Suprema Integration with Genetec Security Center

ADMINISTRATOR GUIDE

Version 1.01
English
EN 102.00.SIWG V1.01A

suprema
SECURITY & BIOMETRICS

CONTENTS

CONTENTS

Introduction

Target Audience

This document describes how to install and configure Suprema Integration with Genetec Security Center. It is intended for system setup specialists as well as system administrators. The system specialists or administrators require basic knowledge of the Genetec Security Center system and Suprema biometric devices.

Features

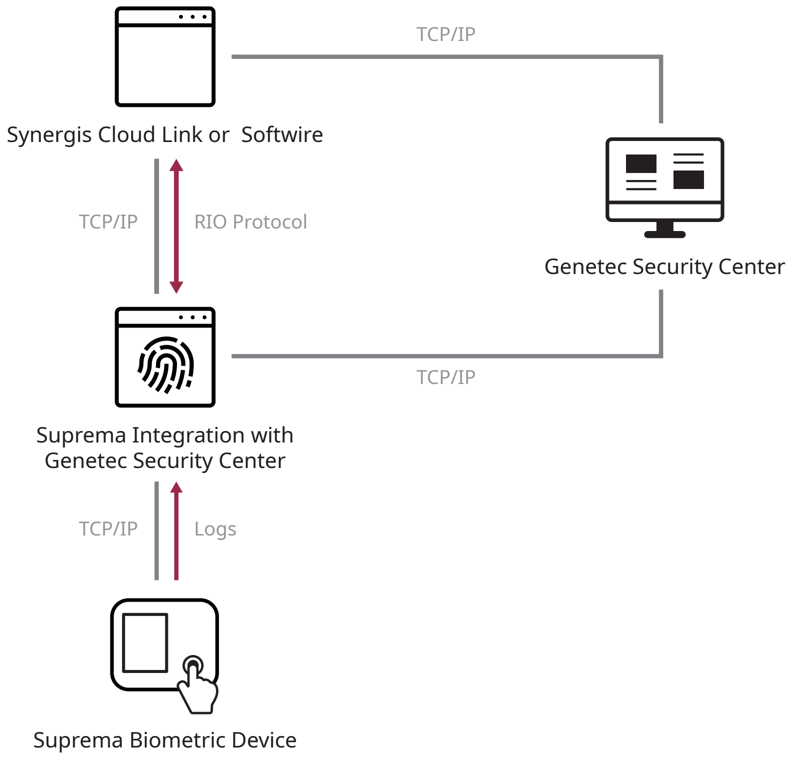
Suprema Integration with Genetec Security Center is a middleware that allows the Genetec Security Center system to communicate with the Suprema biometric devices, which can register a variety of credentials to users from Genetec Security Center and to manage connected devices. With Suprema Integration with Genetec Security Center, you can easily setup and build the biometric access control system for Genetec Security Center using Suprema biometric devices. It also leverages the RIO protocol to allow Suprema biometric devices to control doors without need for an access control panel through direct communication with Synergis Cloud Link or Softwire.

Suprema Integration with Genetec Security Center provides the following features.

- **Enable biometrics**: Use RFID cards and PINs as well as fingerprint and face as credentials.
- **Easy user management**: Real-time user data synchronization between Suprema Integration and Genetec Security Center
- **Easy enrollment and management**: Enroll user's face and fingerprint data directly from Genetec Security Center or Suprema devices which will be polled to the server.
- **Enterprise-level configuration**: Connect and manage up to 1,000 biometric devices.

- For more details on the functionality of Genetec Security Center, refer to its user manual.

System diagram



Installation

System environment

Suprema Integration with Genetec Security Center operates normally in the same system environment as Genetec Security Center.

You can find the minimum system requirements for Genetec Security Center at https://techdocs.genetec.com/r/en-US/Security-Center-Installation-and-Upgrade-Guide-for-Windows-Cluster-5.10/Windows-Failover-Clustering-terminology.

Check the support conditions before installing the Suprema Integration with Genetec Security Center.

Compatible systems and devices

- Operating system
  - Microsoft Windows 10 or later
- Genetec Security Center
  - v5.10.0.0 (357.0)
- Genetec Synergis Softwire
  Genetec Synergis Cloud link
  - v11.2.0 or later
- Suprema Biometric Device
  - FaceStation F2 FW v1.1.1 or later
  - FaceStation 2
  - FaceLite
  - BioStation 2
  - BioStation A2
  - BioStation L2
  - BioLite N2
  - BioEntry W2
  - BioEntry P2
  - CoreStation
  - Secure I/O 2
- USB Fingerprint Scanner
  - BioMini Plus 2

License

You need the following licenses to use Suprema Integration with Genetec Security Center.

- When using the Cloud link
  - GSC-Sy-P or higher tier required (for Synergis license)
  - You need to purchase extra licenses depending on doors you use.
- When using the Softwire
  - GSC-Sy-E-S2T1 required
  - You need to purchase extra licenses depending on doors you use.
- GSC-1SDKSUPREMA-READ (2 licenses per client required)

- For the above license inquiry, please contact Genetec.

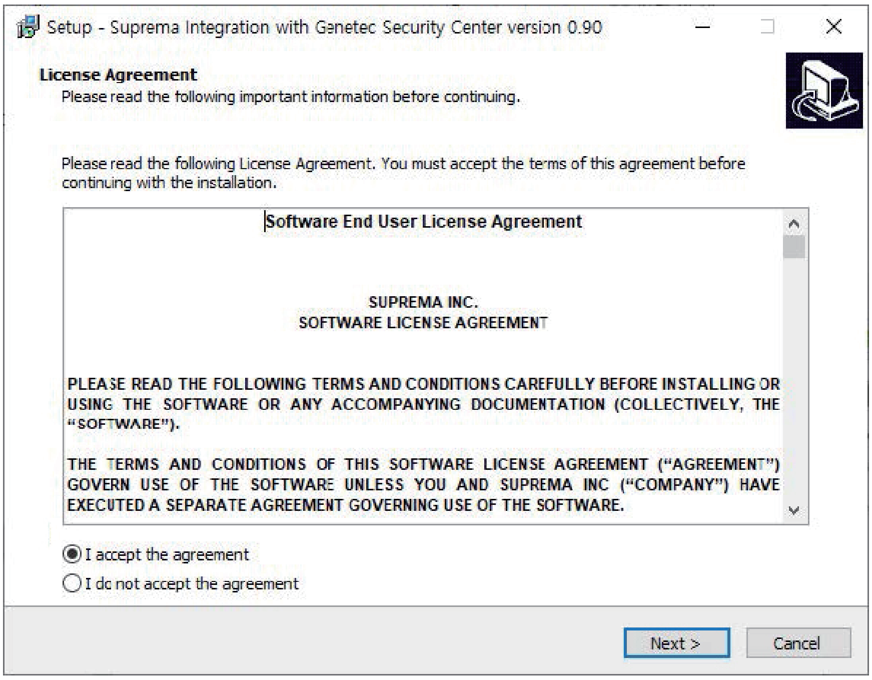
- BioStar 2- integration_Genetec

- For the above license inquiry, please contact Suprema.

Installing the Suprema Integration with Genetec Security Center

- This section describes how to install the Suprema Integration with Genetec Security Center. For more details on the installation of both Genetec Security Center and Config Tool, refer to its manuals.

1. Run the downloaded setup program.
   (ex. 'Integration.With.Genetec.Security.Center.x.x.xx')
2. Select I accept the agreement and click **Next**.



Setup - Suprema Integration with Genetec Security Center version 0.90

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement

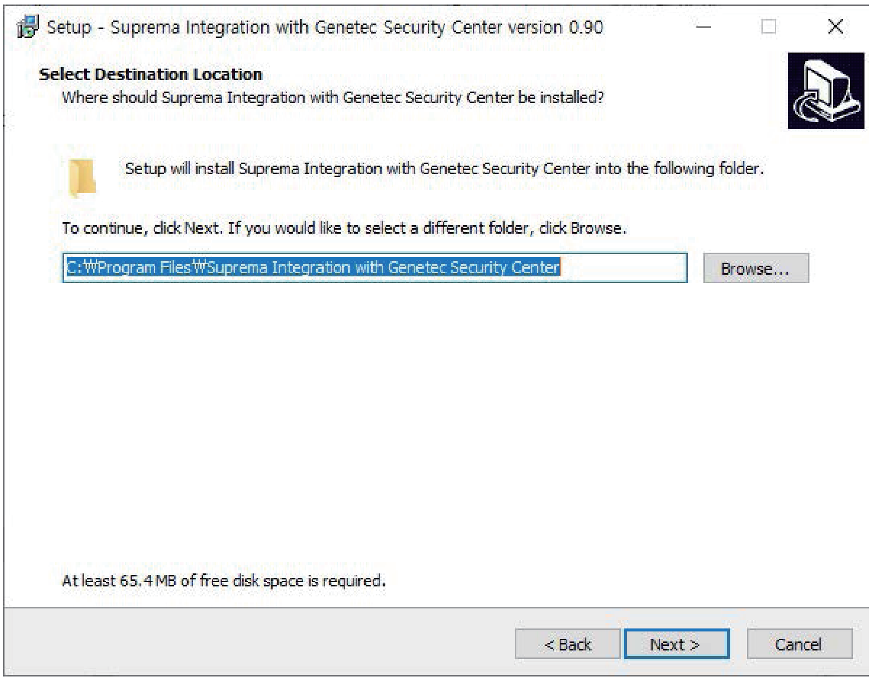
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").

THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN USE OF THE SOFTWARE UNLESS YOU AND SUPREMA INC ("COMPANY") HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING USE OF THE SOFTWARE.

● I accept the agreement
○ I do not accept the agreement

3. Set a path and click **Next**.



Setup - Suprema Integration with Genetec Security Center version 0.90

Select Destination Location

Where should Suprema Integration with Genetec Security Center be installed?

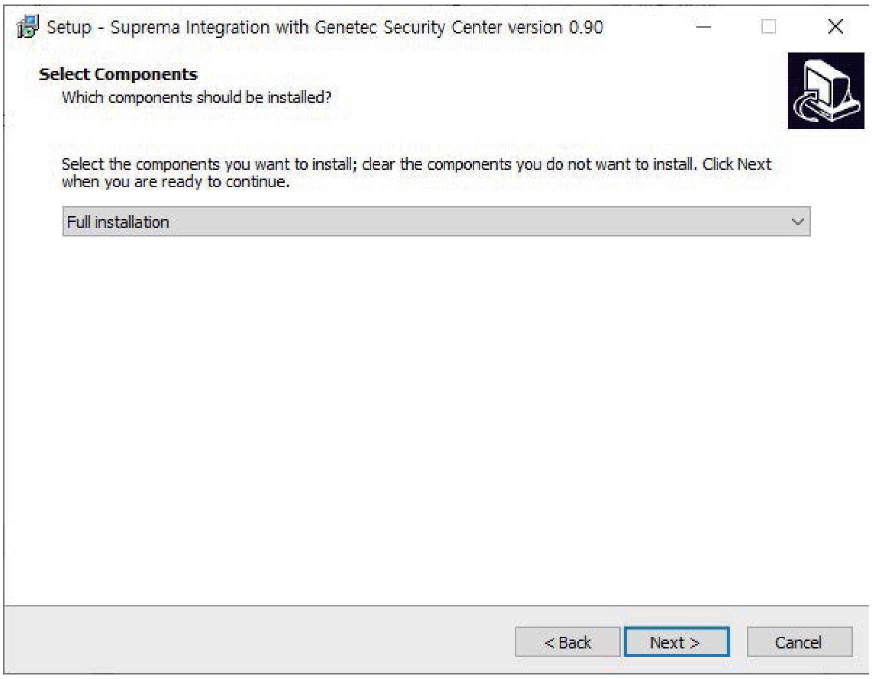
Setup will install Suprema Integration with Genetec Security Center into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩Suprema Integration with Genetec Security Center

At least 65.4 MB of free disk space is required.

