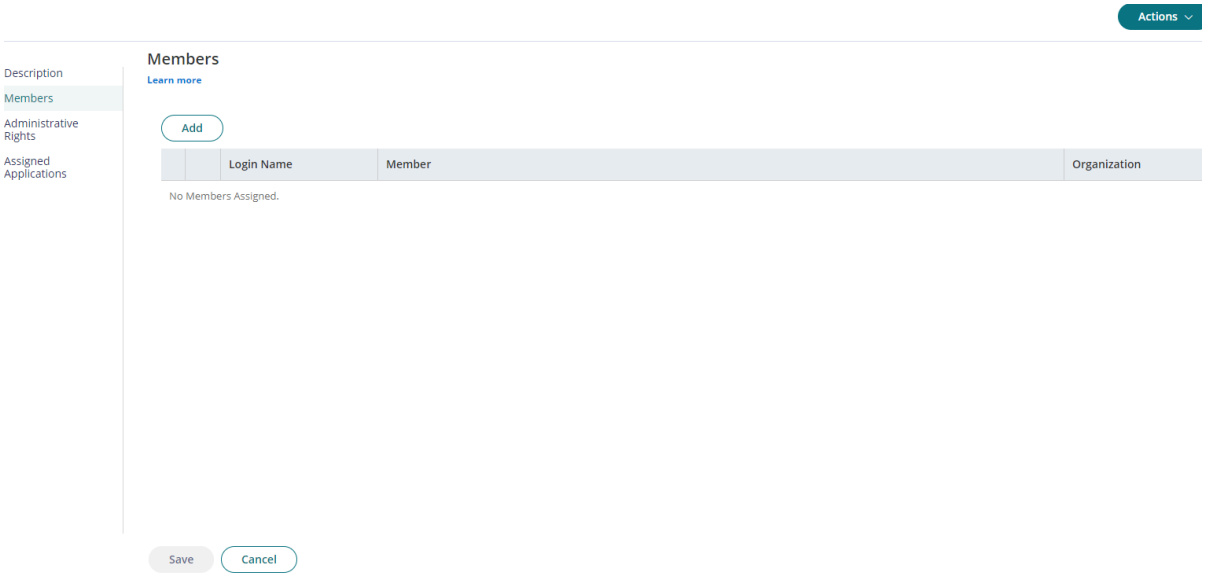
1. Login to CyberArk Identity Admin Portal, and go to “Roles”.



2. Click on “Add Role”, enter Name, and click on Save.



3. Go to “Members”, add members to the Role, and click on Save.



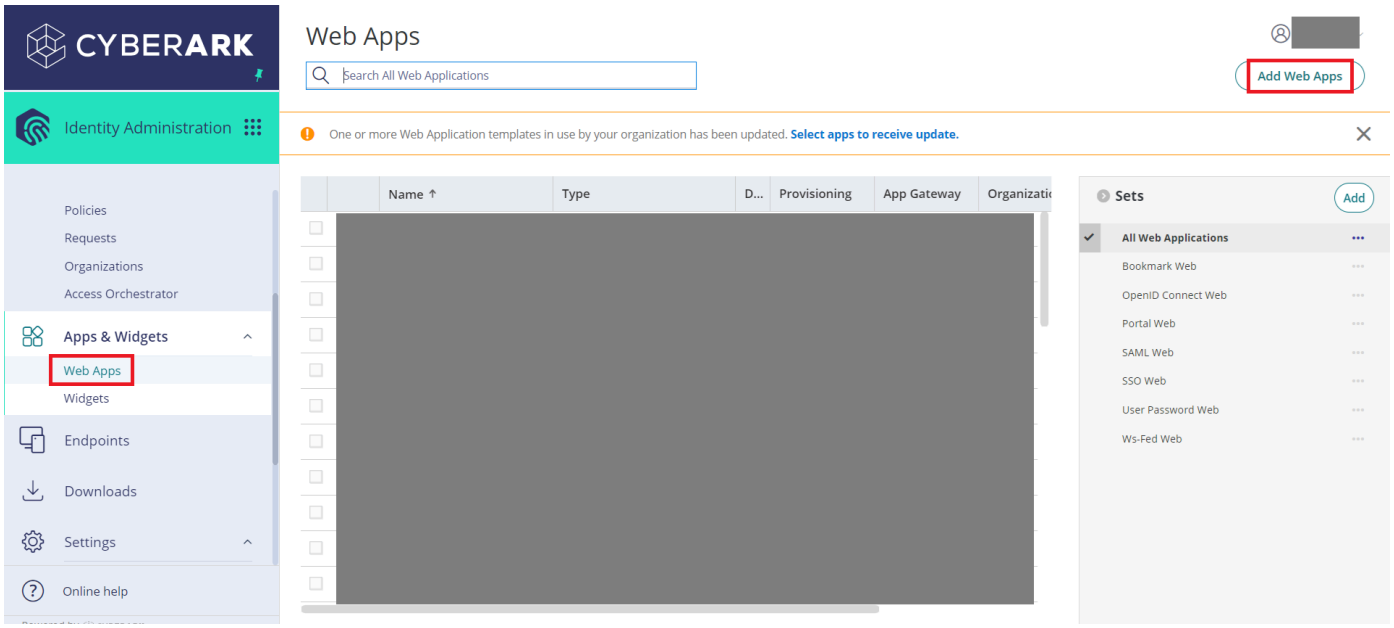
CyberArk Identity OIDC App Configuration

When creating the OIDC application, please note the following details, as they are needed by the Tecnics team to configure your organization's Credenti Admin Portal:

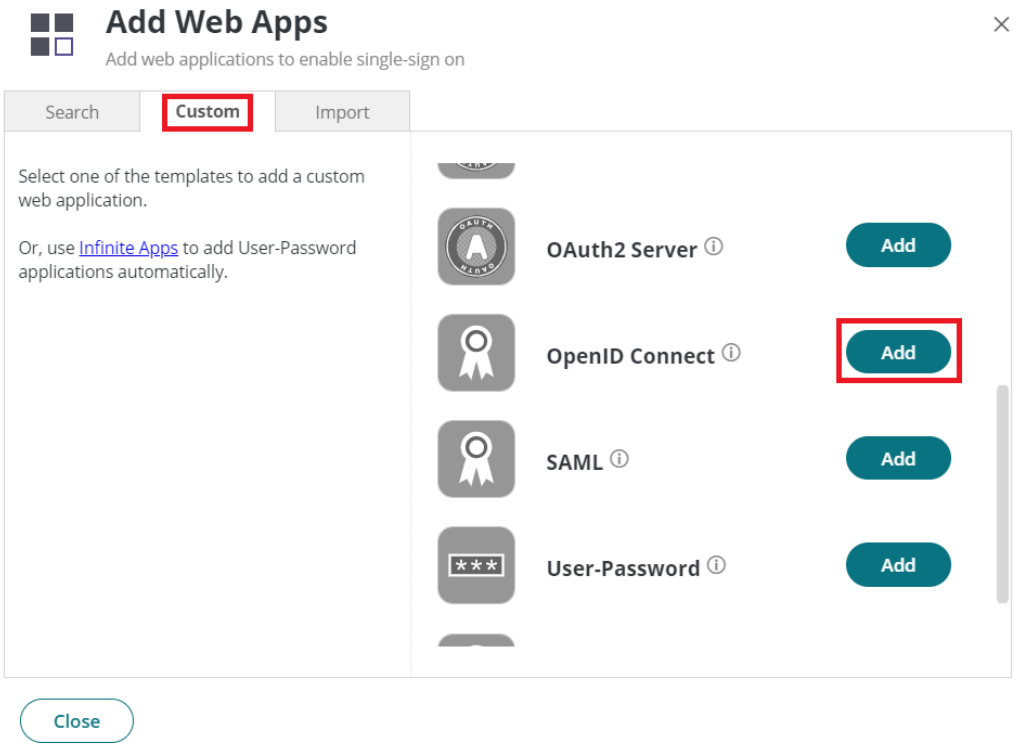
- Client ID
- OpenID Connect Issuer URL

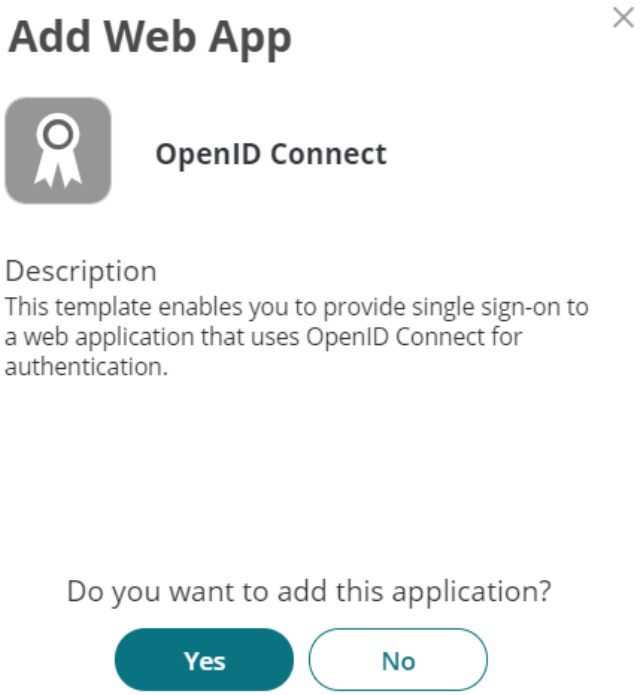
Application Setup in CyberArk Identity:

1. Login as an administrator to CyberArk Identity. Then navigate to Apps & Widgets → Web Apps.
2. Click on “Add Web Apps”.

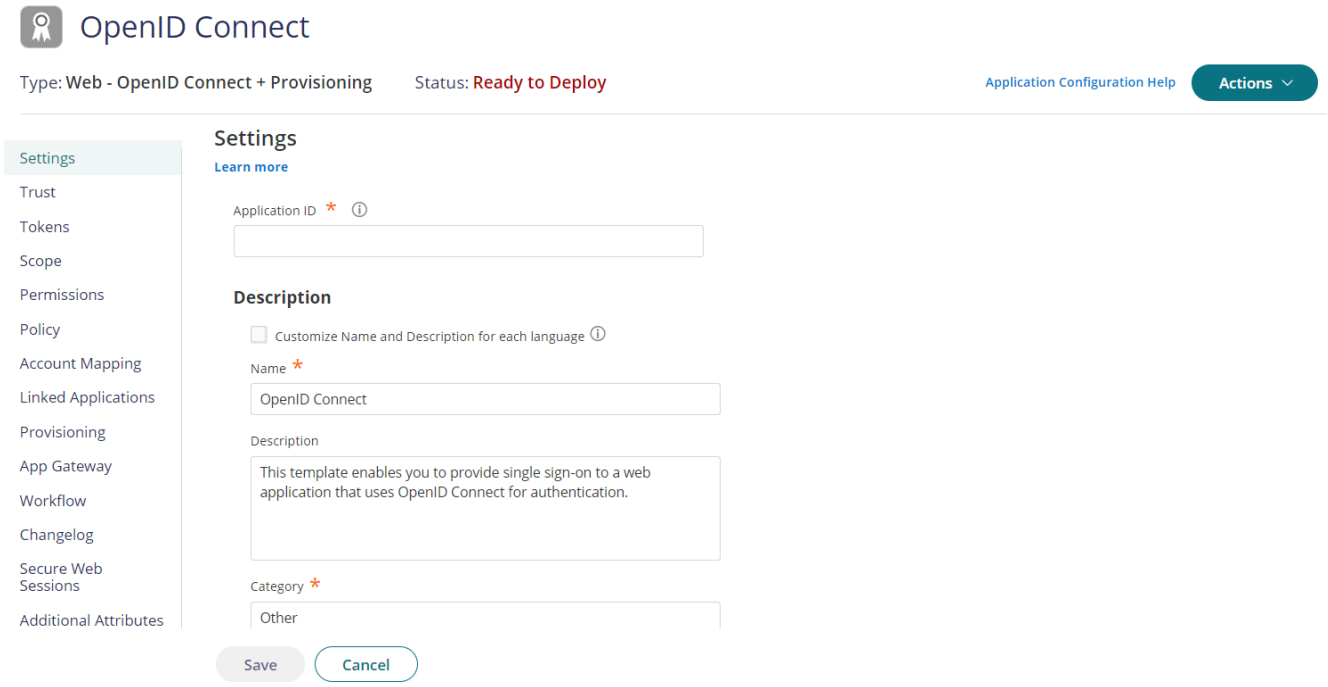


3. Click on “Custom”, and add on OpenID Connect.



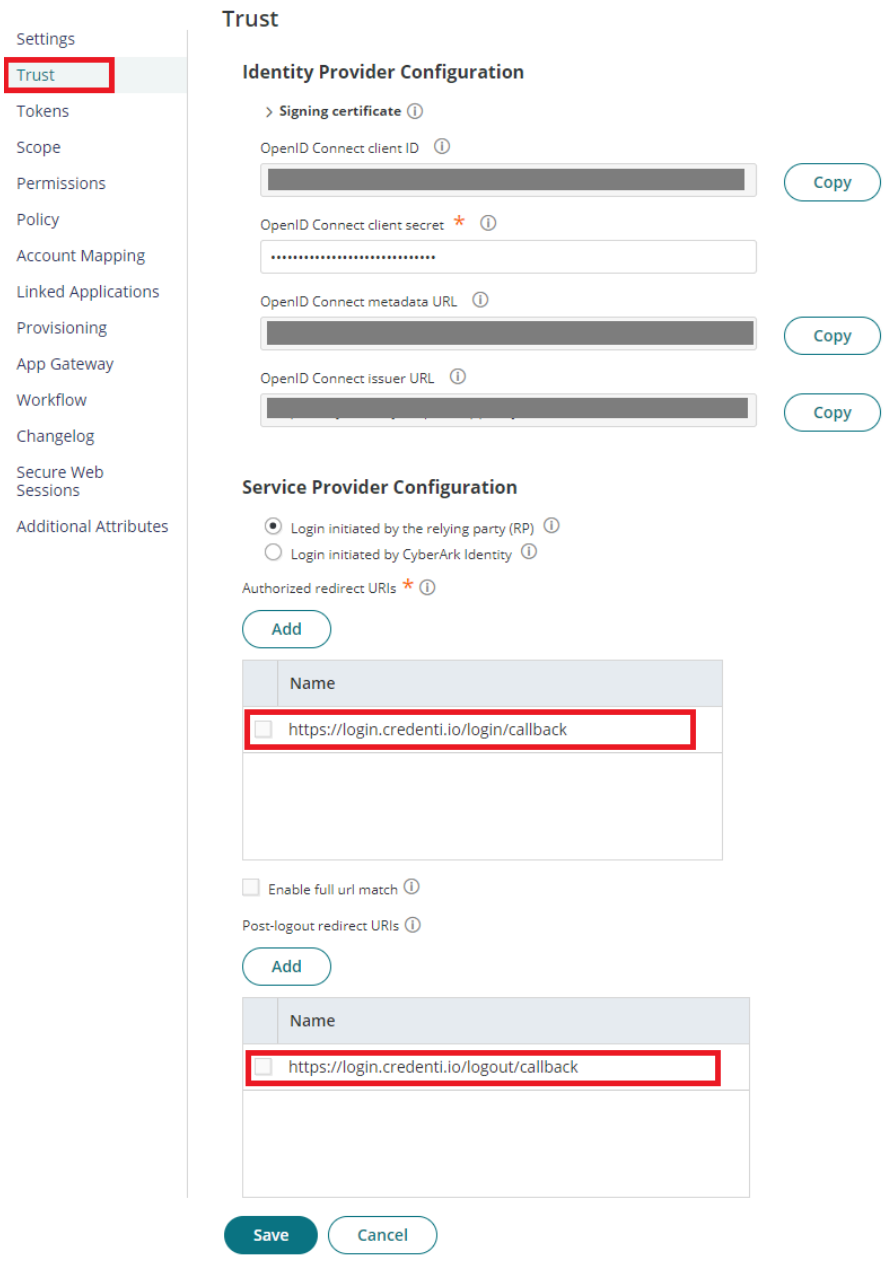


4. Add Below, and click on Save.
    a. Application ID: TecConnect or Credenti
    b. Name: TecConnect or Credenti
    c. Description

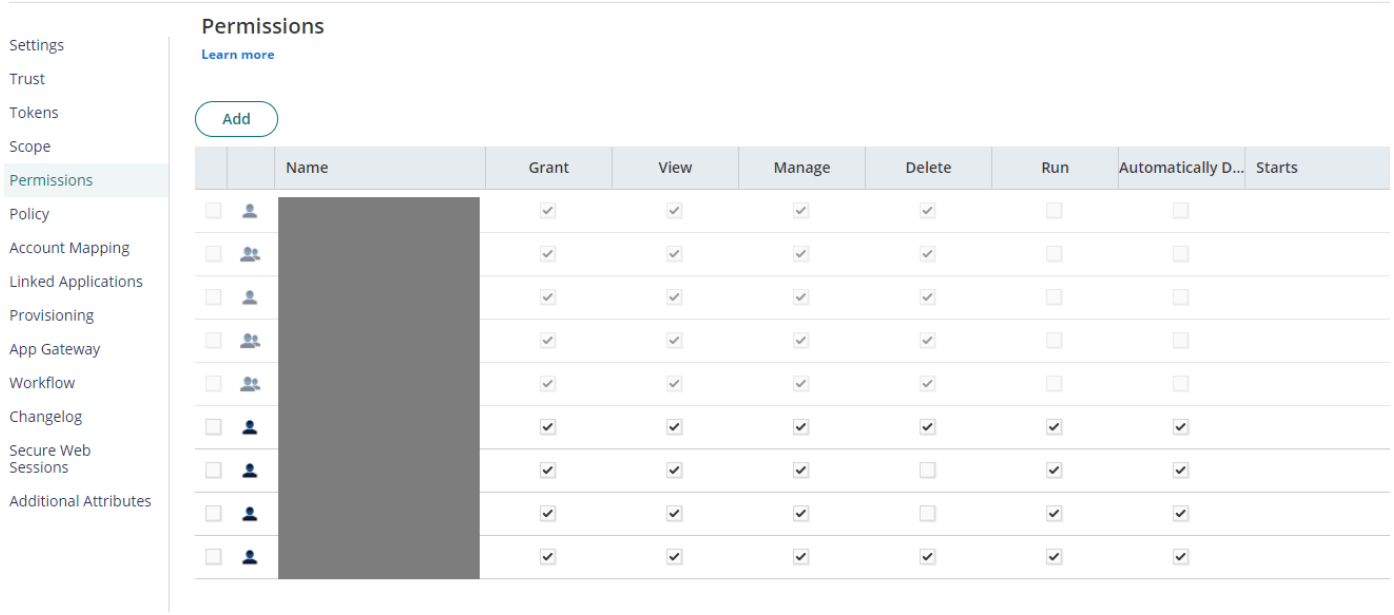


5. Go to “Trust”, add below, and click on Save.
    a. Client Secret
    b. Service Provider Configuration: Login initiated by the relying party (RP)
    c. Authorized Redirect URI: https://login.credenti.io/login/callback
    d. Post-logout Redirect URI: https://login.credenti.io/logout/callback

Note: Please share Client ID and OpenID Connect Issuer URL with Tecnics team.

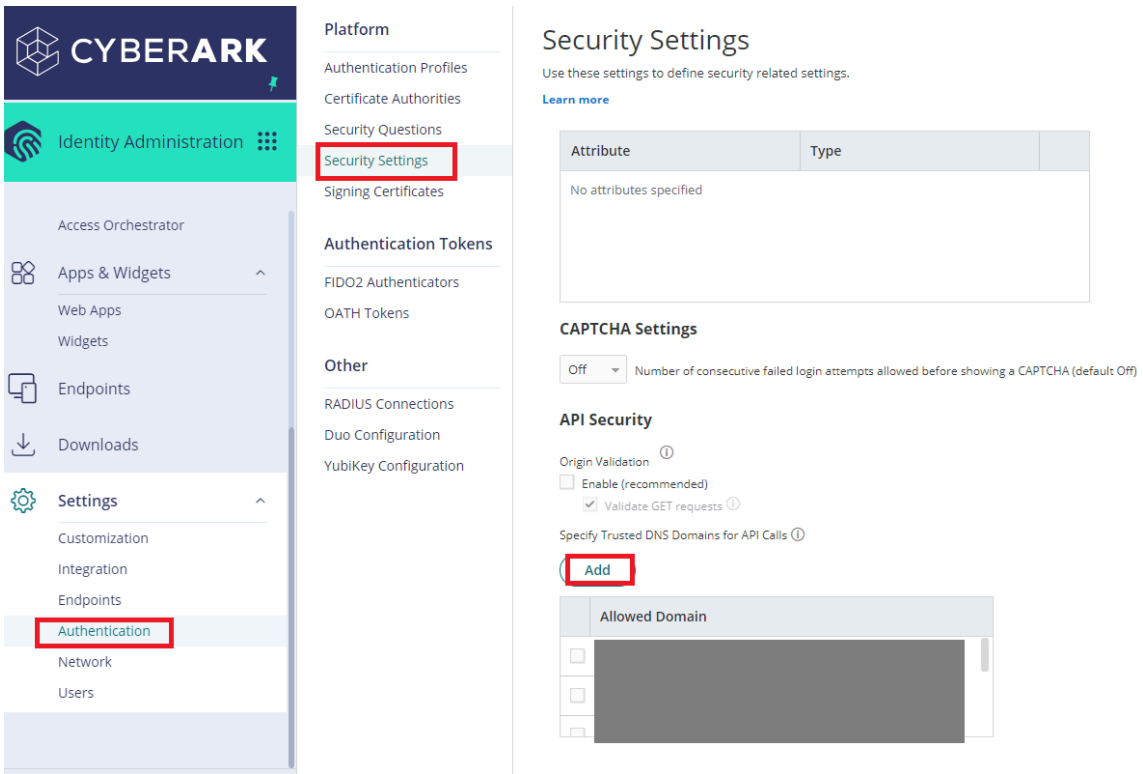


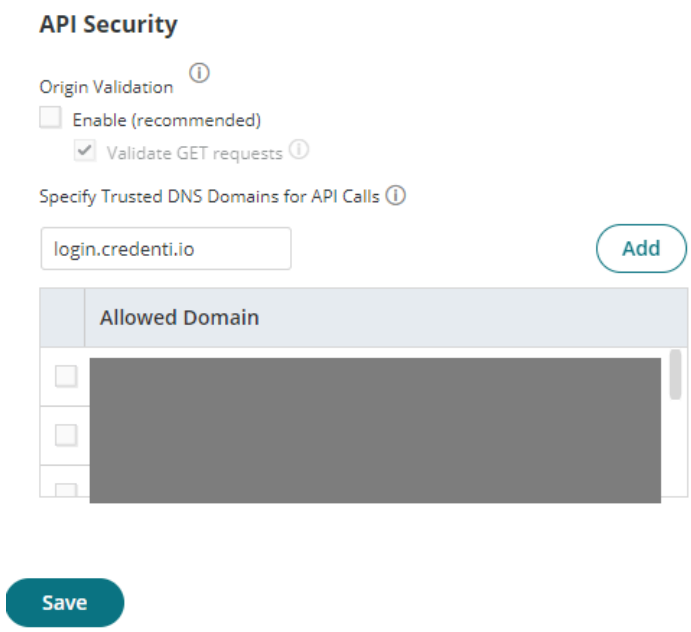
6. Go to the “Permissions” tab, click on “Add”, assign either users or roles that will be using the application, and give the below permissions.
    a. Grant
    b. View
    c. Manage
    d. Run
    e. Automatically Deploy



Add CORS:

To add CORS, go to Settings → Authentication → Security Settings. Under API Security, click on "Add", enter *login.credenti.io*, click on "Add" and Save.





