

中文：

## 西安理工大学统一身份认证 用户帮助手册

### 一、帐号登录

1. 登录学校应用系统，通常会跳转至统一身份认证界面，输入统一身份认证的帐号：您的学号/工号，密码：统一身份认证的密码进行登录。



2. 7 天免登录功能：勾选了 7 天免登陆后，在同一个主机同一浏览器内可直接关闭浏览器的情况下可实现 7 天不需要再次登录。

备注：点击认证登出后该功能失效。

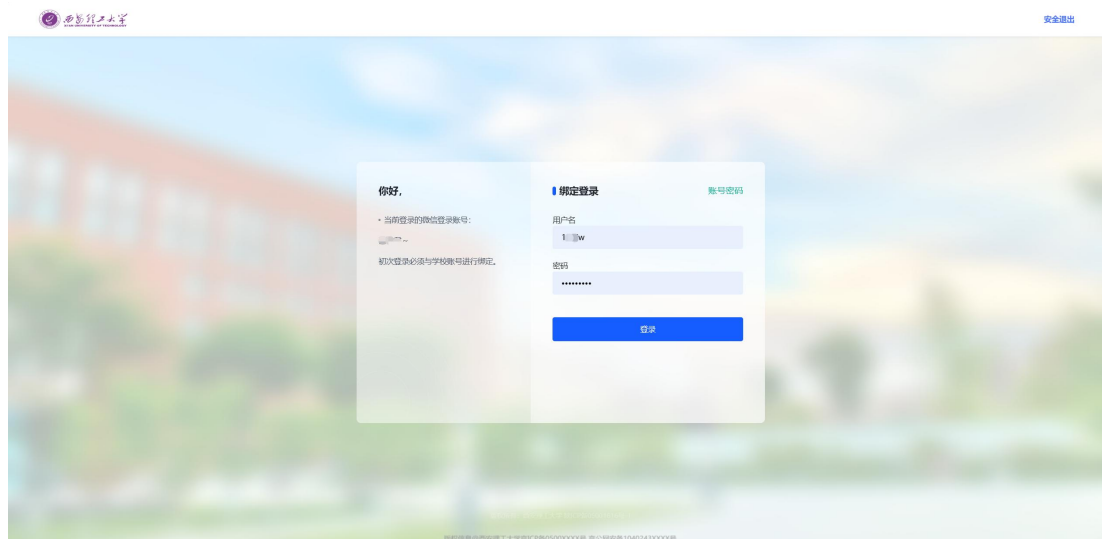


## 二、微信联合登录

1. 登录学校应用系统，通常会跳转至统一身份认证界面，使用微信直接扫描登录页面右侧二维码。



2. 首次微信扫码登录，需要先授权微信并与统一身份认证帐号绑定，填写统一身份认证帐号密码，点击“完成绑定”按钮，验证成功后即绑定成功，后续登录时可直接微信扫码登录。



### 三、生物识别登录

此功能需用户的 pc 或移动设备及浏览器支持人脸或指纹功能，若满足此条件，通过以上两种方式任一种登陆统一身份认证个人中心 <https://ids.xaut.edu.cn/authserver/login>，按图示步骤依次点击，按页面提示开启生物识别登陆；



注：此功能只对本设备本浏览器有效；

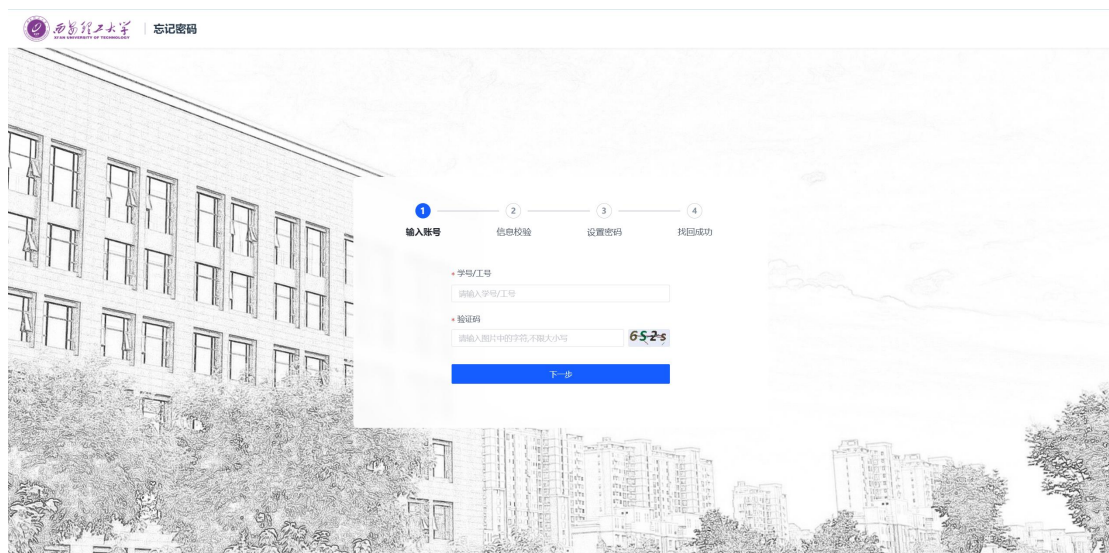
### 四、忘记密码

1. 若用户忘记统一身份认证密码，可点击登录页下方的“忘记密码”，跳转至忘记密码界面。



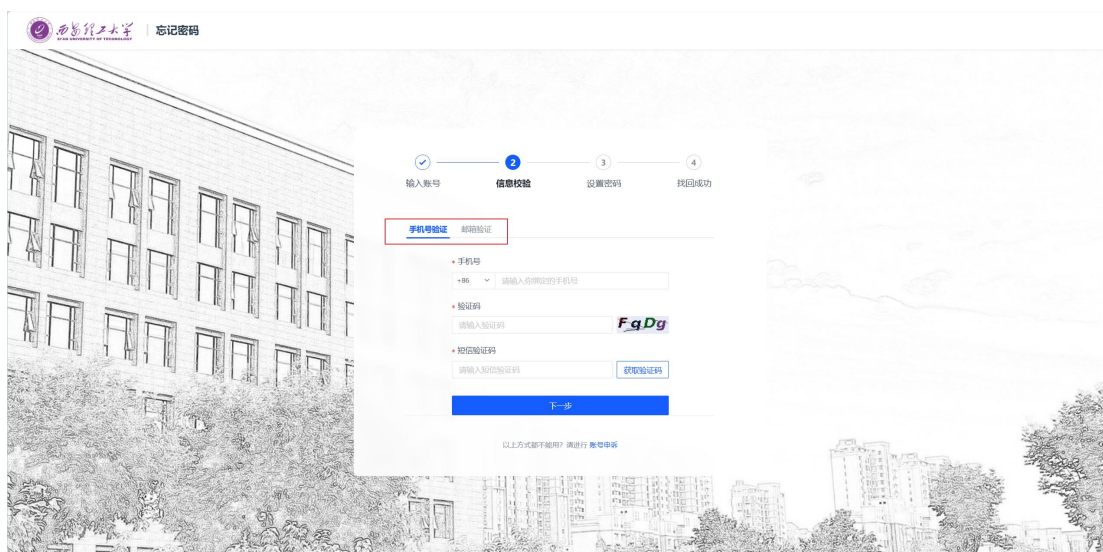
若用户在系统中预留了安全手机或者安全邮箱，则用户可通过安全手机和安全邮箱两种方式，自助重置密码。

