

Smart Lock Management System System Commissioning Manual

Newcapec Electronics Co., Ltd.

Last Updated: 2026.7.15

Table of Contents

1 ENVIRONMENT CHECK AND PREPARATION	5
1.1 MANAGEMENT SYSTEM LOGIN AND PERMISSIONS	5
1.1.1 Default Login Information	5
1.1.2 Role Management	5
1.1.3 Business Data Permissions	7
1.1.4 Mobile App Permissions (Configure as Required)	7
1.2 DEVICE COMMISSIONING PREPARATION	8
1.2.1 Commissioning Mode	8
1.2.2 Card-Reading Environment	9
1.2.3 Fingerprint Enrollment Environment	9
2 SYSTEM BASIC DATA	9
2.1 BASIC INFORMATION MAINTENANCE	9
2.1.1 Department Information	9
2.1.2 Personnel Information	11
2.2 AREA MANAGEMENT	16
2.2.1 Area Information	16
2.2.2 Gateway Area	17
3 DEVICE COMMISSIONING	18
3.1 LoRA GATEWAY CONFIGURATION AND COMMISSIONING	18
3.1.1 Gateway Configuration	18
3.1.2 Create Gateway	20
3.2 LoRA SMART LOCK COMMISSIONING - OPTION 1	21
3.2.1 Create Smart Lock Device	21
3.2.2 Bind the Smart Lock to a Gateway	22
3.2.3 Push the Smart Lock Device to the IoT Platform	23
3.3 LoRA SMART LOCK COMMISSIONING - OPTION 2	23
3.3.1 Smart Lock Commissioning	23
3.3.2 Smart Lock Re-Commissioning	26
3.4 VIRTUAL GATEWAY (Wi-Fi SMART LOCK)	26
3.4.1 Create Gateway	26
3.5 WIFI SMART LOCK COMMISSIONING	27
3.5.1 Smart Lock Commissioning	27
3.5.2 Smart Lock Re-Commissioning	30
4 DEVICE BUSINESS DATA COMMISSIONING	30
4.1 AUTHORIZATION RULE BINDING AND VIEWING	30
4.1.1 Add Authorization	30
4.1.2 Batch Import Authorization	31
4.1.3 View Existing Authorization Rules and Maintenance	31
4.2 VIEW AUTHORIZATION LISTS AND DISTRIBUTION STATUS	33

4.2.1 Authorization List Query	33
4.3 DEVICE OPERATION MONITORING AND DOOR-OPENING RECORDS	35
4.3.1 Smart Lock Monitoring	35
4.3.2 Door-Opening Records View	36
4.3.3 Smart Lock Alert Data	37
4.4 DEVICE PARAMETERS	37
4.4.1 Parameter Planning	37
4.4.2 Parameter Binding	38
4.4.3 Device Parameter Groups	38
5 SMART LOCK COMMON COMMISSIONING OPERATIONS DESCRIPTION	39
5.1 MAINTAIN DOOR-OPENING PASSWORDS	39
5.1.1 Initial Door-Opening Password for Personnel	39
5.1.2 Administrator-Assisted Door-Opening Password Maintenance	39
5.1.3 Users Maintain Their Own Door-Opening Passwords	40
5.2 ENROLL FINGERPRINTS	40
5.2.1 Enroll by Swiping a Card on the Lock	40
5.2.2 Initiate Enrollment from the Mobile App	40
5.2.3 Fingerprint Scanner Enrollment	41
5.3 REMOTE DOOR OPENING	41
5.3.1 PC-Side Remote Door Opening	41
5.3.2 Mobile Remote Door Opening	41
5.3.3 Smart Lock Device Action	41
5.4 OPEN DOOR WITH DYNAMIC PASSWORD	42
5.5 COMMON LoRA GATEWAY OPERATIONS	42
5.5.1 Replace Gateway Device	42
5.5.2 Change Gateway Area	43
5.5.3 Gateway Upgrade	43
5.5.4 Gateway Reset	44
5.5.5 Gateway Data Check	44
5.5.6 Gateway Data Cleanup	46
5.6 COMMON LoRA SMART LOCK OPERATIONS	47
5.6.1 Smart Lock Upgrade	47
5.6.2 Device Removal and Decommissioning	48
6 COMMON ROUTINE MAINTENANCE OPERATIONS	49
6.1 HOW TO LOG IN TO THE GATEWAY WEB PAGE	49
6.1.1 LoRa Gateway Web Page Access	49
6.1.2 SUB-1G Gateway Web Page Access	49
6.2 VIEW AND DOWNLOAD SERVICE LOGS	50
6.2.1 Check Logs When Problems Occur in Management-System Operations	50
6.2.2 Device Communication Logs	51
6.2.3 LoRa Gateway Logs	52
6.3 OFFLINE / CONNECTION ISSUES	53
6.3.1 LoRa Gateway Offline	53

6.3.2 LoRa Smart Lock Offline.....	53
6.3.3 Sublg Base Station Offline.....	53
6.3.4 Sublg Smart Lock Offline.....	54
6.4 AUTHENTICATION SUCCEEDS BUT DOOR DOES NOT OPEN.....	54
6.4.1 Card Swipe Does Not Unlock the Door.....	54
6.4.2 QR-Code Scan Does Not Open the Door.....	56
6.4.3 Facial Recognition Does Not Open the Door.....	56
6.5 HOW TO CREATE SMART LOCK O&M CARDS.....	57
6.5.1 Create an Upgrade Card.....	57
6.5.2 Create an Engineering Commissioning Card.....	57
6.5.3 Create a Parameter Collection Card.....	57

1 Environment Check and Preparation

1.1 Management System Login and Permissions

1.1.1 Default Login Information

After system deployment and commissioning are complete, you can enter the "Smart Lock Management System" module through the login page.

Enter the system login address <http://192.168.10.36:30180> in a browser (change the address according to the customer's site configuration) to open the system. You can bookmark this URL in the local browser for quick access next time.

The system login page is shown below. Enter the "Username" and "Password" in sequence, then log in to the system.



Port 30100 — corresponding address: **Default Tenant Login Address**, generally used temporarily by the super administrator during initial commissioning and configuration. (Default account/password: **acs / Ncap.123456**)

Port 30180 — corresponding address: **Dedicated Tenant Login Address for the School**, **All operations described in this commissioning document are performed through port 30180**. Record the login address for subsequent commissioning and customer use. (Default account/password: **cs / Ncap.123456**)

1.1.2 Role Management

Menu path [System Management - Permission Management - Role Management].
Add or maintain roles.

角色名称:
角色别名:

搜索
重置

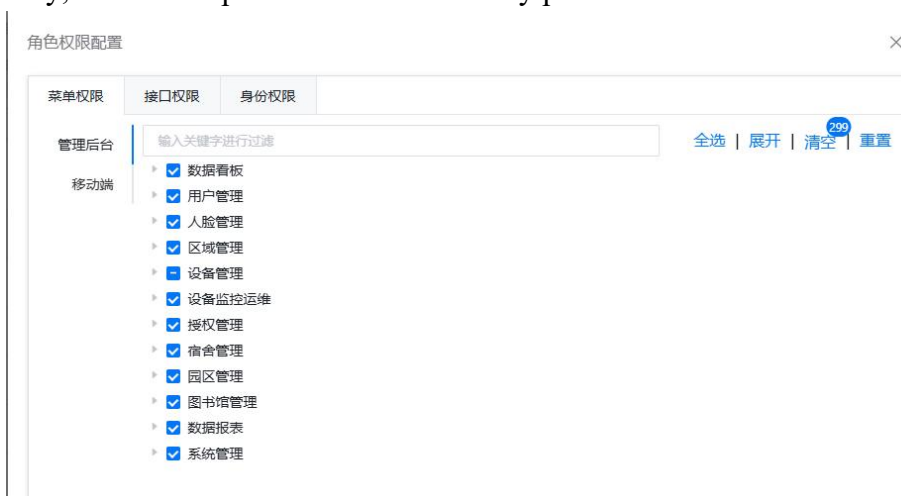
新增
删除

☐	#	角色名称	角色别名	角色排序	操作
☐	1	管理员	admin	2	查看 编辑 删除 更多
☐	2	访客	visitor	3	查看 编辑 删除 更多
☐	3	用户	user	4	查看 编辑 删除 更多
☐	4	家属	family	5	查看 编辑 删除 更多
☐	5	参数审批员	paramApproval	9	查看 编辑 删除 更多
☐	6	业务管理员	Business	10	查看 编辑 删除 更多
☐	7	业务管理	Busi	11	查看 编辑 删除 更多
☐	8	在职人员	work	12	查看 编辑 删除 更多

For permission settings of an existing role, click [More -> Permission Settings] in the list to configure them.



Normally, both menu permissions and identity permissions need to be configured.



For an existing role, configure its user list and managed-department permissions by clicking [More -> User Settings] in the list., The page is shown below.

用户设置

*角色名称: 管理员

1.这里可以配置 该角色包含的 登录用户信息

选择用户: 130503,admin[共2个用户]

部门管理范围: 用户之间管理范围相同 用户之间管理范围不同

2.设置不同用户的管辖部门权限

新增

学工号	管理范围	3.逐个设置人员管辖的 部门权限	
130503	特定范围	历史学院 国际学院	删除
	所属部门及下级部门		删除

保存 取消

1.1.3 Business Data Permissions

Menu path [System Management - Permission Management - Business Data Permissions]. Add or maintain roles.

Set the areas that each person is authorized to manage here. This is an important configuration for hierarchical permission management. Personnel without assigned permissions cannot view areas or devices and therefore cannot perform authorization Management or view authorization information.

角色列表

校级管理员
院系管理员
超级管理员
普通用户
访客

1选择角色

人员列表

输入关键字进行过滤

张24
cpu11

2勾选人员

区域列表

输入关键字进行过滤

门禁区域

1号楼

1层

101
102
103

西校区

1号楼

1层

a-1-101
a-1-102

3勾选 区域列表

1.1.4 Mobile App Permissions (Configure as Required)

Under System Management -- Permission Management -- Mobile App Permissions, configure the mobile permissions available to each job role. Permissions are divided into a menu list and a credential list.

Main Interface

Procedure

1.2 Device Commissioning Preparation

1.2.1 Commissioning Mode

1.2.1.1 NFC Phone Commissioning

- NFC-enabled Android phone — Install the "Smart Lock Mobile Commissioning Assistant" app on the phone.
- Network environment — The NFC phone must connect over Wi-Fi and be able to access the "Smart Lock Management System."

1.2.1.2 Manual Serial-Number Registration

For a small number of LoRa smart locks and gateways, devices can be registered by manually recording their serial numbers.

Photograph the serial-number QR code on each device and record the device

serial numbers one by one.

1.2.2 Card-Reading Environment

When card issuance and card reading are required in the "Smart Lock Management System," a dedicated card-reading environment must be prepared.

The following items are required:

Newcapec Card Reader — Connect the card reader to the client computer.

Card-Reading Service — Download the dedicated card-reading service program and install it on the client computer.

1.2.3 Fingerprint Enrollment Environment

When fingerprints are collected using a "Fingerprint Scanner" connected to a computer, a dedicated fingerprint-enrollment environment must be prepared. (This method is used infrequently.)