Credenti Portal Configuration

Installer Configuration

Note: This setting should be completed before the client installation otherwise the changes may not be applied on the desktop. Re-install of client is needed to reflect any changes made after the installation.

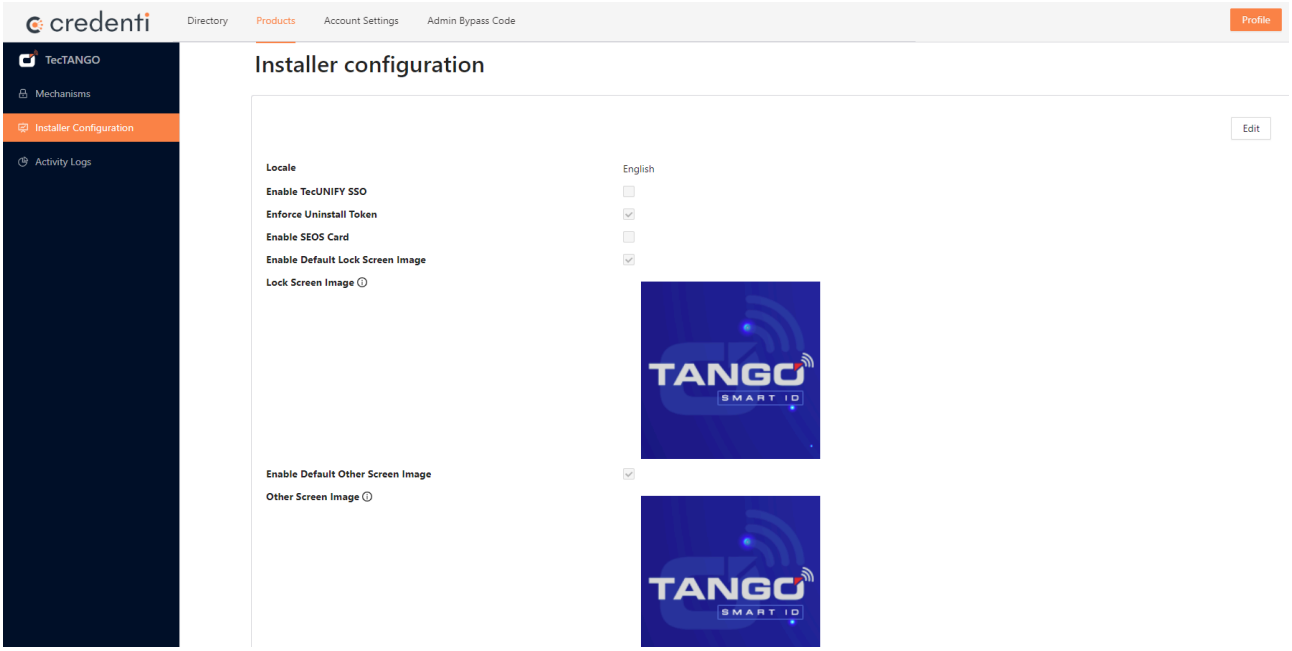
The following installation detail(s) can be configured in the Credenti Admin Portal:

- Language
- Enable TecUNIFY SSO
- Branding

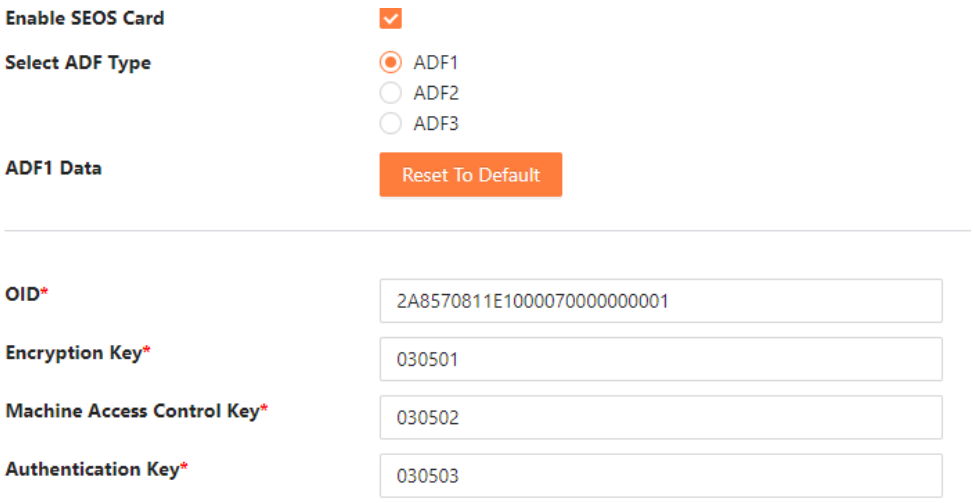
Steps:

1. Login as an admin into the Credenti Admin Portal. Credenti Portal uses CyberArk Identity credentials for login.
   Note: This user should be assigned to the CyberArk Identity OIDC application.

2. Navigate to Products → TecTANGO → Installer Configuration



3. In this section, the following details can be configured:
    a. Language:
        i. English
        ii. French
    b. Enable TecUNIFY SSO
        i. Allows for SSO with TecUNIFY
        ii. TecUNIFY must be installed on the machine prior to TecTANGO installation
    c. Enforce Uninstall Token
        i. When enabled, this requires the Uninstall Token in order to uninstall the application
    d. Enable SEOS Card
        i. Select ADF Type
        ii. OID
        iii. Encryption Key
        iv. Machine Access Control Key
        v. Authentication Key



e. Branding Images:
   i. Default Lock Screen Image:
      1. The image that is shown at the lock screen
      2. Images should be BMP format
      3. Maximum image size of 192px x 192px
   ii. Default Other Screen Image:
      1. The image that is shown when being prompted for challenge factors
      2. Images should be BMP format
      3. Maximum image size of 192px x 192px
   iii. Default IDP MFA Screen:
      1. The image that is shown if IDP MFA is selected in the mechanisms
      2. Image should be PNG format
      3. Recommended image size of 125px x 108px
   iv. Default Enroll Screen Image:
      1. The image that is shown on enrollment screen
      2. Images should be BMP format
      3. Maximum image size of 304px x 186px
   v. System Background Image:
      1. The image that is shown during the TAP OVER process
      2. Images should be BMP format
      3. Desktop Resolution Size

Installer configuration

Edit

Locale	English
Enable TecUNIFY SSO	☐
Enforce Uninstall Token	☑
Enable SEOS Card	☐
Enable Default Lock Screen Image	☑
Lock Screen Image ⓘ	
Enable Default Other Screen Image	☑
Other Screen Image ⓘ	

- Images should be BMP format
- Maximum image size of 192px x 192px

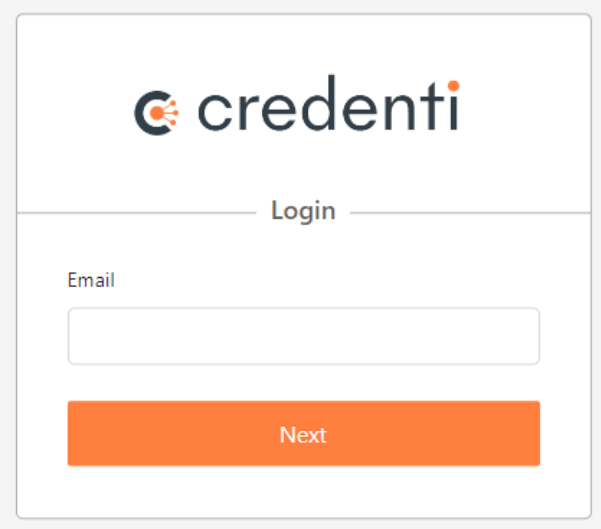
Kiosk User Configuration

TecTANGO can be setup in 2 modes:

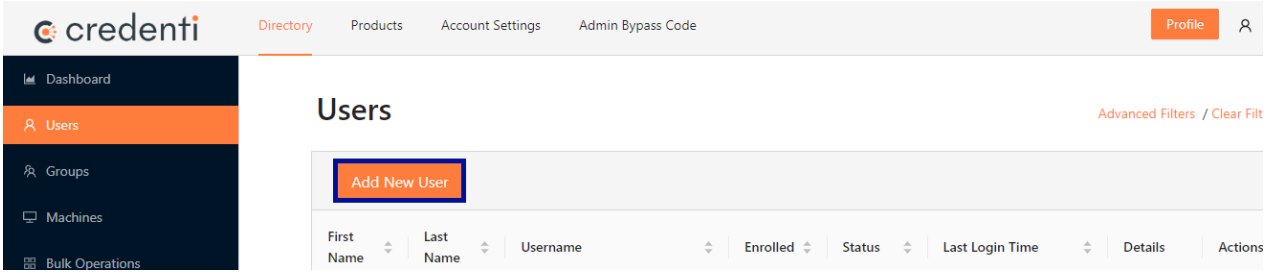
- Single User Mode: Each user logs into the workstation using their credentials
- Kiosk Mode – TecTANGO Managed: The user logging into the workstation is a generic user whose credentials are maintained by TecTANGO
    - Optional Profile Selection feature, which allows the user to choose whether they sign in under their own profile or the generic user profile on the TecTANGO login prompt

The following steps are needed if Kiosk Mode - TecTANGO Managed was chosen as the desired mode:

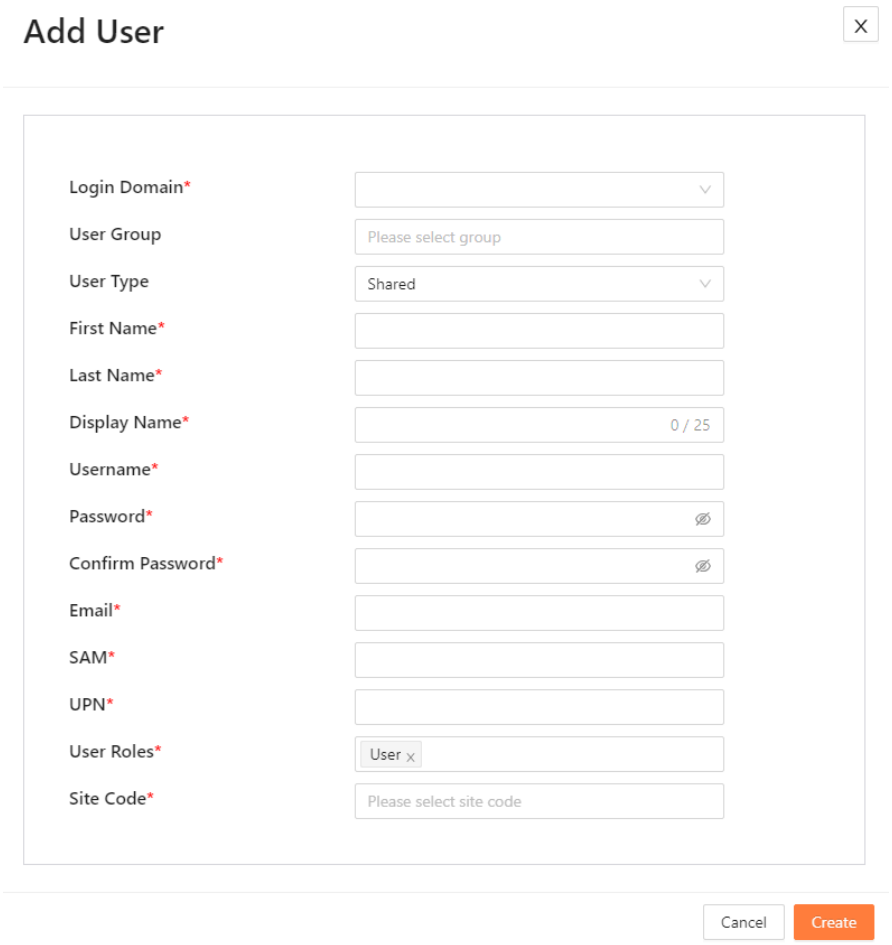
1. Once TecTANGO has been installed on the workstation, login to the Credenti Admin Portal.



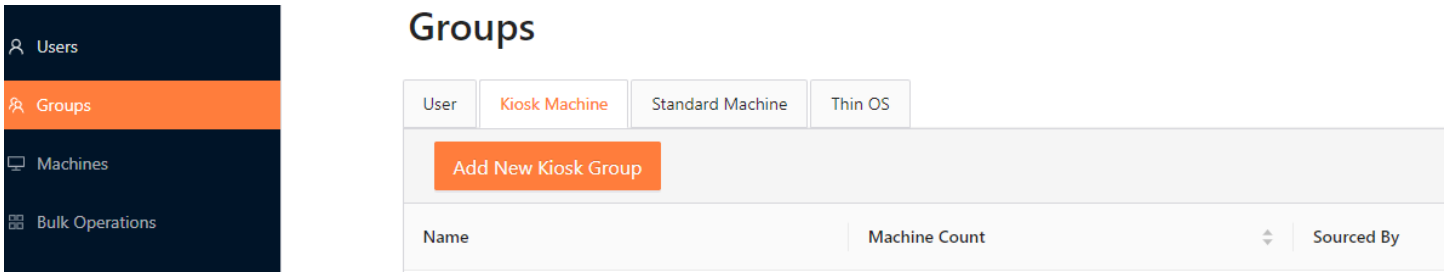
2. Navigate to the Users page, and click “Add New User”.



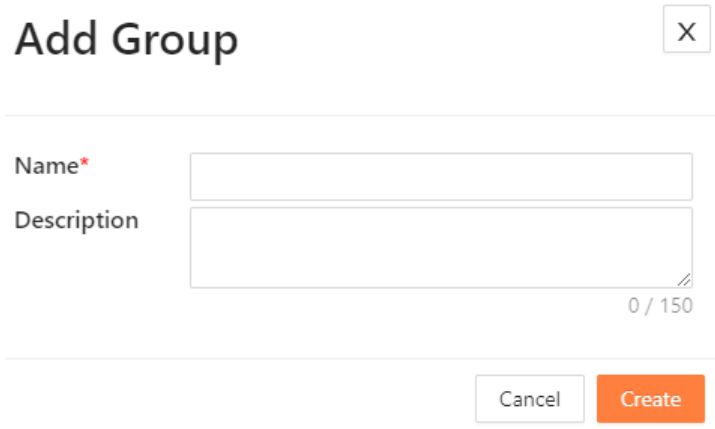
3. Set the user type as Shared. Then add the generic user’s information, including their generic shared password. The generic password should match the generic password on the machine. Click “Create”.



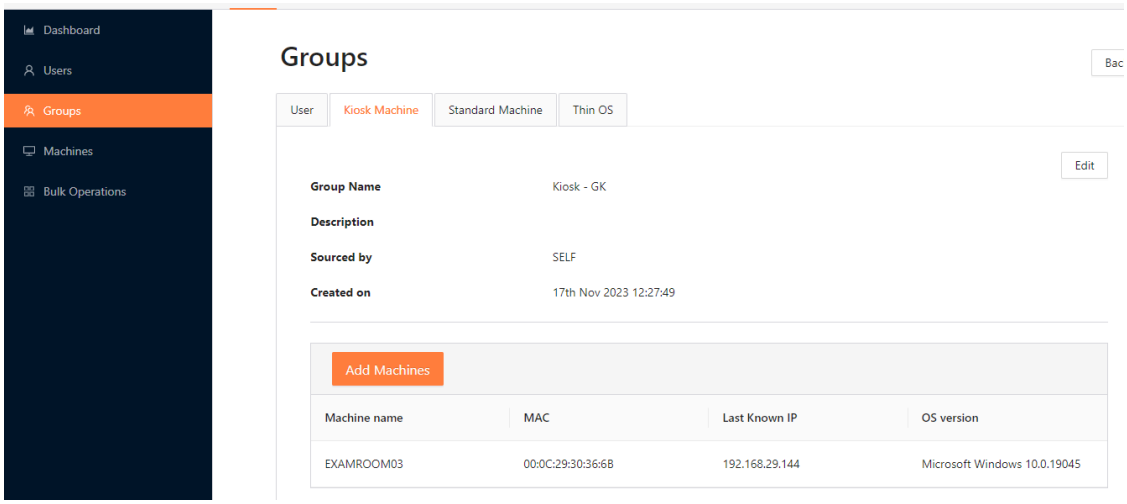
4. Navigate to the Groups page, and select the Kiosk Machine tab.



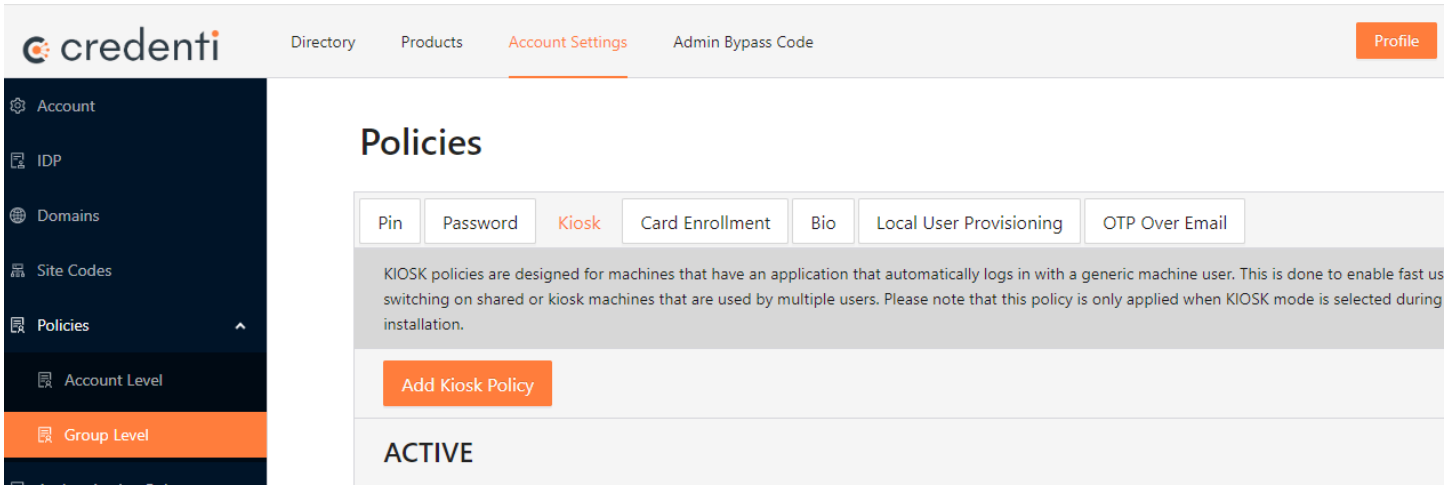
5. Click “Add New Kiosk Group”, and create a new group.



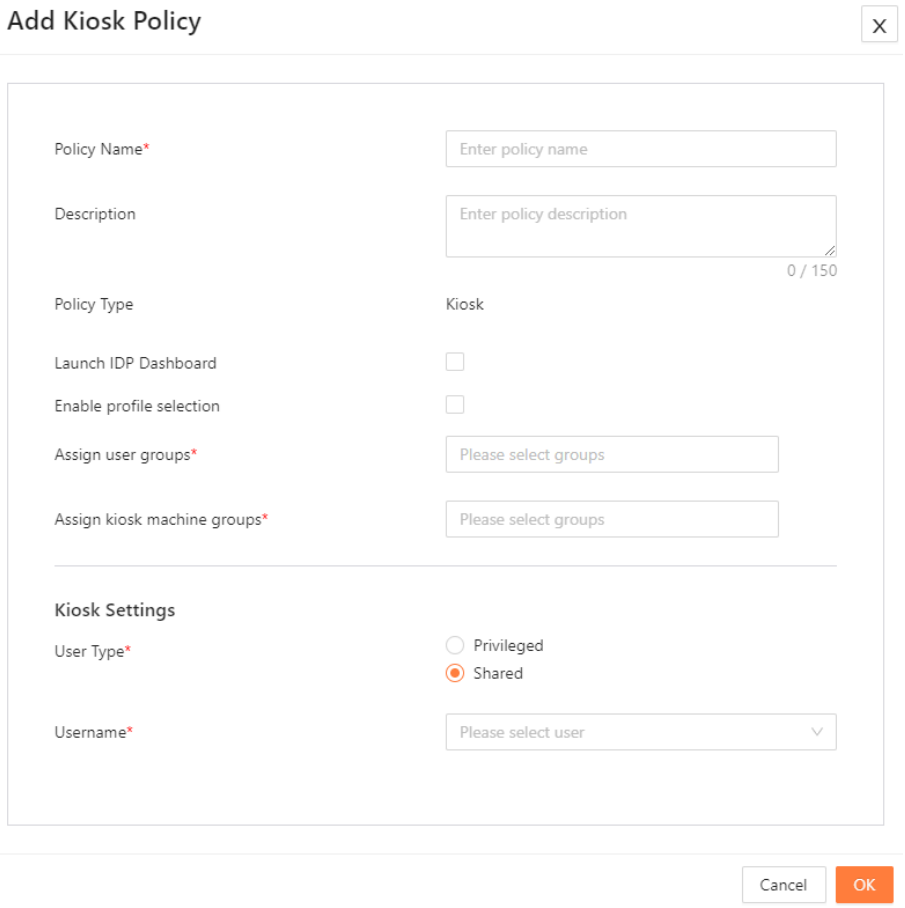
6. In the new Kiosk Group, add the kiosk machines that users will be logging into.
   Note: If you do not see any machines, please come back to this step after TecTANGO is installed on the workstation.