2. 输入忘记密码的学号/工号和随机生成的验证码，再点击下一步。

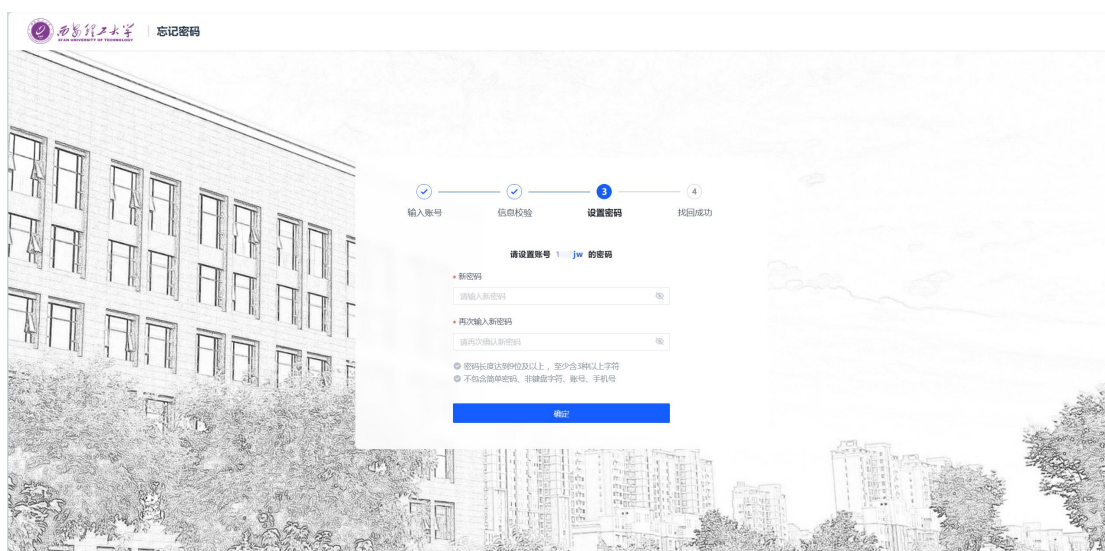


3. 选择找回方式（支持安全手机、安全邮箱），填写提示的信息，系统会给预留的安全手机或安全邮箱，发送验证码，收到验证码后，点击下一步。

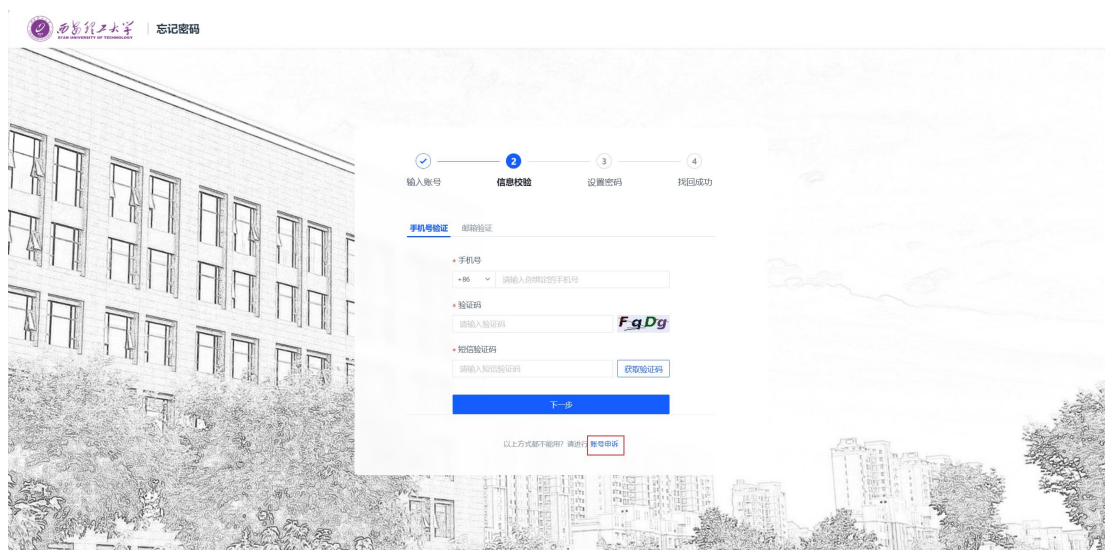




4. 填写新的密码，点击重置密码，则密码重置成功。



5. 若未预留安全手机或安全邮箱，则无法实现自助重置，请点击忘记密码-信息校验 步骤下的 账号申诉 功能进行申诉。



6. 账号申诉界面信息请如实填写,提交后耐心等待管理员审核。  
审核通过后,您预留的手机会收到重置后的密码短信,请注意查收并及时登陆统一身份认证进行密码修改及安全手机、邮箱绑定。

账号申诉

● 为保障您的账号申诉成功,请认真填写以下信息!

**基本信息**

真实姓名

学号/部门

证件类型

证件号码

**上传申诉照片** ● 支持JPG/PNG格式,大小不超过5M

**联系方式**

中国大陆 +86

请输入验证码

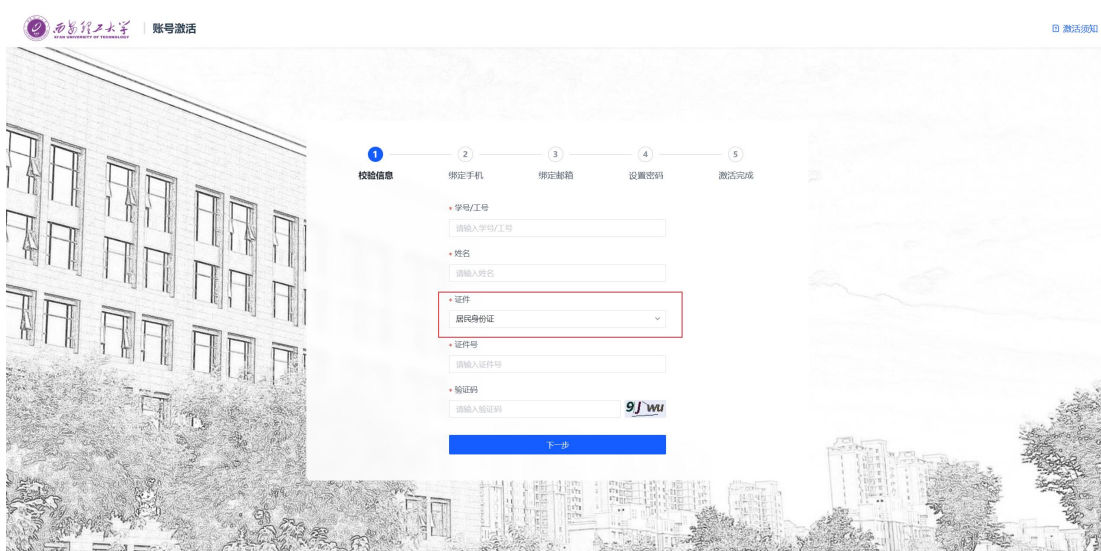
☐ 申诉成功后,若手机号码能联系其他人请选,自动绑定此账号

## 五、帐号激活

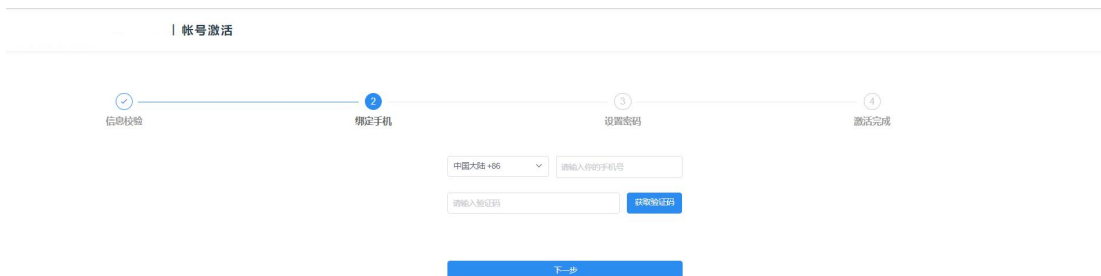
1. 若用户为新进学生或者老师,可点击登录页下方的“帐号激活”,跳转至帐号激活界面。