4 Select a component option and click **Next**.


Setup - Suprema Integration with Genetec Security Center version 0.90
< Back
Next >
Cancel

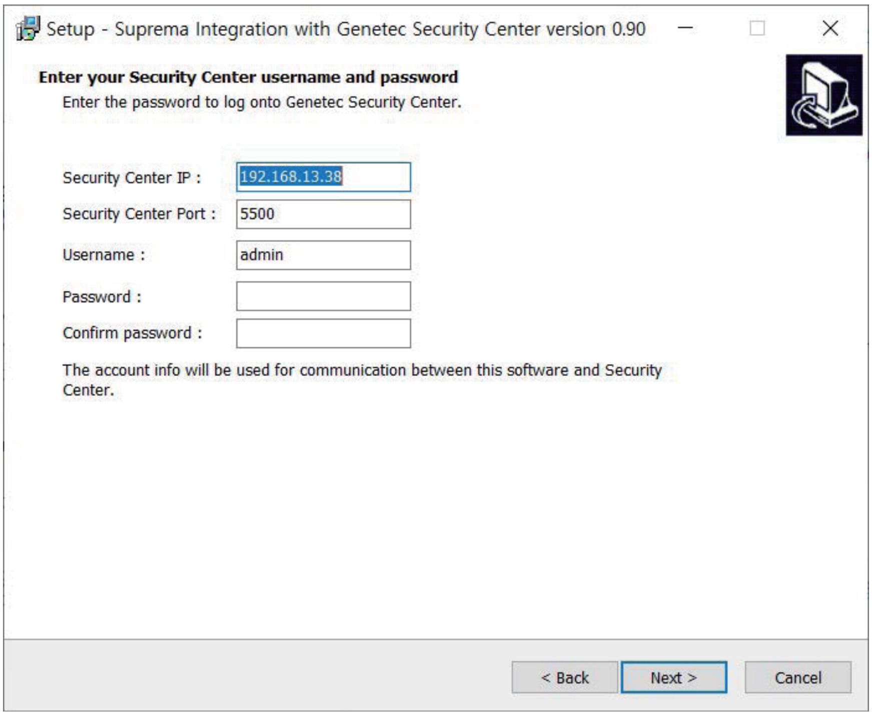
Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

5 Enter an IP address, port number, username, and password for Config Tool, and then click **Next**.


Setup - Suprema Integration with Genetec Security Center version 0.90
< Back
Next >
Cancel

Enter your Security Center username and password

Enter the password to log onto Genetec Security Center.

Security Center IP : 192.168.13.38

Security Center Port : 5500

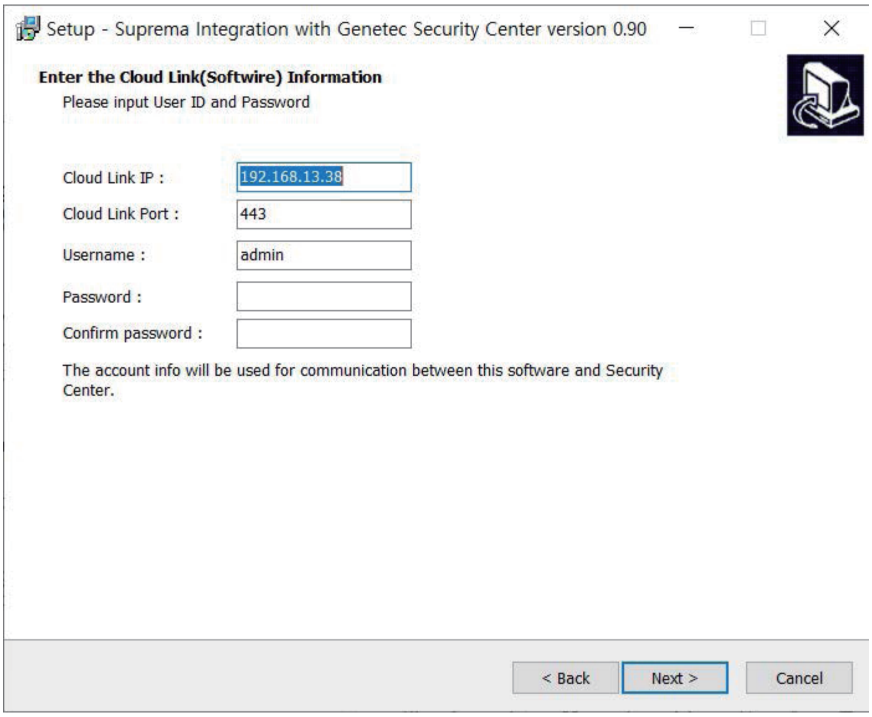
Username : admin

Password :

Confirm password :

The account info will be used for communication between this software and Security Center.

6 Enter an IP address, port number, username, and password for Softwire to communicate between the Suprema Integration software and Genetec Security Center.



Setup - Suprema Integration with Genetec Security Center version 0.90

Enter the Cloud Link(Softwire) Information

Please input User ID and Password

Cloud Link IP : 192.168.13.38

Cloud Link Port : 443

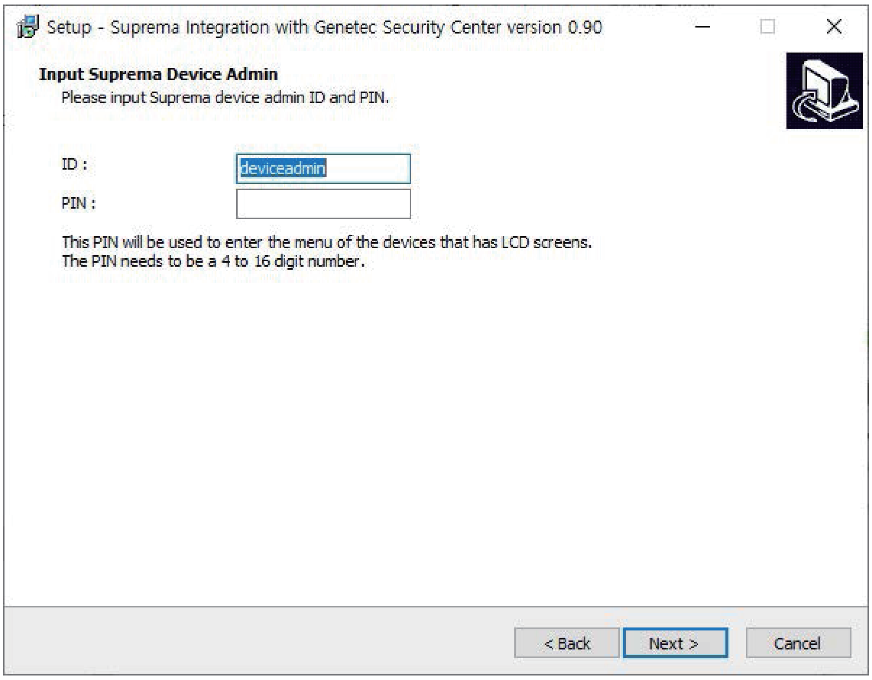
Username : admin

Password :

Confirm password :

The account info will be used for communication between this software and Security Center.

7 Enter the Suprema device admin ID and PIN, and then click **Next**. The ID and PIN set in this step will be used when you log in to Suprema Integration with Genetec Security Center.



Setup - Suprema Integration with Genetec Security Center version 0.90

Input Suprema Device Admin

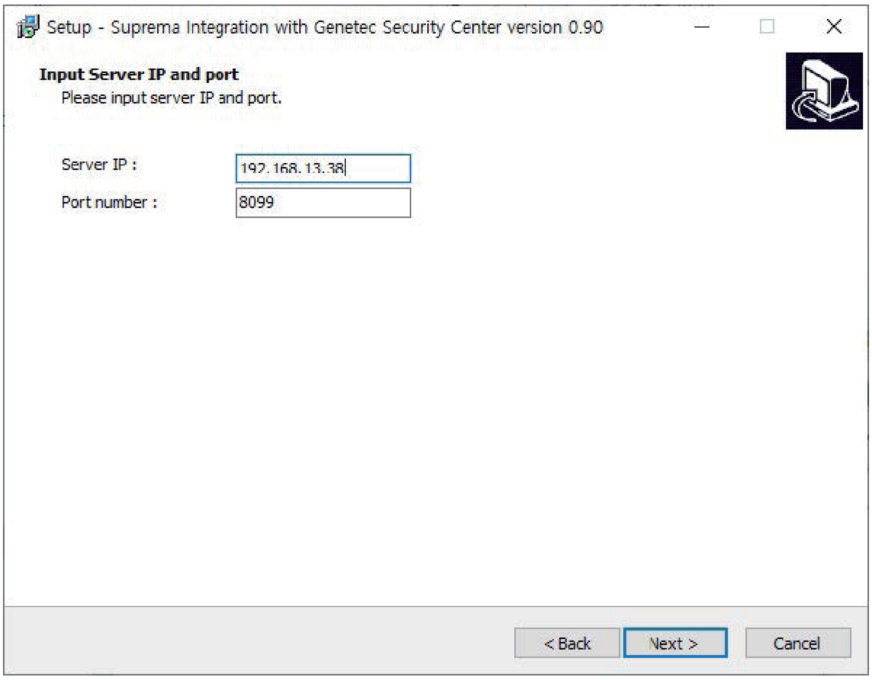
Please input Suprema device admin ID and PIN.

ID : deviceadmin

PIN :

This PIN will be used to enter the menu of the devices that has LCD screens.
The PIN needs to be a 4 to 16 digit number.

8 Enter the IP address and port number of Suprema Integration with Genetec Security Center.



Setup - Suprema Integration with Genetec Security Center version 0.90

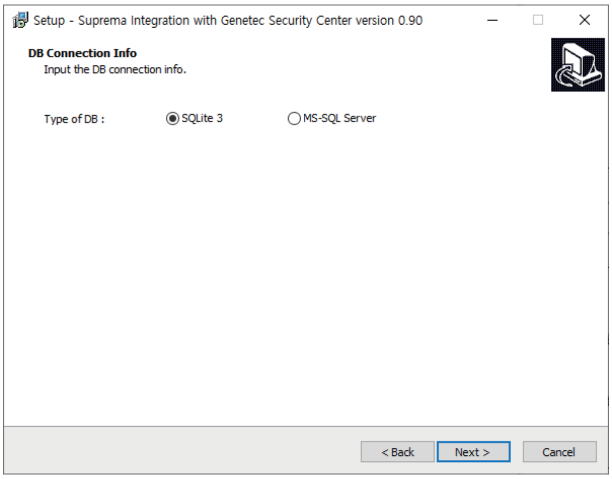
Input Server IP and port

Please input server IP and port.