7. Navigate to the Kiosk Policy tab in the Settings page. Account Settings → Policies → Group Level → Kiosk.



8. Click “Add Kiosk Policy”. Enter the following:
    a. Policy Name: This is the name of the policy that will be used
    b. Description: Enter policy description
    c. Launch IdP Dashboard: If selected, after login, IdP dashboard will be launched with the kiosk user profile
    d. Enable Profile Selection: Select if the user will have the choice to sign in under their own user profile or the generic user profile during login
    e. Assign user group: The users that will be allowed to use the Kiosk Machines
    f. Assign Machine group: Select the Kiosk machine group to which the Kiosk policy applies to
    g. User Type: Select if the user is a privileged user or a shared user
    h. Username: Select the generic shared or privileged user

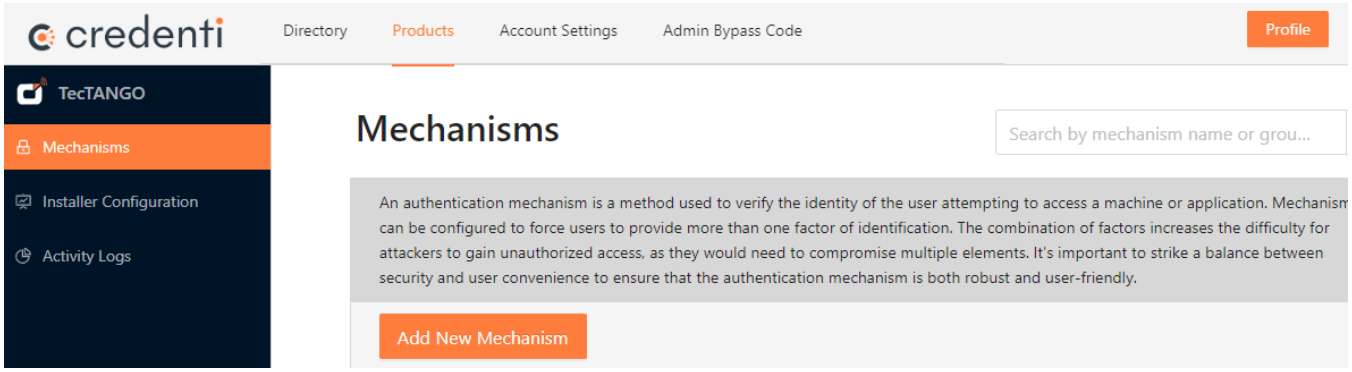


9. Now when any user from the given User Group tries to login to the machines in the machine group, the workstation will be logged with the generic user defined under the Kiosk settings.
    a. If the Kiosk policy is configured with Profile Selection enabled, the user can choose whether they sign in under their own profile or the generic user profile on the TecTANGO login prompt.

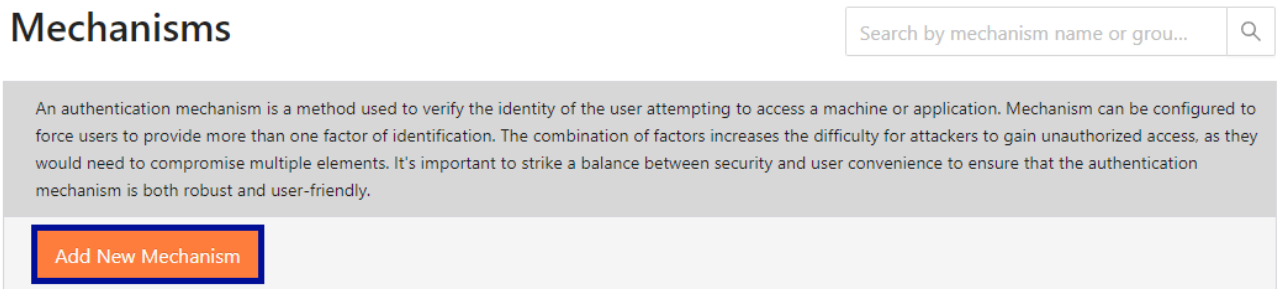
Configure Mechanisms

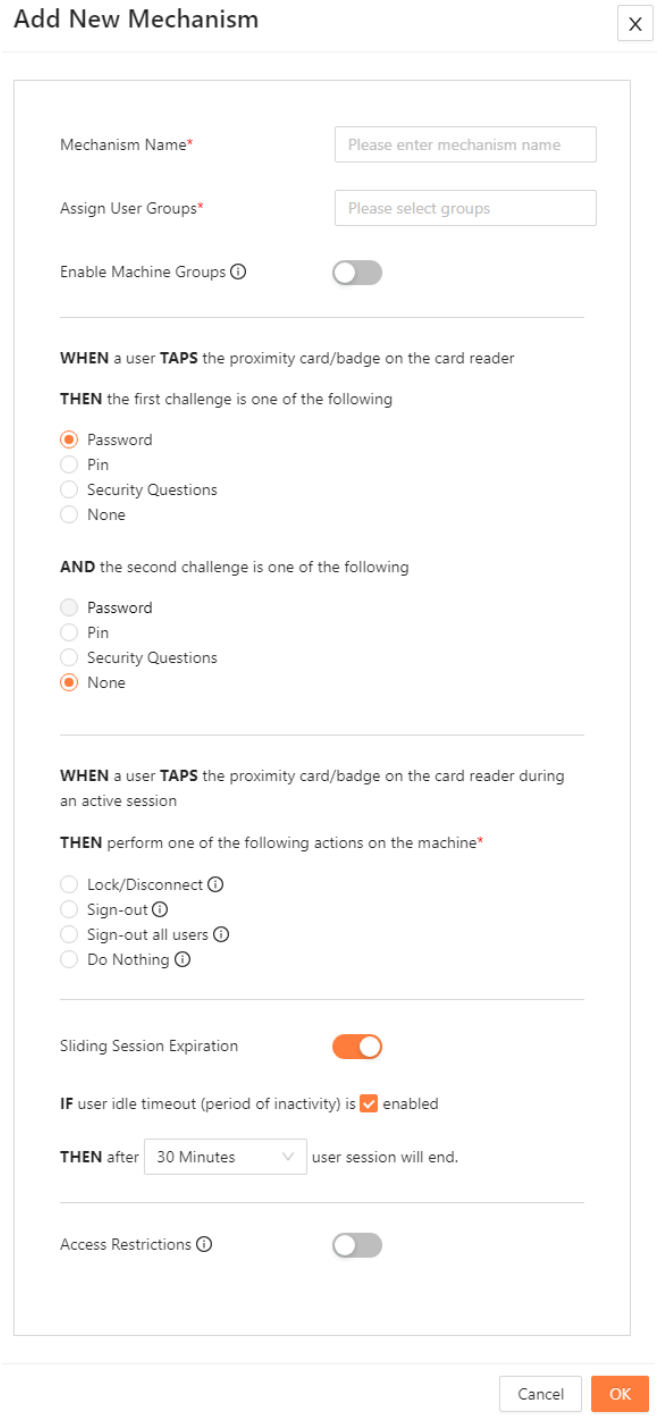
Mechanisms define the behavior of login and logout when the user taps the card. Any password/PIN policies defined for the user are enforced via mechanisms. Different mechanisms can be configured for users based on the group. All the users are assigned to the Default mechanism by default.

To configure the TecTANGO mechanisms, navigate to Products → TecTango → Mechanisms.



Use the “Add a New Mechanism” button to create and enforce a Mechanism for your chosen group.





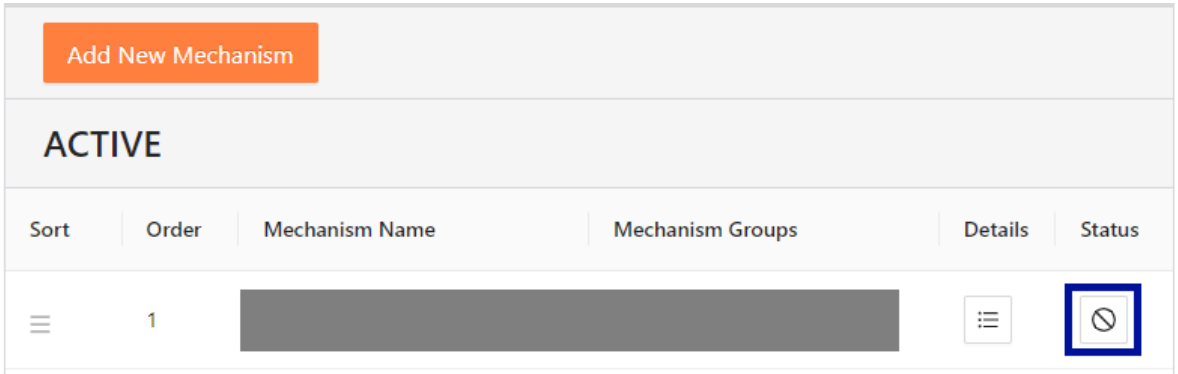
1. Click **Add New Mechanism** to open the Add New Mechanism screen.
    a. Mechanism Name: Enter a descriptive mechanism name
    b. Assigned to groups: Enter a predefined group
2. **Challenge Factors:** Pick from the following options to assign what factors your users will be challenged with when they tap their badge to login. The Admin can set two different types of Challenge factors.
    a. Password: The user will be prompted for Password. Password policies can be configured from the Account Settings page in the Credenti Admin Portal.

   b. PIN: The user will be prompted for PIN. PIN policies can be configured from the Account Settings page in the Credenti Admin Portal. Once enrolled, PIN follows the user.
   c. Security Question: The user will be prompted to answer their chosen security question(s). Security question policies can be configured from the Account Settings page. Once configured, the security question follows the user.
   d. None: The user will not be prompted for any MFA factor
3. **Tap Out Behavior:** Tap out behavior is customizable based on the organization's preference. The following options can be selected:
   a. Lock: The user machine will be locked when tapping the card
   b. Sign Out: The user will sign out when tapping the card
   c. Sign Out All Users: The user will sign out all users when tapping the card
   d. Do Nothing: Neither lock nor sign out will be initiated when tapping the card

   Note: If Tap out action is Sign out/Sign out all users, Tap Over will only secure other users' sessions. It will not login the second user.
4. **Idle Time Period**: You can enable idle time period (period of inactivity) by simply checking the box. After checking the box, you can set a time period in which the machine will remain idle before performing Tap out action for the user.
5. **Access Restriction**: This will allow you to allow/restrict login based on the predefined rules.
6. Click **Create.** This will create the mechanism.
   a. The newly created mechanism will be created in an inactive state. The user will need to **activate** it before the mechanism will take effect. The **POWER BUTTON** beside the Mechanism will need to be clicked to activate it.

Deactivate Mechanism

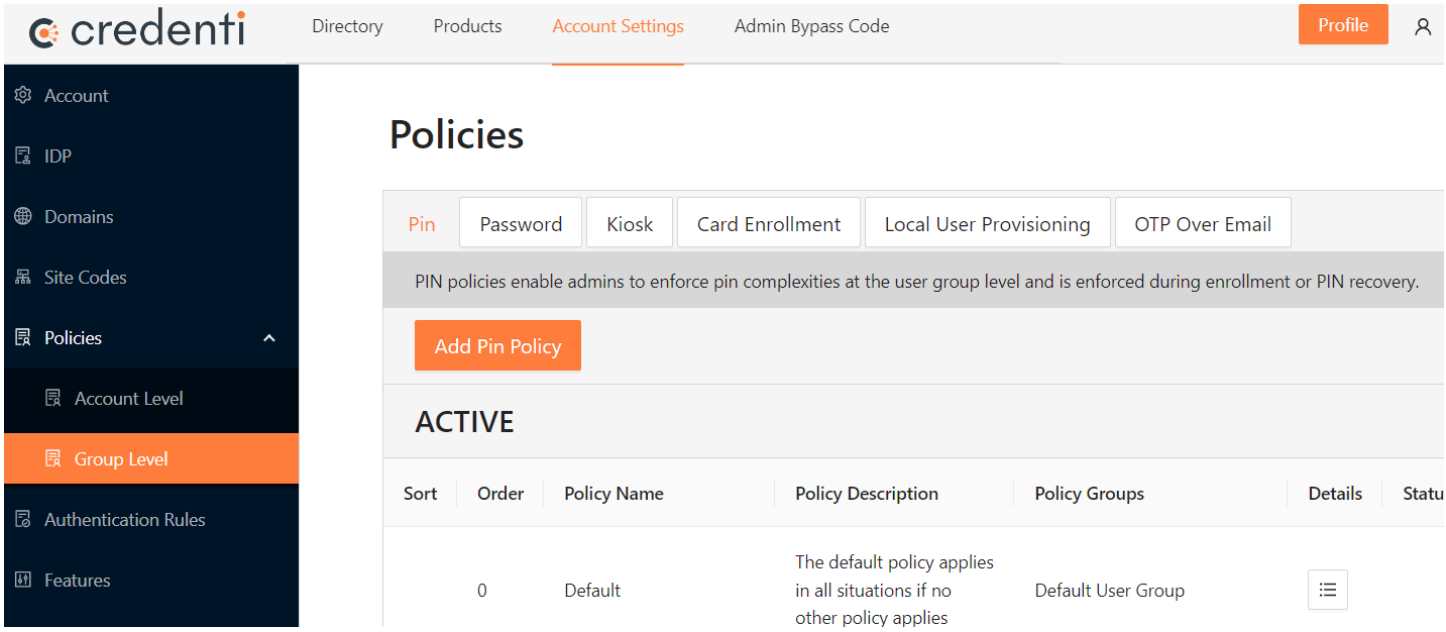
If a mechanism is not needed, then it can be deactivated by clicking on the status against it and changing it to Deactivate.



Policy Configuration

Group Level Policies

Each user can have different policies for PIN, Password, Kiosk machines, or Card Enrollment based on the group they belong to. Go to Account Settings → Policies → Group Level.

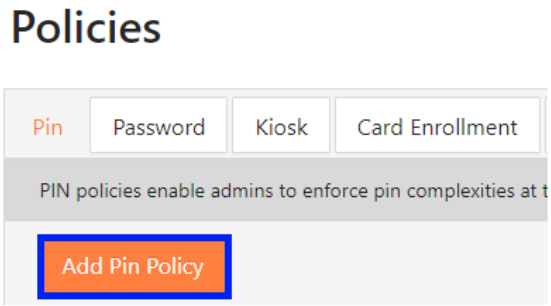


PIN Policy

PIN policies enable admins to enforce PIN complexities at the user group level and are enforced during enrollment or PIN recovery.

Add Pin Policy:

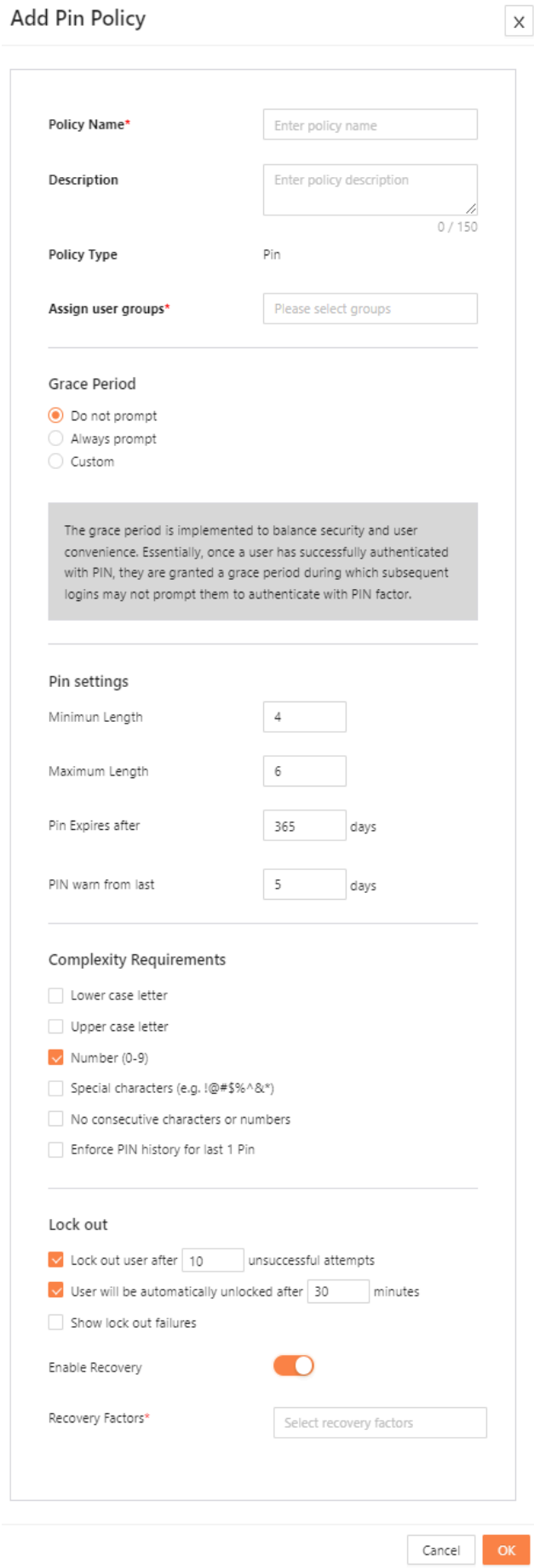
1. Click **Add PIN Policy** to open the Add PIN Policy screen.



2. Enter Policy details:
    a. Policy Name: Enter a Descriptive Policy Name
    b. Description: Describe the policy
    c. Assigned to groups: Enter a predefined group(s) to which this policy would apply
    d. Grace Period: Select how often PIN should be prompted for the user
        i. Do not prompt
        ii. Always prompt
        iii. Custom: Enter the custom time after which user will be prompted for PIN
    e. Minimum Length of the PIN: The minimum number of characters in the PIN required
    f. Maximum Length of the PIN: The maximum number of characters in the PIN allowed
    g. PIN Expires after: Enter days after which PIN will expire

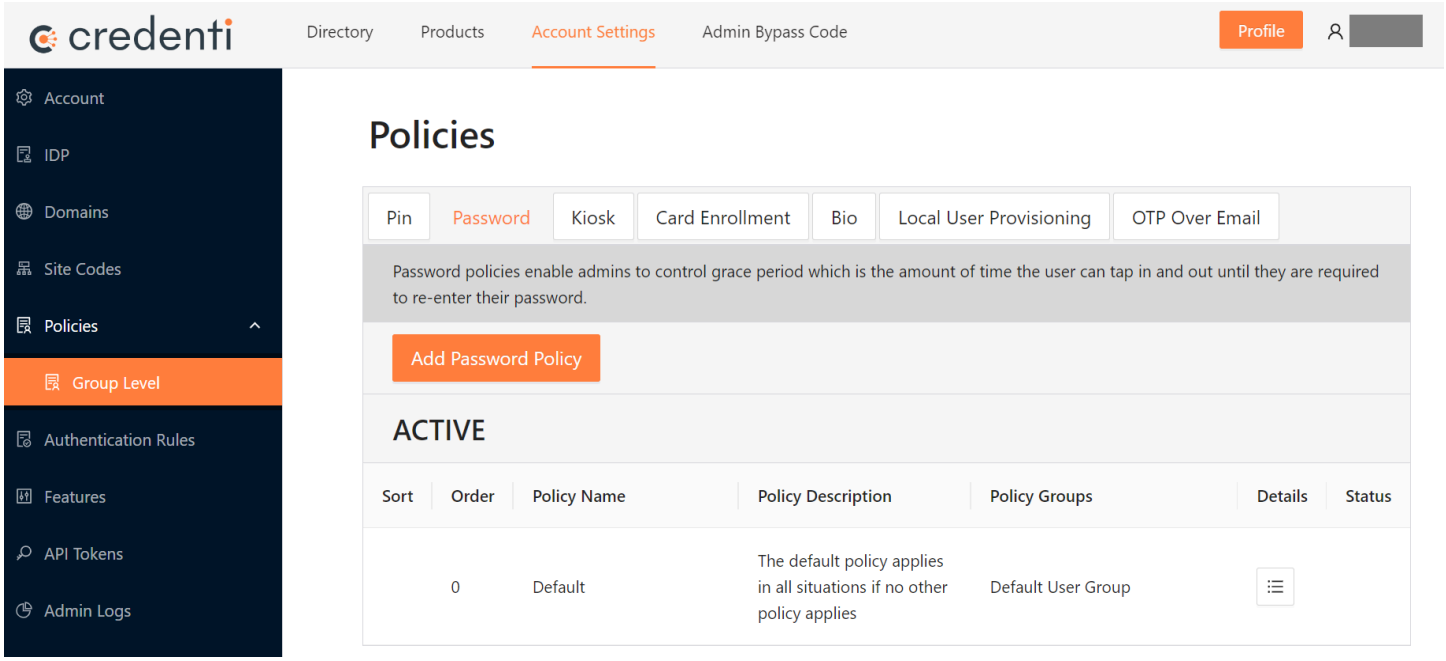
h. PIN warn from last: Enter how many days before PIN expiration does the user want to see the PIN expiry prompt
i. Complexity Requirements:
    i. Lowercase letter: The PIN must contain lowercase letters
    ii. Uppercase letter: The PIN must contain uppercase letters
    iii. Number (0-9): The PIN must contain digits
    iv. Special Characters: The PIN must contain a special character
    v. No Consecutive characters or numbers: The PIN cannot be in a consecutive order. Example: (1234 or abcd)
    vi. Enforce PIN history for last x PIN: User will not be able to use last x PINs
j. Lock out:
    i. Lockout user after x unsuccessful attempts: Enter the number of attempts allowed for the user before they are locked out in Credenti Portal
    ii. Automatic unlock account time: Enter after how long the user's account should be automatically unlocked
    iii. Show lock out failures: Select if you wish to show the failures to the user
k. Enable Recovery: Allow users to recover their forgotten PIN and select the Recovery Factors they must utilize to perform this action. This option is available only if Security Question feature is enabled

3. Click **Create**.
    a. After creating the PIN policy, it will be created in the Inactive Table.
    b. To **activate** the policy, click on the **POWER BUTTON** beside it.


Add Pin Policy
X
Policy Name*
Enter policy name
Description
Enter policy description
0 / 150
Policy Type
Pin
Assign user groups*
Please select groups
Grace Period
Do not prompt
Always prompt
Custom
The grace period is implemented to balance security and user convenience. Essentially, once a user has successfully authenticated with PIN, they are granted a grace period during which subsequent logins may not prompt them to authenticate with PIN factor.
Pin settings
Minimun Length
4
Maximum Length
6
Pin Expires after
365
days
PIN warn from last
5
days
Complexity Requirements
Lower case letter
Upper case letter
Number (0-9)
Special characters (e.g. !@#$%^&*)
No consecutive characters or numbers
Enforce PIN history for last 1 Pin
Lock out
Lock out user after
10
unsuccessful attempts
User will be automatically unlocked after
30
minutes
Show lock out failures
Enable Recovery
Recovery Factors*
Select recovery factors
Cancel
OK

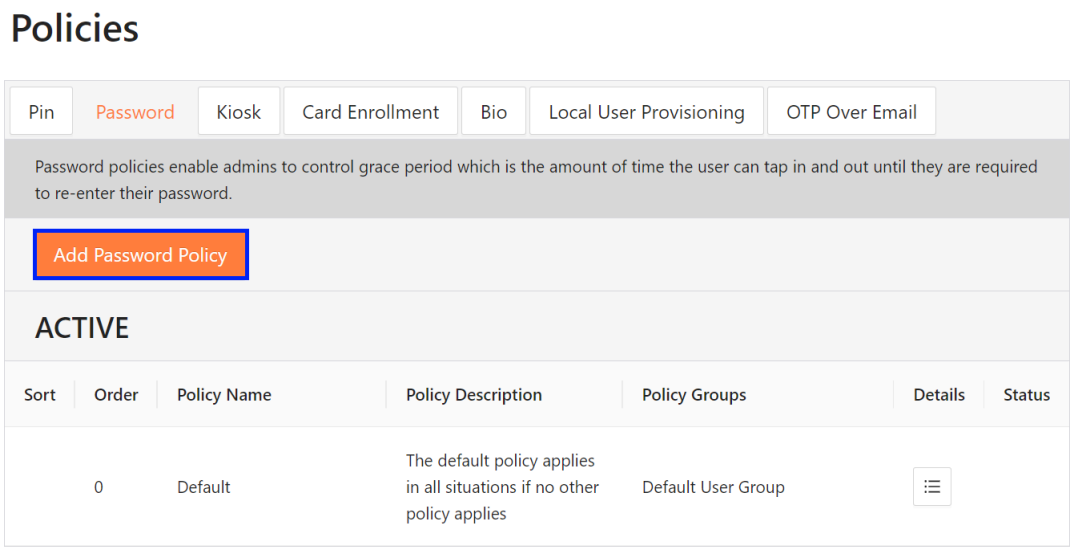
Password Policy

Password policies enable admins to control grace period, which is the amount of time the user can tap in and out until they are required to re-enter their password.