2. 进入“帐号激活”页面后，用户需要填写自己的学号/工号、姓名、证件号码。备注：非外籍人员默认证件类型为身份证号，外籍人员默认为护照。



3. 填写完成信息后点击下一步，需要您再绑定下您的手机号。



4. 输入手机号点击获取验证码，您会收到一个短信验证码，输入



绑定即可，此操作是为了后续您忘记密码找回密码使用。

帐号激活

1 信息校验 2 绑定手机 3 设置密码 4 激活完成

中国大陸 +86 请输入您的手机号

请输入验证码 获取验证码

下一步

5. 绑定完成后进入下一步，设置您的密码。（密码长度须达到9位及以上，至少含3种以上字符）

西安理工大学 帐号激活 激活须知

1 信息校验 2 绑定手机 3 绑定邮箱 4 设置密码 5 激活完成

检测到您在我校已有身份证号，且已绑定手机 139\*\*\*\*2000 和邮箱 w\*\*\*\*\*@xlu.com，如需修改，请激活后至账号与安全页面修改

请设置账号 w\*\*\*\*\* 的密码

新密码 请输入新密码

再次输入新密码 请再次输入新密码

密码长度达到9位及以上，至少含3种以上字符  
不包含简单密码、非键盘字符、数字、手机号  
☒ 设置当前账号为常用账号

确定

6. 完成后点击去登录即可。

西安理工大学 帐号激活 激活须知

设置密码成功

1 信息校验 2 绑定手机 3 绑定邮箱 4 设置密码 5 激活完成

账号绑定成功  
请牢记下列的登录账号

前往登录

## 六、认证登录后功能介绍



## 1、帐号安全界面

### 1) 设置帐号

该页面主要功能是：用户可修改登录密码、设置安全问题、邮箱绑定、手机号绑定，以便忘记密码找回密码。



### 2) 第三方帐号

该页面主要功能是：用户可绑定微信方便快捷登录。



### 3) 关联帐号

该页面主要功能是：若用户有多个帐号在此页面可设置一个帐号为默认帐号，设置了默认帐号后，用户在手机验证码登录或者联合登录后进入为默认帐号。



#### 4) 生物识别

参见本文第四部分内容；

#### 5) 安全令牌

当开启二次验证时，可使用安全令牌进行验证；



## 2、认证记录界面

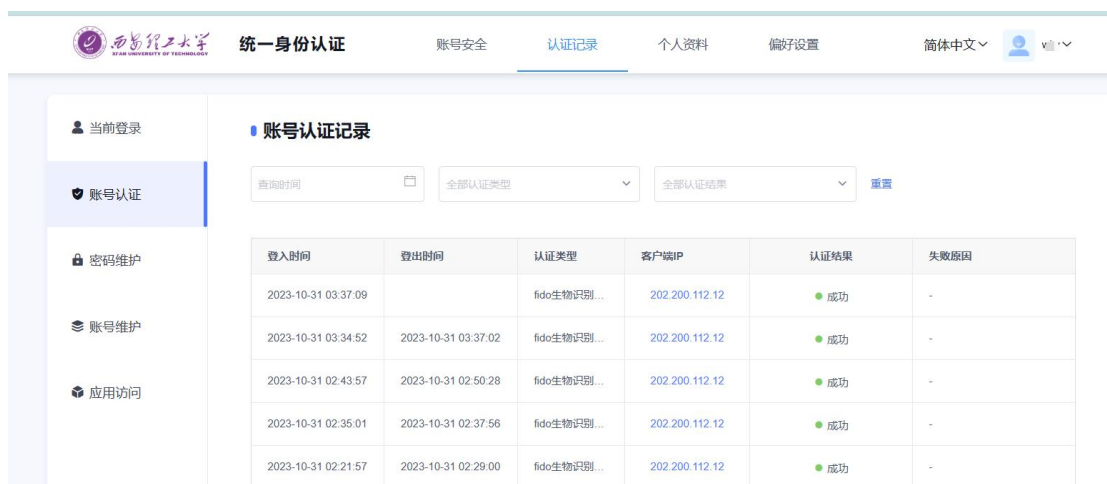
### 1) 当前登录

在此页面用户可查看当前登录的帐号信息，以及免登录模式登录情况，并且可以进行移除操作。



## 2) 帐号认证记录

在此页面记录用户本帐号的认证登录情况。可通过时间、登录类型以及认证结果查看自己帐号的登录记录。



## 3) 密码维护记录

在此页面记录了用户本帐号的密码维护记录。



当前登录  
账号认证  
密码维护  
账号维护  
应用访问

### 密码维护记录

查询时间:  全部操作类型:  全部操作结果:  [重置](#)

| 维护时间                | 操作类型     | 客户端IP          | 操作结果 |
|---------------------|----------|----------------|------|
| 2023-10-31 03:16:10 | 账号激活修改密码 | 202.200.112.12 | 成功   |
| 2023-10-30 21:11:27 | 管理员修改密码  |                | 成功   |
| 2023-10-30 15:01:07 | 管理员修改密码  |                | 成功   |
| 2023-10-30 14:54:12 | 管理员修改密码  |                | 成功   |
| 2023-10-30 11:15:01 | 管理员修改密码  |                | 成功   |
| 2023-10-27 22:36:50 | 管理员修改密码  |                | 成功   |

#### 4) 帐号维护记录

在此页面记录了用户本帐号的维护情况，例如在什么时间段绑定了手机号、邮箱等情况。

当前登录  
账号认证  
密码维护  
账号维护  
应用访问

### 账号维护记录

查询时间:  全部操作类型:  全部操作结果:  [重置](#)

| 维护时间                | 操作类型          | 客户端IP           | 操作结果 |
|---------------------|---------------|-----------------|------|
| 2023-10-27 11:04:16 | 自助编辑账号-绑定邮箱   | 202.200.127.157 | 成功   |
| 2023-10-27 11:03:04 | 自助编辑账号-邮箱解除绑定 | 10.46.55.61     | 成功   |
| 2023-10-27 11:02:38 | 自助编辑账号-绑定邮箱   | 10.46.55.61     | 成功   |
| 2023-10-27 11:01:14 | 自助编辑账号-邮箱解除绑定 | 10.46.55.61     | 成功   |
| 2023-10-27 11:00:28 | 自助编辑账号-绑定邮箱   | 10.46.55.61     | 成功   |