Server IP : 192.168.13.38

Port number : 8099

9 Select the type of DB.

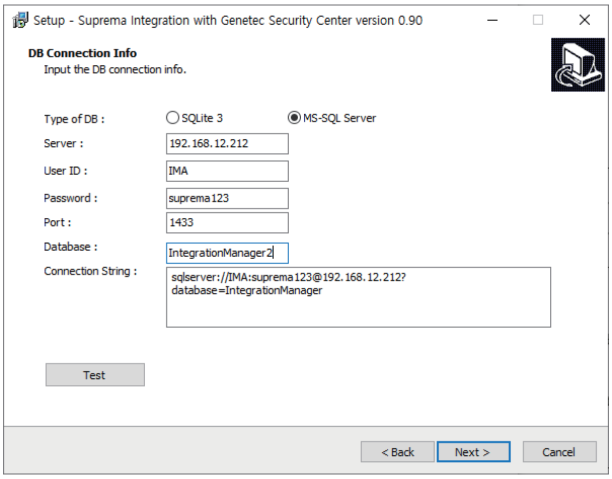


Setup - Suprema Integration with Genetec Security Center version 0.90

DB Connection Info

Input the DB connection info.

Type of DB : ● SQLite 3 ○ MS-SQL Server



Setup - Suprema Integration with Genetec Security Center version 0.90

DB Connection Info

Input the DB connection info.

Type of DB : ○ SQLite 3 ● MS-SQL Server

Server : 192.168.12.212

User ID : IMA

Password : suprema123

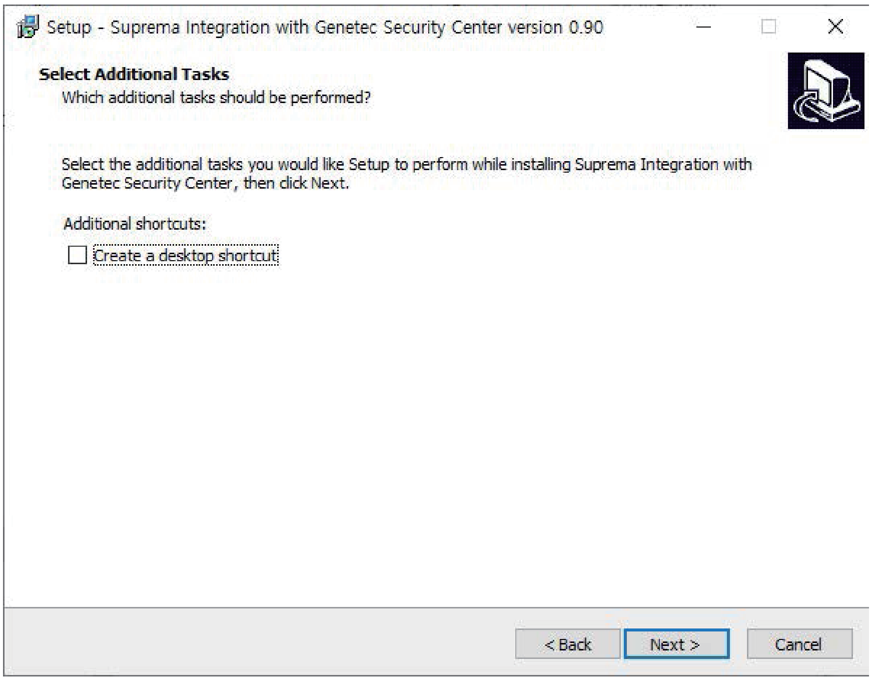
Port : 1433

Database : IntegrationManager2

Connection String : sqlserver://IMA:suprema123@192.168.12.212?database=IntegrationManager

If you select MS-SQL Server, enter each item and click **Test**. It is tested whether it is connected to the DB, and the message displays whether the connection is successful.

10 Select **Create a desktop shortcut** if you want to create a shortcut, and then click **Next**.



Setup - Suprema Integration with Genetec Security Center version 0.90

Select Additional Tasks

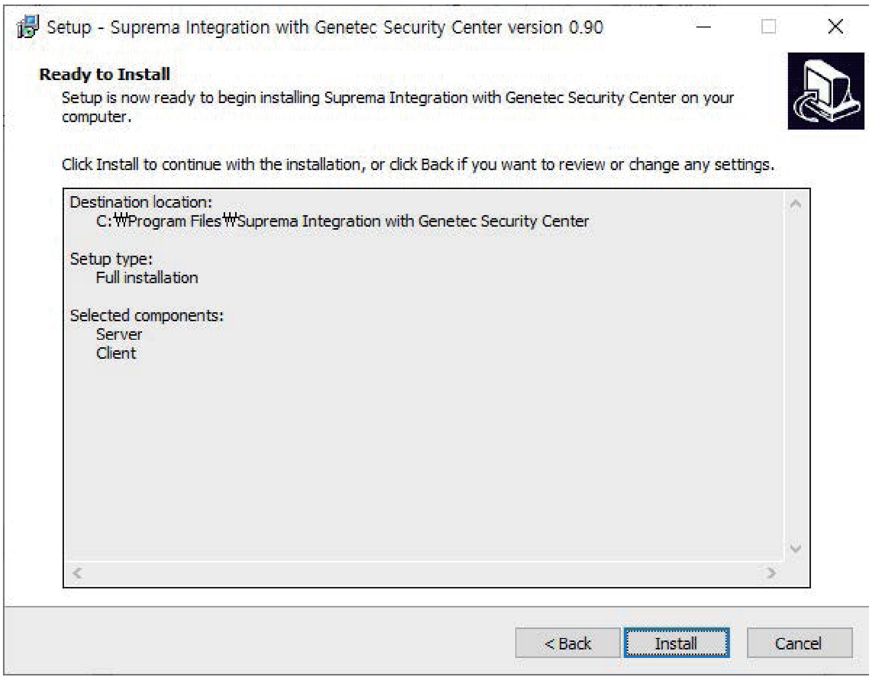
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Suprema Integration with Genetec Security Center, then click Next.

Additional shortcuts:

□ Create a desktop shortcut

11 Click **Install**.



Setup - Suprema Integration with Genetec Security Center version 0.90

Ready to Install

Setup is now ready to begin installing Suprema Integration with Genetec Security Center on your computer.

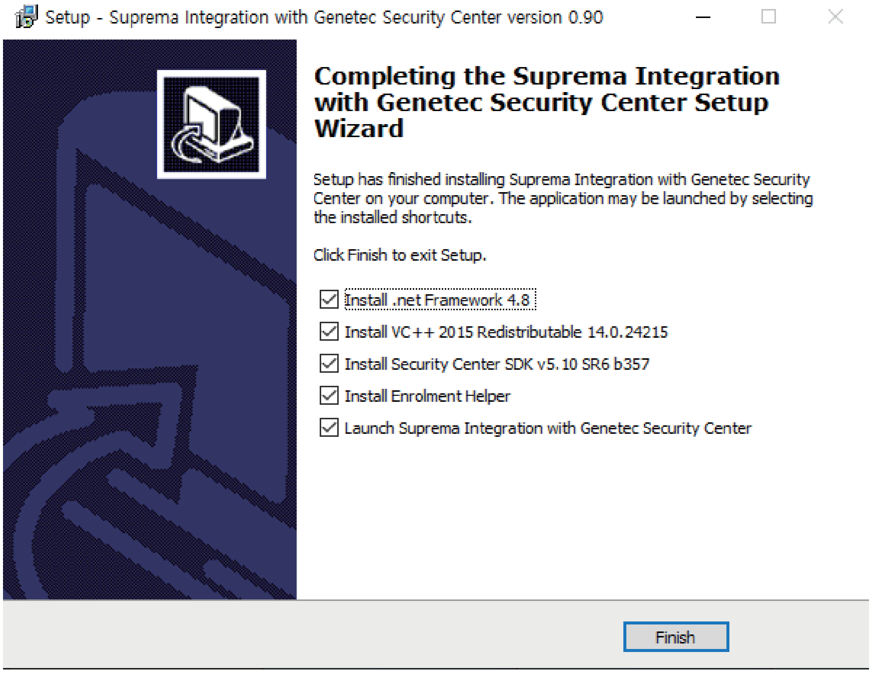
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:₩Program Files₩Suprema Integration with Genetec Security Center

Setup type:
Full installation

Selected components:
Server
Client

12 Select additional programs to install and click **Finish**. You must select the Install Security Center SDK option to proceed the next step.



Setup - Suprema Integration with Genetec Security Center version 0.90

Completing the Suprema Integration with Genetec Security Center Setup Wizard

Setup has finished installing Suprema Integration with Genetec Security Center on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Install .net Framework 4.8

☑ Install VC++ 2015 Redistributable 14.0.24215

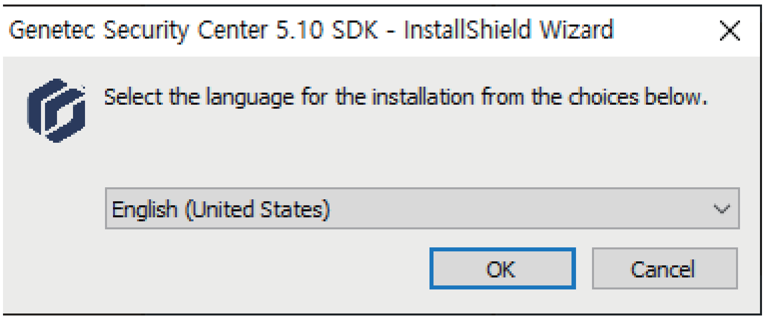
☑ Install Security Center SDK v5.10 SR6 b357

☑ Install Enrolment Helper

☑ Launch Suprema Integration with Genetec Security Center

- If you install the Enrollment Helper, you can also enroll fingerprints by opening a window for fingerprint enrollment directly from Config Tool. For more information on the Enrollment Helper, refer to Enrollment Helper.

13 Select a language to use and click **OK**.

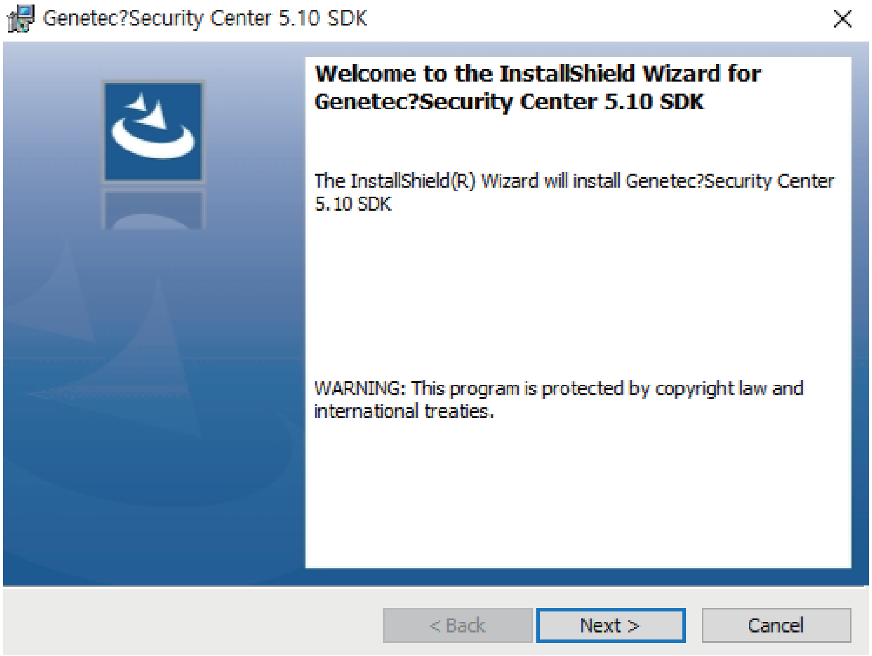


Genetec Security Center 5.10 SDK - InstallShield Wizard

Select the language for the installation from the choices below.