Add Password Policy:

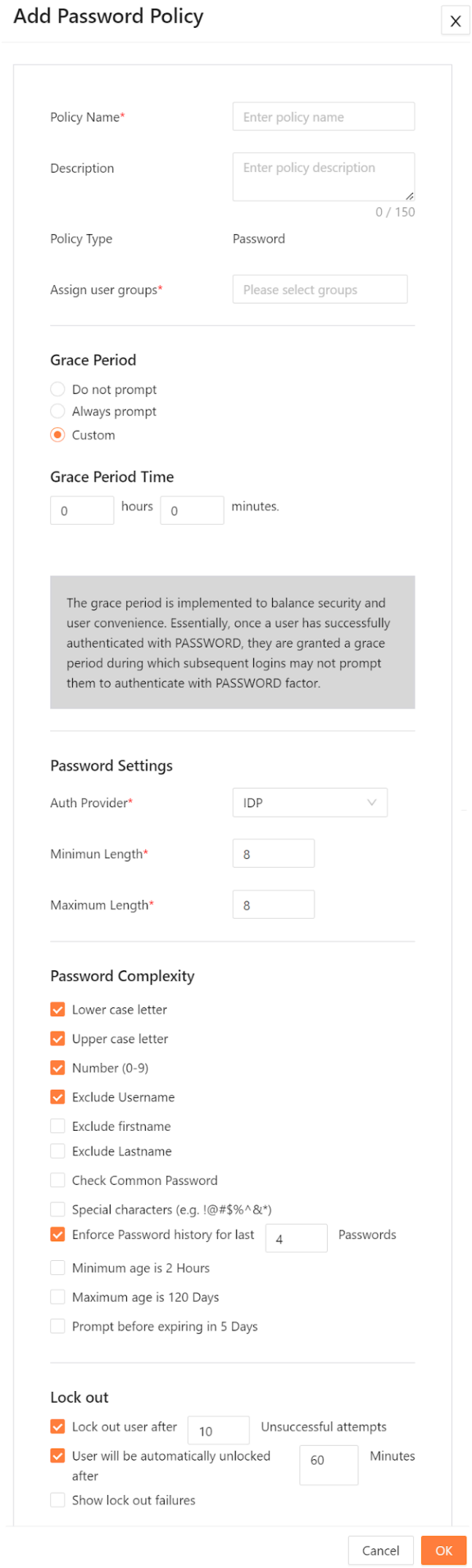
1. Click **Add Password Policy** to open the Add Password Policy screen.



2. Enter Policy details:
    a. Policy Name: Enter a Descriptive Policy Name
    b. Description: Describe the policy
    c. Assigned to groups: Enter a predefined group(s) to which this policy would apply

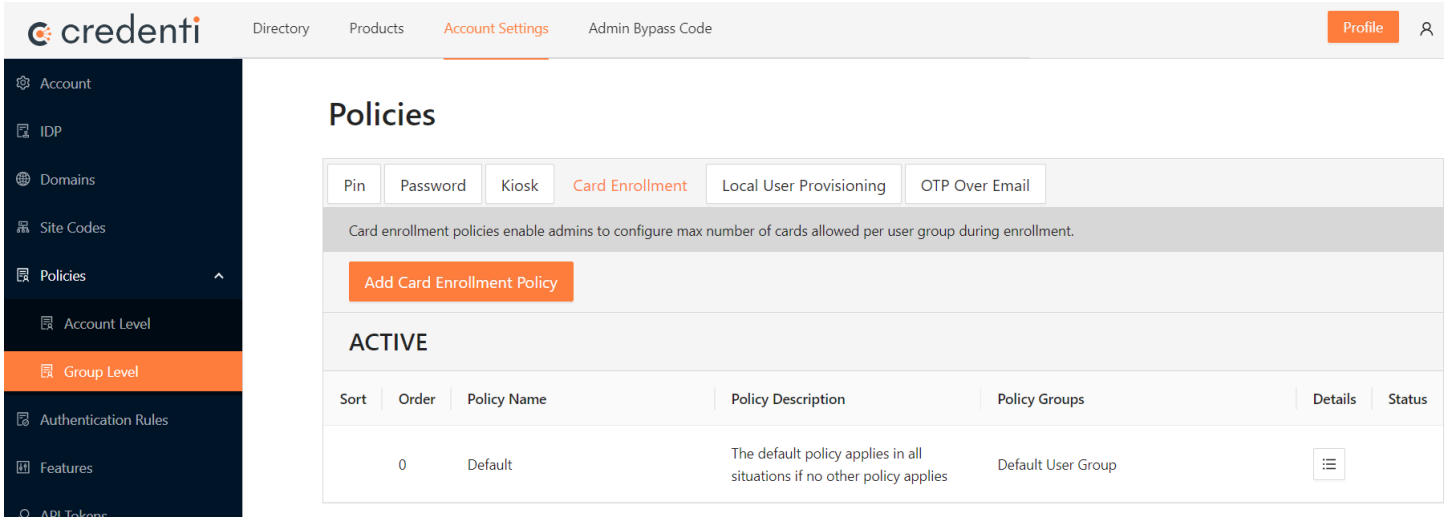
d. Grace Period: Select how often password should be prompted for the user
    i. Do not prompt
    ii. Always prompt
    iii. Custom: Enter the custom time after which user will be prompted for password
e. Auth Provider: Select IdP/Active Directory
f. Minimum Length of the Password: The minimum number of characters required in the Password
g. Maximum Length of the Password: The maximum number of characters allowed in the Password
h. Complexity Requirements:
    i. Lowercase letter: The password must contain lowercase letters
    ii. Uppercase letter: The password must contain uppercase letters
    iii. Number (0-9): The password must contain digits
    iv. Exclude Username: Username will not be allowed as part of the password
    v. Exclude First name: First name will not be allowed as part of the password
    vi. Exclude Last name: Last name will not be allowed as part of the password
    vii. Check common passwords: Commonly used password is not allowed
    viii. Special Characters: The password must contain a special character
    ix. Enforce Password history for last x Passwords
    x. Minimum age: Minimum time before the password can be changed
    xi. Maximum age: Password will be expired after this time
    xii. Prompt before expiring in x days: Enter how many days before password expiration does the user want to see the password expiry prompt
i. Lock out:
    i. Lockout user after x unsuccessful attempts: Enter the number of attempts allowed for the user before they are locked out in Credenti Portal
    ii. Automatic unlock account time: Enter after how long the user's account should be automatically unlocked
    iii. Show lock out failures: Select if you wish to show the failures to the user

3. Click **Create**.
    a. After creating the password policy, it will be created in the Inactive Table
    b. To **activate** the policy, click on the **POWER BUTTON** beside it


Add Password Policy
Policy Name*
Enter policy name
Description
Enter policy description
0 / 150
Policy Type
Password
Assign user groups*
Please select groups
Grace Period
Do not prompt
Always prompt
Custom
Grace Period Time
0
hours
0
minutes.
The grace period is implemented to balance security and user convenience. Essentially, once a user has successfully authenticated with PASSWORD, they are granted a grace period during which subsequent logins may not prompt them to authenticate with PASSWORD factor.
Password Settings
Auth Provider*
IDP
Minimun Length*
8
Maximum Length*
8
Password Complexity
Lower case letter
Upper case letter
Number (0-9)
Exclude Username
Exclude firstname
Exclude Lastname
Check Common Password
Special characters (e.g. !@#$%^&*)
Enforce Password history for last
4
Passwords
Minimum age is 2 Hours
Maximum age is 120 Days
Prompt before expiring in 5 Days
Lock out
Lock out user after
10
Unsuccessful attempts
User will be automatically unlocked after
60
Minutes
Show lock out failures
Cancel
OK

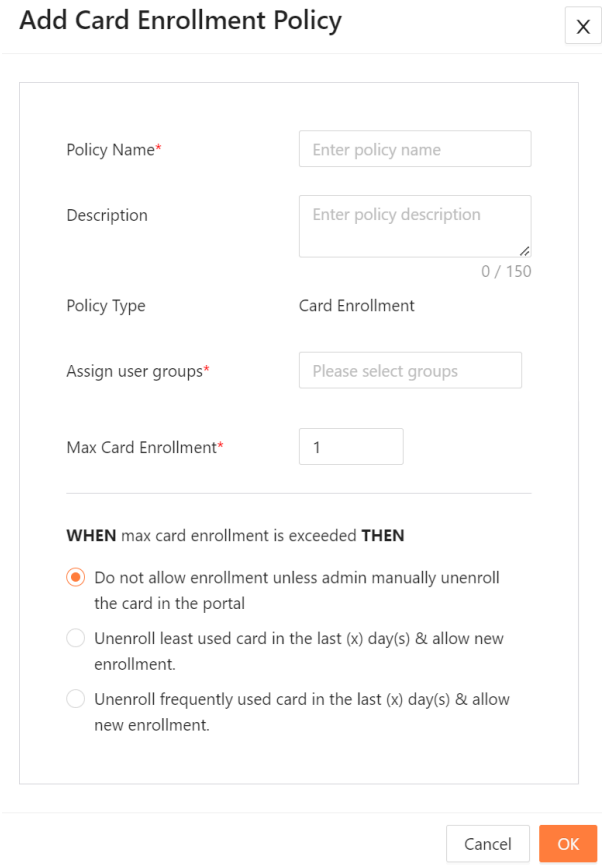
Card Enrollment Policy

Card enrollment policies enable admins to configure the max number of cards allowed per user group during enrollment.



Add Card Enrollment Policy:

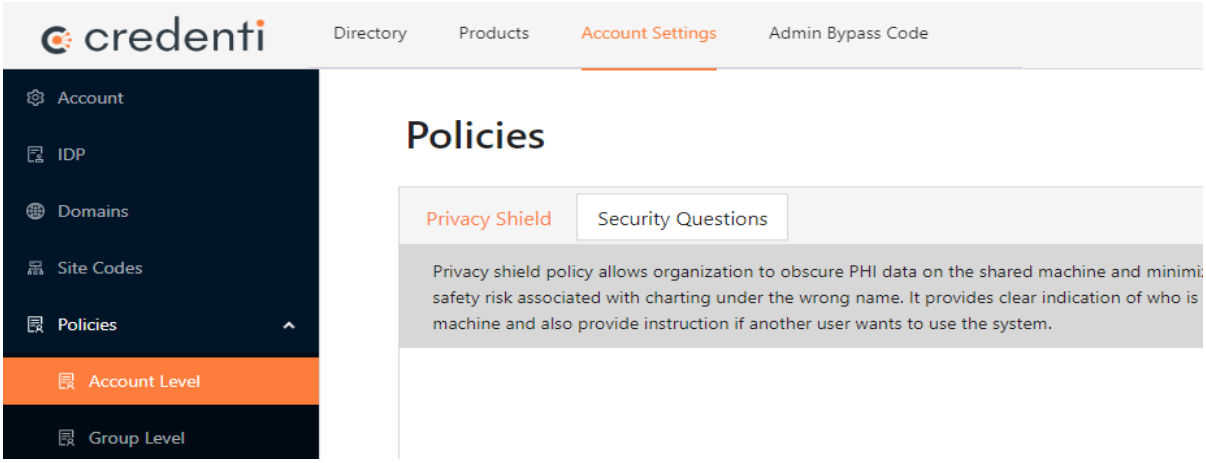
1. Click **Add Card Enrollment Policy** to open Add Card Enrollment Policy screen.
2. Enter below details:
    a. Policy Name: Enter a Descriptive Policy Name
    b. Description: Describe the policy
    c. Assigned to groups: Enter a predefined group(s) to which this policy would apply
    d. Max Card Enrollment: Enter the maximum number of enrollments allowed for the user. Please note that this should be lesser than or equal to the number configured in the backend. Reach out to Tecnics support to determine the number of enrollments allowed for your organization. By default, backend value is set to 1.
    e. When Max Card Enrollment exceeds then: Select the behavior when the maximum enrollments are exceeded for the card.



3. Click **Create**.
    a. After creating the card enrollment policy, it will be created in the Inactive Table.
    b. To **activate** the policy, click on the **POWER BUTTON** beside it.

Account Level Policies

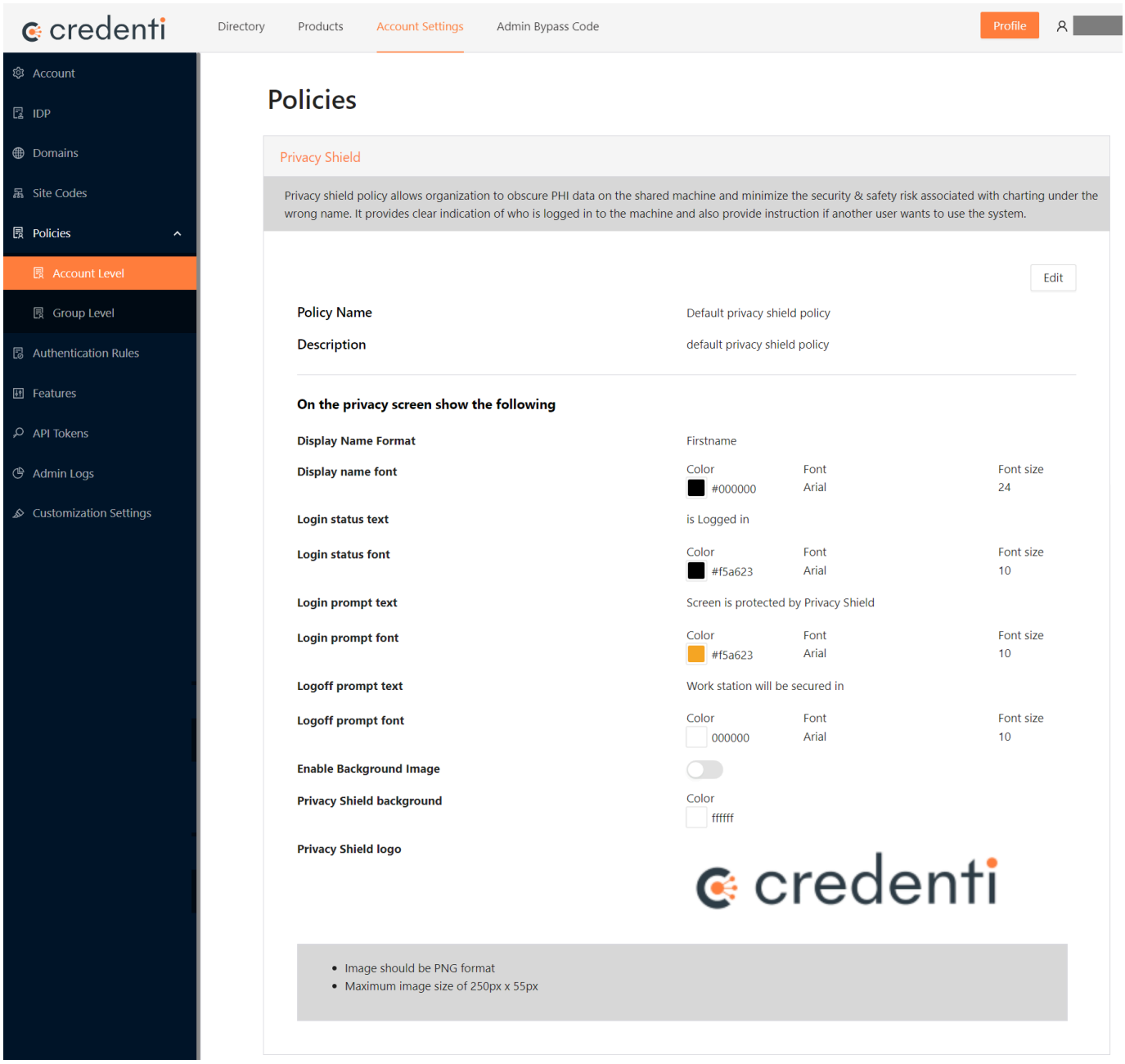
These policies apply to all users, if enabled. Go to Account Settings → Policies → Account Level. *Note: By default, these features are disabled. Please reach out to Tecnics support to enable these features on the backend first. Afterwards, go to Account Settings → Features in the Credenti Admin Portal to enable your requested feature.*



Privacy Shield

Privacy Shield policy allows organizations to obscure sensitive data on the shared machine and minimize the security and safety risk associated with working under the wrong name. It provides clear indication of who is logged into the machine and also provides instruction if another user wants to use the system.

1. Privacy Shield can be set up in the Credenti Admin Portal. In the admin portal, navigate to the Privacy Shield Policy page. Account Settings → Policies → Account Level → Privacy Shield.



2. On this page, the following can be edited:
    a. Display Name Format: How the user's name should appear
    b. Display name font: Font with which the name is shown

c. Login status text: The text that identifies which user is logged in
d. Login Status font: Font with which the login status is shown
e. Login prompt text: The text that instructs the user (if not the logged in user) what to do next
f. Login prompt font: Font with which the login prompt is shown
g. Logoff prompt text: The text that notifies the user that the workstation will be secured in (X) amount of time
h. Logoff prompt font: Font with which the logoff prompt is shown
i. Enable Background Image: The background image that can be shown during Privacy Shield
    i. Must be PNG format
    ii. Must be desktop resolution size
j. Primary Shield background: The color of the Privacy Shield background
k. Primary Shield logo: The logo that can be seen during Privacy Shield
    i. Must be PNG format
    ii. Maximum image size of 250px x 55px

3. To enable Privacy Shield, navigate to TecTANGO mechanisms and enable idle timeout.

IF user idle timeout (period of inactivity) is ☑ enabled

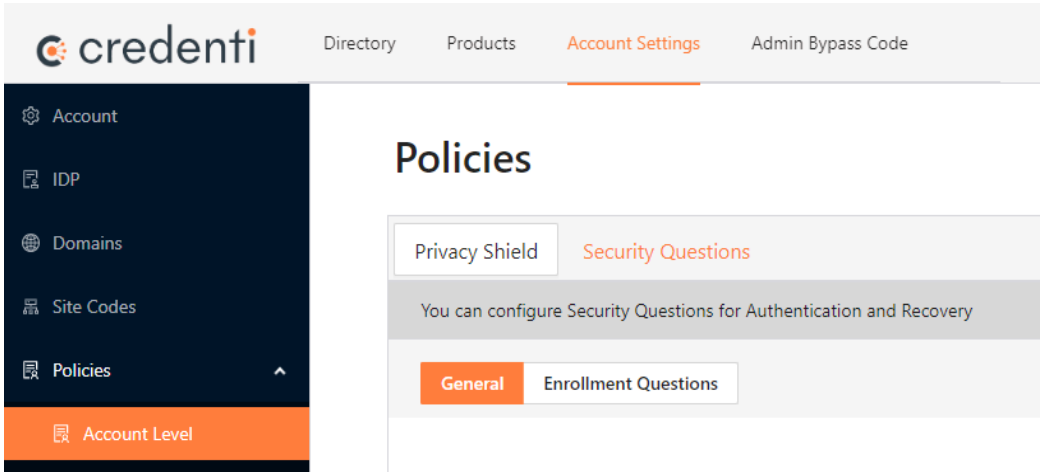
THEN after 15 Minutes user will be locked/signed-out.

4. Once enabled, when a user taps into a machine and after 30 seconds of inactivity, Privacy Shield will go into effect.

Security Questions

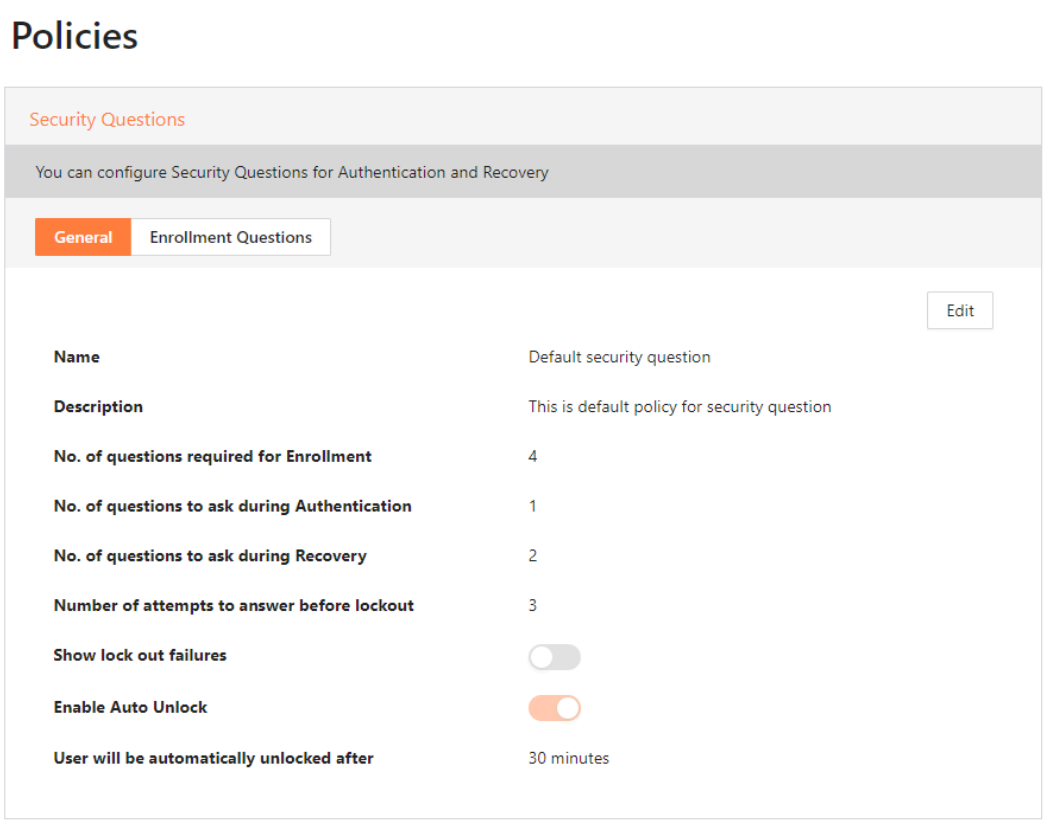
Security question policies allow admins to enforce security question complexities and are enforced during enrollment and recovery.

1. Security Question policies can be set up in the Credenti Admin Portal. In the admin portal, navigate to the Security Question Policy page. Account Settings → Policies → Account Level → Security Questions.