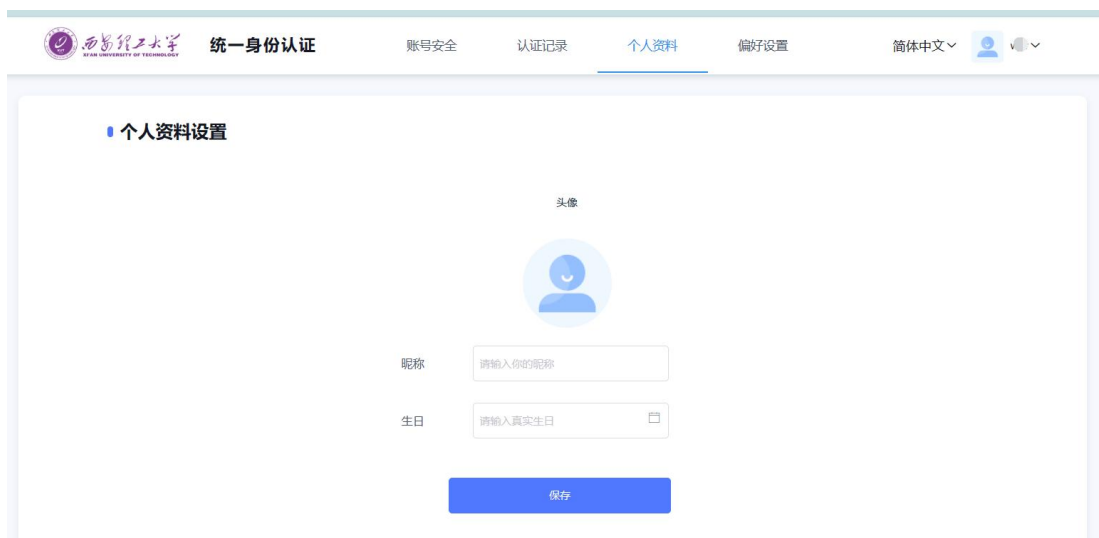
#### 5) 应用访问记录

在此页面记录了用户本帐号的应用访问情况。



### 3. 个人资料

可以设置自己的头像、昵称、生日，当管理员开启允许使用昵称登陆功能时，统一身份认证的账号可以为自己设置的昵称。



### 4. 偏好设置

设置是否允许自己的统一身份认证账号只能在一个浏览器登录；  
设置密码变动后是否通过短信、邮箱进行提醒；



西安理工大学信息化管理处

2023 年 10 月 31 日

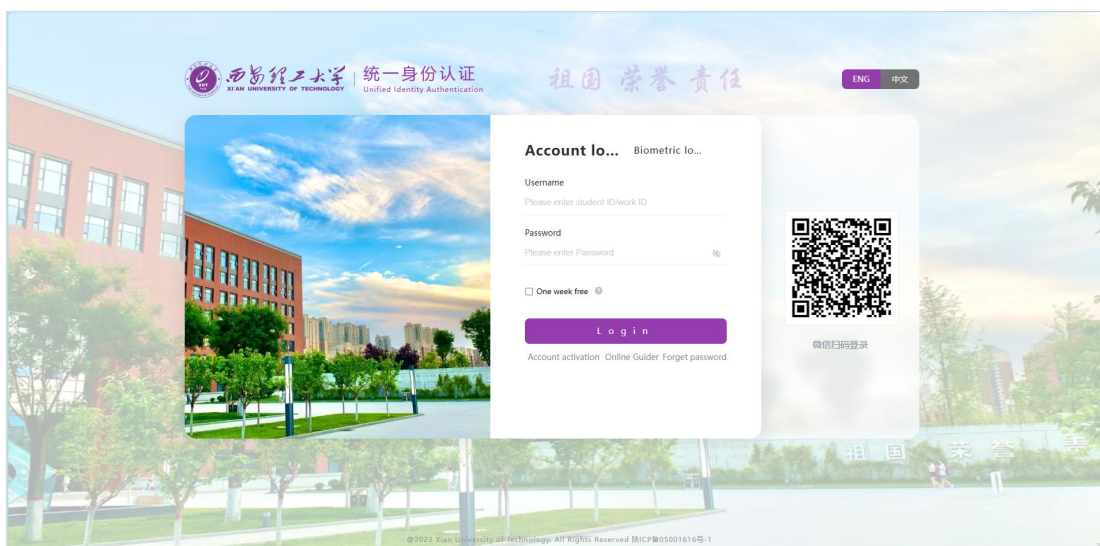


## English:

# Xian University of Technology Unified Identity Authentication User Manual

## 1.Account Login

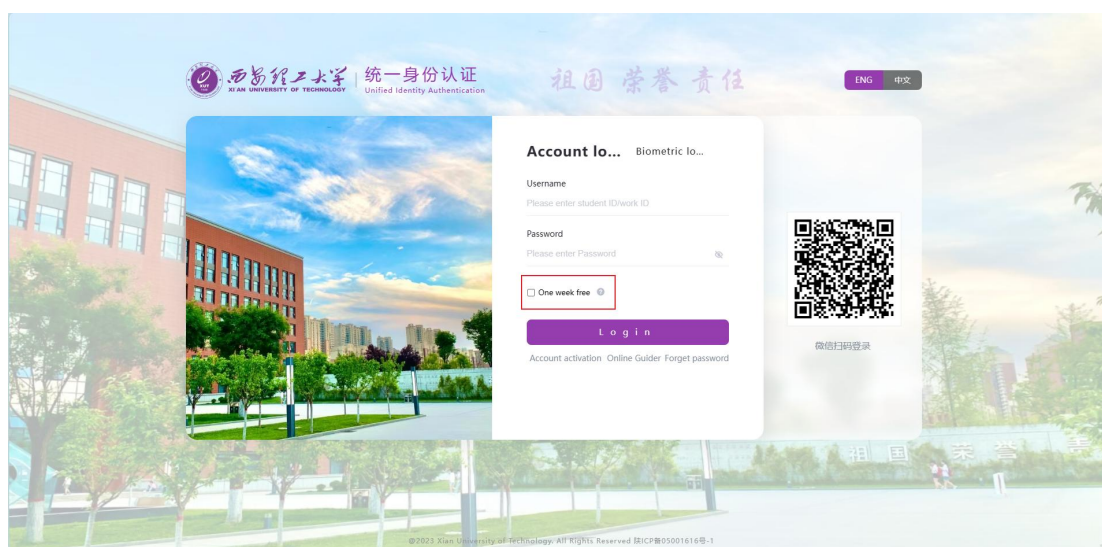
1. To log in to the school application system, you will usually be redirected to the unified identity authentication interface, where you need to enter your unified identity authentication account: your student/employee number, and password: the password for unified identity authentication.



2. 7-day free login function: After checking the 7-day free login option, you can close the browser directly on

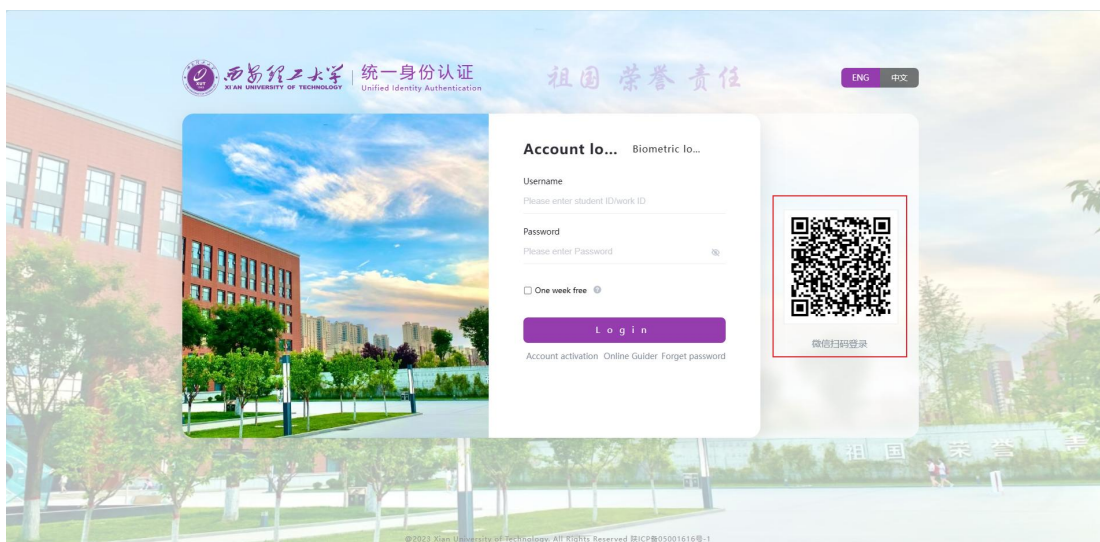
the same machine and the same browser, and you can achieve 7 days without logging in again.

Note: This function will be invalid after clicking authentication logout.

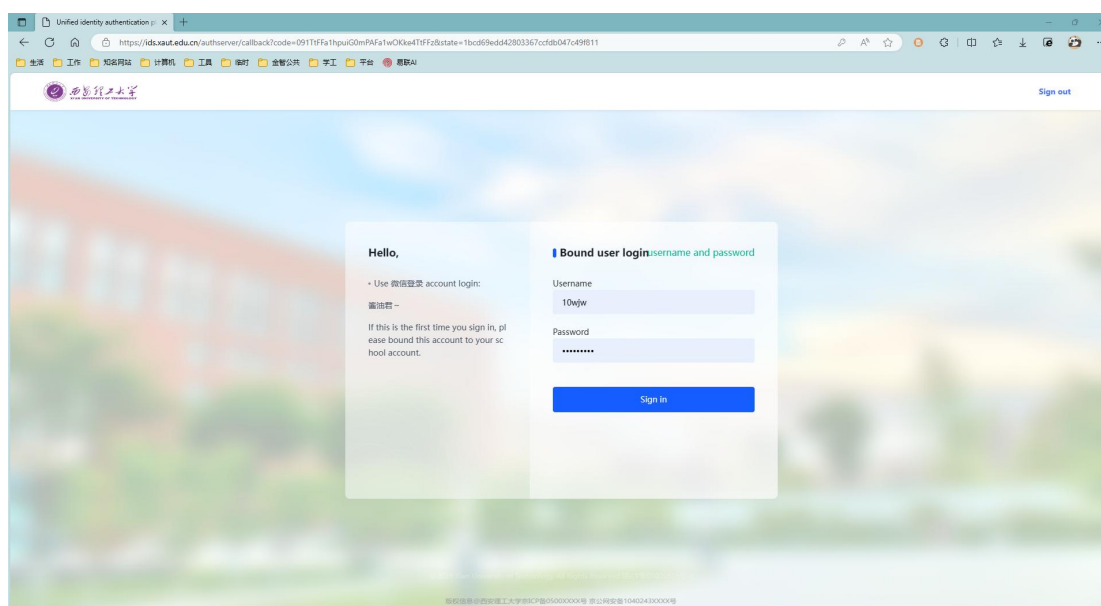


## 2. WeChat Joint Login

1. To log in to the school application system, you will usually be redirected to the unified identity authentication interface, where you can use WeChat to directly scan the QR code on the right side of the login page.



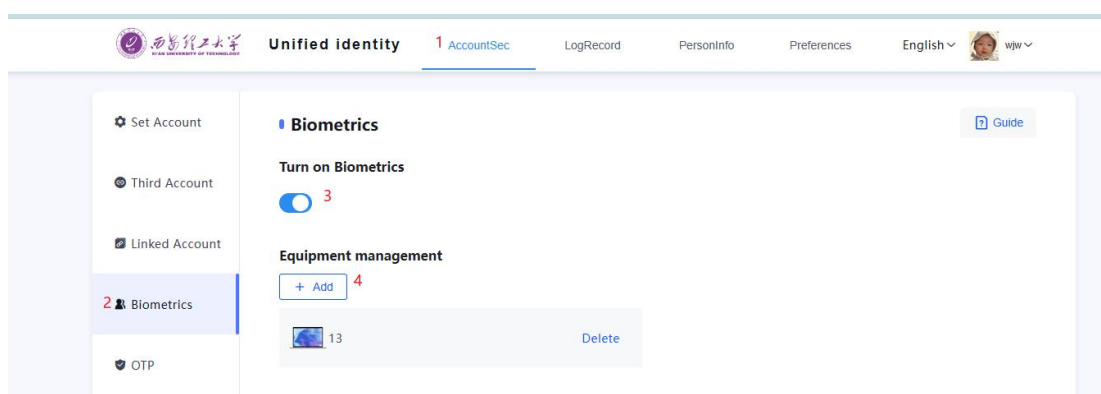
2. The first time you scan the code with WeChat, you need to authorize WeChat and bind it with your unified identity authentication account. Fill in your unified identity authentication account password and click the “Complete Binding” button. After successful verification, the binding is successful, and you can directly scan the code with WeChat to log in later.