The following items are required:

Fingerprint Scanner — Connect the scanner to the client computer.

Fingerprint Enrollment Service — Download the dedicated fingerprint-enrollment service program and install it on the client computer.

2 System Basic Data

2.1 Basic Information Maintenance

2.1.1 Department Information

Menu path [User Management - Department Management].

Department information can generally be synchronized from the One-Card Platform or data center, or maintained and adjusted manually. The [Department Attribute] field can be left blank. .

Note: If department data is synchronized, avoid manual maintenance (such as modification or deletion) whenever possible. Otherwise, manual changes may conflict with synchronized data.

新增

导入

导出

部门名称:

搜索

重置

新开普大学	
历史学院	
国际学院	
安全学院	
出入应用事业部	
新开普大学校友会	

部门名称	部门全称	部门属性	数据来源	备注	操作
校友	新开普大学校友会/校友		同步		编辑 删除
文学院	新开普大学校友会/校友/文学院		同步		编辑 删除
本科生	新开普大学校友会/校友/文学院...		同步		编辑 删除
2011	新开普大学校友会/校友/文学院...		同步		编辑 删除
新闻学	新开普大学校友会/校友/文学院...		同步		编辑 删除
新闻学2班	新开普大学校友会/校友/文学院...		同步		编辑 删除

Department information can be imported. Download the template from the system, complete it as required, and upload it to the system.

导入部门

×

文件上传:

📁 点击上传

请上传 .xls, .xlsx 标准格式文件

导入进度:

0%

导入结果:

模板下载:

📄 点击下载

导入注意事项： 1. 本行导入时不要删除 2. 红色为必填项 3. 部门名称最长30个字符					
一级部门	二级部门	三级部门	四级部门	五级部门	六级部门
演示学校	历史学院	中国史2501			
演示学校	历史学院	中国史2502			
演示学校	历史学院	中国史2503			
演示学校	历史学院	中国史2504			
演示学校	国际学院	外贸2301			
演示学校	国际学院	外贸2302			
演示学校	国际学院	外贸2401			
演示学校	国际学院	外贸2402			
演示学校	国际学院	外贸2501			
演示学校	国际学院	外贸2502			
演示学校	安全学院	信息安全2301			
演示学校	安全学院	信息安全2302			
演示学校	安全学院	信息安全2401			
演示学校	安全学院	信息安全2402			
演示学校	安全学院	信息安全2501			
演示学校	安全学院	信息安全2502			

2.1.2 Personnel Information

Menu path [Personnel Management - Personnel Information].

Personnel information can generally be synchronized from the One-Card Platform or data center, or maintained and adjusted manually.

2.1.2.1 Add Personnel

Normally, only the required fields marked with * need to be completed.



By default, newly added personnel are not allowed to log in to the system. If a person needs to be configured as an operator, expand [More Information] at the bottom of the page, set "System Login" to Enabled, and configure the "Role" information (the menu permissions the operator can use).

The default login password for a newly created standard user is Abc123456.



2.1.2.2 Issue Card

The system supports management and maintenance of existing card information for personnel and can also issue cards to personnel who do not yet have one.

Select a person and click [Issue Card] to open the card-information maintenance page.



On the card-information page shown below, you can maintain the person's existing card information and add physical card information.

Each person can have at most one primary physical card and one secondary physical card.

A virtual card refers to the virtual card number corresponding to a scanned QR code. (It can only be synchronized from the One-Card Platform and cannot be added manually.)





If the card UID is known, enter it directly. To use the "Read Card" function, prepare a card reader and connect it to the operator's client computer. On the client computer, download and install the supporting [Card-Reading Service] before using this function.

2.1.2.3 Fingerprint Maintenance

This function is mainly used to manage fingerprint data for opening smart locks. The system supports management and maintenance of existing fingerprint information and can also register and enroll new fingerprints for personnel.

Select a person who already has fingerprint data and click [Fingerprint Maintenance] to open the fingerprint-information maintenance page.



	姓名	人员编号	部门	身份	性别	状态	有效期
☒	张三	130503	新开普大学/出入应用事业部	在职人员		正常	2099-12-31

The page displays the number of fingerprints enrolled for the person and allows fingerprints to be deleted. After deletion, the change is distributed to the smart lock to remove that person's door-opening fingerprint data.



If a person has no fingerprint data, this function can be used to enroll fingerprints.



To use this function, prepare a fingerprint scanner in advance, connect it to the client computer, and install the supporting [Fingerprint Enrollment Service] on the client computer. Otherwise, collect fingerprint information directly on the smart lock device.



2.1.2.4 Door-Opening Password

This function manages password data used to open smart locks. The password must be a 6-digit numeric code. Overly simple passwords, such as sequential or repeated digits, are not supported.

Select a person and click [Door-Opening Password] to open the password-maintenance page.

Here you can set a door-opening password for a person, or reset/delete the password for a person who already has one.



姓名: 请输入姓名 人员编号: 请输入人员编号 部门: 请选择

当前表格已选择 0 项 清空

☐	姓名	人员编号	部门	身份	性别	状态	有效期	卡唯一号		操作
☐	测试人员	20260600011	新开普大学/出入应...	在职人员		正常	2099-12-31	BC2A723A		查看 编辑 更多
☐	测试部门...	061301	新开普大学/出入应...	在职人员		正常	2099-12-31			查看 编辑 更多
☐	测试=01	20260609001	新开普大学/历史学...	在职人员	男	正常	2099-12-31			查看 编辑 更多
☐	王测试...	171130	新开普大学/出入应...	在职人员		正常	2099-12-31	02A1F7CA		查看 编辑 更多
☐	张测试-认...	210805	新开普大学/出入应...	家属		正常	2099-12-31	C2390D3F		查看 编辑 更多
☐	吴测试	130503	新开普大学/出入应...	在职人员		正常	2099-12-31	21475450		查看 编辑 更多
☐	林测试30	20252171	新开普大学/安全学...	在职人员		正常	2099-12-31	D1250171		查看 编辑 更多

共 82 条 10条/页 < 1 2 3 4 5 6 ... 9 > 前往 1 页

2.1.2.5 Reset Login Password

Locate the person whose password needs to be reset and click [More]-[Reset Login Password]. This resets the person's password to the default login password Ncap.123456.

当前表格已选择 1 项 清空

☒	姓名	人员编号	部门	身份	性别	状态	有效期	卡唯一号		人脸照片	人脸特征	指纹数量	操作
☒	吴测试	130503	新开普大学/出入应用事业部	在职人员		正常	2099-12-31	21475450		无	无	2	查看 编辑 更多

禁用
重置登录密码
删除

2.2 Area Management

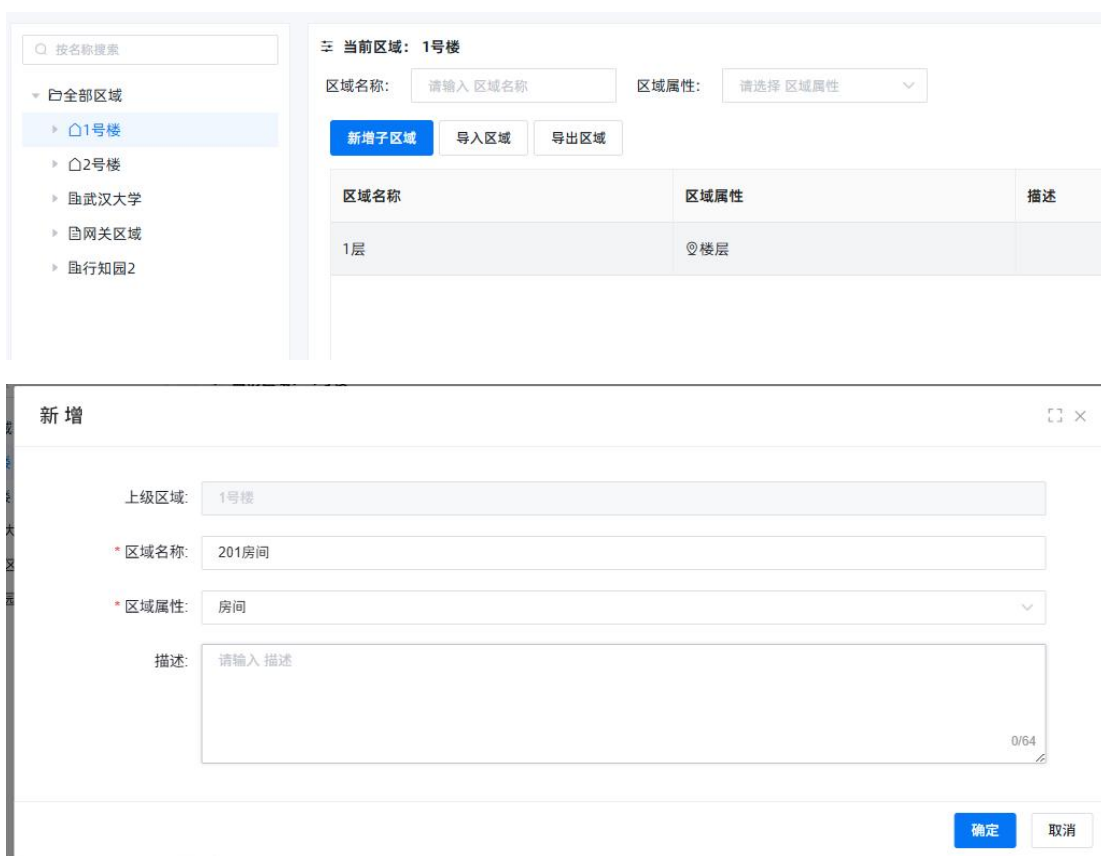
During initial commissioning, it is recommended to first configure the building, floor, room, and gateway-area information for one building. After that building has been commissioned successfully, proceed with the remaining buildings.

2.2.1 Area Information

Maintain area information (campus, building, room) here.

2.2.1.1 Add Sub-Area

Select an area node in the area tree on the left, then click [Add Sub-Area].



按名称搜索

全部区域

- 1号楼
- 2号楼
- 武汉大学
- 网关区域
- 知行园2

当前区域: 1号楼

区域名称: 请输入 区域名称

区域属性: 请选择 区域属性

新增子区域 导入区域 导出区域

区域名称	区域属性	描述
1层	楼层	

新增

上级区域: 1号楼

* 区域名称: 201房间

* 区域属性: 房间

描述: 请输入 描述

0/64

确定 取消

2.2.1.2 Import Areas

The system supports batch import of area information. Download the Excel template, complete the area data, and import it into the system.