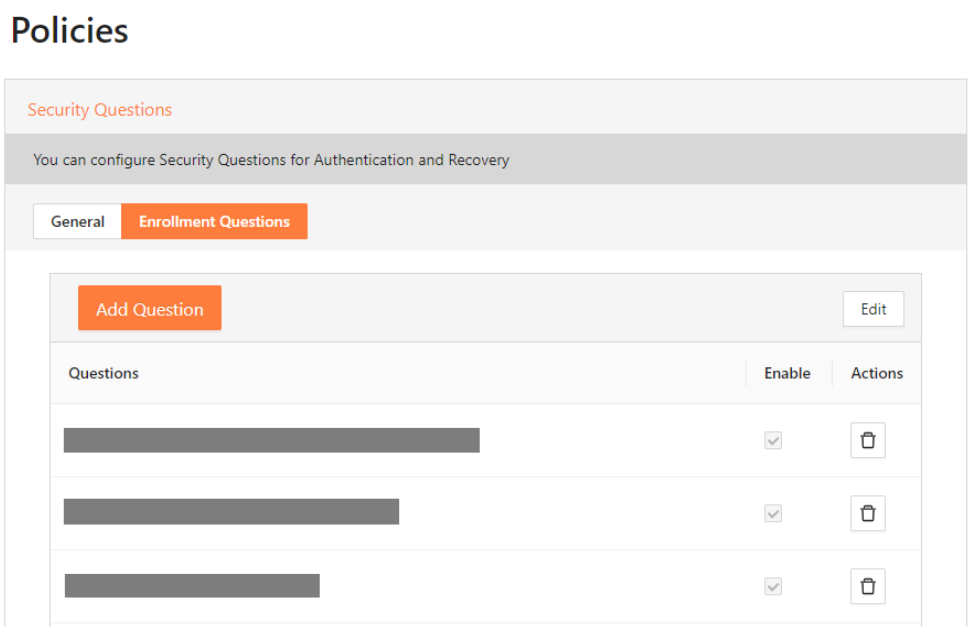


2. Under the **General** tab, the following can be edited:

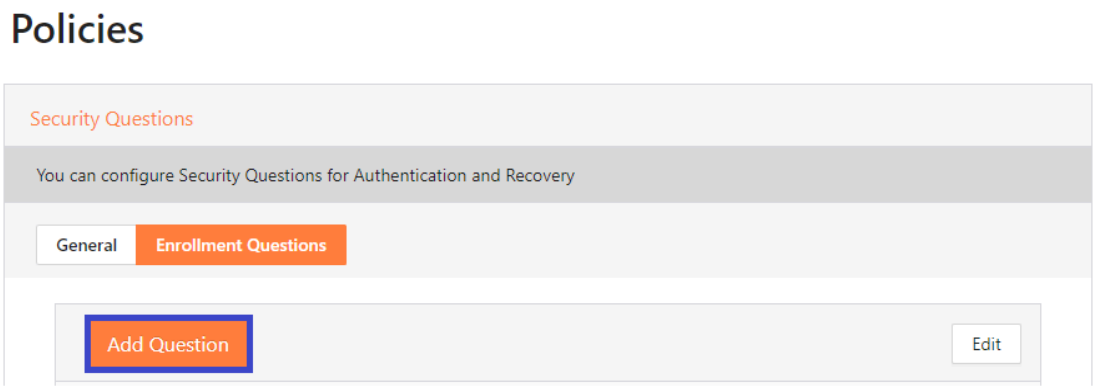
a. Policy Name: Enter a Descriptive Policy Name
b. Description: Describe the policy
c. Number of questions required for enrollment: Number of questions the user must set up during their initial security question enrollment
d. Number of questions to ask during authentication: Number of questions the user must answer in order to authenticate into the workstation
e. Number of questions to ask during recovery: Number of questions the user must answer correctly in order to reset the PIN
f. Number of attempts to answer before lockout: Number of incorrect answers user can give before their account is locked
g. Show lock out failures: Select if you wish to show the failures to the user
h. Automatic unlock account time: Enter after how long the user's account should be automatically unlocked



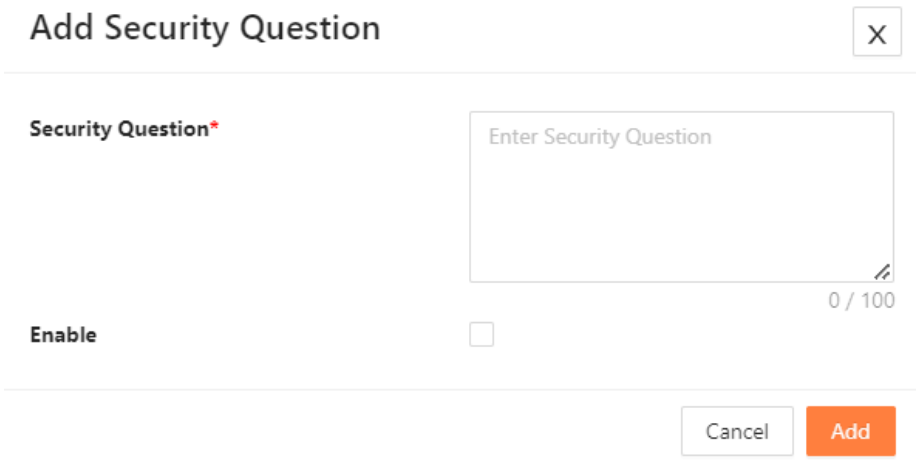
3. Under the **Enrollment Questions** tab, you can enable or delete Security Question prompts to customize what options are displayed to the user during their enrollment.



4. Click **Add Question** to open the Add Security Question screen.



5. Enter your custom security question and select **Enable**. Click **Add**.



Account Settings

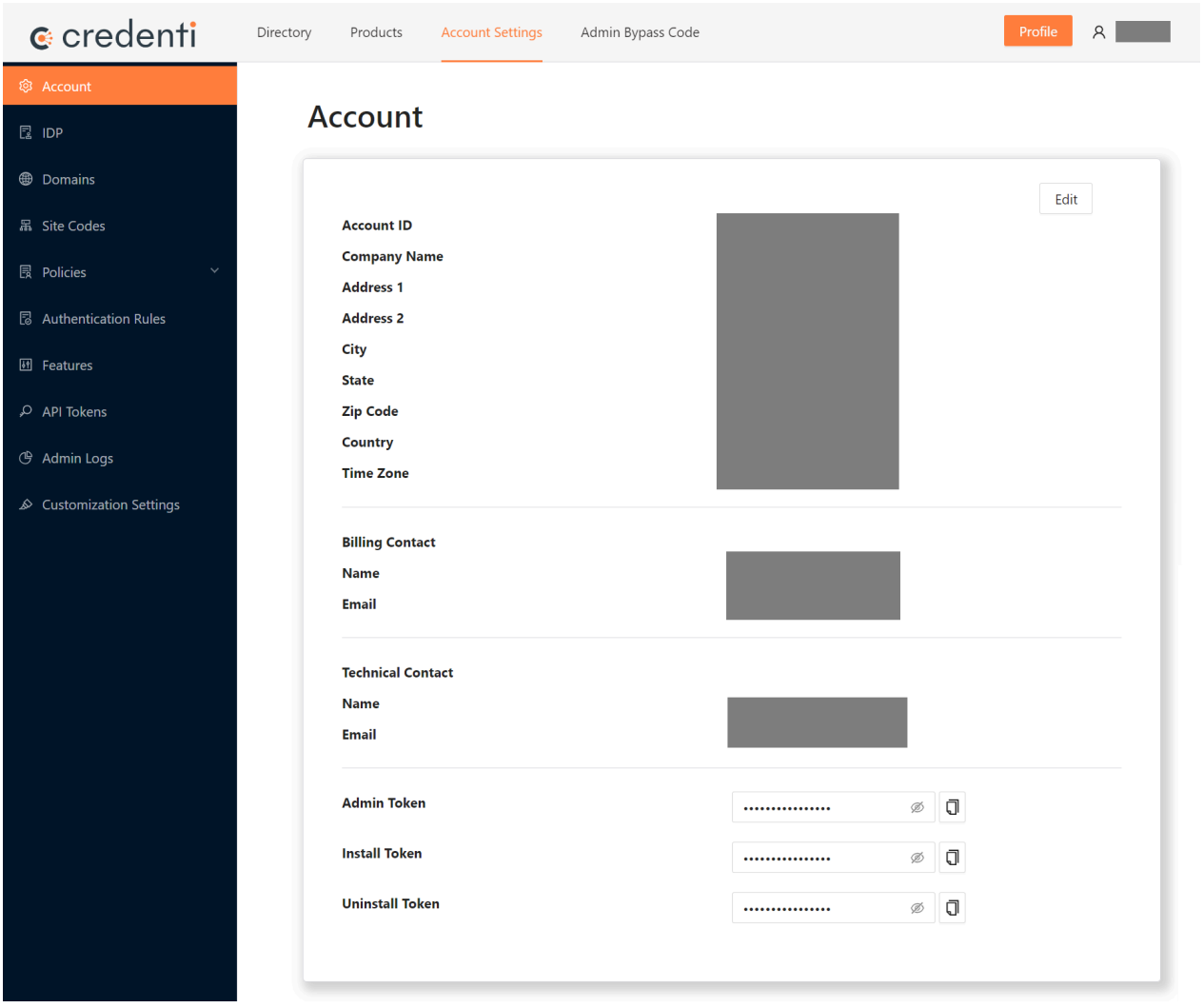
Account

Account page provides the below details:

- Company Name
- Company Address
- Time Zone
- Billing Contact
- Technical Contact
- Install Token
- Uninstall Token

Only Timezone is editable on this screen. To modify any other fields, please contact Tecnics support.

In order to install or uninstall any Tecnics/Credenti products, Install Token and Uninstall Token are required.

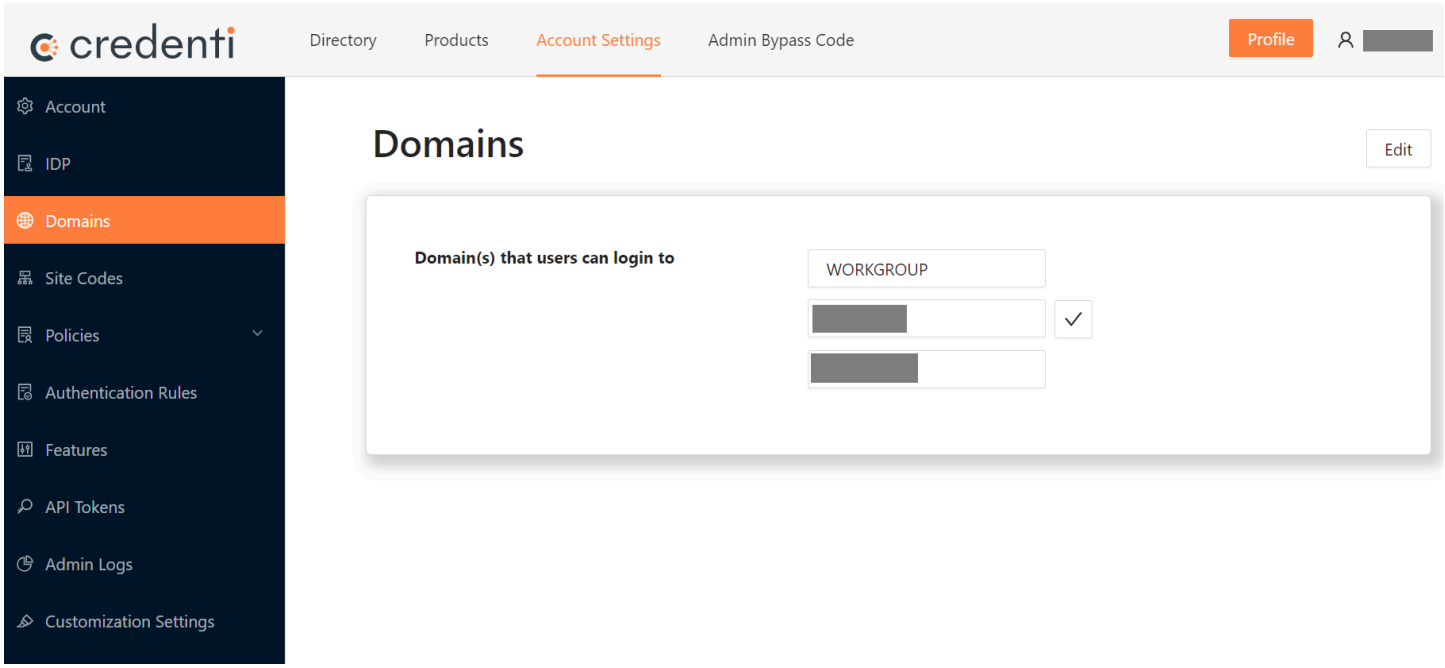


Domains

By default, WORKGROUP domain is added to all accounts. In order to add any other directory domains, click on Edit and add the domain. Select the checkmark to make it the default domain.

On the workstation, when the user tries to use or enroll in any of the Tecnics/Credenti products, a dropdown will be shown with all the domains available on this screen. The dropdown will be defaulted to the default domain.

If the workstation is connected to Azure AD/Entra, please add AzureAD as the domain.



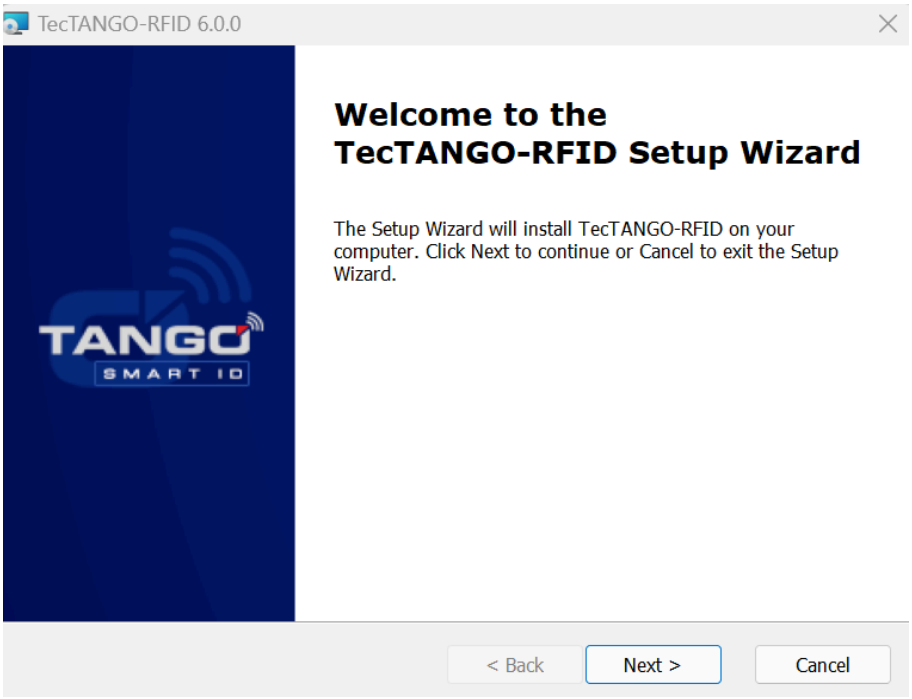
Workstation Configuration

Run the TecTANGO installer provided by Tecnics. If you do not have the installer, please contact Tecnics. The installer deploys a Windows Credential Provider which allows the user to login using a smart card or proximity card.

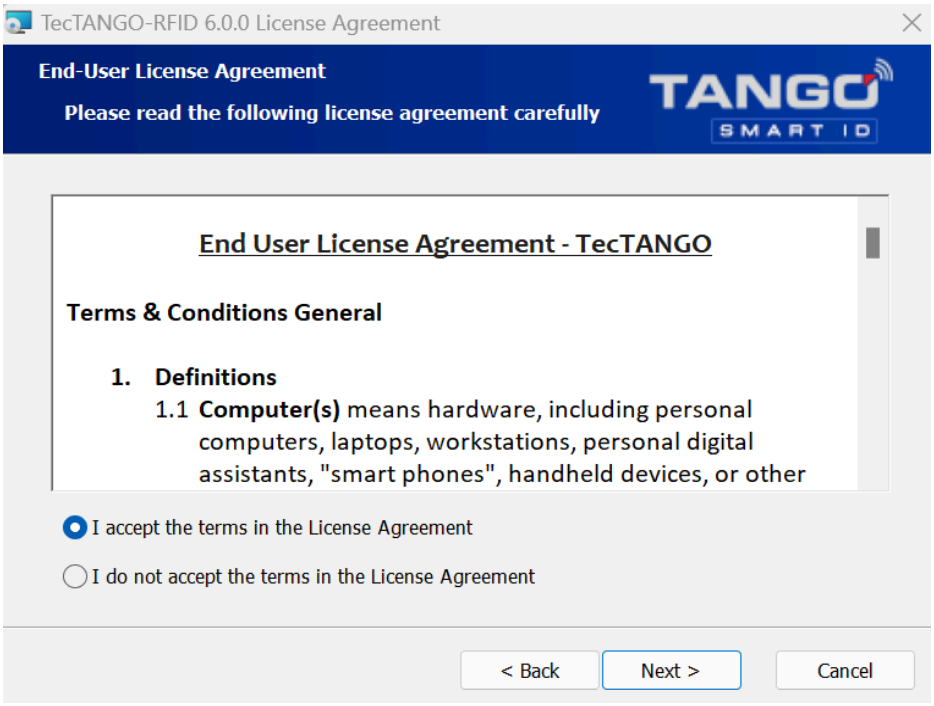
- The installation can be done via:
  - Manual installation
  - Silent installation
  - GPO installation

Manual Installation

1. Prior to TecTANGO installation, if TecUNIFY SSO is required, TecUNIFY must be installed first. If not, proceed to step 2.
2. Run the downloaded msi file, and click Next.

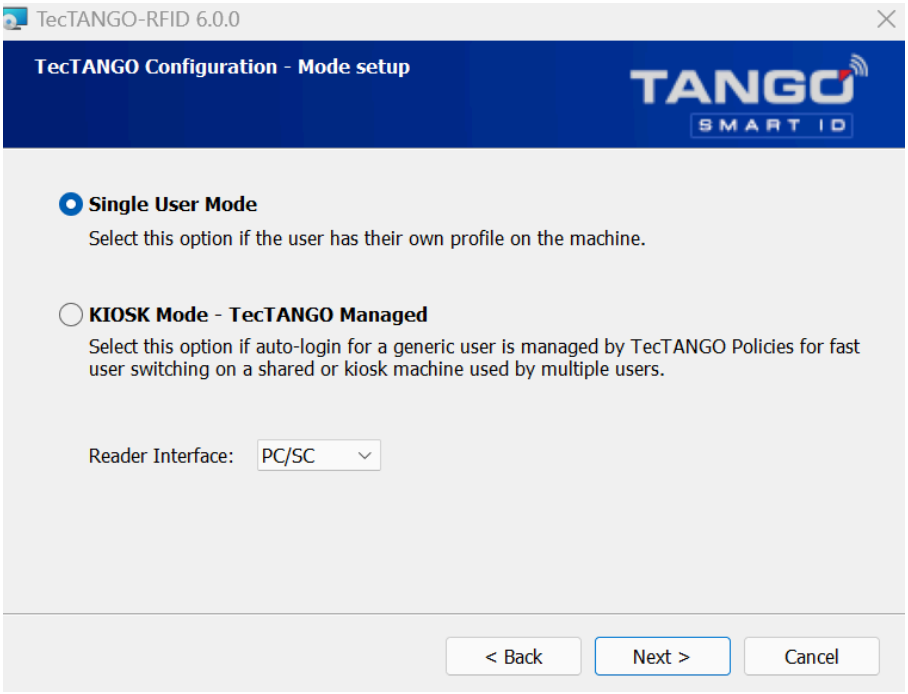


3. Accept the EULA, and click on Next.

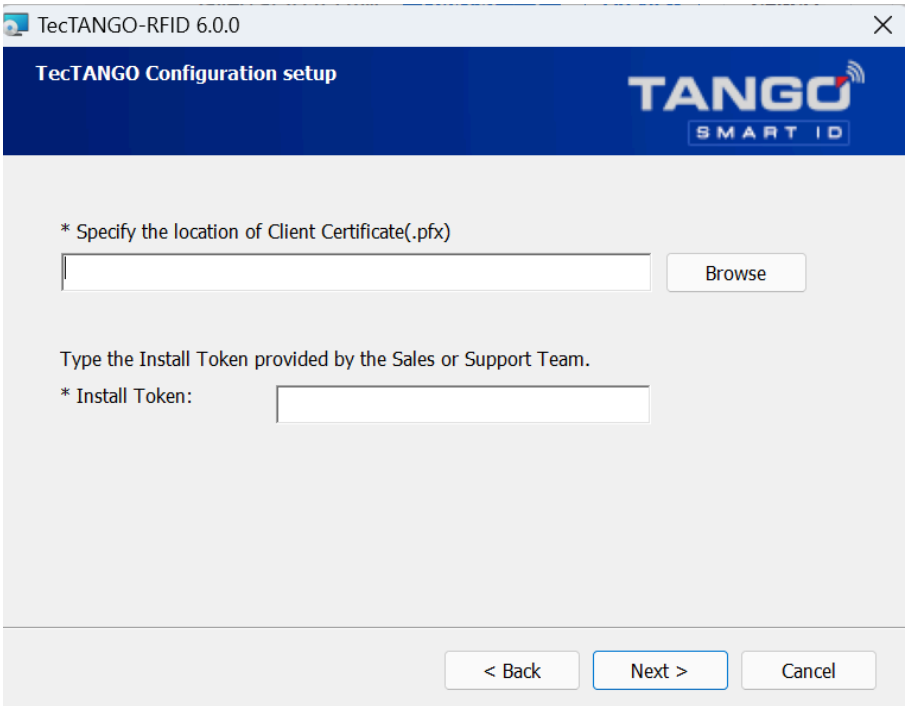


4. Enter the values as described below, and then click Next.
    a. Select User Mode: Based on the given Description
        i. Single User Mode: Select this option if the user has their own profile on the machine
        ii. Kiosk Mode - TecTango Managed: Select this option if auto-login for a generic user is managed by TecTango Policies for fast user switching on a shared or kiosk machine used by multiple users. Follow instructions here to setup kiosk user in Credenti Admin Portal

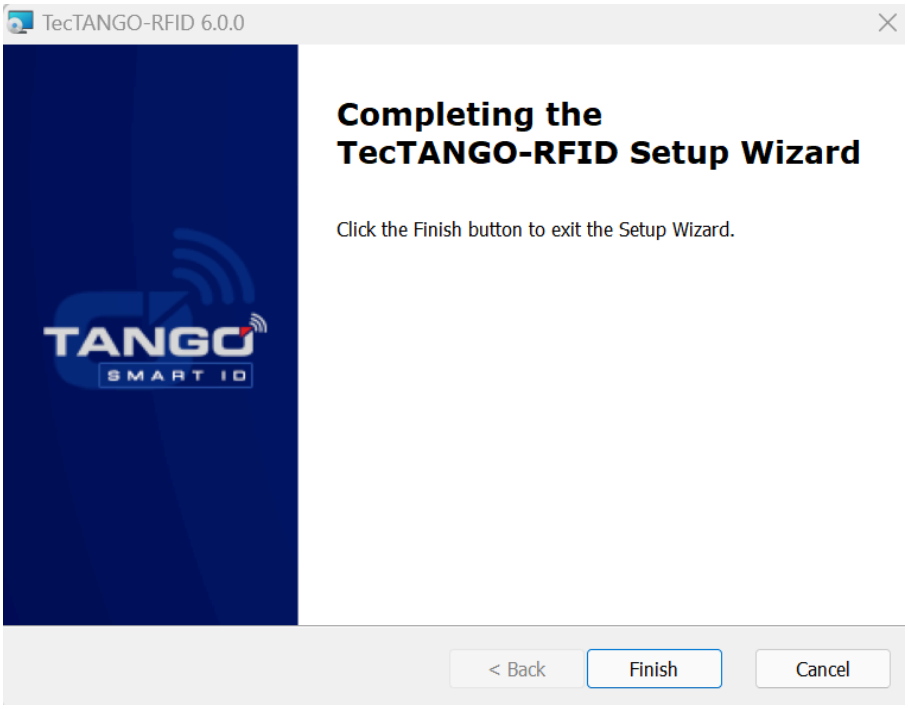
b. Reader Interface: Select the type of reader interface you will be using
    i. PC/SC Reader
    ii. RFIdeas Reader



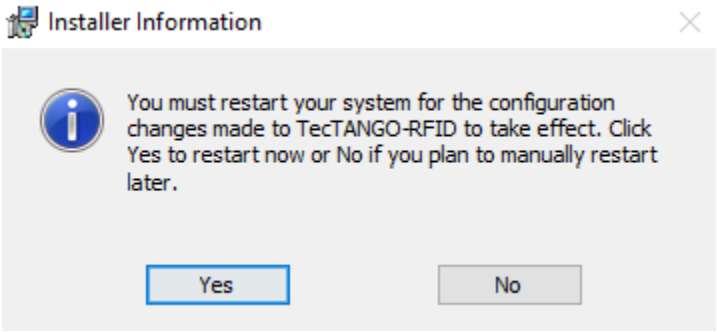
5. Specify the location of the Client Certificate(.pfx): Add the absolute path for the client certificate provided by Tecnics.
6. Add in the Install Token given to you by the Admin. This can also be retrieved from the Credenti Admin Portal, Account Settings page.