### 3. Biometric Login

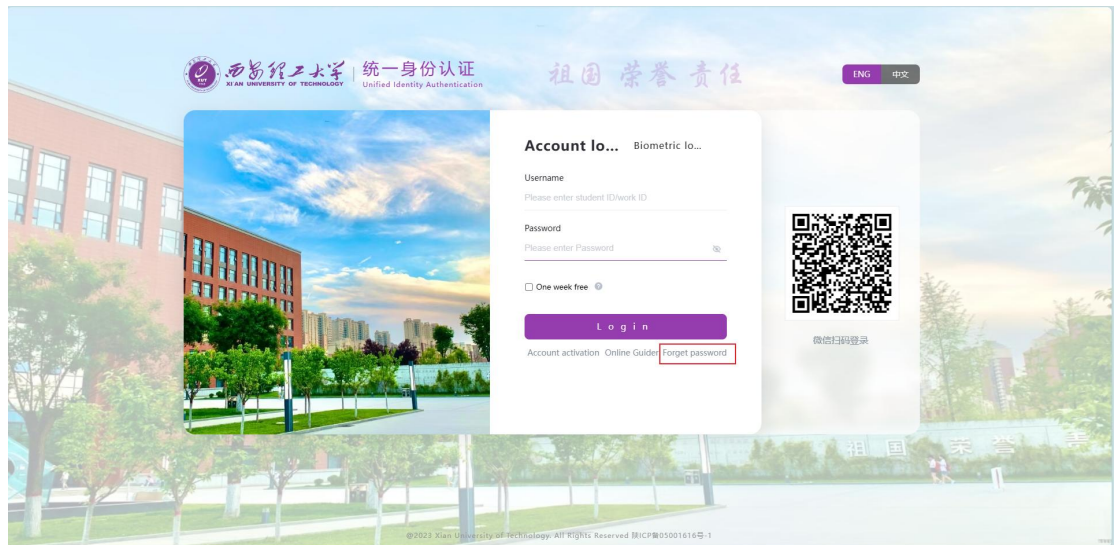
This function requires that your PC or mobile device and browser support face or fingerprint functions. If this condition is met, log in to the unified identity authentication personal center through either of the above two methods <https://ids.xaut.edu.cn/authserver/login>, click on the steps shown in the figure in turn, and follow the page prompts to turn on biometric login;



Note: This function is only valid for this device and this browser;

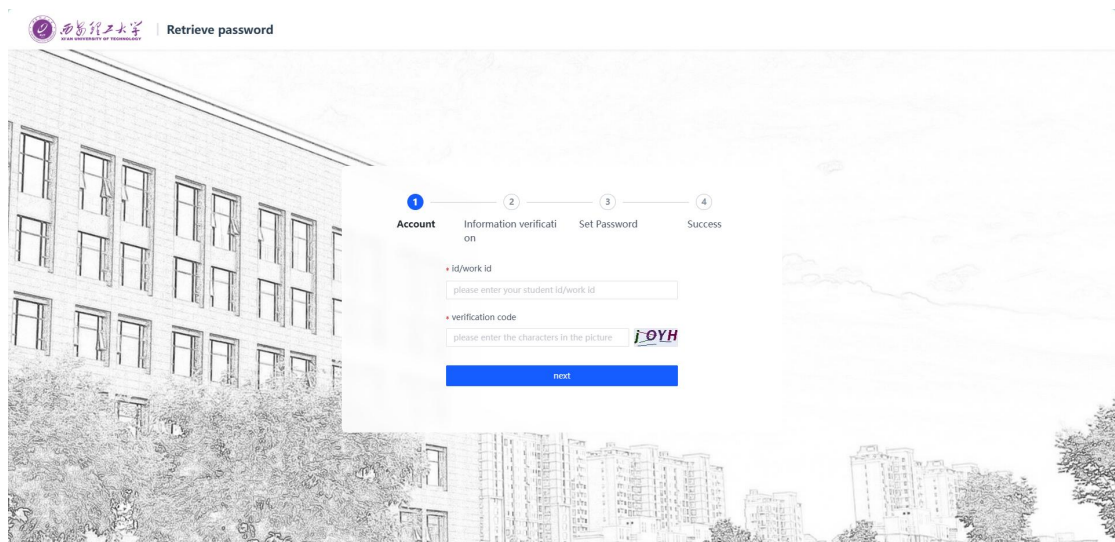
### 4. Forgot Password

1. If you forget your unified identity authentication password, you can click "Forgot Password" at the bottom of the login page and jump to the forgot password interface.



If you have reserved a security phone or security email in the system, you can reset your password by yourself through two methods: security phone and security email.

2. Enter the student/employee number and randomly generated verification code of the forgotten password, and then click Next.



3. Choose a retrieval method (support security phone and security email), fill in the prompted information, and the system will send a verification code to your reserved security phone or security email. After receiving the verification code, click Next.

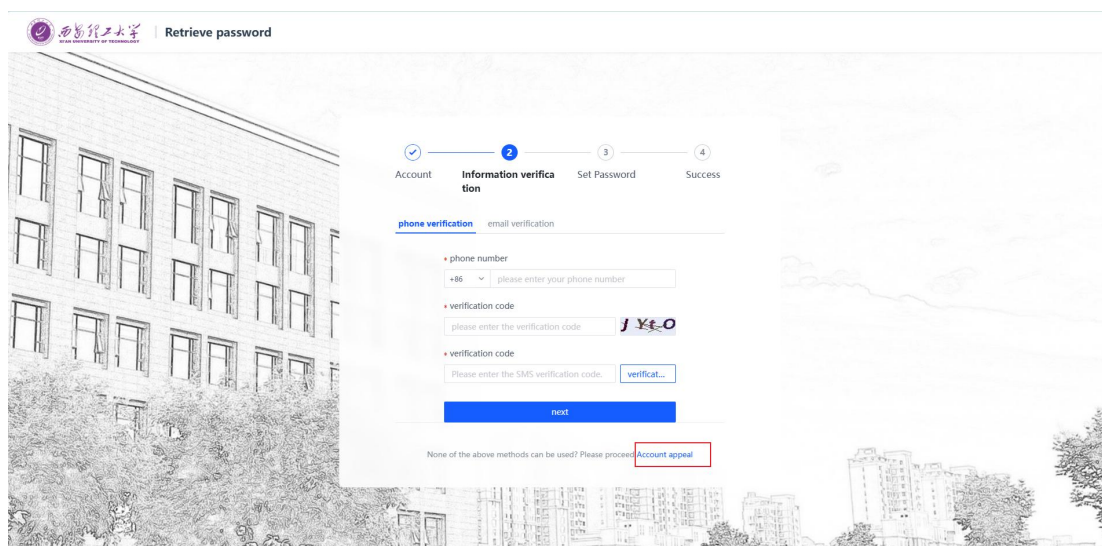
The screenshot shows the 'Retrieve password' interface with a progress bar at the top indicating four steps: 1. Account, 2. Information verification (current step), 3. Set Password, and 4. Success. Under 'Information verification', there are two options: 'phone verification' (selected with a red box) and 'email verification'. The 'phone verification' section includes a 'phone number' field with a dropdown set to '+86' and a text input field, a 'verification code' field with a text input and a 'R4ZD' image, and an 'SMS verification code' field with a text input and a 'verificat...' button. A blue 'next' button is at the bottom. A note at the bottom states: 'None of the above methods can be used? Please proceed Account appeal'.

4. Fill in a new password and click Reset Password, then the password reset is successful.

The screenshot shows the 'Retrieve password' interface with a progress bar at the top indicating four steps: 1. Account, 2. Information verification, 3. Set Password (current step), and 4. Success. The 'Set Password' section is titled 'please set your account 10wjw password'. It includes a 'new password' field with a text input and a 'new password again' field with a text input. Below these are two radio button options: 'Password must have at least 9 chars , 3 types of chars' (selected) and 'The password should not contain element such as simple password,unkeyboard chars user account, user mobile'. A blue 'submit' button is at the bottom.



5. If you have not reserved a security phone or security email, you cannot reset it by yourself. Please click **Forgot Password-Information Verification Step-Account Appeal Function** to appeal.



6. Please fill in the information on the account appeal interface truthfully and wait patiently for the administrator's review after submission. After passing the review, you will receive a text message with your reset password on your reserved phone. Please check it and log in to unified identity authentication as soon as possible to change your password and bind your security phone and email.

Account appeal

● To ensure the success of your account appeal, please fill in the following information carefully!