区域导入

文件上传:

上传

取消

上传

取消

请上传 .xls, .xlsx 标准格式文件

导入进度:

0%

导入结果:

模板下载:

下载

取消

导入注意事项: 1. 本行导入时不要删除 2. 红色为必填项 3. 若区域属性为'其他', 则该区域及其下级区域仅支持手动录入, 不支持导入 4. 需填写完整区域路径, 如: 需要导入楼层时, 其上级园区、楼栋名称均需填写			
园区名称	楼栋名称	楼层名称	房间名称
秦园	1号楼	1层	101
秦园	1号楼	1层	102
秦园	1号楼	1层	103
秦园	1号楼	1层	104
秦园	1号楼	1层	105
秦园	1号楼	1层	106
秦园	1号楼	1层	107
秦园	1号楼	1层	108
秦园	1号楼	1层	109
秦园	1号楼	1层	110
秦园	1号楼	2层	201
秦园	1号楼	2层	202
秦园	1号楼	2层	203
秦园	1号楼	2层	204
秦园	1号楼	2层	205
秦园	1号楼	2层	206
秦园	1号楼	2层	207
秦园	1号楼	2层	208
秦园	1号楼	2层	209
秦园	1号楼	2层	210
秦园	1号楼	3层	301
秦园	1号楼	3层	302
秦园	1号楼	3层	303

2.2.2 Gateway Area

For smart-lock deployments that use gateways, each gateway must also be associated with area information to support hierarchical gateway search.

It is recommended to create a dedicated group of gateway areas, independent of the building hierarchy if desired (Area Attribute = Other), as shown below. Each gateway must correspond to one area node.

Page 17 / of 57

区域名称	区域属性	描述
1号楼2层东	其他 (非园区/楼栋等场景)	
1号楼2层西	其他 (非园区/楼栋等场景)	
1号楼4层西	其他 (非园区/楼栋等场景)	

3 Device Commissioning

3.1 LoRa Gateway Configuration and Commissioning

3.1.1 Gateway Configuration

3.1.1.1 Network Configuration

LoRa gateway default web page address: 192.168.50.86:8092.
Connect the computer directly to the gateway using an Ethernet cable.
The computer IP address must be on the same subnet as the gateway.
Default account/password: admin/ncap@300248 (Change the password promptly.)

On the "Network Configuration" page, configure the data collector's Ethernet "IP Address," "Subnet Mask," "Default Gateway," and "DNS."

For easier management of data collectors, a static IP address is generally recommended. Select "STATIC" as the Ethernet mode, enter the IP address, port, and other information in the corresponding

fields using valid formats, and click "Save" to complete the configuration.

■ Verification After Configuration

Restore the computer to its normal network settings, connect the gateway Ethernet cable to the normal network, and access the gateway web page again in a browser using the configured network information.

3.1.1.2 Service Configuration

After the gateway network configuration in the previous step is complete, proceed with [Service Configuration], also through the web page.

As shown below, configure all of the URL fields with the same values. The IP address is the access IP of the Smart Lock Management System, and the port is generally fixed at 28972:

192.168.1.121:28972

Configuration is now complete.

3.1.2 Create Gateway

3.1.2.1 Record the SN number

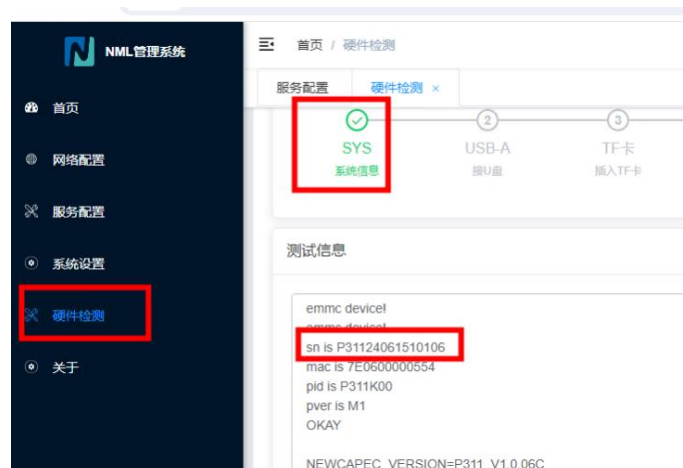
Use the serial number printed below the barcode on the device label, as shown below. When configuring the platform, replace the leading P with 50 before entering it.

Example: If a device SN is P3112208271040, enter it on the platform as 503112208271040.



Other Method:

After logging in to the gateway page, you can also view the device serial number, as shown below.



3.1.2.2 Create Gateway Device

LoRa smart locks support simplified commissioning, and their associated gateway devices must also be set to "TMS Commissioning" mode.

Menu path: "Device Management - Smart Lock Gateway Management."

When creating a LoRa gateway, plan channel groups correctly. Adjacent gateways must not use the same channel group.

The "Area" associated with a gateway is mainly used for categorized search and management. You can create a dedicated branch outside the standard building-area

hierarchy for gateway classification and management.

3.1.2.3 Push Gateway Device to IoT Platform

Select the newly created gateway device and click [Push to IoT Platform].

3.2 LoRa Smart Lock Commissioning - Option 1

Note: If delivered smart locks have QR-code labels and the number of locks is small (≤ 10), they can be commissioned directly by manually recording the smart-lock serial numbers. There is no need to complete the process through the TMS platform, which reduces commissioning effort.

3.2.1 Create Smart Lock Device

Create the smart lock device and record its serial number (from the QR code on the smart lock). As shown below, enter a real and valid SN in the "Device Serial Number" field:

[illegible]

3.2.2 Bind the Smart Lock to a Gateway

Go to "Device Management - Smart Lock Gateway Management." Select a gateway, choose "More - Associate Smart Locks," and locate the smart locks associated with that gateway to bind them, as shown below.

当前区域: 网关区域/1号楼网关

网关名称:

网关序列号:

提交

重置

展开

TMS文件操作

TMS数据传输

新增

导出

推送物联网

网关配置模板

当前表格已选择 0 项 清空

☐	网关名称	网关型号	网关序列号	区域	关联门锁	网关状态	推送物联网状态	操作
☐	1号楼2层西网关	P311K00	5031101101	网关区域/1号楼网关	1个	待激活	未同步	查看 编辑 更多

更换网关

更换区域

关联门锁

删除

关联门锁设备(网关名称:1号楼2层西网关)

门锁名称:

请输入 门锁名称

设备型号:

请选择 设备型号

设备序列号:

请输入 设备序列号

搜索

重置

绑定

解绑

☐	门锁名称	设备型号	设备序列号	区域	操作
☐	1号楼101门锁	I315K1X	0716001	1号楼/1层/101房间	解绑

选择门锁设备

门锁名称:

请输入 门锁名称

设备型号:

请选择 设备型号

设备序列号:

请输入 设备序列号

区域名称:

1号楼

号:

搜索

重置

当前表格已选择 7 项 清空

☒	门锁名称	设备型号	设备序列号	区域
☐	1号楼109门锁	I315F1X	9	秦园/1号楼/1层/109
☒	1号楼108门锁	I315F1X	8	秦园/1号楼/1层/108
☒	1号楼107门锁	I315F1X	7	秦园/1号楼/1层/107
☒	1号楼106门锁	I315F1X	6	秦园/1号楼/1层/106
☒	1号楼105门锁	I315F1X	5	秦园/1号楼/1层/105
☒	1号楼104门锁	I315F1X	4	秦园/1号楼/1层/104
☒	1号楼103门锁	I315F1X	3	秦园/1号楼/1层/103

共 19 条

10条/页

<

1

2

>

前往

2

页

保存

关闭

3.2.3 Push Smart Lock Device to IoT Platform

This pushes smart lock devices created in the system to the IoT service. The devices can communicate over the network only after this operation is complete.

Select one or more smart lock devices and click [Push to IoT Platform].

3.3 LoRa Smart Lock Commissioning - Option 2

3.3.1 Smart Lock Commissioning

Use NFC-enabled Android phone to install the O&M tool "Mobile Commissioning Assistant." The installation package is available in the attachment path "Terminal Supporting Programs\ Smart Lock Commissioning Assistant\".

After installing the app, enable NFC on the phone and set this app (alias: BleNFC) as the default NFC payment application. On Xiaomi phones, select the SIM card wallet as the default payment method.



1. Open the app. First ensure that the phone is connected to the school's Wi-Fi and that this Wi-Fi network can access the system address.
2. In the app, tap [Server Settings], then enter the Smart Lock Management System IP address and port (default port: 28001).
3. On the [Server Settings] screen, enter the tenant ID to be used, tap Finish, and save the configuration.

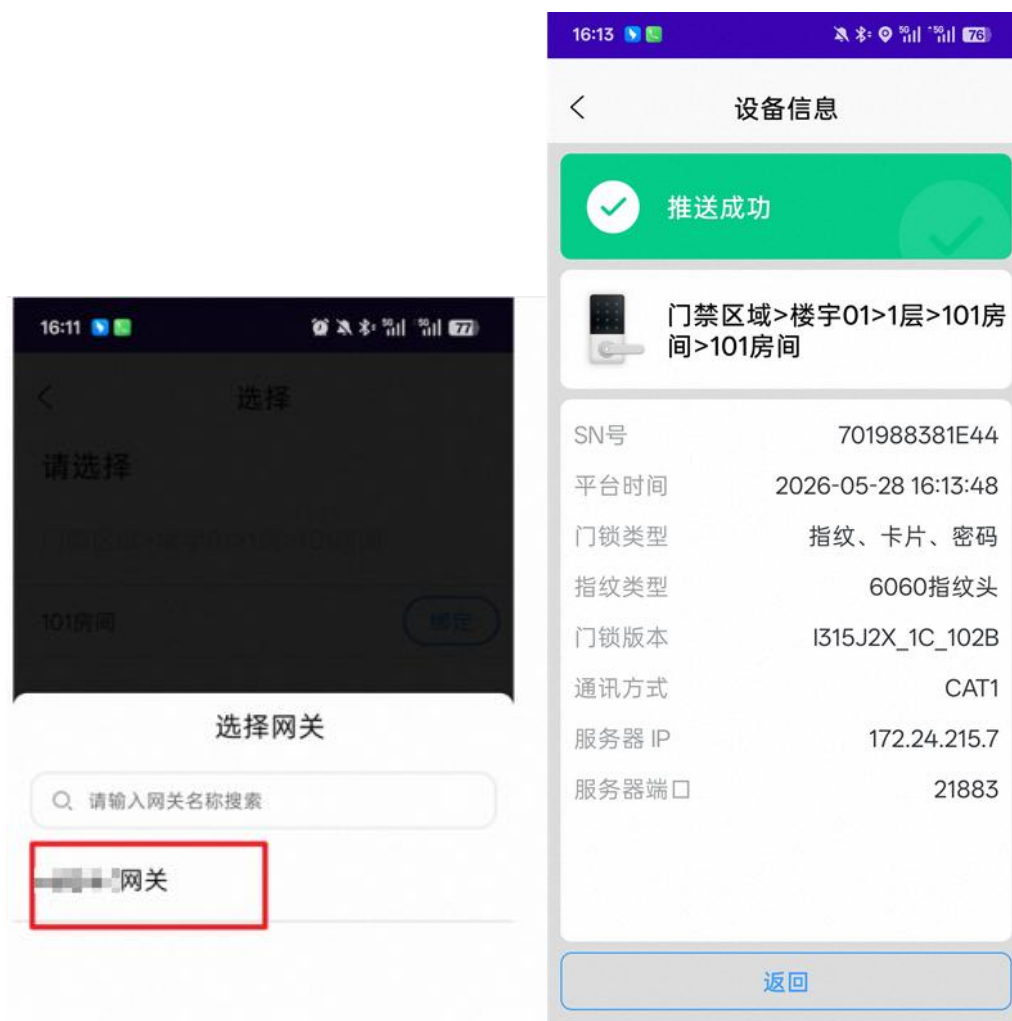


1. Return to the app login page and enter the account and password (the same administrator account and password used for the corresponding customer's Smart Lock Management System), then tap Login.