English (United States)

14 Click **Next**.



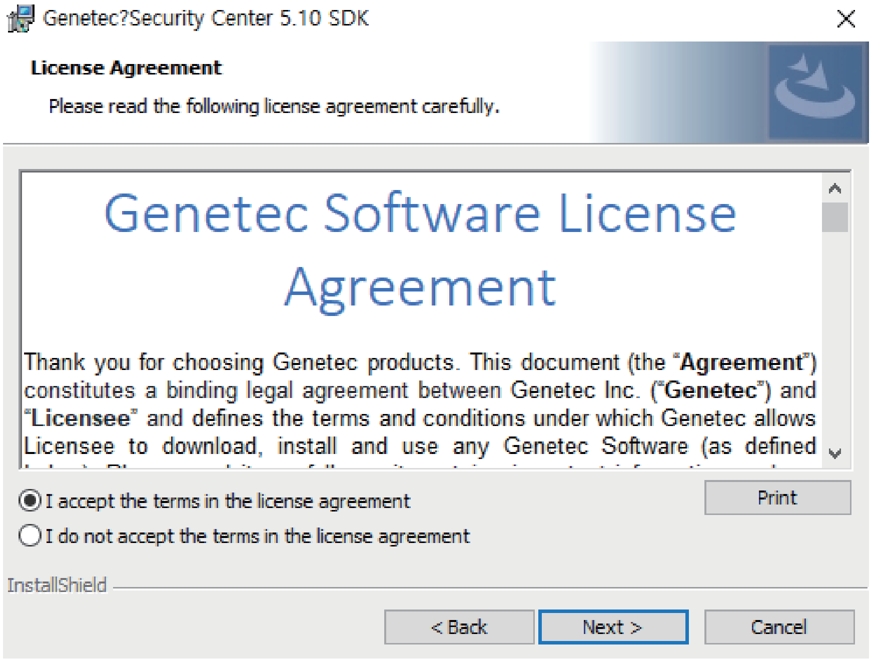
Genetec?Security Center 5.10 SDK

Welcome to the InstallShield Wizard for Genetec?Security Center 5.10 SDK

The InstallShield(R) Wizard will install Genetec?Security Center 5.10 SDK

WARNING: This program is protected by copyright law and international treaties.

15 Select **I accept the terms in the license agreement** and click **Next**.



Genetec?Security Center 5.10 SDK

License Agreement

Please read the following license agreement carefully.

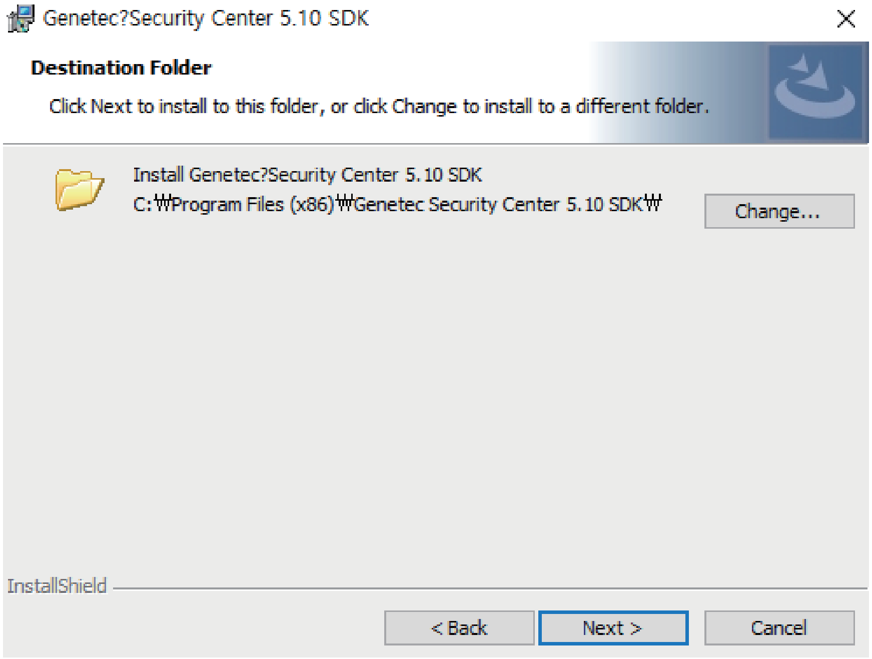
Genetec Software License Agreement

Thank you for choosing Genetec products. This document (the "**Agreement**") constitutes a binding legal agreement between Genetec Inc. ("**Genetec**") and "**Licensee**" and defines the terms and conditions under which Genetec allows Licensee to download, install and use any Genetec Software (as defined

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

16 Set a path and click **Next**.



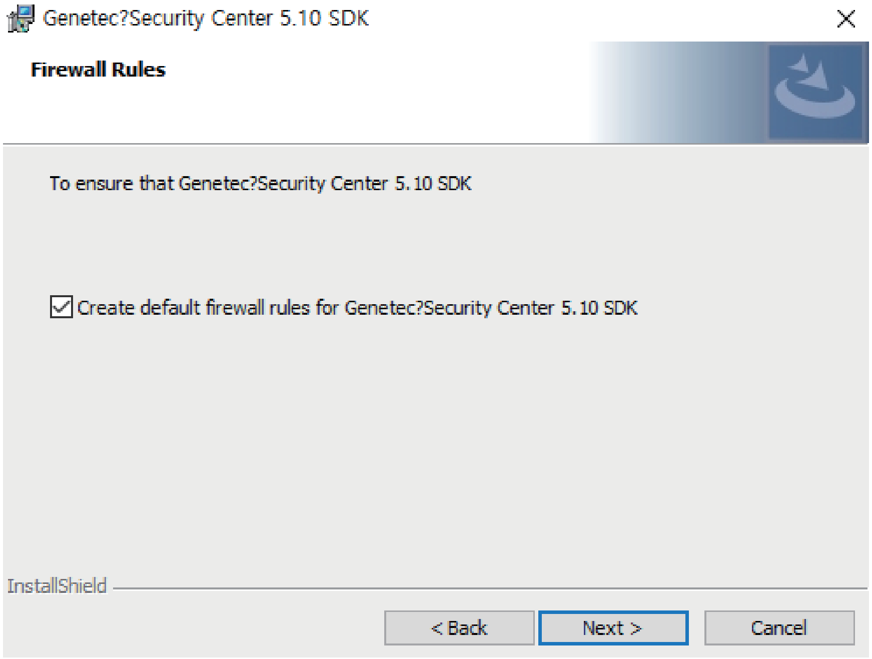
Genetec?Security Center 5.10 SDK

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Genetec?Security Center 5.10 SDK
C:₩Program Files (x86)₩Genetec Security Center 5.10 SDK₩

17 Select whether to create default rules and click **Next**.



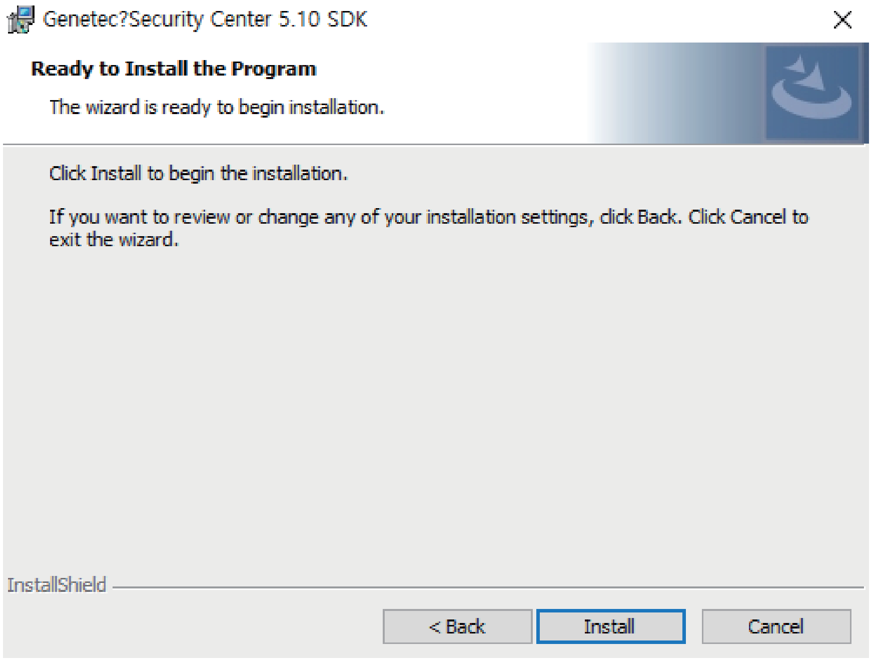
Genetec?Security Center 5.10 SDK

Firewall Rules

To ensure that Genetec?Security Center 5.10 SDK

☑ Create default firewall rules for Genetec?Security Center 5.10 SDK

18 Select whether to update the software automatically when it is available and click **Install**.



Genetec?Security Center 5.10 SDK

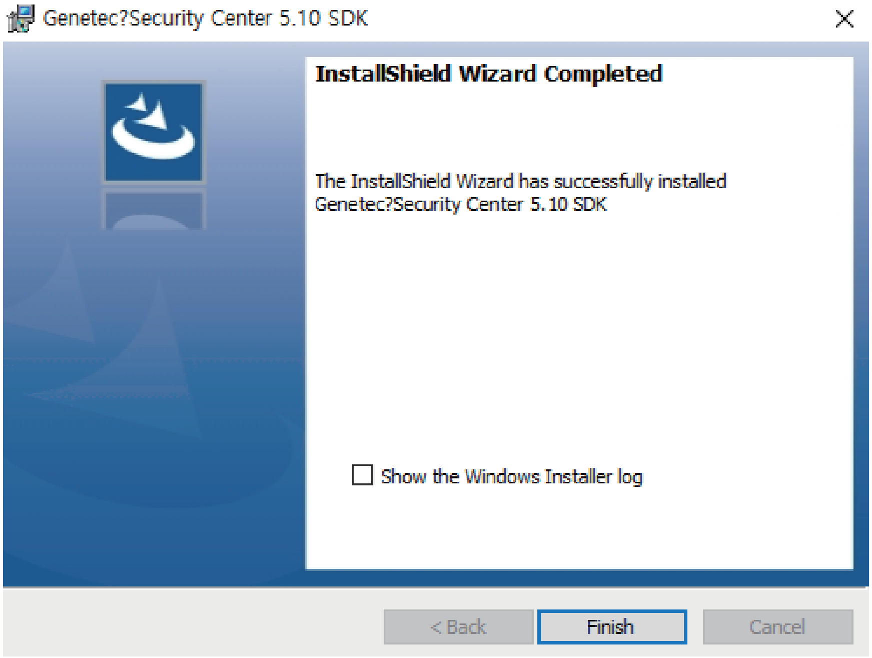
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

19 Click **Finish** to finish the installation.



Genetec?Security Center 5.10 SDK

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Genetec?Security Center 5.10 SDK

☐ Show the Windows Installer log

Getting started

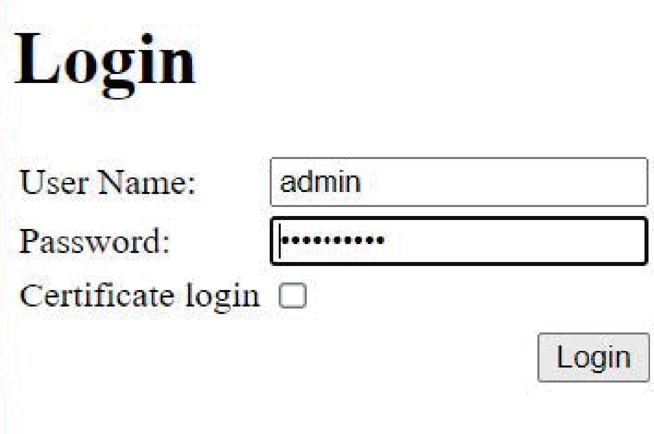
Setting up the RIO Protocol

Before using Suprema Integration with Genetec Security Center, you need to setup the RIO Protocol for direct communication to Synergis Cloud Link or Softwire.