**Basic Information**

• actual name:

• type of certificate:

• ID number:

• College/Department:

**Upload complaint photo** @Support JPG / PNG format, and the size is not more than 5 M

**Contact information**

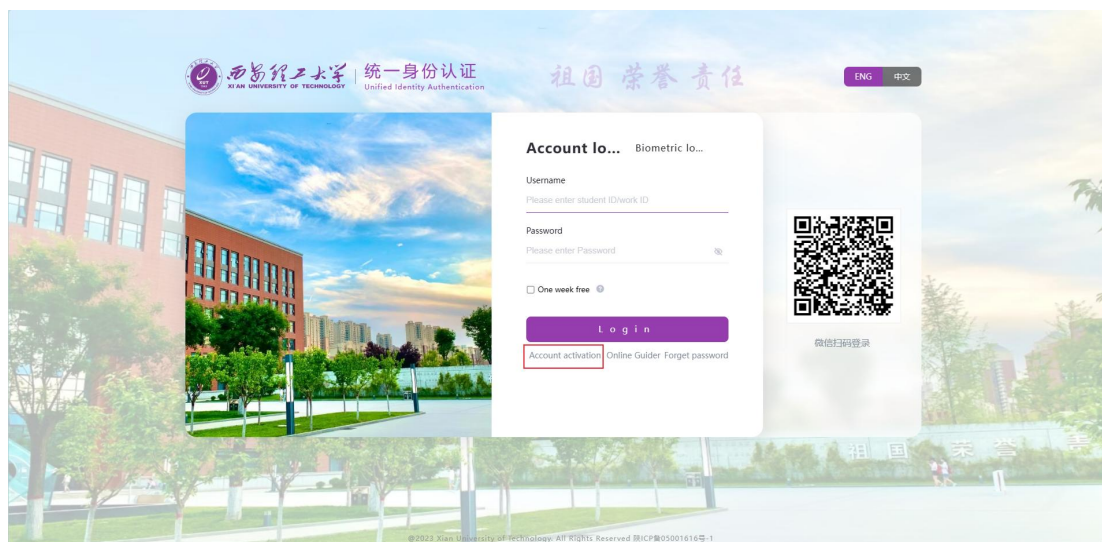
• Select:

• please enter verification code:

☒ After successful appeal, if there is no other person binding the mobile phone number or email, this account will be automatically bound

## 5.Account Activation

1. If you are a new student or teacher, you can click “Account Activation” at the bottom of the login page and jump to the account activation interface.



2. After entering the “Account Activation” page, you need to fill in your student/employee number, name, and ID number. Note: For non-foreigners, the default ID type is ID number, and for foreigners, it is passport.

Account activation

Activation tip

1 2 3 4  
Authenticate Bind phone Set password Activation complete

• Id/work id  
enter student id/work id

• name  
please enter your name

• ID type  
Passport

• ID  
Please enter your ID

• verification code  
please enter verification code

next

3. After filling in the information, click Next, and you need to bind your mobile phone number.

Account activation

Activation tip

1 2 3 4  
Authenticate Bind phone Set password Activation complete

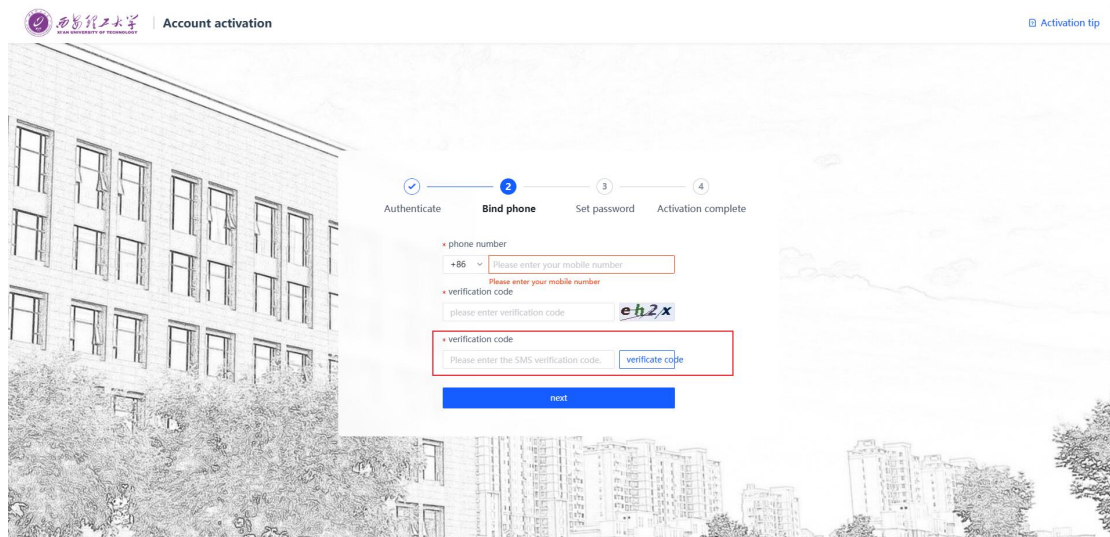
• phone number  
+86 Please enter your mobile number

• verification code  
Please enter verification code

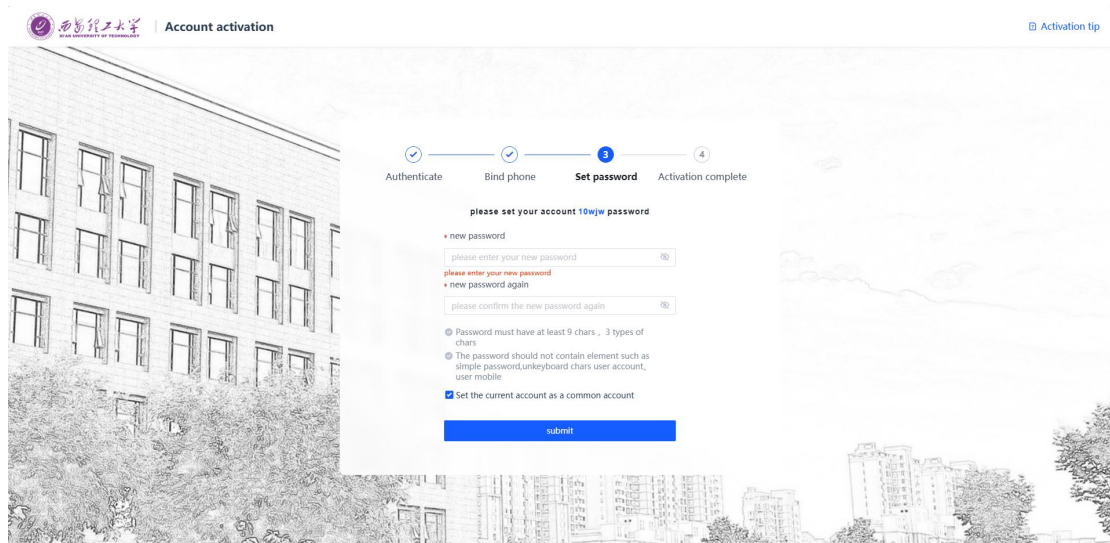
• verification code  
Please enter the SMS verification code. verify code

next

4. Enter your mobile phone number and click Get Verification Code. You will receive a text message verification code. Enter it and bind it. This operation is for you to retrieve your password when you forget your password later.

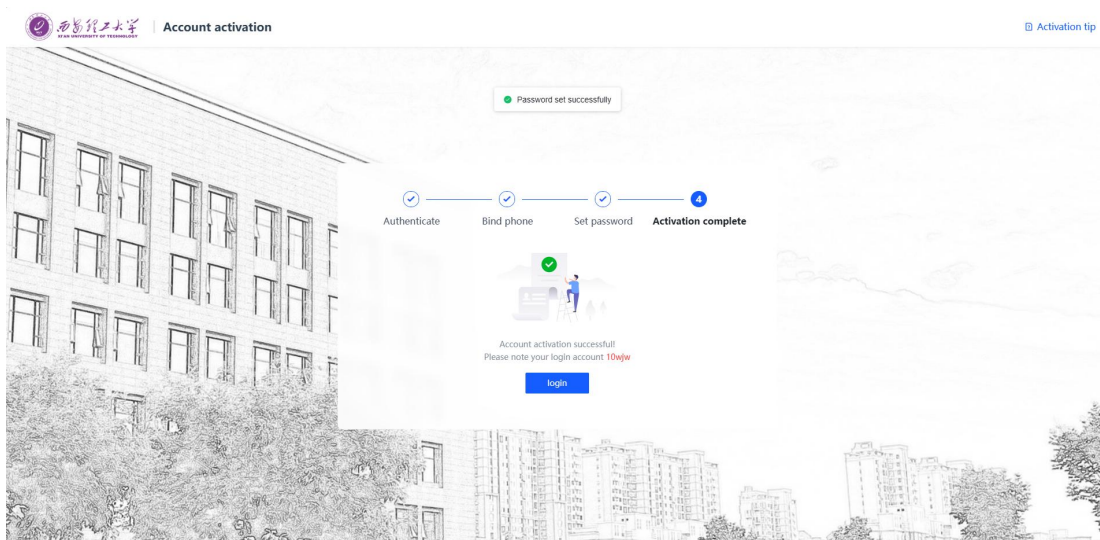


5. After binding, go to the next step and set your password. (The password length must be 9 digits or more, and contain at least 3 or more characters)