6. After login, locate the room according to the smart lock's area information and tap [Bind Device].





3.3.2 Smart Lock Re-Commissioning

If the smart lock was installed in the wrong location, such as the wrong room, how do I re-commission it?

In the mobile Commissioning Assistant, locate the smart lock for that room and tap [Remove]. Then select the correct location, bind it again, and move the phone close to the smart lock to re-commission it.

3.4 Virtual gateway (Wi-Fi Smart Lock)

3.4.1 Create Gateway

Menu "Device Management - Smart Lock Gateway Management": Add a virtual gateway. For Wi-Fi/4G smart-lock commissioning, each customer needs only one virtual gateway in the Smart Lock Management System.

Principle:

The IP address and port entered here are used by smart lock terminals for direct connection and are written to the lock when the lock is commissioned via mobile NFC.

Network Requirement:

For Wi-Fi smart locks, an internal-network address can be entered above, provided that the smart lock terminal can access it.

3.5 Wi-Fi Smart Lock Commissioning

3.5.1 Smart Lock Commissioning

Use NFC-enabled Android phone to install the O&M tool "Mobile Commissioning Assistant." The installation package is available in the attachment path "Terminal Supporting Programs\ Smart Lock Commissioning Assistant".

After installing the app, enable NFC on the phone and set this app (alias: BleNFC) as the default NFC payment application. On Xiaomi phones, select the SIM card wallet as the default payment method.



1. Open the app. First ensure that the phone is connected to the school's Wi-Fi

and that this Wi-Fi network can access the Smart Lock Managementsystem address.

2. In the app, tap [Server Settings], then enter the Smart Lock Management System IP address and port (default port: 28001).

3. On the [Server Settings] screen, enter the tenant ID to be used, tap Finish, and save the configuration.

4. "Wi-Fi Settings" must be configured. Enter the Wi-Fi information that the smart lock will connect to. During commissioning, this information is written to the lock so that it can connect to Wi-Fi.

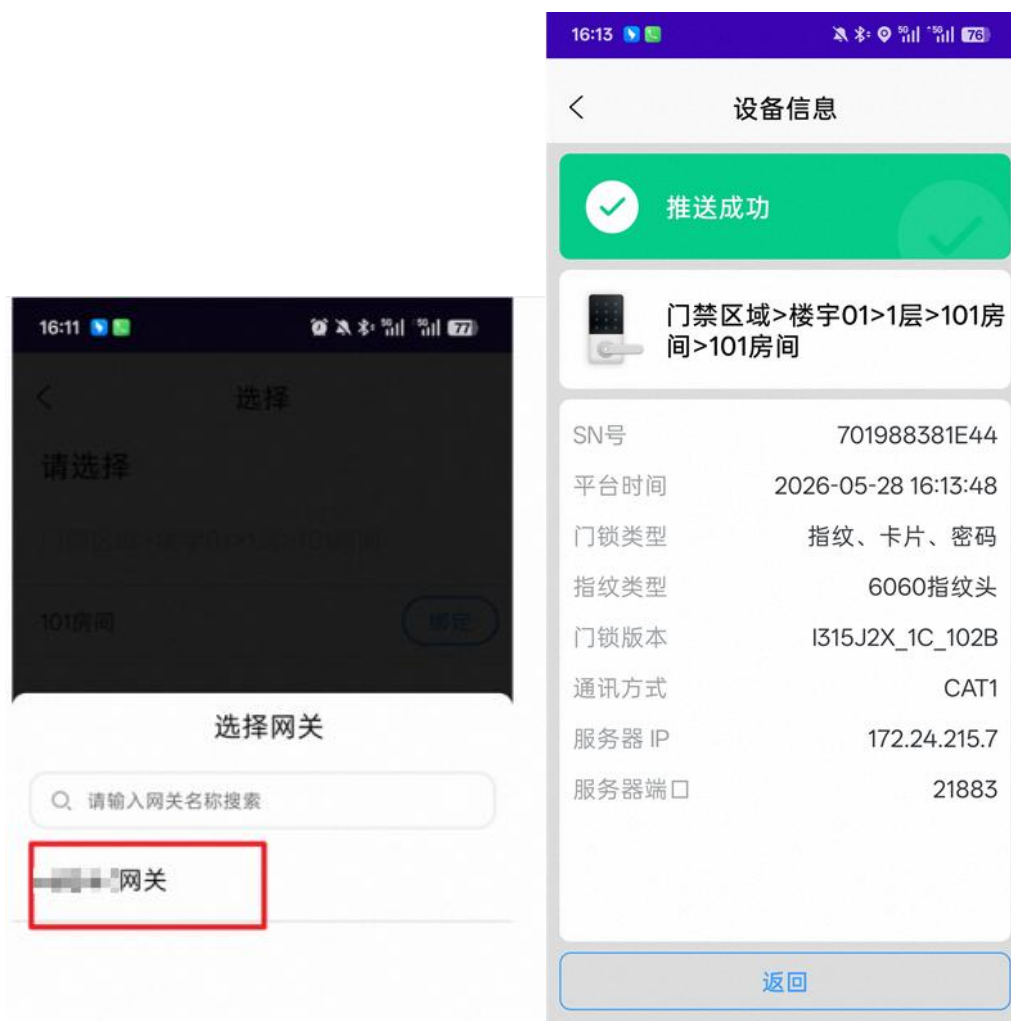


5. Return to the app login page, enter the account and password (the same administrator account and password used for the corresponding customer's Smart Lock Management System), then tap Login.



6. After login, locate the room according to the smart lock's area information and tap [Bind Device].





3.5.2 Smart Lock Re-Commissioning

If the smart lock was installed in the wrong location, such as the wrong room, how do I recommission it?

In the mobile Commissioning Assistant, locate the smart lock for that room and tap [Remove]. Then select the correct location, bind it again, and move the phone close to the smart lock to recommission it.

4 Device Business Data Commissioning

4.1 Authorization Rule Binding and Viewing

4.1.1 Add Authorization

Normally, **personnel are bound to areas (rooms)**.

Due to the characteristics of smart locks, authorization by other dimensions is generally not recommended, such as department or identity mapped to devices or

device groups.

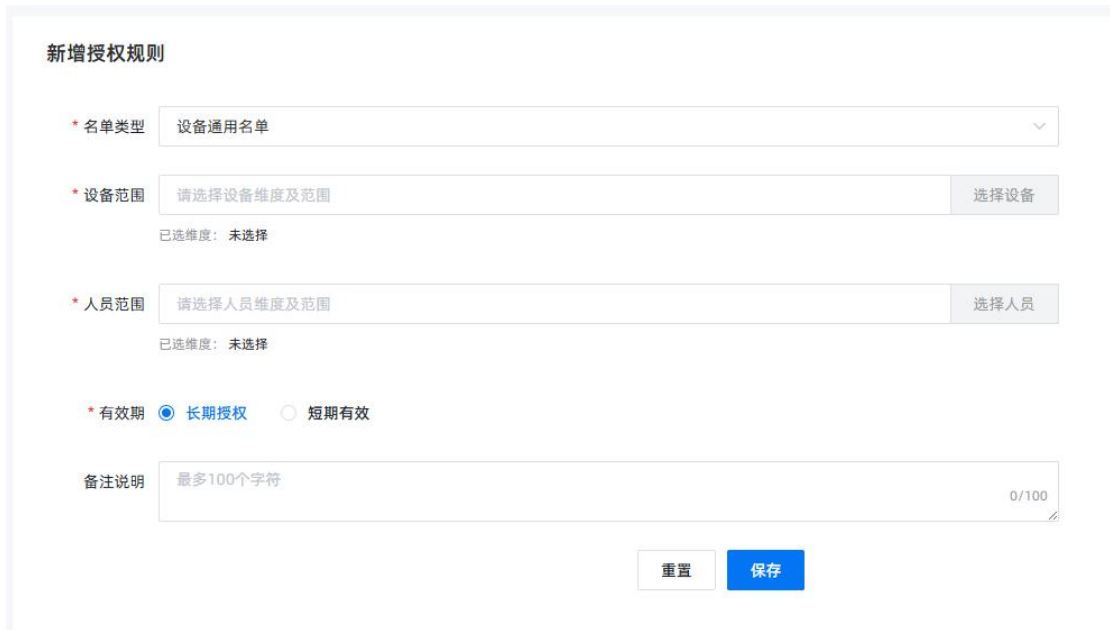
For "List Type," normally keep the default value "General Device List."

For "Device Scope," **it is recommended to select "By Area"**, although "By Device" is also supported.

For "Personnel Scope," **it is recommended to select "By Personnel."**:

Normally, authorization scopes do not need to be configured by department or personnel tag.

Menu path [Authorization Management —>Add Authorization],



4.1.2 Batch Import Authorization

Three batch-authorization methods are supported: batch grant area permissions to personnel, batch remove all area permissions from users, and batch remove all user permissions under an area.



According to actual requirements, download the corresponding Excel template, complete the data, and import it into the system.

4.1.3 View Existing Authorization Rules and Maintenance

Menu path [Authorization Management -> Device Authorization Rules]. Query authorization lists by area or device, then cancel the corresponding authorization as needed.

Query and maintain existing authorization rules by device/area and add new authorization as needed. Note: Lists authorized "By Device" can only be queried "By Device"; lists authorized "By Area" can only be queried "By Area."

授权的人员信息 当前查询维度: 按设备

人员 2 部门 0 人员标签 1

人员信息: 请输入姓名/人

添加授权 复制授权 取消授权 清空授权

当前表格已选择 0 项 清空

☐	姓名	人员编号	设备名称	有效期	创建时间	操作
☐	张认证01	210805	203房间-正式	长期授权	2026-06-18 1...	取消授权 编辑时间
☐	吴	130503	203房间-正式	长期授权	2026-06-18 1...	取消授权 编辑时间

共 2 条 10条/页 < 1 > 前往 1 页

Cancel Authorization — Select the authorization information to be canceled, then remove the existing authorization rule.

Add Authorization — Add new authorization for the device/area. In the pop-up page, select authorization by personnel or department.

人员选择

说明: 先按部门树定位范围, 再通过姓名/人员编号搜索并勾选人员记录, 适合少量精确授权。

按部门名称搜索

- 新开普大学
- 新开普大学校友会

按姓名/人员编号搜索

☐	姓名	人员编号	部门
暂无数据			

已选人员 (0个) 清空

暂未选择人员

共 0 条 < 1 >

授权时间: ☒ 长期授权 ☐ 短期有效

关闭 确定

Copy Authorization — Use the current device/area as the source and copy its authorization list to another device/area.