Enabling the RIO Protocol on Synergis Cloud Link or Softwire

1. Enter the following URL into your browser. You need to change [IP-address] with the IP address of your Synergis Cloud Link or Softwire.
   https://[IP-address]/Features/DuiRIO/Enabled/Set?value=true

2. Log in to Softwire.



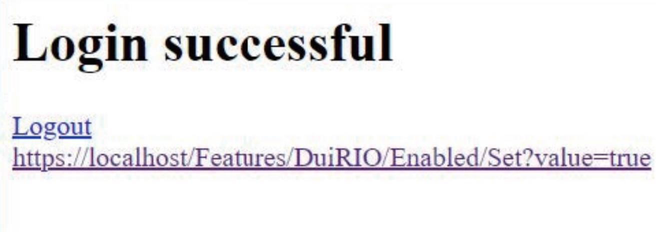
Login

User Name: admin

Password: •••••••••••

Certificate login □

3. Click the link.



Login successful

Logout

https://localhost/Features/DuiRIO/Enabled/Set?value=true

If the login is successfully done, you will receive a confirmation indicating 'Feature enabled'.

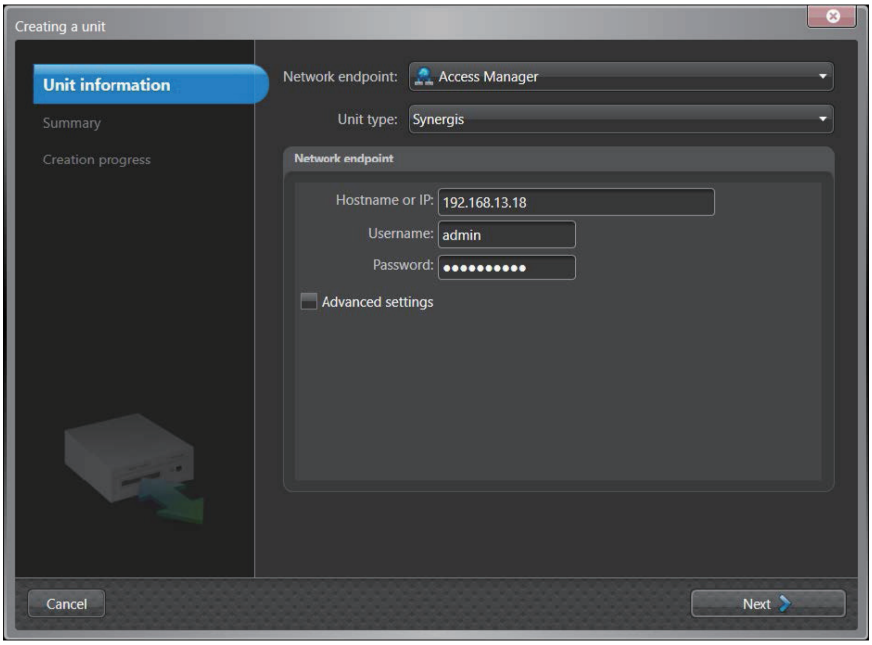
Creating an access control unit

You should create an access control unit in Config Tool before using Suprema Integration with Genetec Security Center.

1 Run **Config Tool**.

2 Click **Config Tool** > **Tasks** > **Access control** and click **Access control unit** at the bottom left corner of the window.

3 Enter an IP address and the same password that you are using in Softwire, and then click **Next**.



Creating a unit

Network endpoint: Access Manager

Unit type: Synergis

Network endpoint

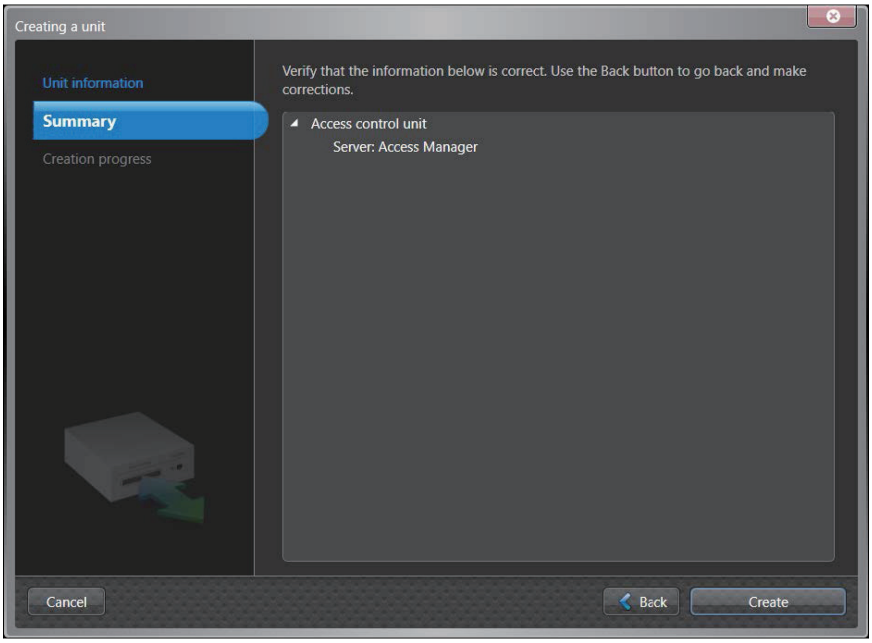
Hostname or IP: 192.168.13.18

Username: admin

Password: ●●●●●●●●●●

□ Advanced settings

4 Check the information and click **Create**.

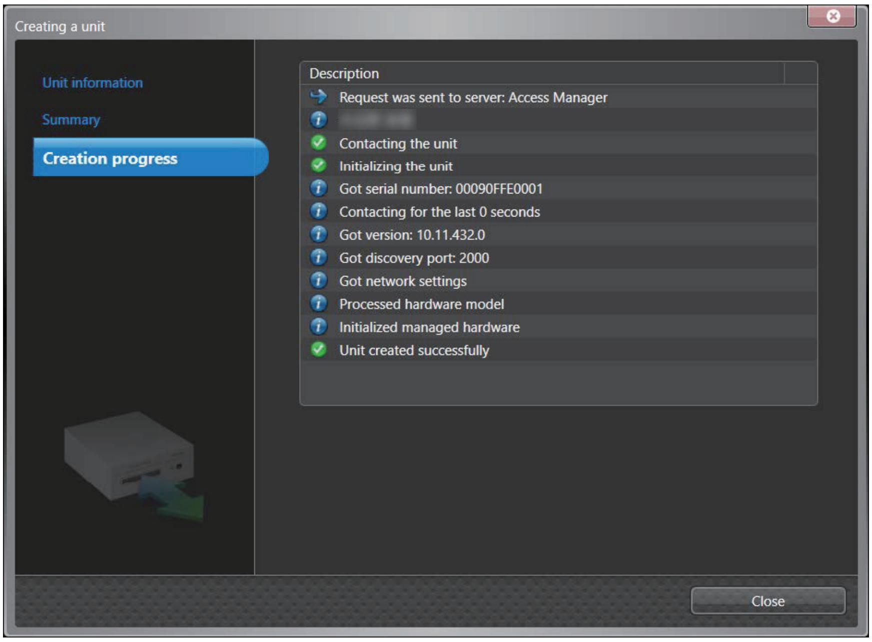


Creating a unit

Verify that the information below is correct. Use the Back button to go back and make corrections.

Access control unit
Server: Access Manager

5 Click **Close**.



```
Description
Request was sent to server: Access Manager
[redacted]
Contacting the unit
Initializing the unit
Got serial number: 00090FFE0001
Contacting for the last 0 seconds
Got version: 10.11.432.0
Got discovery port: 2000
Got network settings
Processed hardware model
Initialized managed hardware
Unit created successfully
```

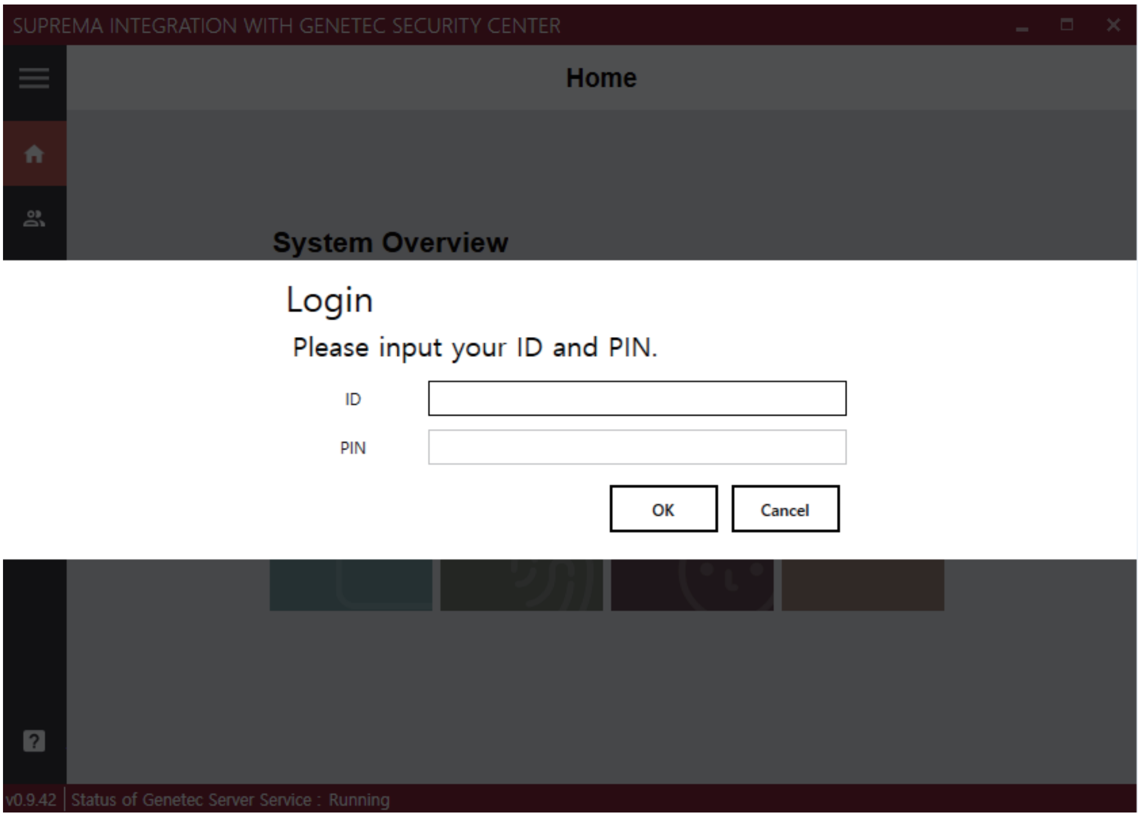
The access control unit has been created under **Access Manager**. After creating the access control unit, check that the RIO tap successfully appears. Click **Tasks** > **Access Control** > **Role and units**, select the access control unit, and then click **Hardware** > **RIO**.

- To learn how to install Config Tool, refer to its manual.

Login

Log in with the device administrator account.