6. Click Go Login after completion.



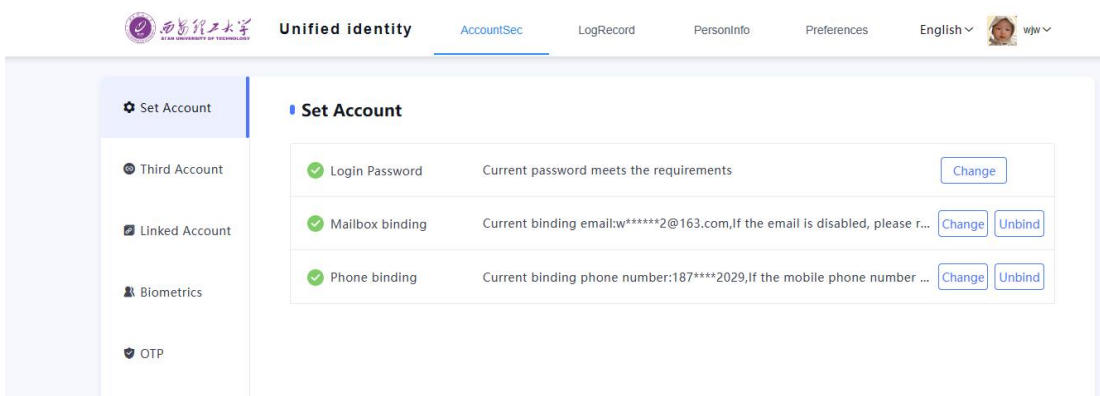


## 6.Function Introduction after Authentication

### Login

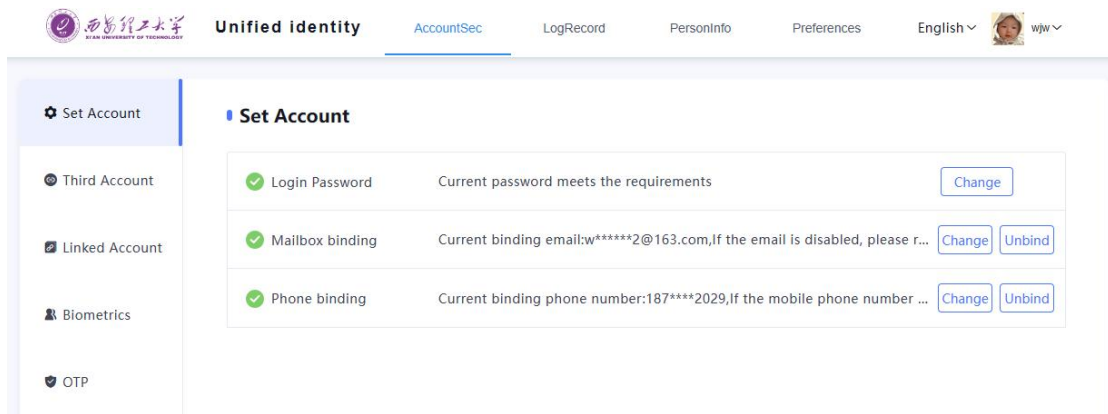
#### 1. Account Security Interface

1) Set Account The main functions of this page are: users can modify their login password, set security questions, bind email, bind mobile phone number, etc., for retrieving passwords when they forget their passwords.

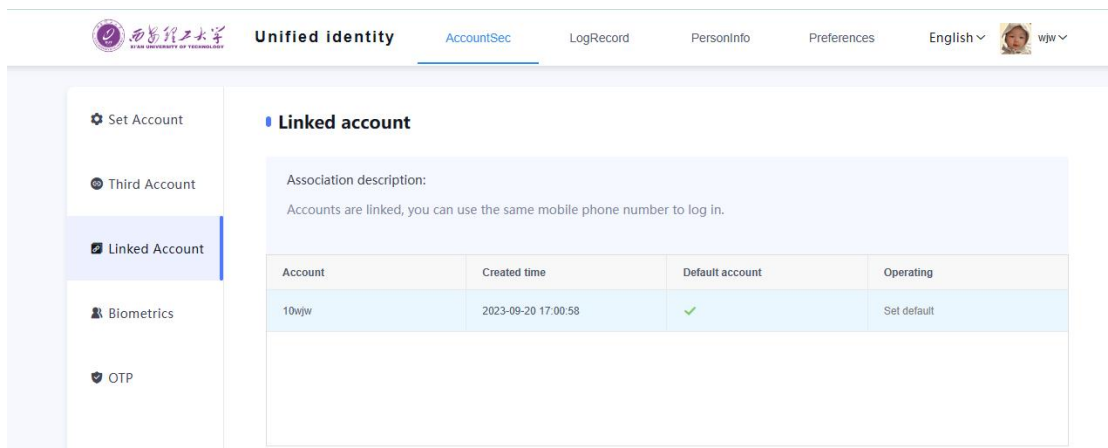


2) Third-party Account The main function of this page is: users can bind WeChat for convenient and fast login.

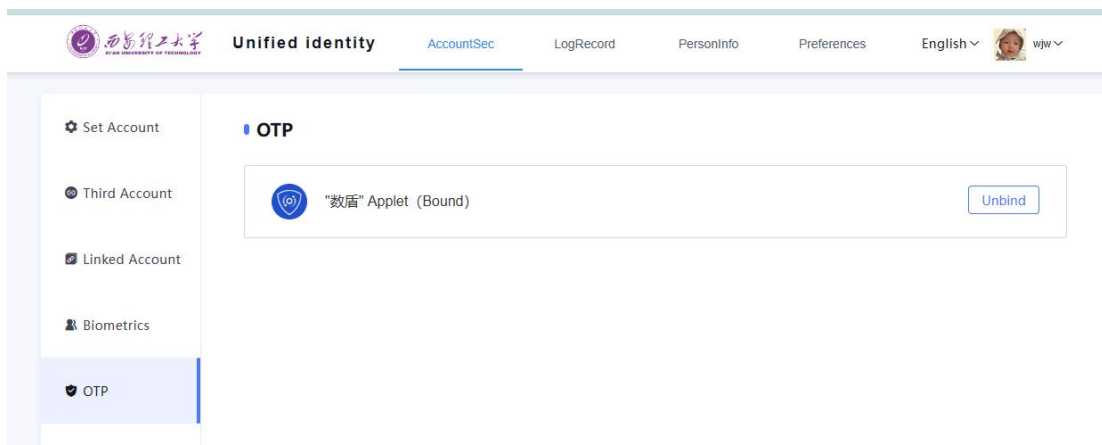




3) Associated Account The main function of this page is: if users have multiple accounts, they can set one account as the default account on this page. After setting a default account, users can enter their default account after logging in with mobile phone verification code or joint login.



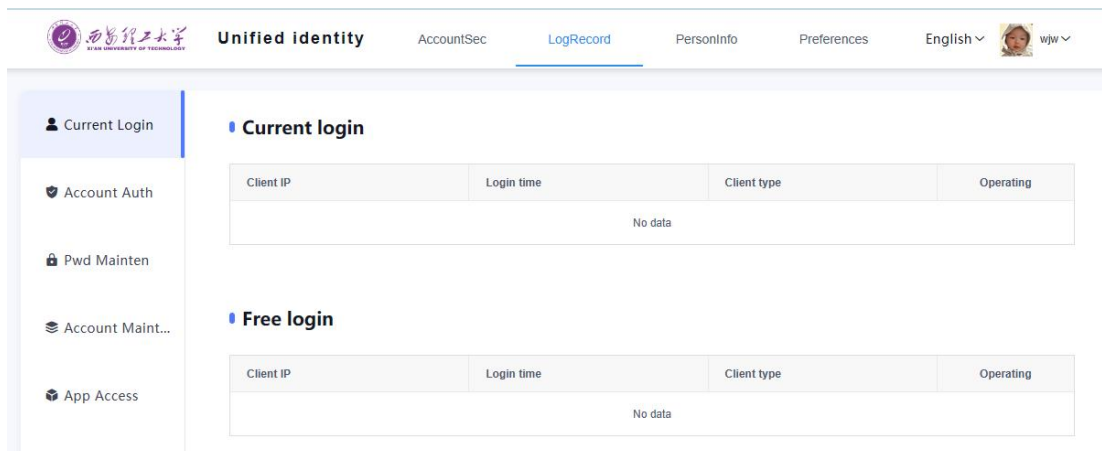
4) Biometric Recognition See Part 4 of this document;  
5) Security Token When two-step verification is turned on, you can use a security token for verification;



## 2. Authentication Record Interface

### 1) Current Login

On this page, users can view the account information of the current login, as well as the login status of the free login mode, and can perform removal operations.



### 2) Account Authentication Record

This page records the authentication login status of the user's account. You can view your account login record by time, login type, and authentication result.