复制授权信息

复制授权来源

按设备：203房间-正式

选择要复制授权的人员信息维度

☒ 人员
☒ 部门
☒ 人员标签

复制授权目标

选择

关闭

确定

4.2 View Authorization Lists and Distribution Status

4.2.1 Authorization List Query

This function queries authorization lists in the system and their data-distribution status. Queries are normally performed by device.

人员信息：

区域/设备：

下发状态：

全部

授权状态：

有效

名单类型：

设备通用名单

所在部门：

设备序列号：

搜索

重置

导出

☐	区域/设备	姓名	人员编号	所在部门	区域全称	设备序列号	介质列表	授	操作
☐	203房间-正式	王宏业-测...	171130	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	203房间-正式	林予初20	20252161	新开普大学-安全学院-信...	2号楼/2层/203房间	4931525062...			授权关系
☐	203房间-正式	吴少飞	130503	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码 ...		授权关系
☐	203房间-正式	张喜龙-认...	210805	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	人脸平板1	张三(外部)	9000000...		武汉大学/梅园1舍	333			授权关系

共 5 条

10条/页

<

1

>

前往 1 页

The "Credential List" shows the authentication methods that the person can use to open the door on the device. Hover over a credential to display details such as the card number.

设备序号	介质列表	授权状态	下发状态	开始时间	结束时间	操作
4931525062...	卡 密码	有效	未下发	-	-	授权关系
4931525062...		有效	未下发	-	-	授权关系
4931525062...	C2390D3F ...	有效	未下发	-	-	授权关系
4931525062...	卡 密码	有效	未下发	-	-	授权关系
333		有效	未下发	2026-...	2026-...	授权关系

"Distribution Status" If the status is "Not Distributed," the data has not yet been sent to the device. The displayed status usually has a delay of 1 - 3 minutes.

"Authorization Relationship" can be used to view detailed information about the authorization list and trace the source from which the authorization list was generated.

授权关系

授权名单详情

对应授权规则详情

姓名	吴	人员编号	130503
所在部门	新开普大学-出入应用事业部		
区域全称	2号楼/2层/203房间		
设备名称	203房间-正式	设备序号	4931525062010119
介质	卡 密码 指纹	下发状态	未下发
名单类型	设备通用名单	授权时间类型	长期
版本号	49		

授权关系

授权名单详情

对应授权规则详情

人员维度:	人员 吴 503
设备维度:	设备 203房间-正式 (1000019)
授权时间:	长期授权
创建时间:	2026-06-18 17:16:33 - admin (admin)

4.3 Device Operation Monitoring and Door-Opening Records

4.3.1 Smart Lock Monitoring

This function provides monitoring and O&M for intelligent devices, including smart locks and smart-lock gateways. The page has three tabs: Data Summary, Smart Locks, and Smart-Lock Gateways.



Distribution Consistency: Use this option to filter the distribution status of device authorization lists. If distribution is inconsistent, the device requires attention. Click [Inconsistent] in the list to view the details.

设备名称	设备序列号	联机情况	电量	电压值(V)	信号强度	门状态	区域	操作
2门锁	22222222	脱机				关闭	行知园2/1号楼/1层/101	远程开门 远程运维
2号楼101门锁	2026052901	脱机				关闭	2号楼/1层/101房间	远程开门 远程运维
202门锁	I315250427...	脱机				关闭	2号楼/2层/202-扫码开通	远程开门 远程运维
203房间-正式	4931525062...	脱机	82%	5.742	82	关闭	2号楼/2层/203房间	远程开门 远程运维

Inconsistencies are categorized as "Platform to Gateway" and "Gateway to Smart Lock," allowing the specific stage of an authorization-list mismatch to be identified.

名单下发不一致性情况

从平台到网关从网关到门锁

不一致情况汇总

设备名称	203房间-正式	设备序列号	4931525062010119	未下发数量	26
版本号对比	平台: 51, 网关: 0	名单数量对比	平台: 4, 网关: 0		

未下发的名单列表

姓名: 请输入 姓名

人员编号: 请输入 人员编号

搜索

重置

姓名	人员编号	开始时间	结束时间	状态	介质	名单类型
测试人员.	20260600011			无效	卡	设备通用...
测试人员.	20260600011			无效	卡	设备通用...
测试人员	20260600011			无效	卡	设备通用

共 26 条10条/页<123>前往1 页

Remote Door Opening: When the device is online, you can open the door, set it to normally open, or lock it remotely.

Remote O&M: Includes clearing authorization lists, fingerprint enrollment, and status reporting. After using "Fingerprint Enrollment," select the person whose fingerprint needs to be enrolled and initiate enrollment for that person. The person can then continue fingerprint enrollment on the smart lock device.

4.3.2 Door-Opening Records View

After checking the door-opening action on the smart lock terminal, Menu path [Data Reports - Detailed Data-Smart Lock Door-Opening Records], can be searched by access time, authentication method, and other conditions.

Primarily provides Personnel successfully open the door on the smart lock device; successful door-opening records are displayed, and the supported device type is limited to smart locks.and supports searches within a selected date range by area, device, device group, name, student/employee ID, authentication method, and other dimensions.

区域

部门

设备

请输入区域名称

1号楼

2号楼

武汉大学

测试密钥下发

网关区域

行知园2

起止日期:

2026-06-24 00:00:0 - 2026-06-30 23:59:5

姓名:

请输入姓名

人员编号:

请输入人员编号

认证方式:

请选择认证方式

身份:

请选择身份

搜索

重置

导出

☐	#	通行时间	姓名	人员编号	人员部门	人员身份	区域
☐	1	2026-06-24 18:20:05	测试人员.	20260600011	出入应用事业部	在职人员	203
☐	2	2026-06-24 18:20:05	测试人员.	20260600011	出入应用事业部	在职人员	203
☐	3	2026-06-24 10:52:39	测试人员.	20260600011	出入应用事业部	在职人员	203
☐	4	2026-06-24 10:52:31	测试人员.	20260600011	出入应用事业部	在职人员	203
☐	5	2026-06-24 10:24:54	测试人员.	20260600011	出入应用事业部	在职人员	203

共 9 条

10条/页

<

1

>

前往

1

页

4.3.3 Smart Lock Alert Data

On the Menu path [Data Reports - Detailed Data-Smart Lock Alert Data], You can view door-opening failures and smart-lock alert data..

区域

设备

请输入区域名称

1号楼

2号楼

武汉大学

测试密钥下发

网关区域

行知园2

认证方式:

请选择 认证方

预警类型:

请选择 预警类

起止日期:

2026-06-24 00:00:0 - 2026-06-30 23:59:5

姓名:

请输入 姓名

人员编号:

请输入 人员编

搜索

重置

☐	通行时间	人员信息	区域	设备名称	设备型号	预警类型	操作
☐	2026-06-30 15:38:03		行知园2	F972-174test	F9721B1	防拆报警	
☐	2026-06-30 15:31:24		203房间	203房间-正式	I315K2X-FG6060	OK	
☐	2026-06-30 14:32:19		行知园2	F972-174test	F9721B1	防拆报警	
☐	2026-06-29 08:30:23		行知园2	F972-174test	F9721B1	防拆报警	
☐	2026-06-25 16:23:32		行知园2	F972-174test	F9721B1	防拆报警	
☐	2026-06-25 10:32:24		行知园2	F972-174test	F9721B1	防拆报警	

共 12 条

10条/页

<

1

2

>

前往

1

页

4.4 Device Parameters

4.4.1 Parameter Planning

If dormitory buildings and office buildings use different device-parameter sets, create the two parameter sets in advance and bind each set to the corresponding devices.

If no separate parameter sets are required, use the default parameter set already provided by the system.

4.4.2 Parameter Binding

Both gateways and smart locks can be bound to parameter groups. When editing devices under "Smart Lock Management" or "Smart Lock Gateway Management," you can view and maintain the bound parameter-group information.

Special Note:

Multiple smart locks under the same gateway must use the same parameter group; otherwise, additional parameter groups will not take effect.

4.4.3 Device Parameter Groups

Menu path "Device Management - Device Parameter Management - Device Parameter Groups." Here you can maintain parameter items in existing groups, copy groups to create new ones, and perform related operations.

4.4.3.1 Gateway Parameter Groups

Normally no maintenance is required, so this section does not describe them separately.

4.4.3.2 Smart Lock Parameter Groups

Normally, only the items under "Common Parameters" need to be maintained, as described below:



1) Smart-lock card-reading mode, corresponding parameter "Card-Reading Security Level": 0 = read card serial number; 1 = read card content.

When card-content reading is configured: If the card is a CPU card issued by the V8 One-Card Platform, there is no need to read a system card or parameter card.;

If the card is an M1 card or CPU card under the T6 One-Card Platform, after the parameter settings have been distributed and taken effect, swipe the system card and parameter card once on the smart lock terminal.;

2) Unlock Mode: 0 = automatically relock after card swipe; 1 = swipe card to

unlock and swipe card again to lock.

3) Smart Lock Identity Authorization Policy: Controls the time periods during which personnel with different identities may open the lock. This function is used infrequently and does not need to be configured unless specifically required.

4) Door-Opening Authentication Methods: These are not configured through platform parameters; they are determined by the smart lock model. For example, whether a lock supports QR-code scanning or card swiping depends on the specific product model.

5 Smart Lock Common Commissioning Operations

Description

5.1 Maintain Door-Opening Passwords

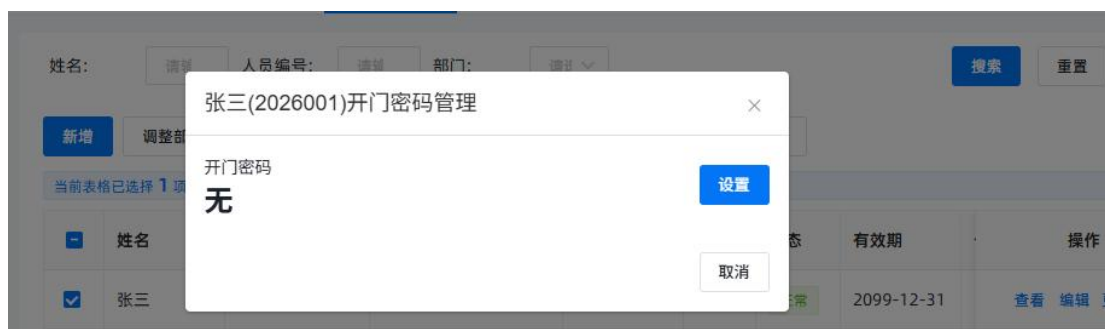
5.1.1 Initial Door-Opening Password for Personnel

Menu path "System Management - Parameter Configuration - Door-Opening Password Rules." Configure the smart-lock door-opening password rules for personnel here. You can also initialize passwords according to a specified rule for personnel who currently have no door-opening password..



5.1.2 Administrator-Assisted Door-Opening Password Maintenance

Menu path "User Management - Personnel Information." Select a person and choose [Door-Opening Password].



5.1.3 Users Maintain Their Own Door-Opening Passwords

In the mobile [Door Opening Assistant], users can maintain their own door-opening passwords.

5.2 Enroll Fingerprints

5.2.1 Enroll by Swiping a Card on the Lock

Prerequisite: The person must have a valid authorization list on the terminal.