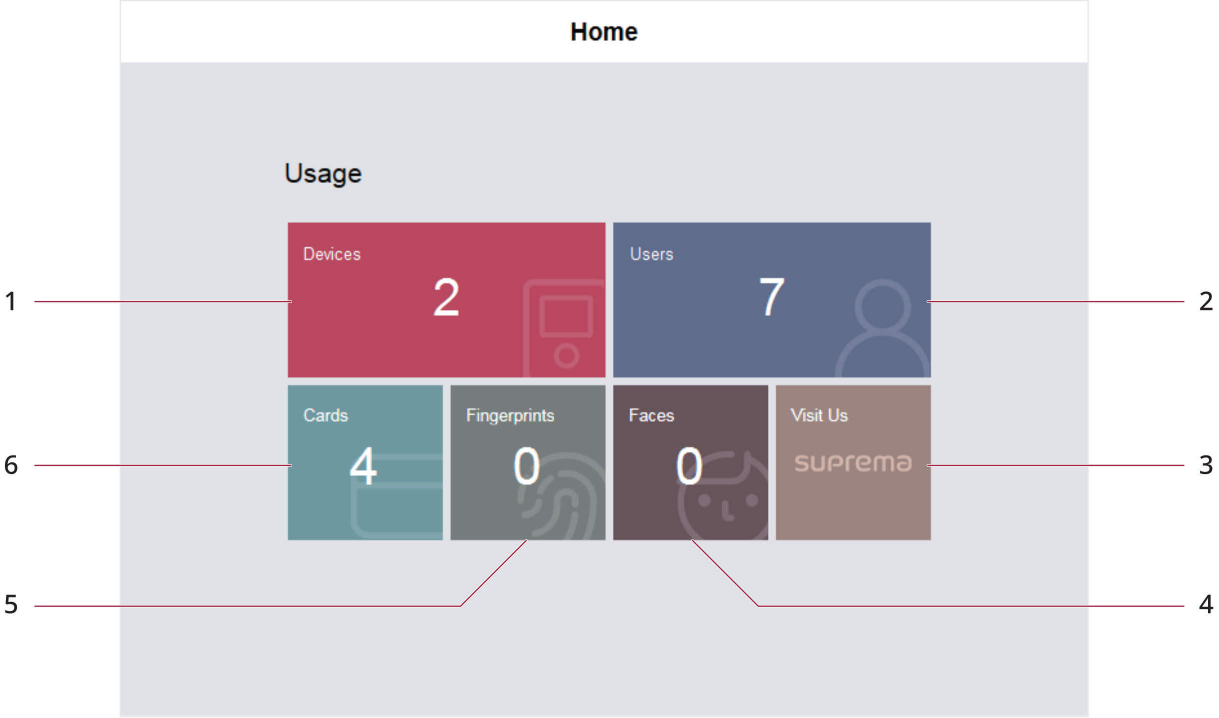
The ID is '**deviceadmin**', and PIN is the password you set when you installed Suprema Integration with Genetec Security Center.



SUPREMA INTEGRATION WITH GENETEC SECURITY CENTER
Home
System Overview
Login
Please input your ID and PIN.
ID
PIN
OK
Cancel
v0.9.42
Status of Genetec Server Service : Running

Home

The **Home** menu is the starting point for accessing all menus of the Suprema Integration with Genetec Security Center. You can also check the number of registered devices, users, faces, fingerprints, and cards.Open the AEOS\AEserver\ standalone\configuration folder.



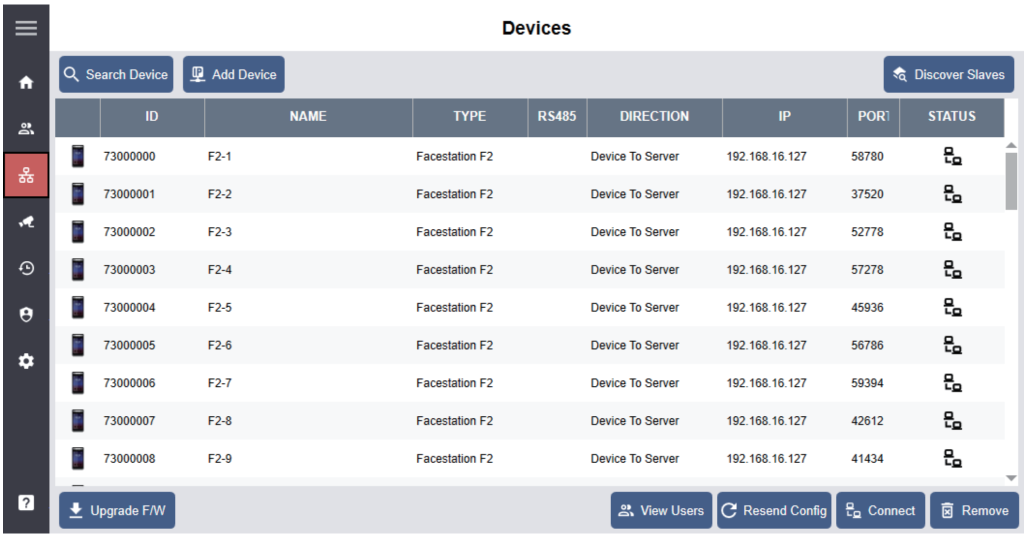
No.	Description	No.	Description
1	View the number of connected devices.	**4**	View the number of registered faces.
2	View the number of registered users.	**5**	View the number of registered fingerprints.
3	Access the Suprema website.	**6**	View the number of registered cards.

Devices

Devices overview

You can use the Devices menu to add, delete or edit registered devices, fetch the user information registered within the device to the server or upgrade the firmware.

- You can set access rules to registered devices in Config Tool. To learn how to set access rules, refer to its manual.



ID	NAME	TYPE	RS485	DIRECTION	IP	PORT	STATUS
73000000	F2-1	Facestation F2		Device To Server	192.168.16.127	58780	
73000001	F2-2	Facestation F2		Device To Server	192.168.16.127	37520	
73000002	F2-3	Facestation F2		Device To Server	192.168.16.127	52778	
73000003	F2-4	Facestation F2		Device To Server	192.168.16.127	57278	
73000004	F2-5	Facestation F2		Device To Server	192.168.16.127	45936	
73000005	F2-6	Facestation F2		Device To Server	192.168.16.127	56786	
73000006	F2-7	Facestation F2		Device To Server	192.168.16.127	59394	
73000007	F2-8	Facestation F2		Device To Server	192.168.16.127	42612	
73000008	F2-9	Facestation F2		Device To Server	192.168.16.127	41434	

- **Search Device**: You can search for devices connected to Suprema Integration with Genetec Security Center and register them.
- **Add Device**: You can add a device by entering the IP of the device.
- **Discover Slaves**: You can search and add slave devices connected to the device.
- **Upgrade F/W**: You can upgrade the device’s firmware.
- **View Users**: You can see a list of users stored on devices.
- **Resend Config**: You can apply device settings configured in the **Settings** menu to devices.
- **Connect**: You can reconnect the selected device to the Suprema Integration with Genetec Security Center.
- **Remove**: You can remove the selected device from the Suprema Integration with Genetec Security Center.

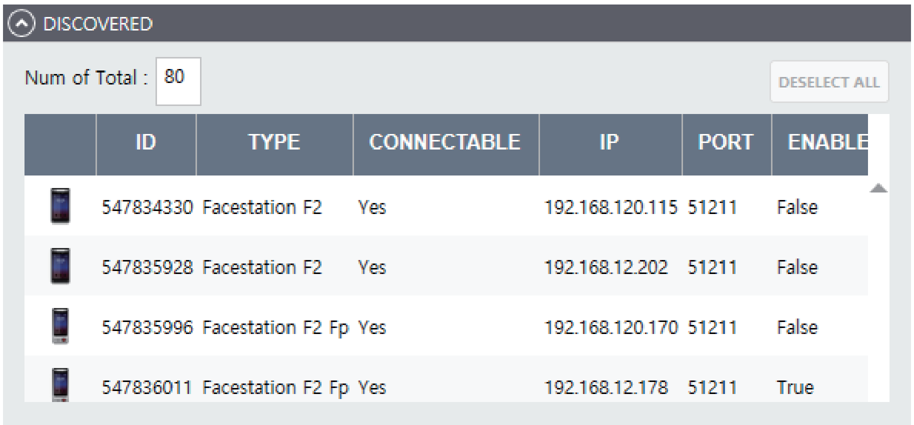
Device registration

Adding a device automatically

You can automatically search for devices connected to Suprema Integration with Genetec Security Center and register them. Before searching for devices, check whether they are correctly connected. When adding multiple devices at once, it will be more convenient to know the ID, device type and IP address information of each device in advance.

1 Click 🖧.

2 Click **Search Device**. All available devices will appear.



DISCOVERED

Num of Total : 80

	ID	TYPE	CONNECTABLE	IP	PORT	ENABLE
	547834330	Facestation F2	Yes	192.168.120.115	51211	False
	547835928	Facestation F2	Yes	192.168.12.202	51211	False
	547835996	Facestation F2 Fp	Yes	192.168.120.170	51211	False
	547836011	Facestation F2 Fp	Yes	192.168.12.178	51211	True

3 Select a device to connect and click **REGISTER**.

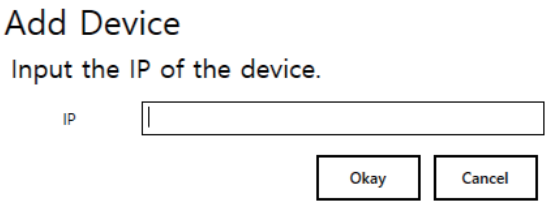
Adding a device manually

You can add a device manually by entering the IP of the device.

1 Click 🖧.

2 Click **Add Device**.

3 Enter the IP of the device to register and click **Okay**.



Add Device

Input the IP of the device.

IP

- Up to 1,000 biometric devices can be connected.

Sending a connection request from the device

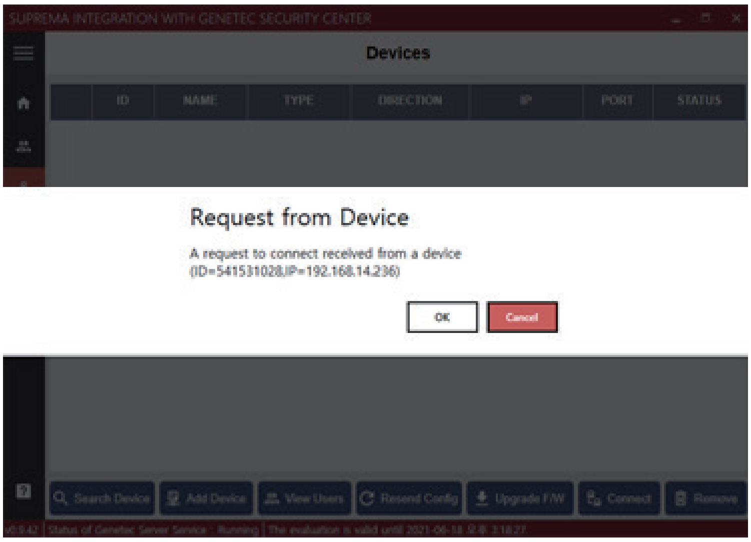
You can send a connection signal from the device to Suprema Integration with Genetec Security Center with the input information directly. The steps may vary depending on the device you use. For more details, refer to the manual. In this section, FaceStation F2 is in use.