7. Click *Finish* to install TecTANGO.



8. Restart the machine and try to login using your smart card or proximity card.



Silent Installation

1. Open command prompt as an administrator and browse to the location of TecTANGO-RFID.msi.
2. Run the following command for silent installation:
    a. MACHINE_MODE: This is to determine the Machine mode
        i. If the user has their own profile on the machine: “STANDARD”
        ii. If auto-login for a generic user is managed by TecTANGO Policies for fast user switching on a shared or kiosk machine used by multiple users: “KIOSK”
    b. READER: This is to determine the reader type
        i. If the interface is PcscReader: “PcscReader”
        ii. If the interface is PcProxReader: “PcProxReader”
    c. CLIENTCERTFILE: Specify the location of the Certificate File(.pfx) along with the file name.

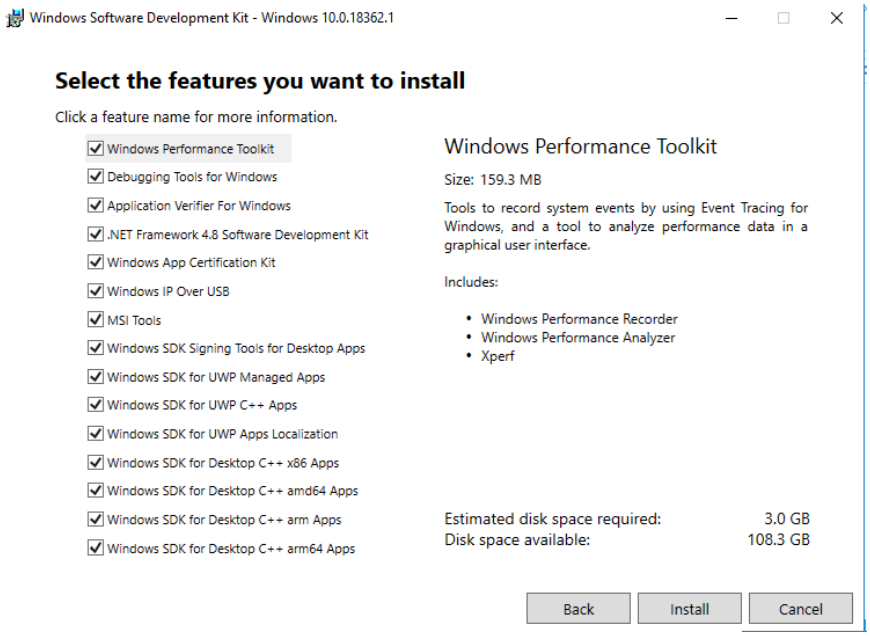
d. INSTALLTOKEN: Enter the Install Token given by Tecnics or found in the Admin Portal: “installtoken”

*msiexec.exe /i "TecTANGO-RFID_Installer.msi" MACHINE_MODE="STANDARD or KIOSK" READER="PcscReader or PcProxReader" INSTALLTOKEN="TecTango API Install Token" CLIENTCERTFILE="Path for client .pfx certificate" /quiet /l*v TecTANGO_InstallerLogs.txt*

Installation through GPO

1. Install ORCA tool to generate MST file

- Download the Windows 10 SDK from the following link: [Windows 10 SDK Download] (https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk).
- Extract or mount the downloaded ISO file.
- Right-click on **WinSDKSetup.exe** and select "Run as administrator".
- Choose the installation path and click "Next".
- Select the appropriate options for Windows Kits Privacy and click "Next".
- Accept the License Agreement and proceed.
- On the "Select the features you want to install" screen, select all features and click "Install".



- After installation, verify if the Orca tool is listed in "Programs & Features." If not, search for "orca" in the installation path (<<Installation Path>>/Windows Kit/10/), and run the corresponding executable to configure Orca.
- Once configured, the "Orca" entry will appear in "Programs & Features".

2. Create a Distribution Point

To publish or assign a computer program, you must create a distribution point on the publishing server. To do this, follow these steps:

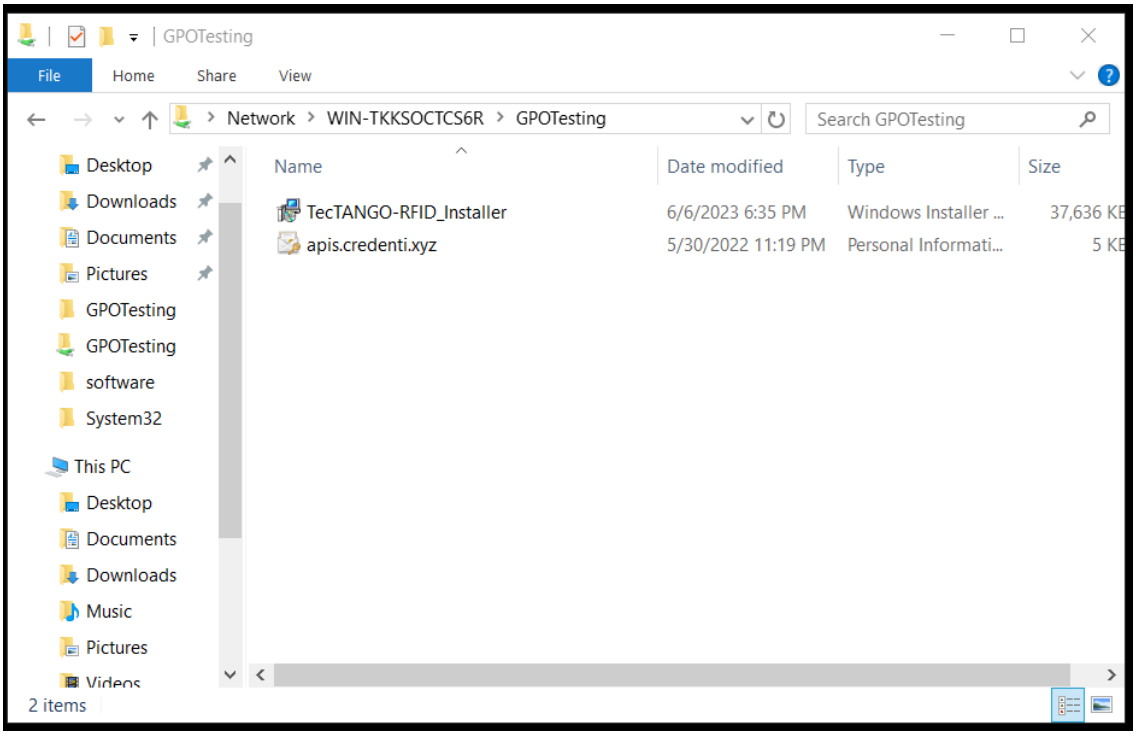
2.1 Create a Shared Network Folder

- Log in to any AD member server with administrator privileges.

- Create a shared network folder where you will store the TecTANGO-RFID installer package (.msi file) for distribution.
- Configure appropriate permissions on the shared folder to allow access to the distribution package.

2.2 Copy the MSI and MST Files

- Copy the TecTANGO-RFID_Installer.MSI file and the corresponding .MST file (if any) to the distribution point.
- Ensure that any additional files such as logos or certificate files mentioned in the MST generation process are also present in the distribution point.



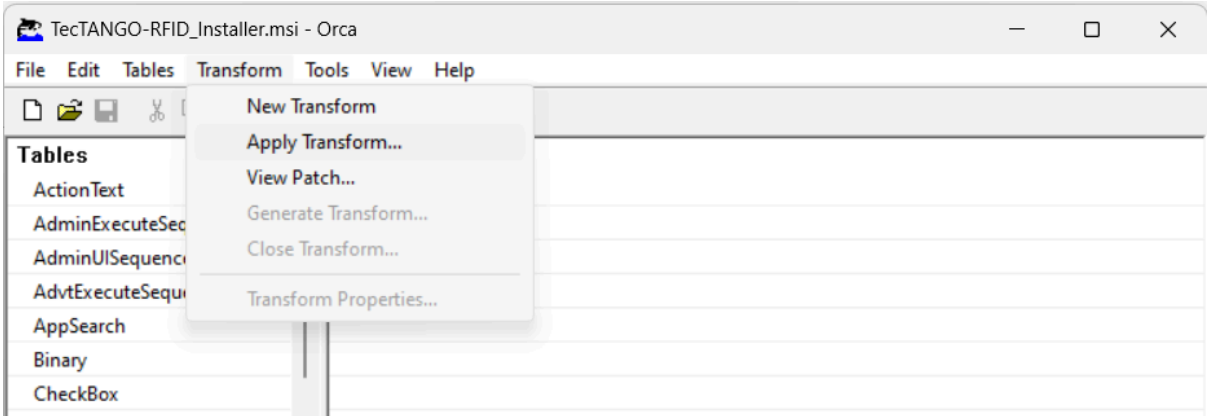
3. Generate the Transformation File (.MST) using ORCA

3.1 Open the TecTANGO-RFID Installer.MSI with ORCA

- Navigate to the folder where the TecTANGO-RFID_Installer.MSI file is located.
- Right-click on the .MSI file and select "Edit with Orca".

3.2 Create a New Transform

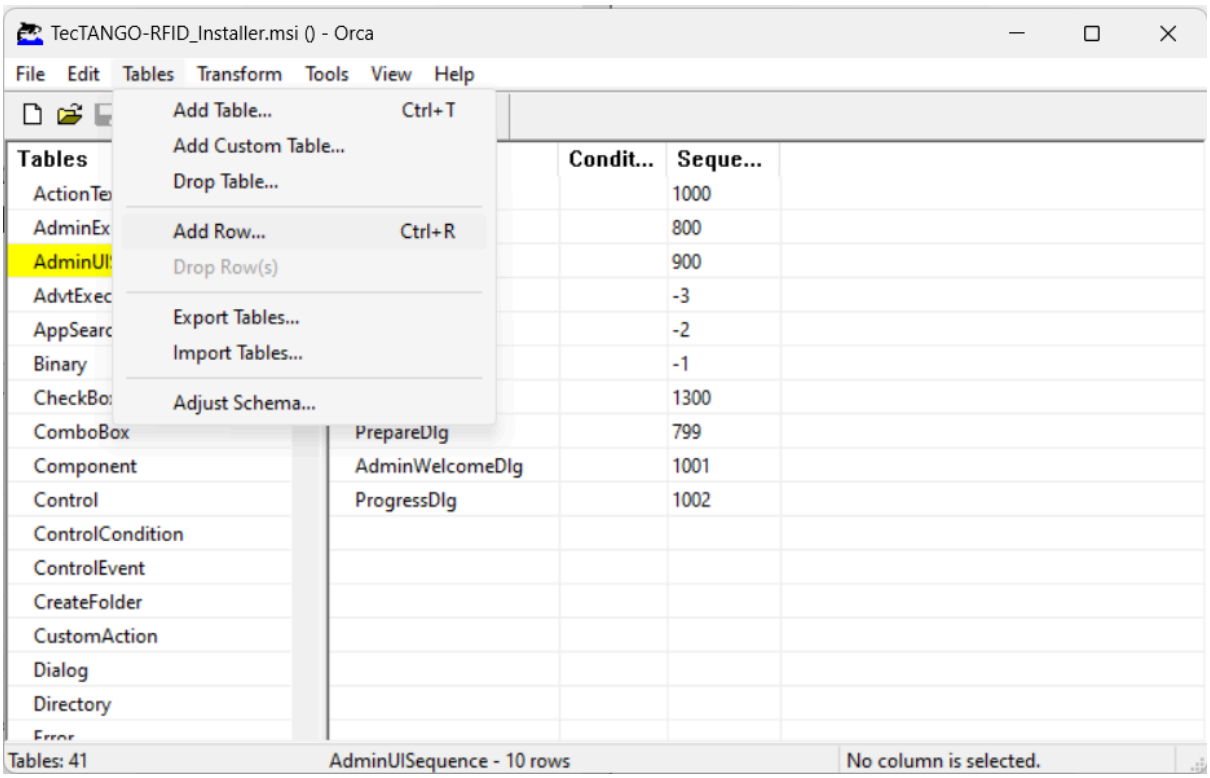
- In the Orca tool, go to the "Transform" menu and click on "New Transform".



3.3 Modify Property Values

- Under the "Tables" section, locate the "Property" table.
- Modify the following property values for the corresponding entries:
- **IAgree**: Set the value to "Yes".
- **MACHINE_MODE**: Set the value to either STANDARD, or KIOSK, based on your requirements.

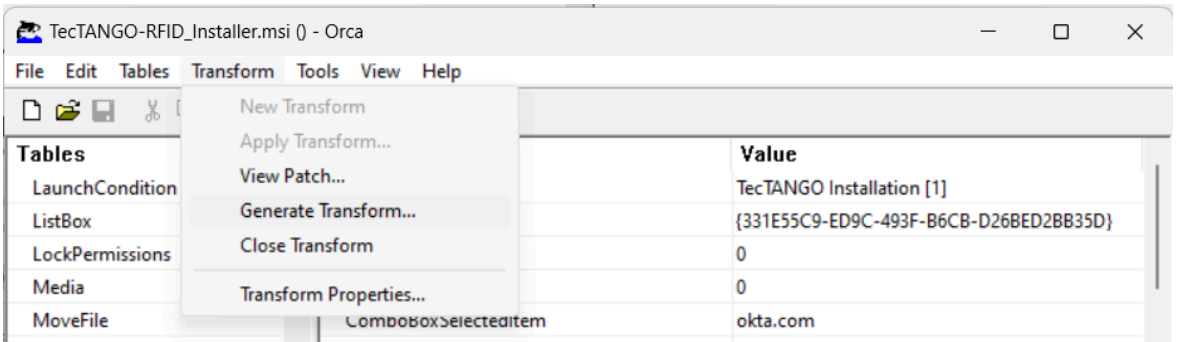
Add additional properties by clicking "Add Row".



- **CLIENTCERTFILE:** Set the value of client certificate file path [from the distribution point (UNC path)].
  Example: \\WIN-TKKSOCTCS6R\GPOTesting\apis.credenti.io.pfx
- **READER**: Set the value to either PcscReader or PcProxReader, based on your requirements.
- **INSTALLTOKEN**: Set the value of Install Token shared by sales team.

3.4 Generate and Save the MST File

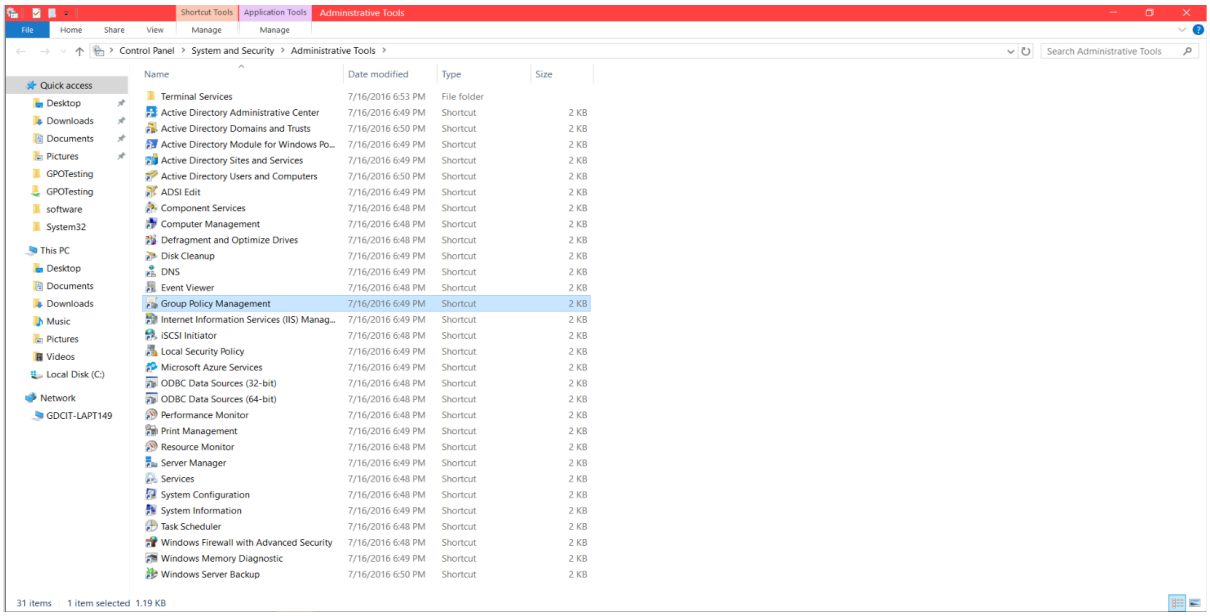
- In the Orca tool, go to the "Transform" menu and click on "Generate Transform".
- Save the MST file in the desired location [the distribution point (UNC path)].



4. Create a Group Policy Object (GPO)

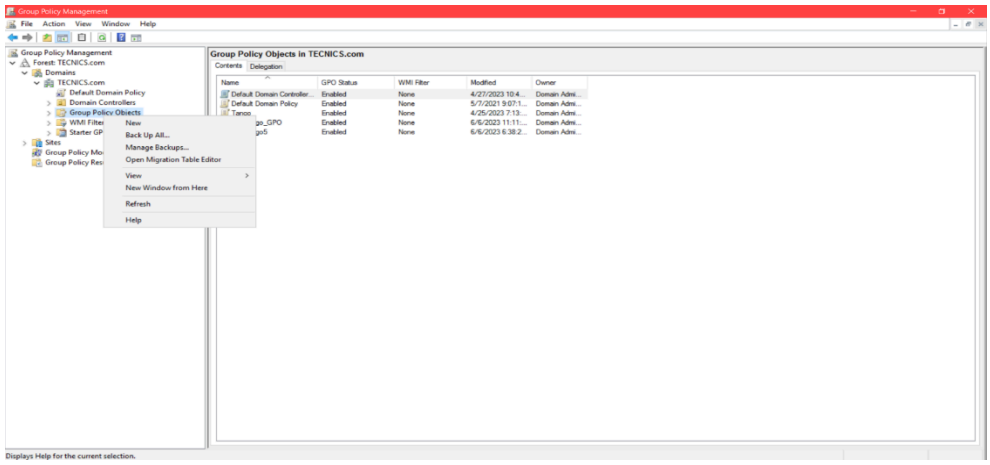
4.1 Open Group Policy Management Console

- Click on the Start button, go to "Programs," select "Administrative Tools," and then click on "Group Policy Management".

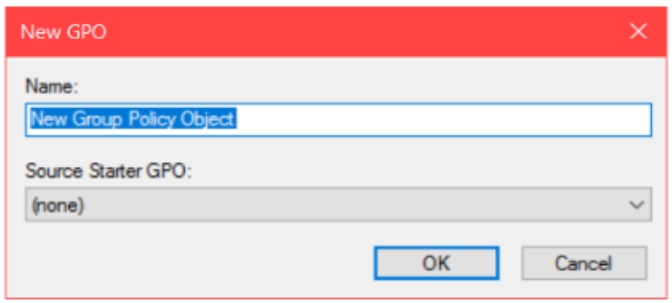


4.2 Create a New GPO

- Navigate to "Forest: YOURDOMAIN" > "Domains" > "YOURDOMAIN" > "Group Policy Objects".
- Right-click on the "Group Policy Objects" folder and select "New".



- Provide a name for the new GPO and click "OK".



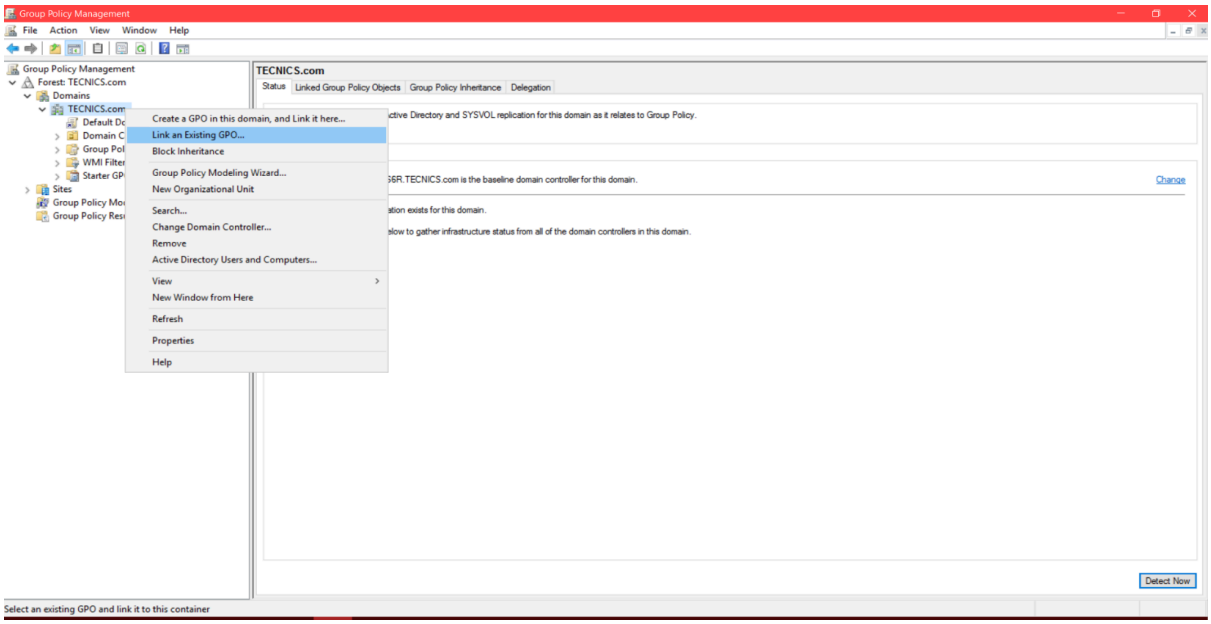
4.3 Configure Security Filtering (Optional)

- Select the new GPO and go to the "Security Filtering" section.
- Add specific computer names or the group "Domain Computers", group to limit the GPO's application.