Wake the device using the smart-lock keypad, then enter the command. The lock prompts you to swipe a card. Swipe the authorized physical card and follow the voice prompts to enroll two fingerprints. Enrollment is then complete.

Enrollment commands differ by smart lock type:

Command for LoRa/4G/Wi-Fi smart locks: *1#

Command for SUB-1G smart locks: *#

5.2.2 Initiate Enrollment from the Mobile App

In the mobile Door Opening Assistant, go to "Me" — "Fingerprint" to enroll or remove fingerprints.



After the remote command is sent from the mobile app, .

For LoRa smart locks, wake the device using the smart-lock keypad, then enter *9# to start fingerprint enrollment.

SUB-1G smart locks do not require terminal-side operation; fingerprint enrollment can be initiated automatically.

5.2.3 Fingerprint Scanner Enrollment

Prerequisite: A dedicated fingerprint scanner has been purchased..
Menu path "User Management - Personnel Information." Select a person and choose [Fingerprint Maintenance].

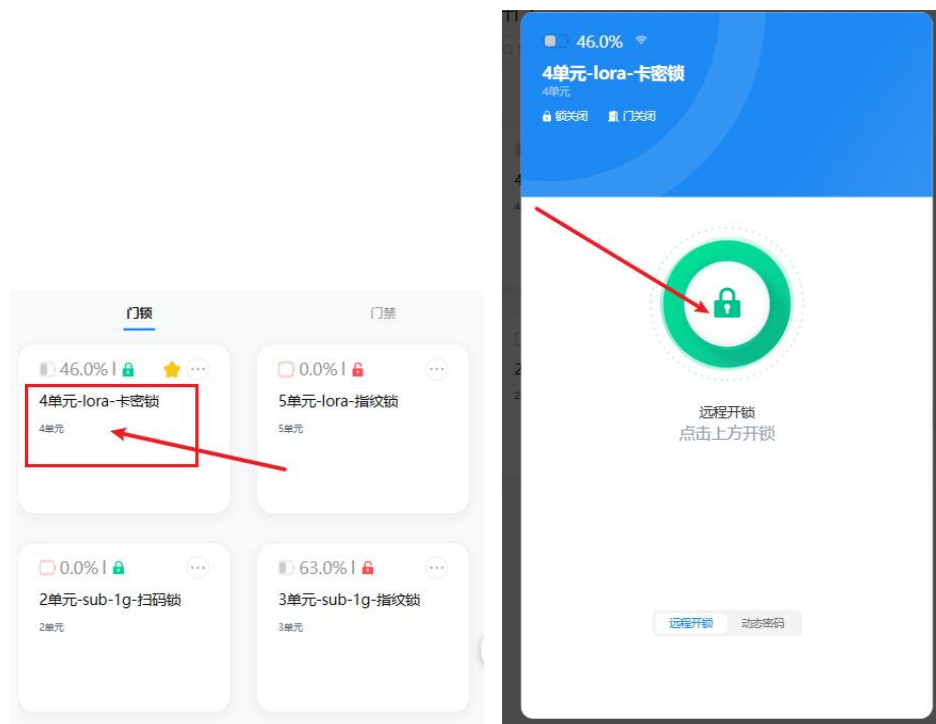
5.3 Remote Door Opening

5.3.1 PC-Side Remote Door Opening

Menu path [Device O&M Monitoring - Smart Lock Monitoring]], On the Smart Lock page, locate the specified device and use the "Remote Door Opening" function..

5.3.2 Mobile Remote Door Opening

In the mobile Door Opening Assistant, tap the corresponding device icon under "Open Door," then open the door from the expanded page.



5.3.3 Smart Lock Device Action

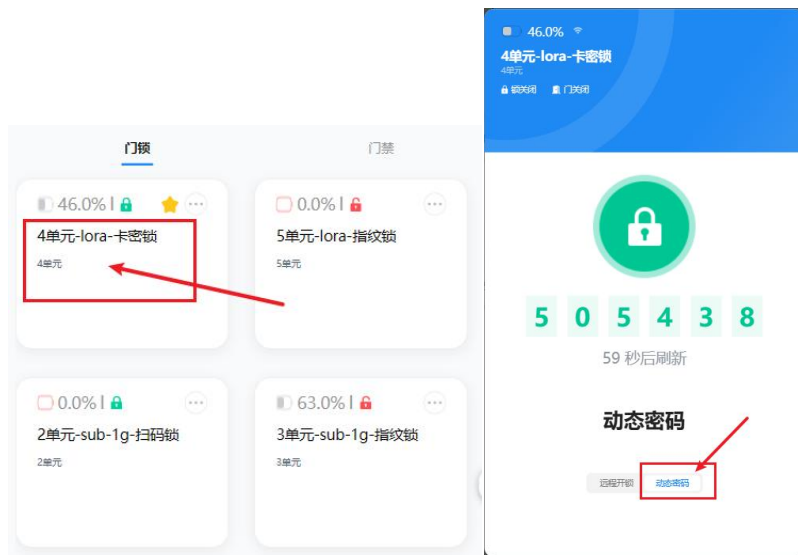
For LoRa/4G/Wi-Fi smart locks, after a remote command is sent, the corresponding action must be performed on the smart lock terminal before the door can open: wake the device using the smart-lock keypad and enter the command *9# to unlock the door.

For SUB-1G smart locks, after a remote command is sent, no action is required

on the terminal; the door opens directly.

5.4 Open Door with Dynamic Password

In the mobile Door Opening Assistant, tap the corresponding device icon under "Open Door," then select the [Dynamic Password]] tab on the expanded page. A six-digit door-opening password is displayed.



Wake the device using the smart-lock keypad, then enter the six-digit password to unlock the door.

5.5 Common LoRa Gateway Operations

5.5.1 Replace Gateway Device

If a gateway fails, remove the old gateway and replace it with a new one. As shown below, select the gateway device, then choose "More - Replace Gateway."



更换网关

网关名称: 1号楼2层西网关

当前序列号: 50311081201

* 新网关序列号: 请输入 新网关序列号

请输入设备序列号

确定

取消

5.5.2 Change Gateway Area

If the area bound to a gateway needs to be changed, select the gateway device and choose "More - Change Area," as shown below.

按名称搜索

全部区域

中山大学勤香园

科学校区求索园

当前区域: 中山大学勤香园/区域网关/1号楼2层东

网关名称: 请输入 网关名称

网关序列号: 请输入 网关序列号

搜索

重置

展开

TMS文件操作

TMS数据上传

新增

导出

推送到物联网

网关配置模版

当前表格已选择 1 项 清空

☒	网关名称	网关型号	网关序列号	区域	关联门锁	网关状态	推送物联网状态	操作
☒	1号楼2层西网关	P311K00	50311081201	中山大学勤香园/网关区域/1号楼2层东	0 个	待激活	未同步	查看 编辑 更多

更换网关

更换区域

关联门锁

删除

更换区域

网关名称: 1号楼2层西网关

当前区域: 中山大学勤香园/网关区域/1号楼2层东

* 选择新区域: 请选择区域

确定

取消

5.5.3 Gateway Upgrade

The gateway software supports OTA upgrades.

5.5.3.1 Download Software Package

Download the latest gateway upgrade package from the IoT platform. The minimum version is P311-APP_v0.0.1-2026-06-30-1516.



5.5.3.2 Upload Upgrade Package

Under "OTA Upgrade - Upgrade Package Management," upload the new software upgrade package.

5.5.3.3 Create Upgrade Task

Under "OTA Upgrade - Upgrade Task Management," create an upgrade task, select the upgrade package created above, select the smart-lock gateway devices to upgrade, and wait until the device upgrade is complete.

5.5.4 Gateway Reset

Use factory reset with caution. It is generally performed only when a gateway has configuration issues or abnormal communications. With the data collector (LoRa gateway) powered on, press and hold the button to the left of the power port for more than 5 seconds, then release it. The data collector restores factory settings. After the reset, the gateway Ethernet and network-connection parameters are reset. With the data collector (LoRa gateway) powered on, briefly press the button to the left of the power port to restart the gateway.

5.5.5 Gateway Data Check

Open the LoRa gateway page in a browser.

Address: <http://gateway-IP:8092>

Default credentials: developer/ncap@300248 (older gateways: admin/ncap@300248)

1. Query Smart Lock Device Information

Key: /Dev/Device

2. Query Parameters

Key: /Lock/PData

3. Query Authorization List

Key: /Lock/NLD. This shows the lists under the smart lock, including the corresponding user ID, primary card, secondary card, virtual card, fixed password, fingerprint, facial data, and more.

key	操作
/Lock/NLD/303147112B003000	删除
/Lock/NLD/3332470E46002E00	删除
/Lock/NLD/3431470529004C00	删除

View Facial Credential: Key: /FACE

数据库 MODB Key /EIG/90

对应了数据库中udc_user_finger表中的数据，盒子中有该数据表示

Log in to the gateway through SSH using the command shown below. Replace the IP 192.168.50.24 with the actual gateway IP address. Default password: ncap.300248

```
ssh root@192.168.50.24
```

```
[Alert.ALERTWORK] > ssh root@192.168.50.24
sh: /usr/bin/xauth: not found
#
```

Command to delete gateway data:
rm -rf /data/data/Boxioserver/Data/DB
Restart Gateway
reboot

5.6 Common LoRa Smart Lock Operations

5.6.1 Smart Lock Upgrade

The smart lock embedded software supports two upgrade methods: OTA upgrade and upgrade-card upgrade.

5.6.1.1 OTA Upgrade

OTA transmission is generally slow. The duration is largely independent of the number of smart locks being upgraded—upgrading one lock and upgrading 50 locks take roughly the same time. Transmission and successful upgrade typically require more than 30 minutes.

■ Upload Software Package

In the Smart Lock Management System, go to [Device Management - OTA Upgrade - Upgrade Package] and upload the software package. For now, obtain the package from the attachments; later, download it from the IoT platform.



Parameters:

File Category — MCU Firmware

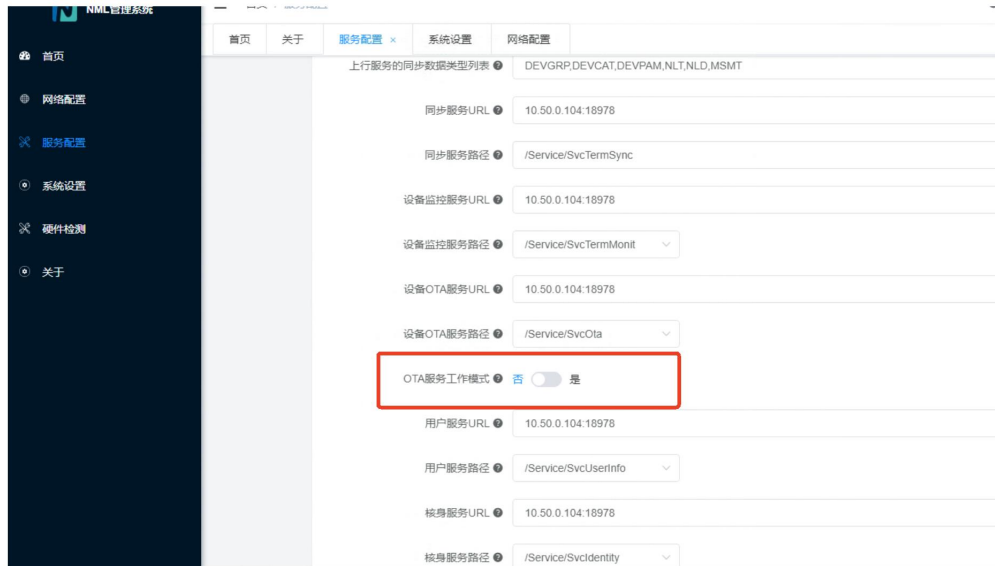
Device Category — Smart Lock

Upgrade Package Version — Must be defined strictly according to the version number and must not contain Chinese characters.