1 On the device, press 88 > **NETWORK**.

2 Press **Server** and activate **Device -> Server**.

3 Enter the IP address on **Server IP**. The device will automatically request the connection to the server.

4 On the server, press **OK**.



Request from Device

A request to connect received from a device (ID=541531028,IP=192.168.14.236)

v0.9.42 | Status of Genetec Server Service : Running | The evaluation is valid until 2021-06-18 오후 3:18:27

The device is added on the list.

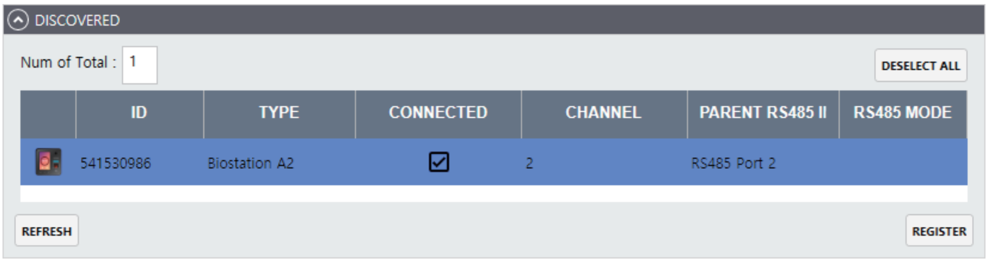
Slave device search and registration

You can easily expand your access control system network by adding slave devices to existing master devices. Master devices and slave devices can be connected together via RS-485.

1 Click 品.

2 Select the master device to search for slave devices and click **Discover Slaves**.

3 The list of slave devices connected to the master device is shown. If the devices you are looking for are not shown on the list, click **REFRESH** to search for the devices again.



Num of Total : 1

	ID	TYPE	CONNECTED	CHANNEL	PARENT RS485 II	RS485 MODE
	541530986	Biostation A2	☑	2	RS485 Port 2	

4 Select the device to add, and click **REGISTER**.

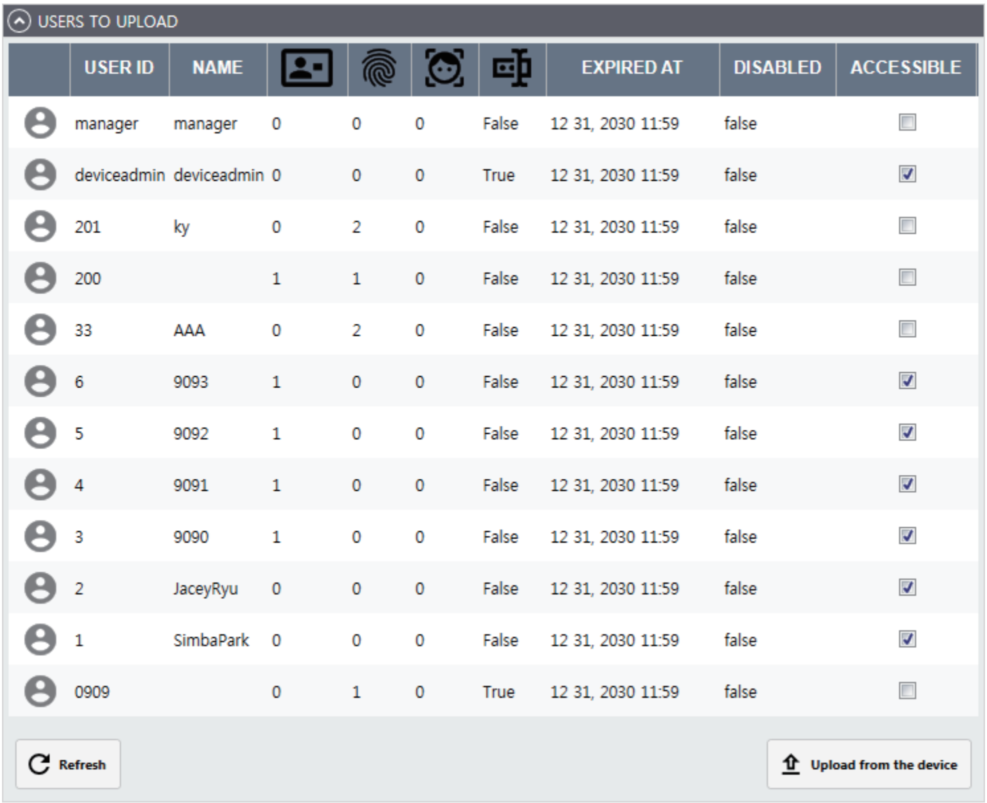
Uploading users registered from devices

You can view the list of users stored on the device and import the users to the server.

1 Click 🖧.

2 Click a device and click **View Users** to view the list of users.

3 Select all users to upload to the server and click **Upload from the device**.



USERS TO UPLOAD

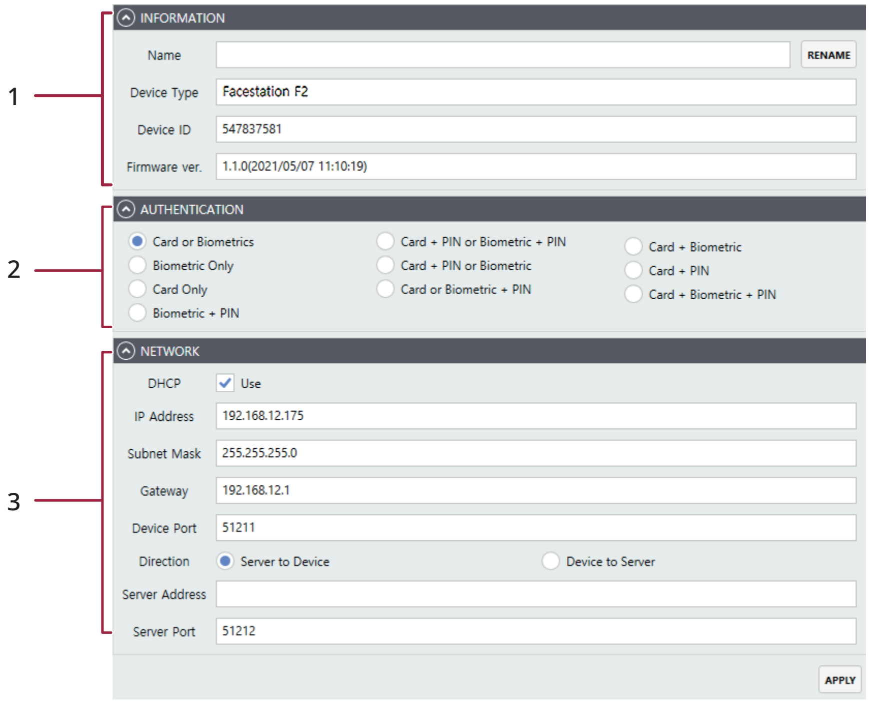
	USER ID	NAME					EXPIRED AT	DISABLED	ACCESSIBLE
	manager	manager	0	0	0	False	12 31, 2030 11:59	false	☐
	deviceadmin	deviceadmin	0	0	0	True	12 31, 2030 11:59	false	☑
	201	ky	0	2	0	False	12 31, 2030 11:59	false	☐
	200		1	1	0	False	12 31, 2030 11:59	false	☐
	33	AAA	0	2	0	False	12 31, 2030 11:59	false	☐
	6	9093	1	0	0	False	12 31, 2030 11:59	false	☑
	5	9092	1	0	0	False	12 31, 2030 11:59	false	☑
	4	9091	1	0	0	False	12 31, 2030 11:59	false	☑
	3	9090	1	0	0	False	12 31, 2030 11:59	false	☑
	2	JaceyRyu	0	0	0	False	12 31, 2030 11:59	false	☑
	1	SimbaPark	0	0	0	False	12 31, 2030 11:59	false	☑
	0909		0	1	0	True	12 31, 2030 11:59	false	☐

Editing device settings and information

You can edit information of registered devices.

1 Double-click the device to edit. Or, right-click on the device and click **Device Config**.

2 Edit the necessary fields of the INFORMATION, AUTHENTICATION, and NETWORK.



INFORMATION

Name		RENAME
Device Type	Facestation F2	
Device ID	547837581	
Firmware ver.	1.1.0(2021/05/07 11:10:19)	

AUTHENTICATION

● Card or Biometrics	○ Card + PIN or Biometric + PIN	○ Card + Biometric
○ Biometric Only	○ Card + PIN or Biometric	○ Card + PIN
○ Card Only	○ Card or Biometric + PIN	○ Card + Biometric + PIN
○ Biometric + PIN		

NETWORK

DHCP	☑ Use	
IP Address	192.168.12.175	
Subnet Mask	255.255.255.0	
Gateway	192.168.12.1	
Device Port	51211	
Direction	● Server to Device	○ Device to Server
Server Address		
Server Port	51212	

APPLY

No.	Item	Description
1	INFORMATION	Edit the name of the device or see the device information. • **Name**: Enter a device name. • **Device Type**: View the device type. • **Device ID**: View the device ID. • **Firmware ver.**: View the kernel version.
2	AUTHENTICATION	Configure the authentication modes of the device.
3	NETWORK	Configure the connection settings. • **DHCP**: Select this option to allow the device to use a dynamic IP address. • **IP Address**: Enter network settings of the device. • **Subnet Mask**: Enter network settings of the device. • **Gateway**: Enter network settings of the device. • **Device Port**: Enter a port to be used by the device. • **Direction**: Select the direction. • **Server Address**: Enter the IP address of the Suprema Integration with the Genetec Security Center server. • **Server Port**: Enter the port number of the Suprema Integration with the Genetec Security Center server.

3 Click **APPLY** to save the settings.

Resending configuration

You can apply device settings configured in the **Settings** menu to devices.

- Make sure that Global Device Configuration is set up correctly before running Resend Config.

1 Click 🖧.

2 Click a device to apply settings and click **Resend Config**.
If you click **Resend Config** with nothing selected, the settings are applied to all devices.

Upgrading firmware

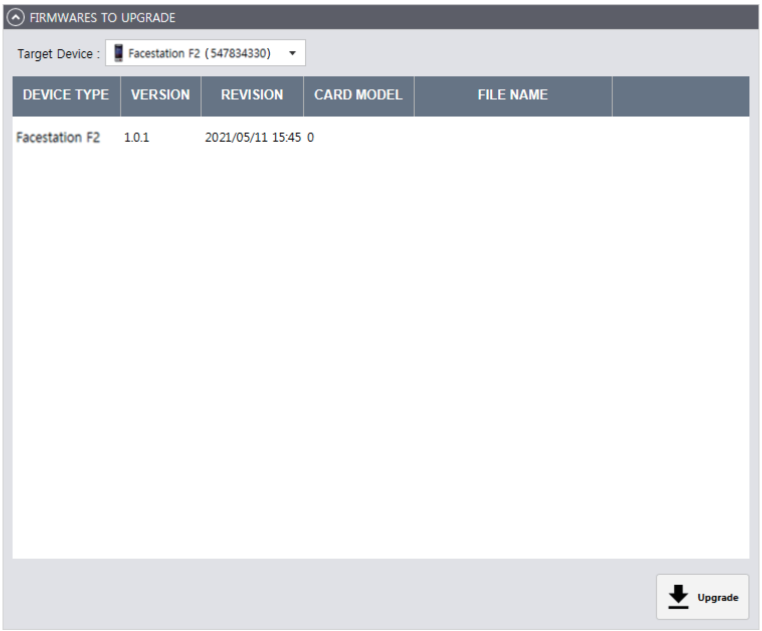
You can easily upgrade the firmware on any device connected to Suprema Integration with Genetec Security Center without any additional connection or action.

Copy the firmware files that you have downloaded to the following folder. If the folder does not exist, you need to create it.