Skip this step if you want the software deployed on all computers.

4.4 Link the GPO

- Right-click on the "YOURDOMAIN" folder and select "Link an existing GPO".



- Choose the newly created GPO from the list and click "OK".

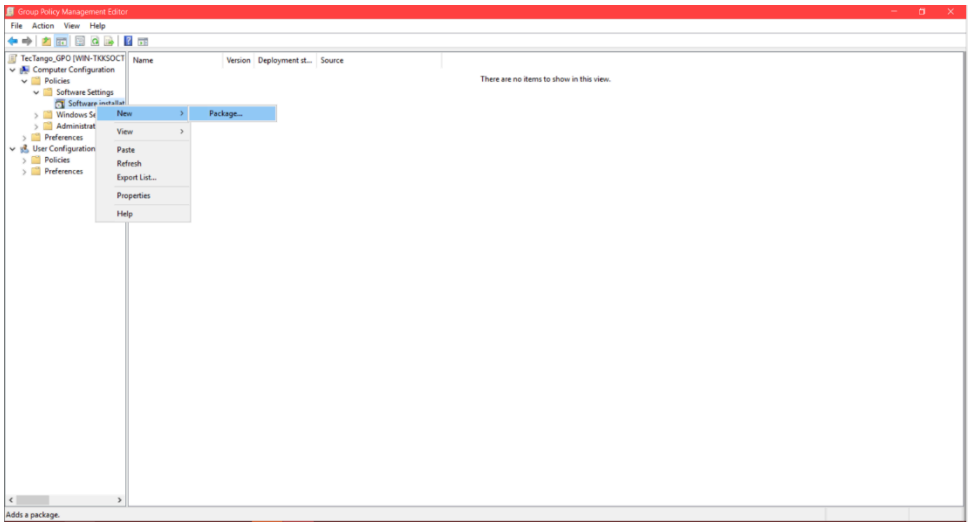
5. Assign the Package

5.1 Open Group Policy Management Editor

- Right-click on the new GPO and select "Edit".

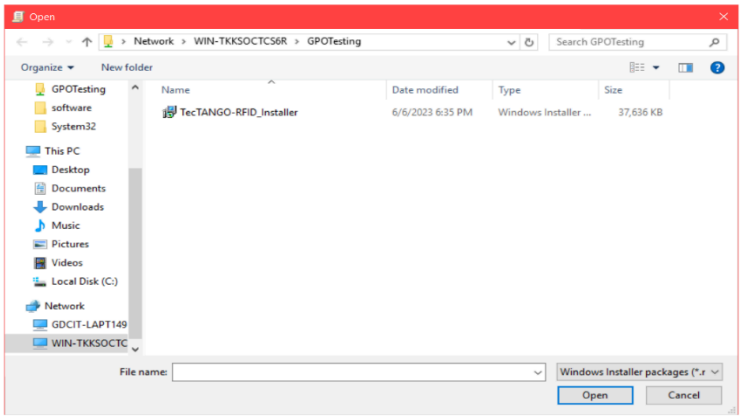
5.2 Navigate to Software Settings

- In the Group Policy Management Editor, go to "Computer Configuration" > "Policies" > "Software Settings" > "Software installations".



5.3 Add a Software Package

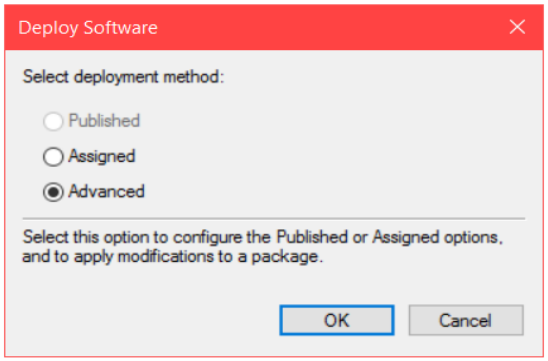
- Right-click inside the empty pane on the right and select "New" > "Software Package".



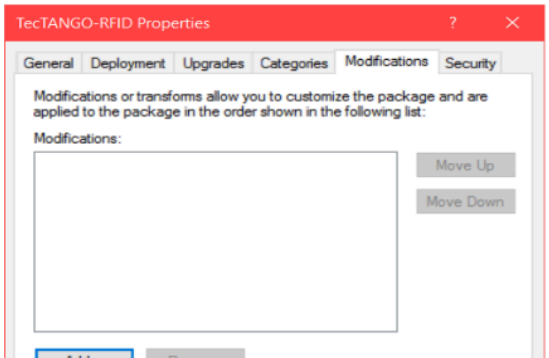
- Enter the full UNC path of the shared installer package (MSI file). Example: \\file server\share\file name.msi. Avoid using the Browse button.
- Click "Open".

5.4 Select Deployment Method and Add MST File

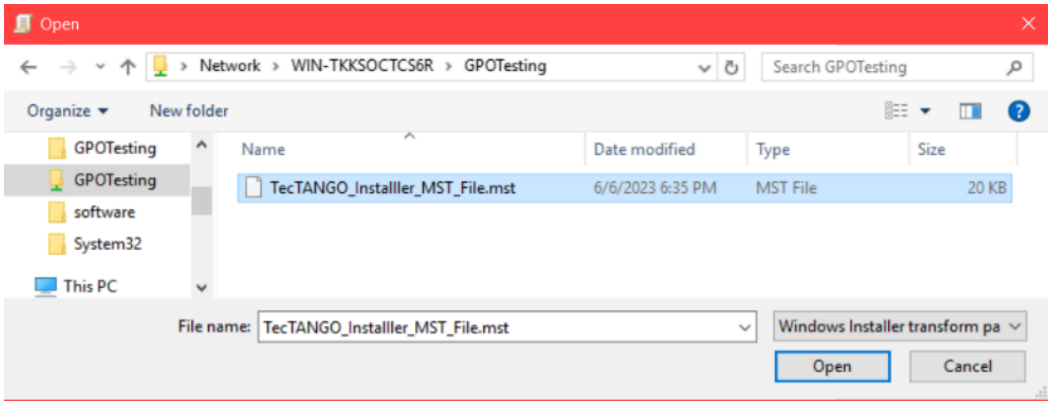
- Select the deployment method as "Advanced" and click "OK".



- Switch to the "Modifications" tab and click "Add".



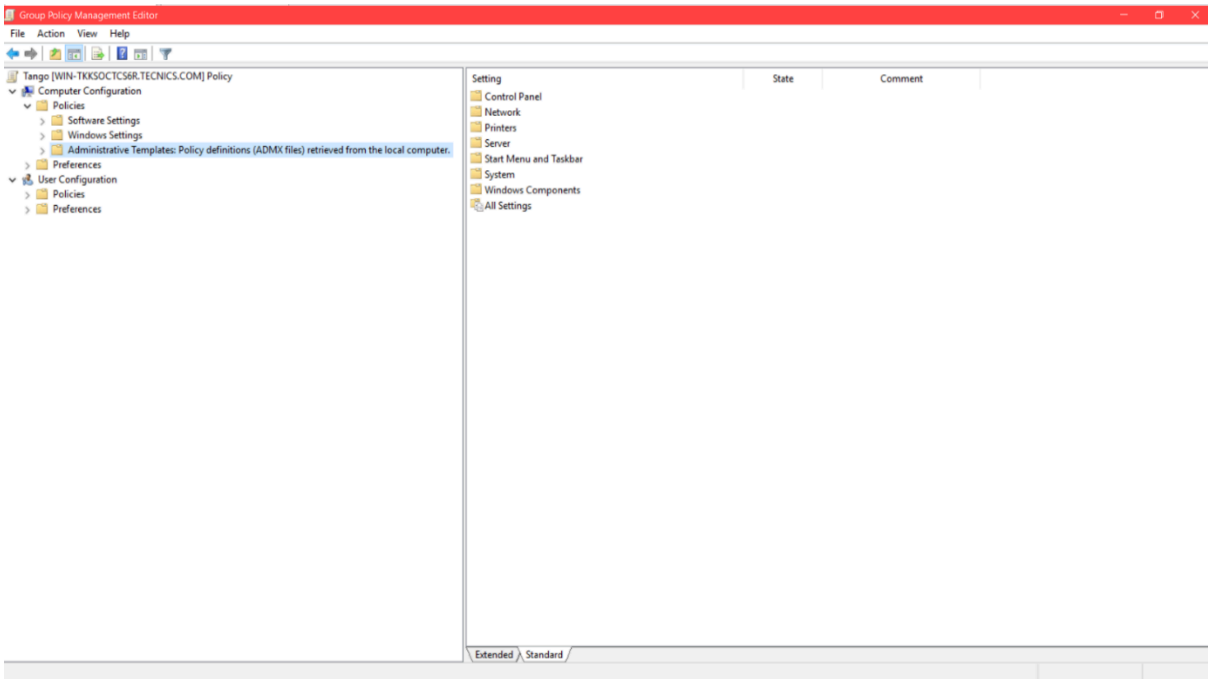
- Browse and select the .MST file from the distribution point (UNC path).



- Click "OK".

6. Changes to Group Policy Object Permissions

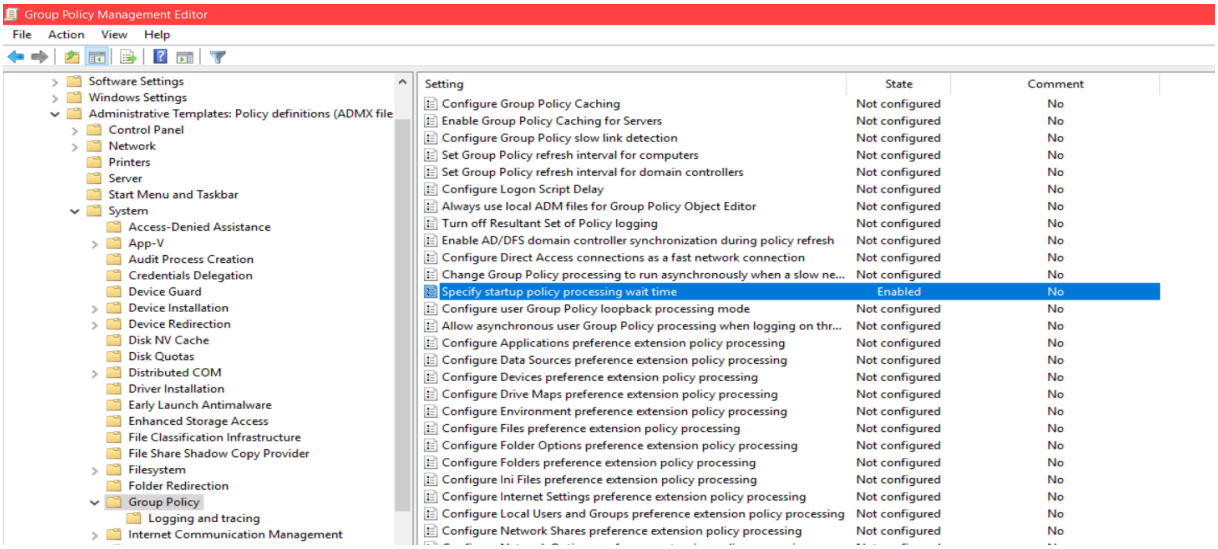
- Navigate to Administrative Templates - In the Group Policy Management Editor, go to "Computer Configuration" > "Policies" > "Administrative Templates Policy definitions…"



6.1 Specify Startup Policy Wait Time:

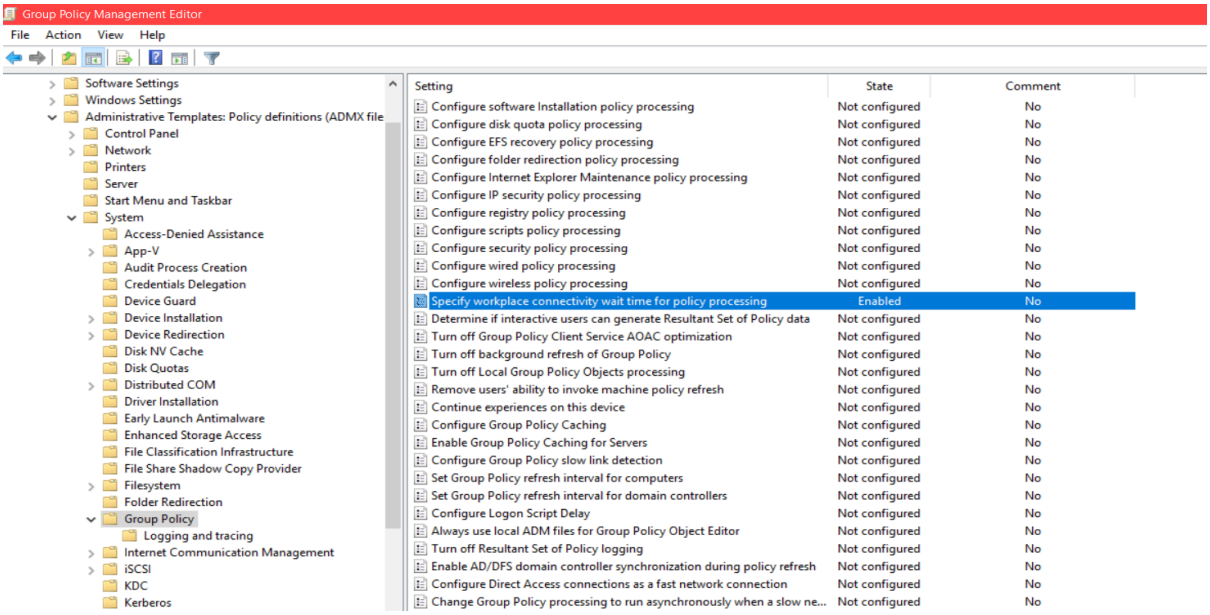
- Under **"Administrative Templates Policy definitions…" > "System" >" Group Policy" locate "Specify startup policy wait time".**
- Double-click on the policy to open the properties.
- Select the "Enabled" option to enable the policy.

- Configure the wait time by entering the desired value in the provided field. The wait time is specified in seconds.
- Click "OK" to save the changes.



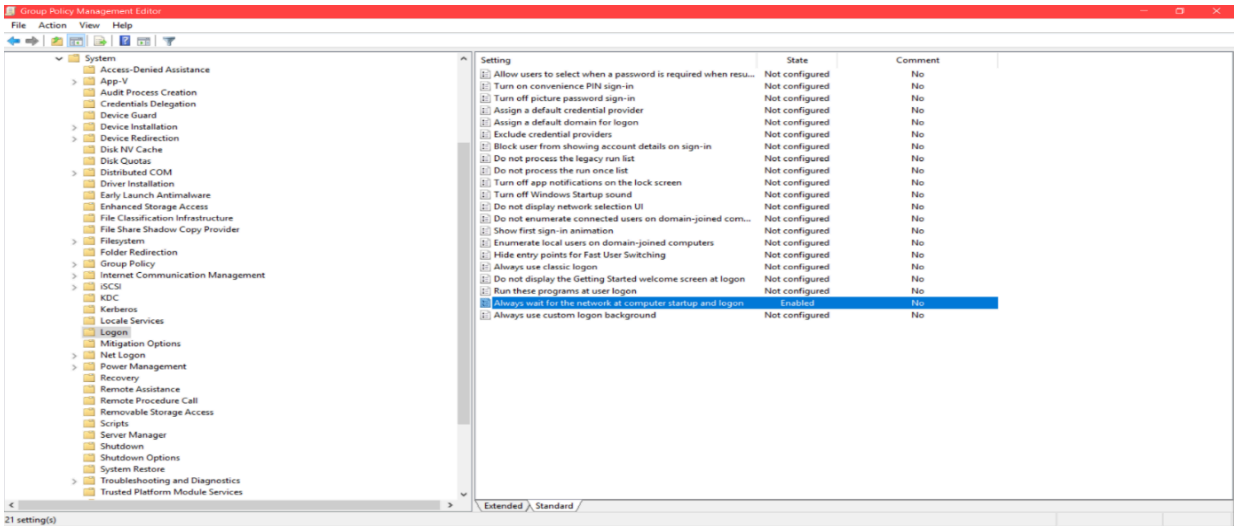
6.2 Specify Workplace Connectivity Wait Time for Policy

- Under **"Administrative Templates Policy definitions…" > "System" > "Group Policy" locate "Specify Workplace connectivity wait time for policy".**
- Double-click on the policy to open the properties.
- Select the "Enabled" option to enable the policy.
- Configure the wait time by entering the desired value in the provided field. The wait time is specified in seconds.
- Click "OK" to save the changes.



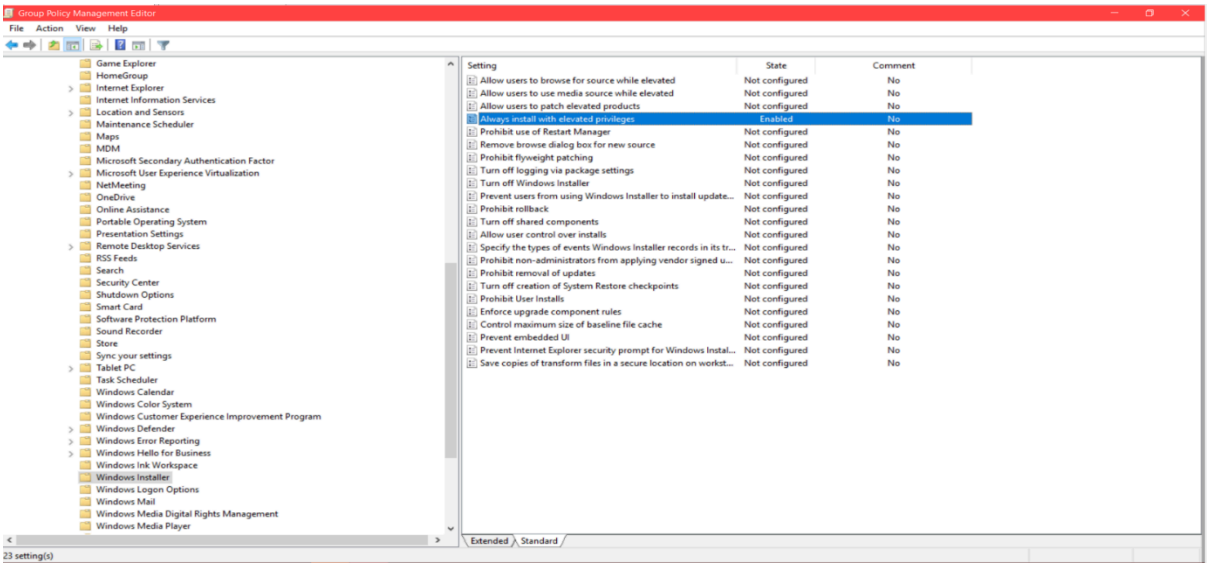
6.3 Always Wait for Network at Computer Startup and Logon

- Under **"Administrative Templates Policy definitions…" > "System" > "Logon" locate "Always Wait for Network at Computer Startup and Logon".**
- Double-click on the policy to open the properties.
- Select the "Enabled" option to enable the policy.
- Click "OK" to save the changes.



6.4 Always Install with Elevated Privileges

- Under **"Administrative Templates Policy definitions…" > "Windows Components" > "Windows Installer" locate "Always Install with Elevated Privileges".**
- Double-click on the policy to open the properties.
- Select the "Enabled" option to enable the policy.
- Click "OK" to save the changes.

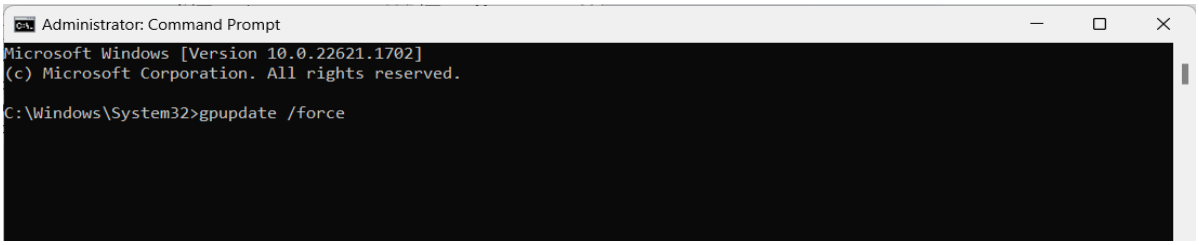


7. Update Group Policy and Restart Client Machines

7.1 Update Group Policy

- Log in to the AD member server as an administrator.

- Open the command prompt as an administrator.
- Run the following **command** to update the policy on all computers: **gpupdate /force**.



7.2 Restart Client Machines

- After completing the update, restart the client machines for the changes to take effect.

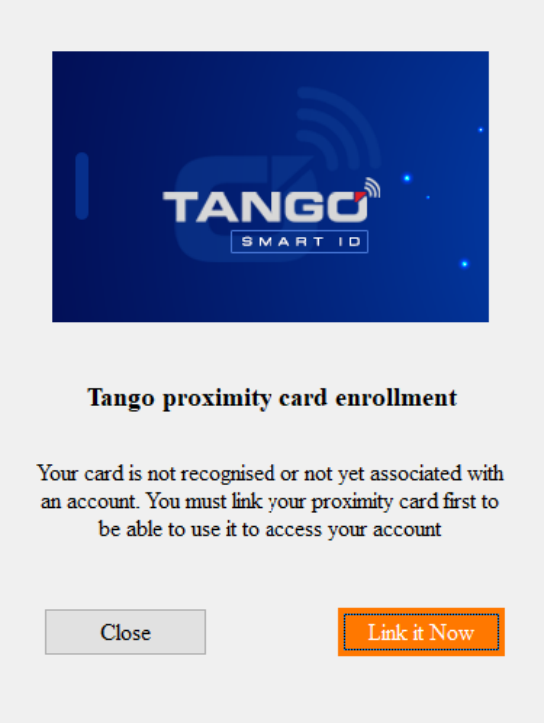
User Experience After Installation

Card Enrollment for the User

In this mode, the workstation or laptop is connected to the internet, and TecTANGO can reach the CyberArk Identity cloud.