■ Create Upgrade Task

Go to [Device Management - OTA Upgrade - Upgrade Tasks], create a new upgrade task, and configure the upgrade according to actual requirements.

Note: LoRa OTA packages are sent to the gateway, which acts as a proxy to deliver the OTA upgrade to smart locks. Check the gateway service configuration and enable OTA service operating mode.



5.6.1.2 Upgrade Using an Upgrade Card

1. Create an Upgrade Card

Use the Smart Lock Card Programming Tool. A high-capacity CPU card is required. Tool path: "Supporting Programs/Smart Lock Card Programming Tool."

2. Swipe the Upgrade Card

After the upgrade card is created, it can be swiped on multiple smart locks to perform the upgrade.

5.6.2 Device Removal and Decommissioning

After performing [Remove] on a device, its status changes to [Removed]. It can then be [Installed] again at another location.

After performing [Decommission] on a device, its status changes to [Decommissioned]. The device can no longer be enrolled or commissioned again.

If a device in Removed or Decommissioned status needs to be deleted and is no longer required, query it in the database and remove it manually.

```
SELECT * FROM `dev_info` order by device_id desc;
```

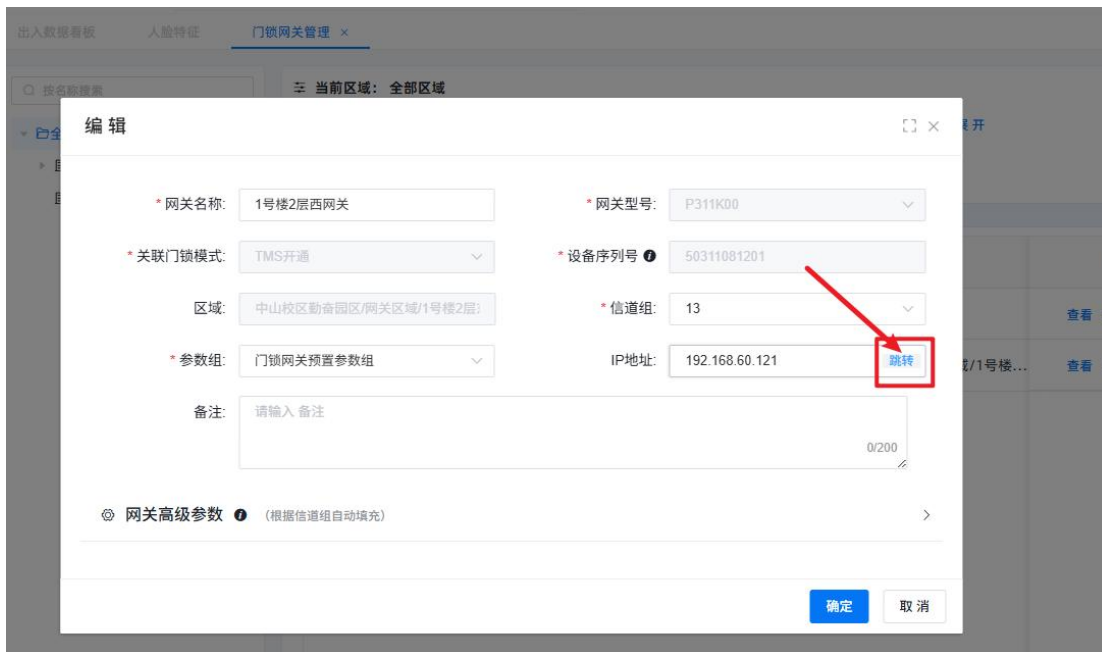
6 Common Routine Maintenance Operations

6.1 How to Log In to the Gateway Web Page

6.1.1 LoRa Gateway Web Page Access

Method 1: Enter the address directly in a browser using the format IP:8092.

Method 2: Under "Device Management - Smart Lock Gateway Management," locate the gateway device, click Edit, then click [Go] next to the IP address to open the gateway page automatically.



The screenshot shows a web interface for managing LoRa gateways. A modal window titled '编辑' (Edit) is displayed over a background of a gateway management table. The modal contains the following fields:

- * 网关名称: 1号楼2层西网关
- * 网关型号: P311K00
- * 关联门锁模式: TMS开通
- * 设备序列号: 50311081201
- 区域: 中山校区勤斋园区/网关区域/1号楼2层
- * 信道组: 13
- * 参数组: 门锁网关预置参数组
- IP地址: 192.168.60.121
- 备注: 请输入备注

A red arrow points to a blue button labeled '跳转' (Jump) located next to the IP address field. At the bottom of the modal are '确定' (Confirm) and '取消' (Cancel) buttons.

The gateway's default username and password are developer/ncap@300248 (older gateways: admin/ncap@300248)., Change them promptly when using the device on site.

6.1.2 SUB-1G Gateway Web Page Access

Default web page address: 192.168.50.34. Connect the computer directly to the gateway using an Ethernet cable. The computer IP address must be on the same subnet as the gateway.

Access address: Gateway IP address

Default account/password: admin/admin (Change the password promptly on site.)

6.2 View and Download Service Logs

6.2.1 Check Logs When Problems Occur in Management-System

Operations

On the Light Cloud Platform or Container Platform, locate the "Smart Lock Management System" service named "Smart Lock Management Core Service" to view and download logs.

Real-time logs can be viewed or downloaded as shown below.

出入核心服务 运行中

英文名称: acs-serve | 应用: zhqjyypt | 镜像: harbor.newcapec.cn/zhqjyypt/acs-serve-v-3.0.0-20260716

总览 监控 日志 扩缩容 服务配置项 端口 存储 服务调度配置 内核参数

实时日志 历史日志

2026-07-17 15:51:10.017 INFO 1 --- [dPool-2/3639941] c.n.job.core.executor.XxxJobExecutor: >>>>>>>> xxi-job regist JobThread success, jobId:33, handler:com.newcapec.udc.job.core.handler.impl.MethodJobHandler@253aa34b[class com.newcapec.modules.job.handler.JobFaceHandler#sfSyncPhotoHandler]

2026-07-17 15:51:10.013 INFO 1 --- [3-1784274670011] c.n.modules.job.handler.JobFaceHandler: ===== sfSyncPhotoHandler定时任务 =====

2026-07-17 15:51:10.016 INFO 1 --- [3-1784274670011] o.s.core.mp.plugins.SqlLogInterceptor:

===== Sql Start =====

Execute SQL: select 'id', param_name, param_value, param_enc from acs_sys_param where (param_name like 'face.%' and is_deleted = 0)

Execute Time: 0.621ms

===== Sql End =====

2026-07-17 15:51:10.017 ERROR 1 --- [3-1784274670011] c.n.mu.job.impl.UserFaceJobService: 人脸平台访问信息配置不完整: com.newcapec.modules.userface.dto.FaceRemoteDto@c66ed5b

2026-07-17 15:51:10.017 ERROR 1 --- [3-1784274670011] c.n.modules.job.handler.JobFaceHandler: 照片同步任务>>>>>>>>失败:

org.springframework.core.log.exception.ServiceException: 人脸平台访问信息配置不完整

2026-07-17 15:51:11.388 INFO 1 --- [acs-scheduler-4] o.s.core.mp.plugins.SqlLogInterceptor:

===== Sql Start =====

Execute SQL: select ID, K, V from acs_key_val where (K = 'acs:taskpass_comp_last_id')

Execute Time: 1.039ms

===== Sql End =====

2026-07-17 15:51:11.388 INFO 1 --- [acs-scheduler-4] c.n.system.schedule.PassRecordCompTask: 通行记录补偿任务本次lastid: 0

2026-07-17 15:51:11.391 INFO 1 --- [acs-scheduler-4] o.s.core.mp.plugins.SqlLogInterceptor:

===== Sql Start =====

Execute SQL: select id, 'rec_id', 'dev_id', 'user_id', 'io_flag', 'result_code', 'dev_time', 'req_time', 'meta_data', 'credentials', 'credentials_type' from acs_record where ('dev_time' <= 1784274611388 and id > 0) order by id asc limit 500

Execute Time: 0.783ms

===== Sql End =====

2026-07-17 15:51:33.051 INFO 1 --- [2-1784274600013] c.n.udc.job.core.thread.JobThread: >>>>>>>> xxd-job JobThread stopped, hashCode:Thread[xxd-job, JobThread-771233908,1472-1784274600,13,10,main]

2026-07-17 15:51:33.055 INFO 1 --- [8-1784274600014] c.n.udc.job.core.thread.JobThread: >>>>>>>> xxd-job JobThread stopped, hashCode:Thread[xxd-job, JobThread-260869416,22788-178427460,0014,10,main]

已连接 等待服务打印日志...

请输入关键词

跟随 下载 清除

To download historical or complete logs, follow the procedure shown below.

出入核心服务 运行中

英文名称: acs-serve | 应用: zhqjyypt | 镜像: harbor.newcapec.cn/zhqjyypt/acs-serve-v-3.0.0-20260716

更新 停止

总览 监控 日志 扩缩容 服务配置项 端口 存储 服务调度配置 内核参数

实例状态

1 运行中

内存

2.04GB / 4.00GB 51.03%

CPU

0.06 Core / 0 Core 0%

运行实例

状态	名称	负载 / 容器IP	主机节点名称 / IP	更新时间	操作
运行中	v3ttaxn40j6x29kpbv1qit4w	77.88.0.33 (ingress) / 77.88.1.43 (container)	swarmanager1/192.168.60.127	2026-07-17 14:53:45	详情 控制台 日志 文件上传/下载



6.2.2 Device Communication Logs

6.2.2.1 Real-Time Viewing

Log in to the IoT platform and view logs for the device associated with the issue. Menu path: "Device Management - Devices." Locate the specific device and click [Details], as shown below.