The screenshot shows the 'Account authentication record' page. The top navigation bar includes 'Unified identity', 'AccountSec', 'LogRecord' (selected), 'PersonInfo', 'Preferences', 'English', and a user profile 'wjl'. The left sidebar has 'Current Login', 'Account Auth' (selected), 'Pwd Mainten', 'Account Maint...', and 'App Access'. The main content area has a title 'Account authentication record' and filters: 'Query time' (calendar icon), 'All certification types' (dropdown), 'All certification results' (dropdown), and a 'Reset' button. Below the filters is a table with 6 columns: 'Login time', 'Logout time', 'Certification type', 'Client IP', 'Certification result', and 'Fail reason'.

| Login time          | Logout time         | Certification type | Client IP       | Certification result | Fail reason           |
|---------------------|---------------------|--------------------|-----------------|----------------------|-----------------------|
| 2023-11-01 11:23:56 |                     | fido               | 202.200.127.157 | Success              | -                     |
| 2023-11-01 11:19:01 |                     | fido               | 202.200.127.157 | Fail                 | Account not activated |
| 2023-11-01 11:18:56 |                     | fido               | 202.200.127.157 | Fail                 | Account not activated |
| 2023-11-01 11:00:36 | 2023-11-01 11:00:41 | fido               | 202.200.127.157 | Success              | -                     |

### 3) Password Maintenance Record

This page records the password maintenance record of the user's account.

The screenshot shows the 'Password maintenance record' page. The top navigation bar is the same as the previous screenshot. The left sidebar has 'Current Login', 'Account Auth', 'Pwd Mainten' (selected), 'Account Maint...', and 'App Access'. The main content area has a title 'Password maintenance record' and filters: 'Query time' (calendar icon), 'All operation types' (dropdown), 'All operation results' (dropdown), and a 'Reset' button. Below the filters is a table with 4 columns: 'Maintenance time', 'Operation type', 'Client IP', and 'Operation result'.

| Maintenance time    | Operation type         | Client IP       | Operation result |
|---------------------|------------------------|-----------------|------------------|
| 2023-11-01 11:23:34 | activate edit password | 202.200.127.157 | Success          |
| 2023-10-31 03:16:10 | activate edit password | 202.200.112.12  | Success          |
| 2023-10-30 21:11:27 | Manage edit password   |                 | Success          |
| 2023-10-30 15:01:07 | Manage edit password   |                 | Success          |

### 4) Account Maintenance Record

This page records the maintenance status of the user's account, such as binding a mobile phone number, email address, etc. during what time period.

The screenshot shows the 'Unified identity' system interface. The top navigation bar includes 'Unified identity', 'AccountSec', 'LogRecord' (selected), 'PersonInfo', 'Preferences', 'English', and a user profile 'wjw'. The left sidebar has 'Current Login', 'Account Auth', 'Pwd Mainten', 'Account Maint...' (selected), and 'App Access'. The main content area is titled 'Account maintenance record'. It features a search bar with 'Query time' (calendar icon), 'All operation types' (dropdown), 'All operation results' (dropdown), and a 'Reset' button. Below is a table with 4 columns: 'Maintenance time', 'Operation type', 'Client IP', and 'Operation result'.

| Maintenance time    | Operation type                 | Client IP       | Operation result |
|---------------------|--------------------------------|-----------------|------------------|
| 2023-11-01 11:00:25 | Auto edit account-email bind   | 202.200.127.157 | Success          |
| 2023-11-01 09:56:12 | Auto edit account-phone bind   | 221.226.41.179  | Success          |
| 2023-11-01 09:32:52 | Auto edit account-phone unbind | 221.226.41.179  | Success          |
| 2023-10-31 11:37:49 | Auto edit account-phone bind   | 202.200.127.157 | Success          |

## 5) Application Access Record

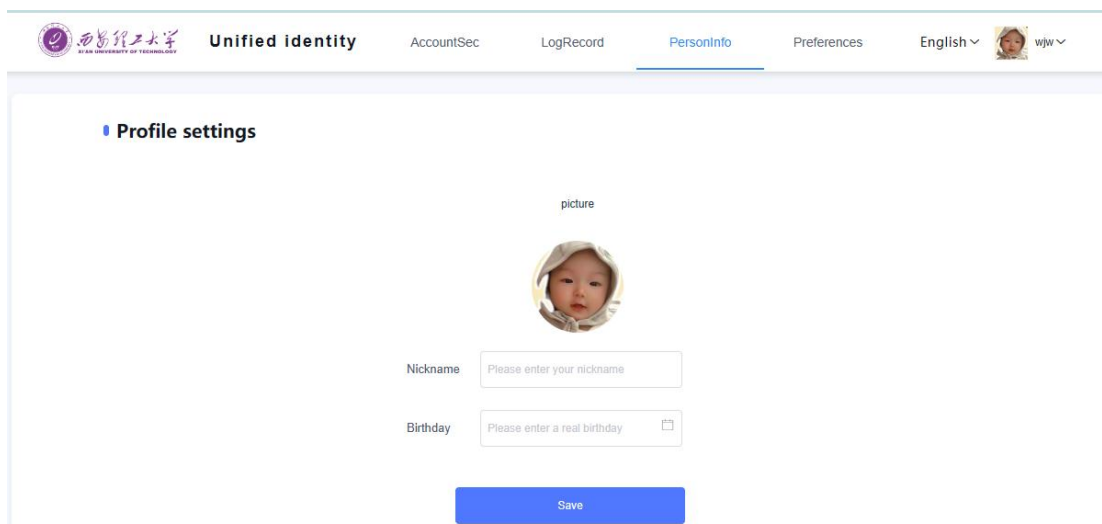
This page records the application access status of the user's account.

The screenshot shows the 'Unified identity' system interface. The top navigation bar includes 'Unified identity', 'AccountSec', 'LogRecord' (selected), 'PersonInfo', 'Preferences', 'English', and a user profile 'wjw'. The left sidebar has 'Current Login', 'Account Auth', 'Pwd Mainten', 'Account Maint...', and 'App Access' (selected). The main content area is titled 'Application access record'. It features a search bar with 'Please select an application' (dropdown), 'Query time' (calendar icon), 'All certification results' (dropdown), and a 'Reset' button. Below is a table with 3 columns: 'Access time', 'Application Name', and 'Certification result'.

| Access time         | Application Name | Certification result |
|---------------------|------------------|----------------------|
| 2023-11-01 10:42:11 |                  | Success              |
| 2023-10-31 15:48:13 |                  | Success              |
| 2023-10-31 14:38:29 |                  | Success              |

## 3. Personal Information

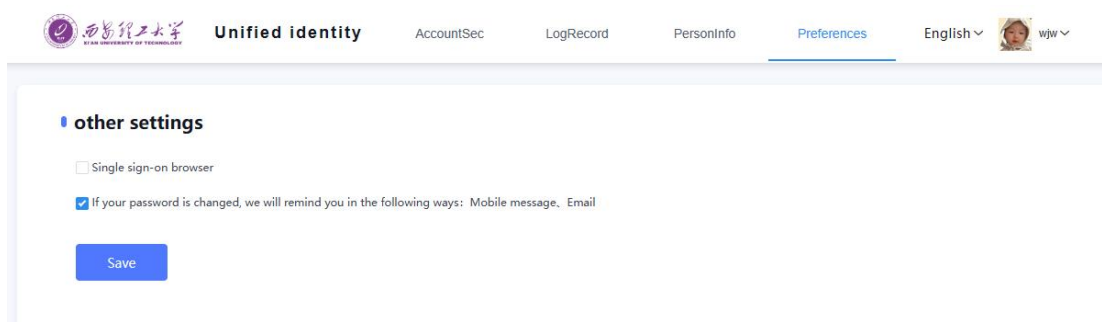
You can set your avatar, nickname, birthday, and when the administrator turns on the function of allowing to log in with a nickname, the unified identity authentication account can be set to your own nickname.



The screenshot shows the 'Profile settings' page. At the top, there is a navigation bar with the university logo, 'Unified identity', and links for 'AccountSec', 'LogRecord', 'PersonInfo' (active), 'Preferences', 'English', and a user profile icon. The main content area is titled 'Profile settings'. It features a circular profile picture placeholder labeled 'picture'. Below the picture are two input fields: 'Nickname' with the placeholder text 'Please enter your nickname' and 'Birthday' with the placeholder text 'Please enter a real birthday' and a calendar icon. A blue 'Save' button is located at the bottom of the form.

## 4. Preference Settings

Set whether to allow your unified identity authentication account to only log in on one browser; Set whether to remind by SMS or email after password change;



The screenshot shows the 'other settings' page. At the top, there is a navigation bar with the university logo, 'Unified identity', and links for 'AccountSec', 'LogRecord', 'PersonInfo', 'Preferences' (active), 'English', and a user profile icon. The main content area is titled 'other settings'. It contains two settings: 'Single sign-on browser' with an unchecked checkbox, and 'If your password is changed, we will remind you in the following ways: Mobile message, Email' with a checked checkbox. A blue 'Save' button is located at the bottom of the form.

Xian University of Technology Information Management Office  
October 31, 2023