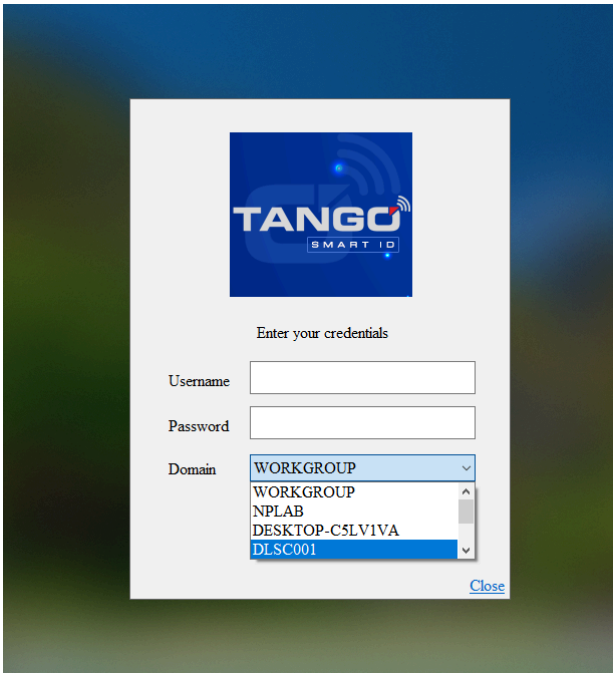
1. Tap the card on the reader.

2. Users will be prompted to link the card to an account. Click on *Link it Now*.



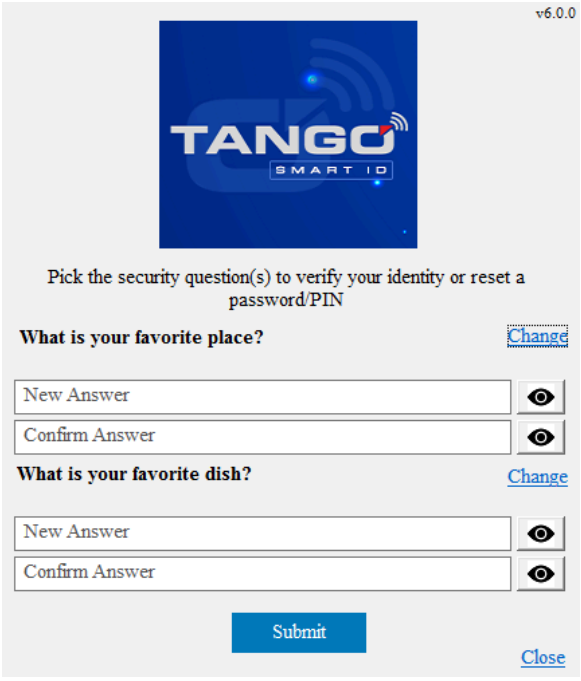
3. User will then be prompted to enter their credentials.

4. Based on the domain of the user, a dropdown menu will appear with all the domains present in the organization, and the user can choose their domain. Click on *Enroll*.



5. Based on the policies configured, the user would be prompted for the below screens.
    a. If PIN is selected as a sign-on policy, they will see a prompt for setting up PIN.

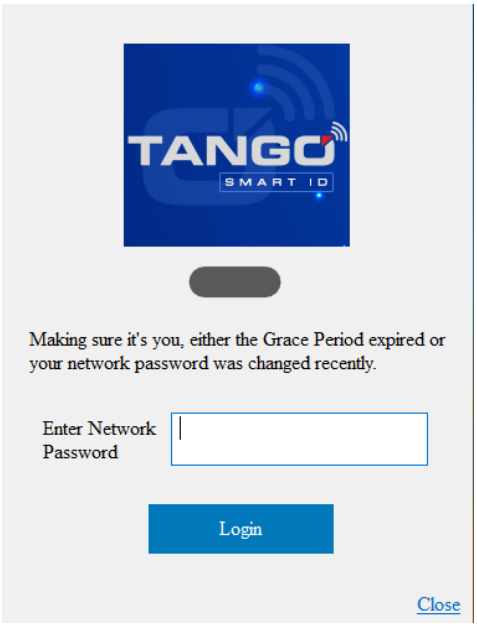
    b. If Security Question is selected as a sign-on policy or recovery factor, the user will see a screen for setting up Security Question(s).



Windows Login in Online Mode

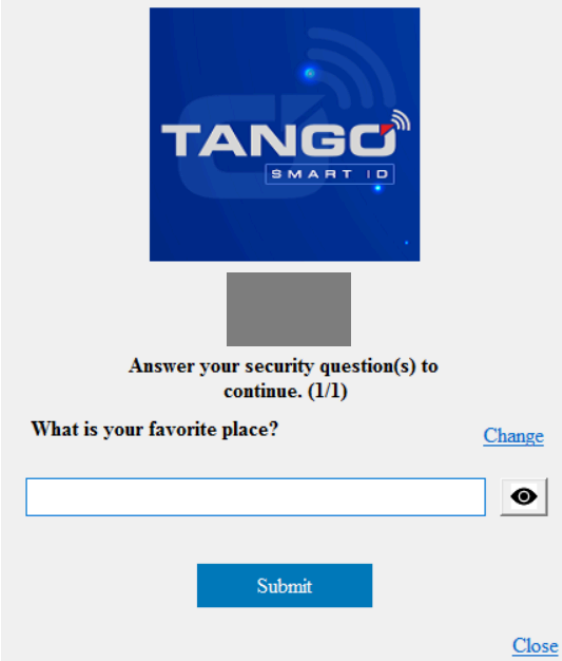
1. User taps the smartcard or proximity card.

2. If Password is set as a policy, they will be prompted for the network password based on the Grace Period applied in the Password Policy.



3. If PIN is set as a policy, they will be prompted to enter the PIN.

4. If Security Question is set as a policy, they will be prompted to complete the authentication.



5. After completing the authentication, the user will be taken to the desktop.
    a. If TecTANGO is in Single User Mode, the user's desktop profile will open.
    b. If TecTANGO is in Kiosk Mode, the shared profile that was set up in the Admin Portal will open.
        i. If TecTANGO is in Kiosk mode and profile selection has been added to the policy, the user can choose between the shared profile or their own personal profile.

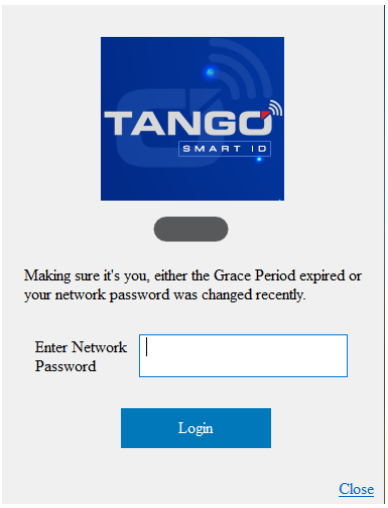
Windows Login in Offline Mode

Note: In order to login to the workstation with TecTANGO while offline, the user must be enrolled and have logged in at least once in online mode.

If the user doesn't have a network connection, the following login experience will occur:

1. User taps the smartcard or proximity card.

2. If Password is set as a policy, they will be prompted for network password based on the Grace Period applied in the Password Policy.
3. If PIN is set as a policy, they will be prompted to enter the PIN.

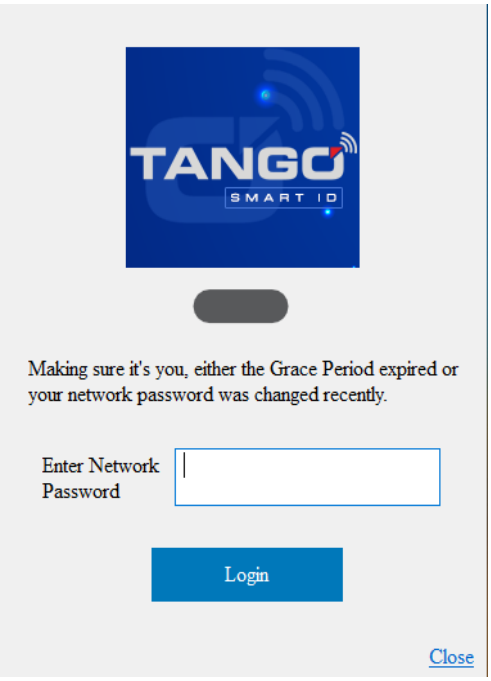


Forgot PIN

If a user forgets their PIN, they can do a self-service PIN reset.

1. On the login screen after they tap their card to the reader, they must click the link that says “I forgot my PIN”.

2. The user then enters their network password, and clicks *Login*.



3. If Security Question is enabled for recovery in the Credenti Admin portal, then they will be prompted to answer the security question(s). This can be more than one question.

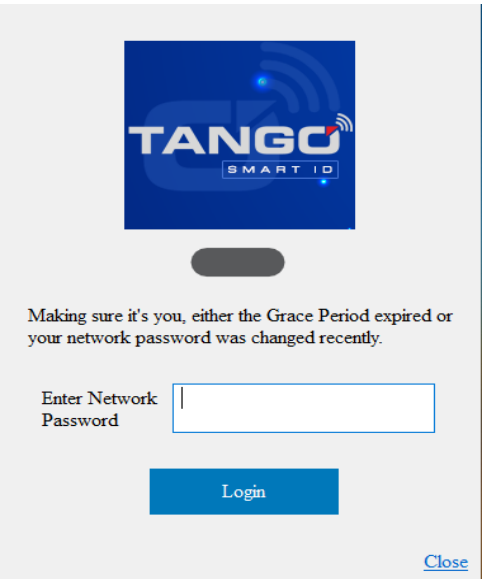
4. The user will then be prompted to create their new PIN.

5. The user will now be able to use this PIN for future logins.

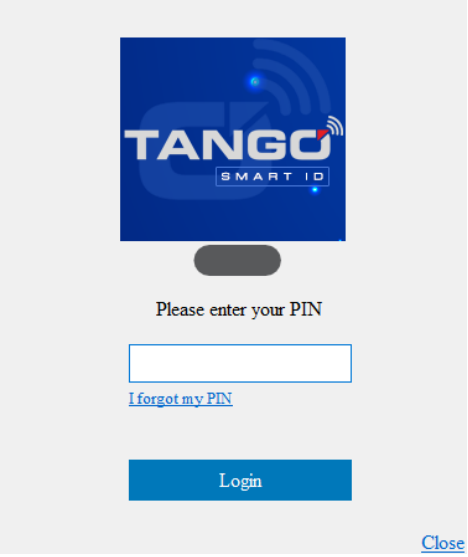
Changed Password

If a user's password has changed, the next time they try to enter their workstation they will be prompted for their new password.

1. The user taps their card to the reader and is prompted for their network password.



2. The user will then be prompted for any secondary MFA such as their PIN or Security Question, if any were configured.

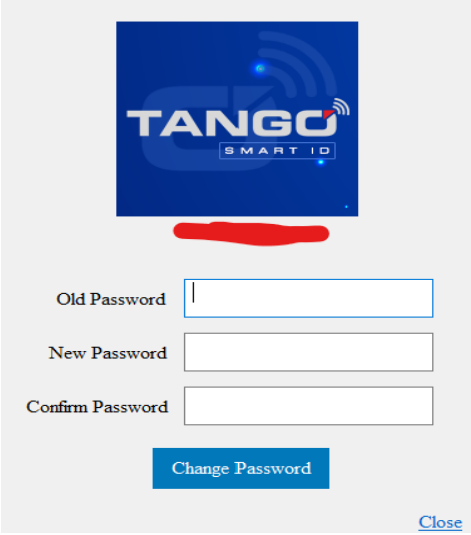


3. The user will then be entered into the workstation.

Expired Password

If a user's password has expired, the next time they try to enter their workstation they will be prompted to create a new password.

1. The user taps their card and is asked to change their password. The user will need to enter their old password, create their new password, and re-enter the new password.



2. The user will then be asked to authenticate into the workstation and will use the new password.

Privacy Shield

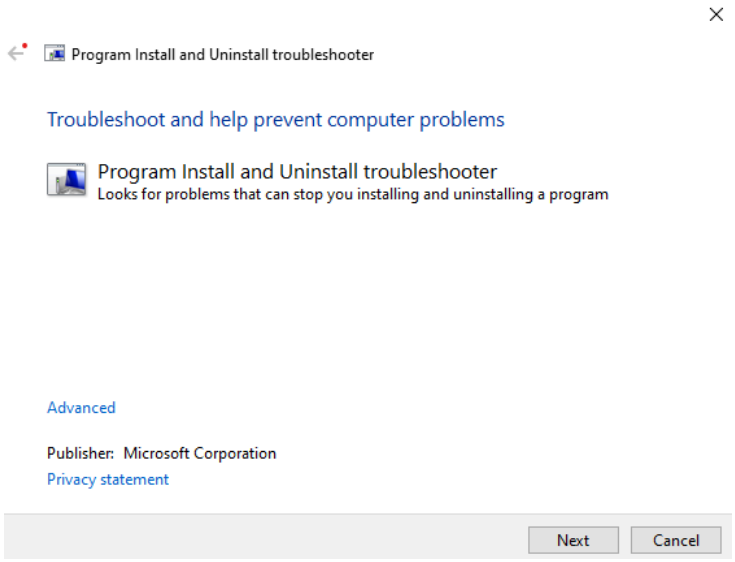
If Privacy shield is enabled, after the idle time out period, the user will see the customized shield.

Uninstall TecTANGO

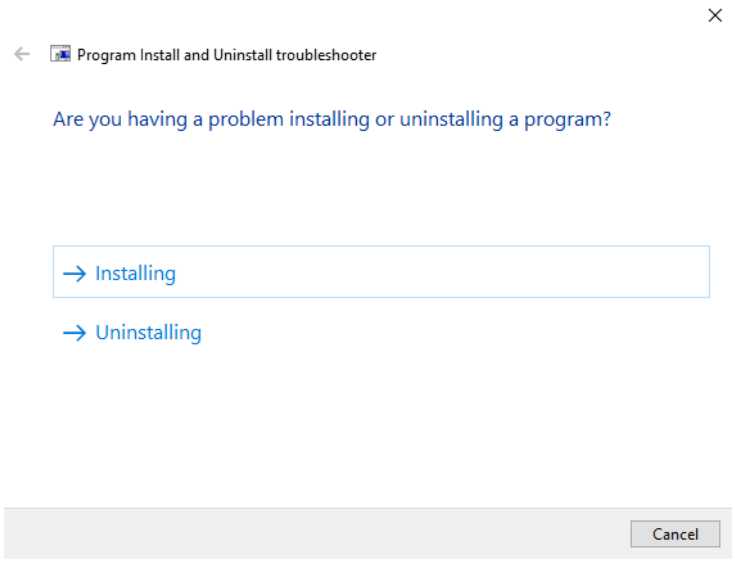
Uninstall Corrupted Installation

In order to uninstall or repair a corrupt installation, please download the tool from below link:
https://support.microsoft.com/en-in/help/17588/windows-fix-problems-that-block-programs-being-installed-or-removed

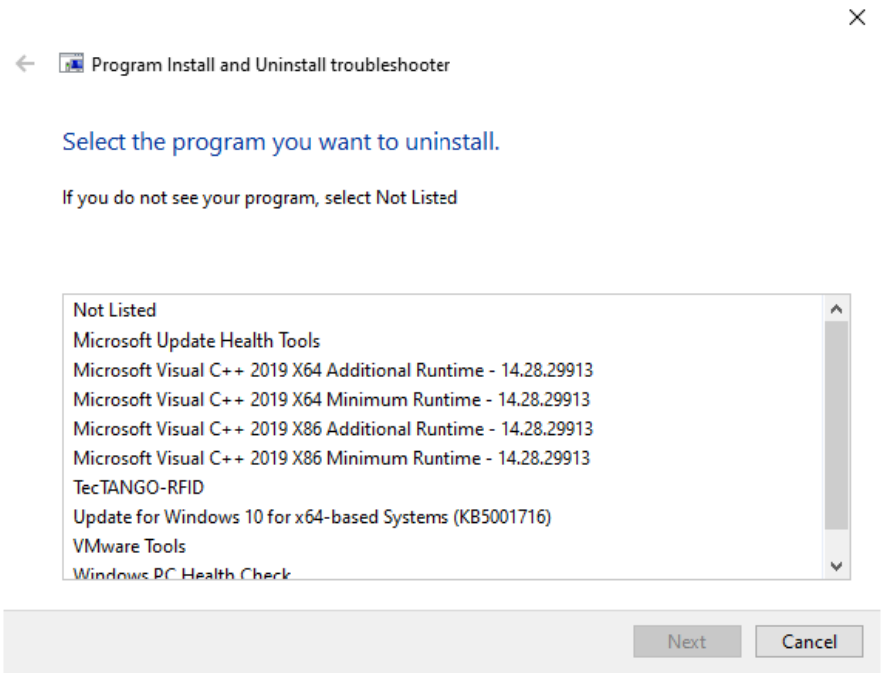
1. Run the downloaded file, and click on Next.



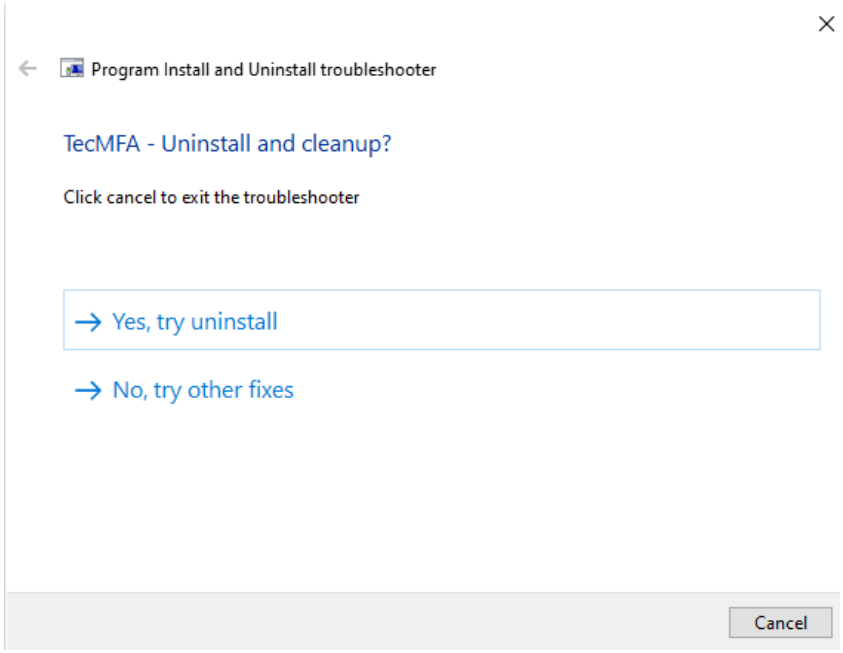
2. Select Uninstalling.



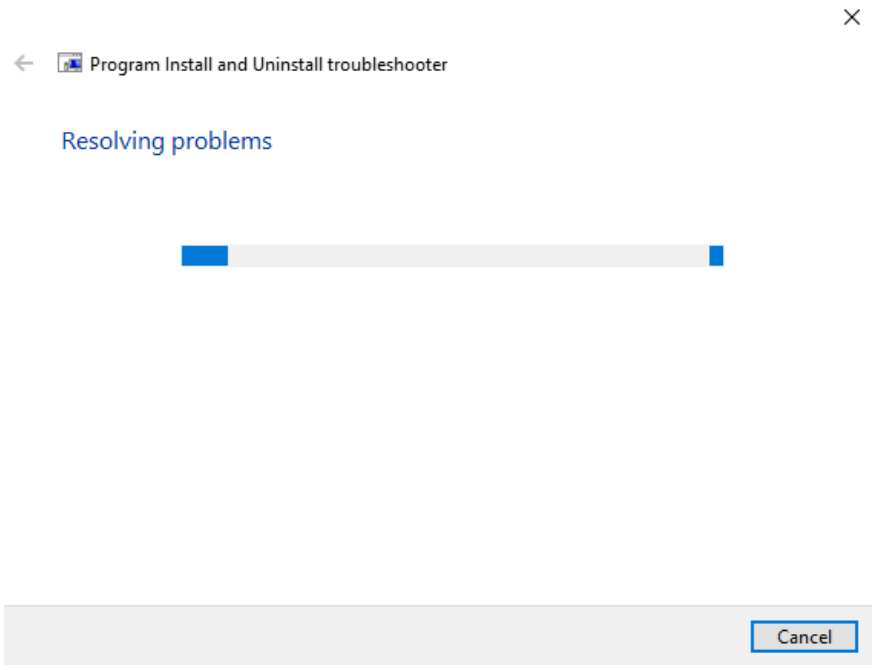
3. Select TecTANGO-RFID, and click on Next.

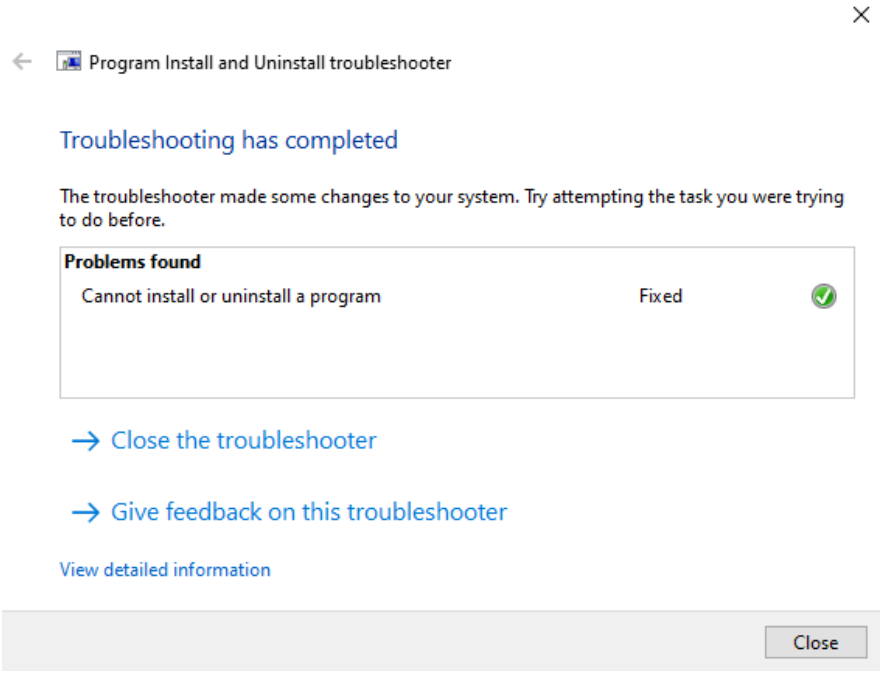


4. Click on Yes, try uninstall.

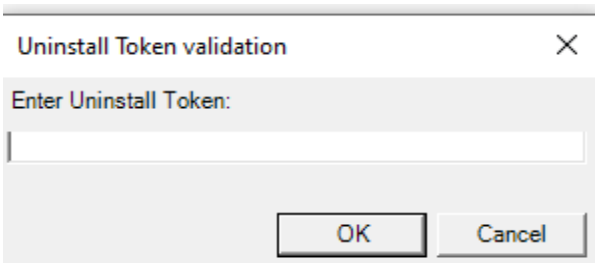


5. The tool will try to resolve the problems and uninstall the application.





6. You will be prompted to validate the Uninstall Token in order to complete the application uninstall. You can find the uninstall token under Account Settings → Account → Uninstall Token in the Credenti Admin Portal.



Uninstall TecTANGO

TecTANGO can be uninstalled from PowerShell by following these instructions. Please note that you will be required to update the Uninstall Token value before running the uninstall command. You can find the uninstall token under Account Settings → Account → Uninstall Token in the Credenti Admin Portal.