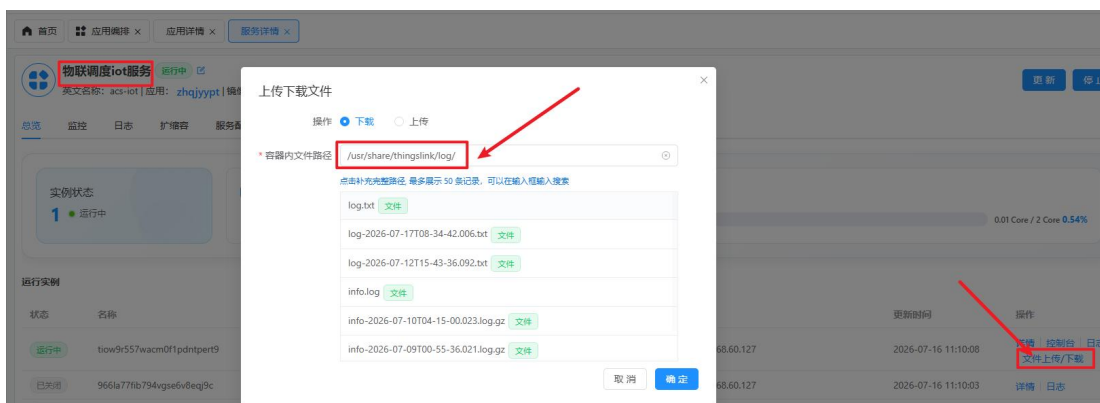
Open the [Activity Trace] page to view the actual device requests and responses.



6.2.2.2 Download Historical Logs

On the Light Cloud Platform or Container Platform, locate the "Smart Lock Management System" service named "IoT Scheduling Service" to view and download logs.

The log directory inside the container is /usr/share/thingslink/log/.



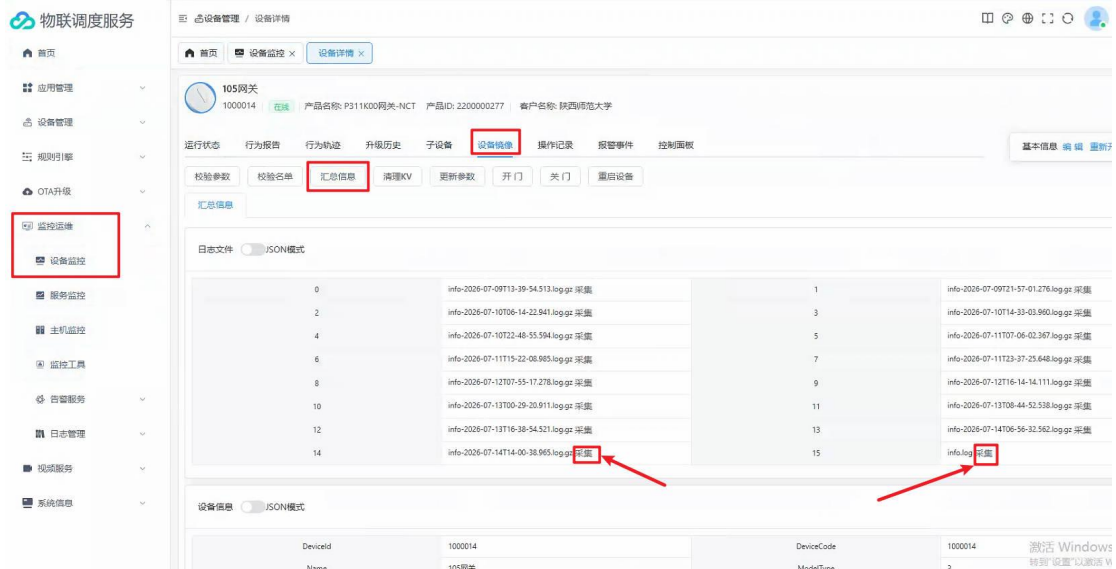
6.2.3 LoRa Gateway Logs

Sometimes LoRa gateway logs need to be downloaded. Use the following method to download and view them.

Log in to the IoT platform. Menu path: "Monitoring & O&M - Device Monitoring." Locate the specific gateway device and click Details, as shown below.



On the "Device Mirror" page, click "Summary Information." The gateway log list shown below is loaded. Click [Collect] after the log file name you want to download to retrieve that log.



6.3 Offline / Connection Issues

6.3.1 LoRa Gateway Offline

On the "Device Monitoring & O&M - Smart Lock Monitoring", check whether the LoRa gateway is online.

If the gateway is offline -

1. Check the gateway configuration and gateway software version.
2. Check the gateway logs.

6.3.2 LoRa Smart Lock Offline

On the "Device Monitoring & O&M - Smart Lock Monitoring", check whether the smart lock is online.

If the smart lock is offline, possible causes include:

Channel-group mismatch — The gateway channel-group parameter may have been changed on the platform after the smart lock was commissioned.

Channel interference — Channel groups were not planned and configured according to the recommended gateway planning rules.

Antenna not installed correctly — Check the antenna installation.

Signal obstruction — Check the antenna installation position.

Excessive distance — Check the smart lock installation distance and re-plan the deployment.

Low battery (10%) — A smart lock cannot come online when its battery level is too low.

6.3.3 Sub1g Base Station Offline

Under Device Management - Device Monitoring, check whether the SUB-1G base

station is online.

If the base station is offline -

1. Check the gateway configuration, gateway software version, and restart the base station.

6.3.4 Sub1g Smart Lock Offline

On the "Device Monitoring & O&M - Smart Lock Monitoring", check whether the smart lock is online.

If the smart lock is offline, possible causes include:

Channel mismatch — The gateway channel parameter may have been changed on the platform after the smart lock was commissioned.

Antenna not installed correctly — Check the antenna installation.

Signal obstruction — Check the antenna installation position.

Excessive distance — Check the smart lock installation distance and re-plan the deployment.

Low battery (10%) — A smart lock cannot come online when its battery level is too low.

Newly joined device — When a new smart lock is commissioned, the displayed online status of all devices may be affected for about 2 minutes. This is only a status-display refresh and does not affect the actual connection status of the devices.

6.4 Authentication Succeeds but Door Does Not Open

6.4.1 Card Swipe Does Not Unlock the Door

■ Platform-Side Check

1. Authorization List Query - Check whether an authorization list exists.

人员信息:

请输入姓名/人员编号

区域/设备:

请选择区域/设备

下发状态:

全部

授权状态:

有效

名单类型:

设备通用名单

所在部门:

请选择部门

设备序列号:

请输入设备序列号

搜索

重置

导出

☐	区域/设备	姓名	人员编号	所在部门	区域全称	设备序列号	介质列表	授	操作
☐	203房间-正式	王	171130	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	203房间-正式	林	20252161	新开普大学-安全学院-信...	2号楼/2层/203房间	4931525062...			授权关系
☐	203房间-正式	吴	130503	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码 ...		授权关系
☐	203房间-正式	张	210805	新开普大学-出入应用事业部	2号楼/2层/203房间	4931525062...	卡 密码		授权关系
☐	人脸平板1	张	9000000...		武汉大学/梅园1舍	333			授权关系

共 5 条

10条/页

<

1

>

前往

1

页

- 1) If a list exists, check whether the credential list includes [Card]. If [Card] is absent, the person's card status is abnormal.
- 2) If [Card] is present, continue troubleshooting on the Personnel Information page. Select the person, click [Issue Card], and check whether the card number and card status are normal.



- 3) If no list exists, authorization binding has not been configured, or the correct list was not generated after authorization binding. Go to [Device Authorization Rules] and check the configuration. Query the authorization list by area or device and add the correct authorization.



■ LoRa Gateway Data Check

Log in to the gateway page and check whether the gateway KV data is normal.

■ Sub1g Base Station Packet Capture

Capture and analyze data packets between the server program (port 15035) and the specified base station.

■ Connection Status Check

6.4.2 QR-Code Scan Does Not Open the Door

The checks are the same as for a card swipe that does not unlock the door, with the following additional check:

The issue is usually caused by an incorrect key being distributed, preventing the terminal from decoding the QR code.

Check the earlier section " Smart Lock QR-Code Configuration."

6.4.3 Facial Recognition Does Not Open the Door

The checks are the same as for a card swipe that does not unlock the door, with the following additional check:

This is usually caused by missing facial-algorithm feature data or incorrect configuration, preventing the terminal from recognizing the face.

Note that the algorithm type corresponding to the smart lock is: Megvii Algorithm KS-L100

组织机构: 输入关键字进行过滤
 姓名/学工号: 请输入
 算法类型: 旷视算法-L100
 人脸特征: 有特征
 重置 查询 展开

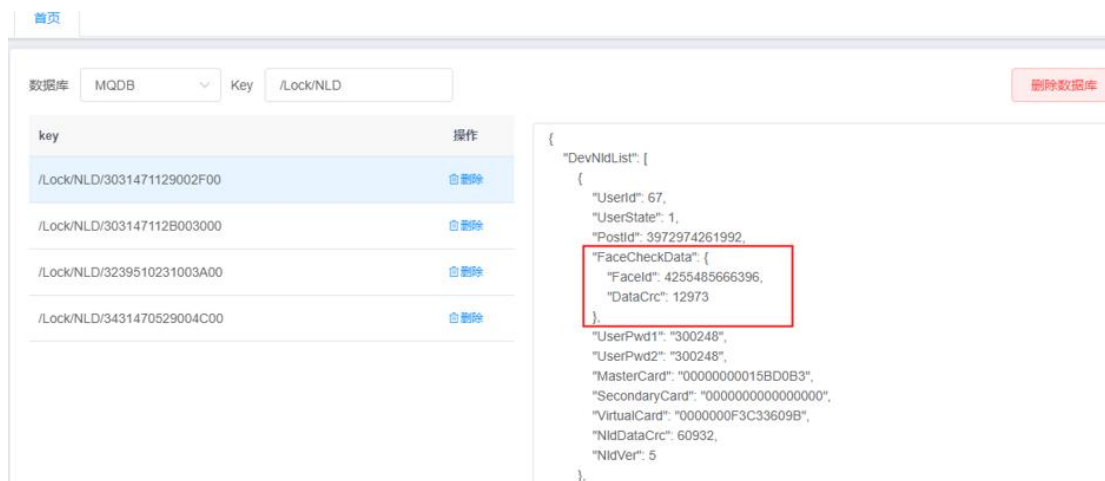
抽取特征 导出特征

组织机构: 新开普大学, 新开普大学校友会

姓名	学号	人员身份	算法底库照片	算法名称	算法版本	人脸特征	特征状态	更新时间	操作
刘	000715	在职人员		旷视算法	KS-L100	VFVaWU 1RQU...	正常	2026-07-17 10:40:24	重新提取
蒋	241002	在职人员		旷视算法	KS-L100	VFVaWU 1RQU...	正常	2026-07-15 11:01:54	重新提取
李	000065	在职人员		旷视算法	KS-L100	VFVaWU 1RQU...	正常	2026-07-03 11:22:26	重新提取

After authorization, on the [Authorization List Query] page, check whether the person on the device has the [Face] credential.

For further troubleshooting, check the corresponding gateway and inspect the authorization list in KV data to determine whether facial feature data is missing.



6.5 How to Create Smart Lock O&M Cards

Tool path: "Supporting Programs/Smart Lock Card Programming Tool."

6.5.1 Create an Upgrade Card

This card stores the embedded firmware. Swiping it on a smart lock triggers the smart lock firmware upgrade.

6.5.2 Create an Engineering Commissioning Card

Used for functions such as card-based door-opening tests before the smart lock is connected and commissioned..

6.5.3 Create a Parameter Collection Card

Used to collect parameter configuration information from a smart lock when on-site issues occur, enabling further analysis..