1 Click 🖧.

2 Select a device and click **Upgrade F/W**.

3 Select the firmware file and click **Upgrade**.



FIRMWARES TO UPGRADE

Target Device : Facestation F2 (547834330)

DEVICE TYPE	VERSION	REVISION	CARD MODEL	FILE NAME
Facestation F2	1.0.1	2021/05/11 15:45	0	

Connecting a device

You can reconnect the selected device from the Suprema Integration with Genetec Security Center.

1 Click 🖧.

2 Select devices to reconnect and click **Connect**.

Removing a device

You can delete the selected device from the list.

1 Click 🖧.

2 Select devices to delete and click **Remove**.

Other settings

You can reboot or reset to factory default by selecting individual devices. You can also edit other settings, such as a lock or unlock the device.

1 Click 🖧.

2 Right-click the device for which you want to edit the settings.

3 Select and set the item to edit.

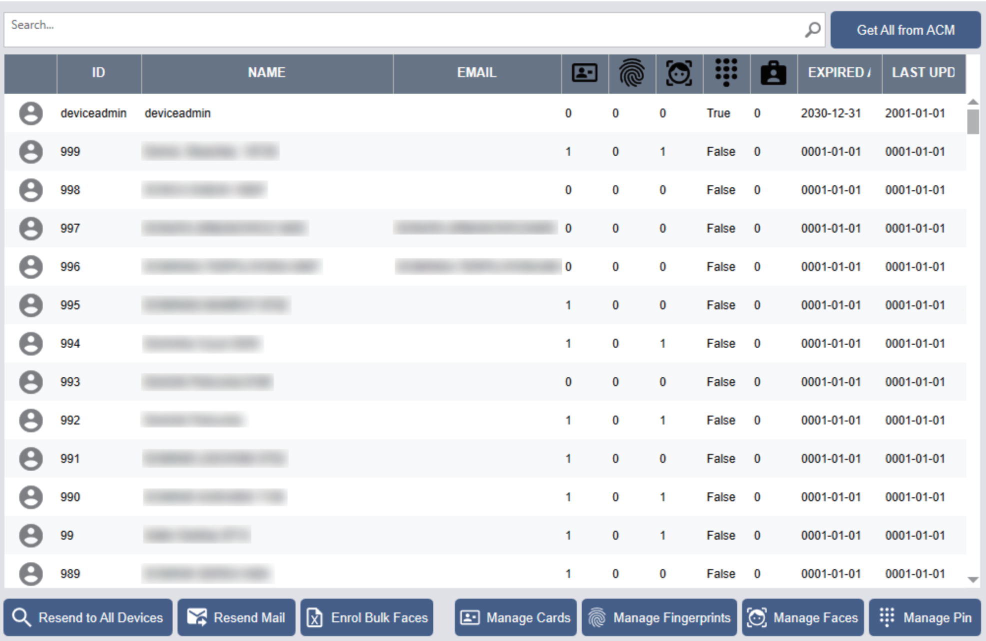
- **Rename**: You can change the device name.
- **Resync**: Delete all user data in the device and send the user data of the server.
- **Reboot**: You can restart the device.
- **Here I am**: You can check the location of the device by making a sound on the selected device.
- **Lock**: You can lock the device. When a device is locked, the user cannot authenticate on that device.
- **Unlock**: You can unlock the device.
- **All alarms off**: You can turn off all alarms on the device.
- **Factory Reset**: You can delete all data and root certificate on the device and reset the settings. The network settings will not be reset.
- **Delete All Users**: Delete all user data.
- **Device Config**: You can edit the device settings.

Users

Users overview

The list of users registered in the Genetec Security Center system is automatically synchronized to Suprema Integration with Genetec Security Center. Also, if the users are deleted or registered in the Genetec Security Center system, the revised list is automatically synchronized in real-time to Suprema Integration with Genetec Security Center. You can register various credentials by selecting a user from the Users menu in Suprema Integration with Genetec Security Center.

Users



	ID	NAME	EMAIL						EXPIRED /	LAST UPD
	deviceadmin	deviceadmin		0	0	0	True	0	2030-12-31	2001-01-01
	999	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
	998	[redacted]		0	0	0	False	0	0001-01-01	0001-01-01
	997	[redacted]	[redacted]	0	0	0	False	0	0001-01-01	0001-01-01
	996	[redacted]	[redacted]	0	0	0	False	0	0001-01-01	0001-01-01
	995	[redacted]		1	0	0	False	0	0001-01-01	0001-01-01
	994	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
	993	[redacted]		0	0	0	False	0	0001-01-01	0001-01-01
	992	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
	991	[redacted]		1	0	0	False	0	0001-01-01	0001-01-01
	990	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
	99	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
	989	[redacted]		1	0	0	False	0	0001-01-01	0001-01-01

- **Search⋯**: Search for users by entering the username or ID.
- **Get All users from ACM**: Import user data manually stored in the Genetec Security Center system.
- **Resend to All Devices**: Send users to all devices connected to Suprema Integration with Genetec Security Center.
- **Resend Mail**: Send the visual face remote enrollment link to users via email. Users can access the link from their mobile device and enroll their visual face directly.
- **Enroll Bulk Faces**: Enroll user's visual face by importing CSV.
- **Manage Cards**: Select the card value to communicate with a controller.
- **Manage Fingerprints**: Add, edit, or delete a user's fingerprint template.
- **Manage Faces**: Add, edit, or delete a user's face template.
- **Manage Pin**: Add, edit, or delete a user's Pin.

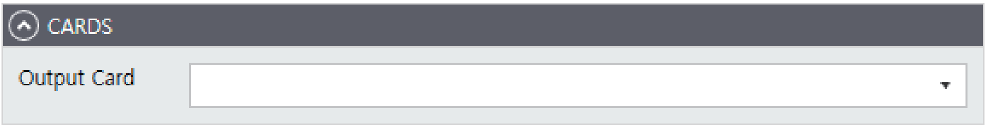
Selecting a card

When a user authenticates with a biometric credential on the device, Suprema Integration with Genetec Security Center sends that user's card ID to the controller. Select the card you want to send to the controller.

1 Click 👥.

2 Select users and click **Manage Cards**.

3 Select the output card.



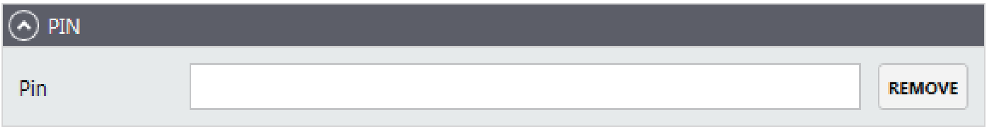
4 Click **APPLY** to save the settings.

Enrolling a PIN

1 Click 👥.

2 Select users and click **Manage Pin**.

3 Enter a PIN to use.



4 Click **APPLY** to save the settings.

Enrolling fingerprint

On the Suprema Integration with Genetec Security Center server, you can enroll user's fingerprints by selecting the device or USB fingerprint scanner. Or, you can also select the user on the device with an LCD display to enroll the fingerprint directly.

Whether you enroll the fingerprint on a server or on a specific device, that user's information is synchronized in real time on all devices connected to Suprema Integration with Genetec Security Center.

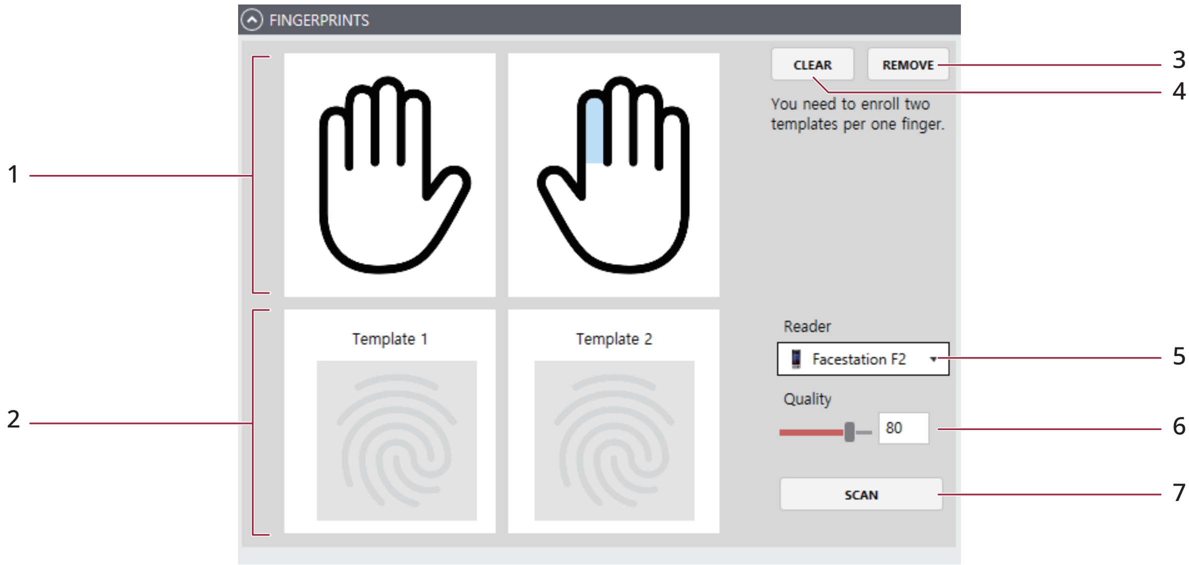
- You can register up to 10 fingerprints per user.
- If the fingerprint authentication rate is low, delete the existing fingerprint information and add a new fingerprint.
- For best fingerprint scanning quality, make sure to cover the entire surface of the fingerprint sensor with the finger. We recommend using the index finger or the middle finger.

Server

1 Click 👥.

2 Select a user and click **Manage Fingerprints**.

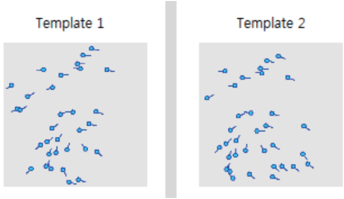
3 Configure the settings.



You need to enroll two templates per one finger.

Reader: Facestation F2

Quality: 80

No.	Item	Description
1	Finger Selection	Select a finger from image to enroll a fingerprint.
2	Fingerprint Image	This section shows the analysis of the fingerprint enrolled. 
3	CLEAR	Delete all registered fingerprints templates.
4	REMOVE	Delete a selected fingerprint template.

5	Reader	Select a device or USB fingerprint scanner to enroll the fingerprint with. **NOTE** • Only devices connected to Suprema Integration with Genetec Security Center are displayed in the Reader list. Register the device first by referring to Adding a device automatically and then enroll fingerprints.
6	Quality	Select a fingerprint enrollment quality level. Any fingerprint which does not meet the quality requirement will not be enrolled.
7	SCAN	Click SCAN and then place a finger on the fingerprint scanner or the device sensor.

4 Click **APPLY** to enroll the fingerprint.

Device

You can view the added user in the user list of the device connected to Suprema Integration with Genetec Security Center.

- This section uses the FaceStation F2 as an example. The user interface such as the name of functions and the shape of icons may be different for each device.
- For how to register fingerprint of each device, refer to the user guide of the device.

1 On the device, press ⊞ and authenticate with the Admin level credential.

2 Press **USER** and select a user to enroll a fingerprint.

3 Press **Fingerprint**.

4 Press ⊕ and enroll a fingerprint. Scan the fingerprint of a finger you wish to enroll, and then scan the fingerprint of the same finger again.

Enrolling a face

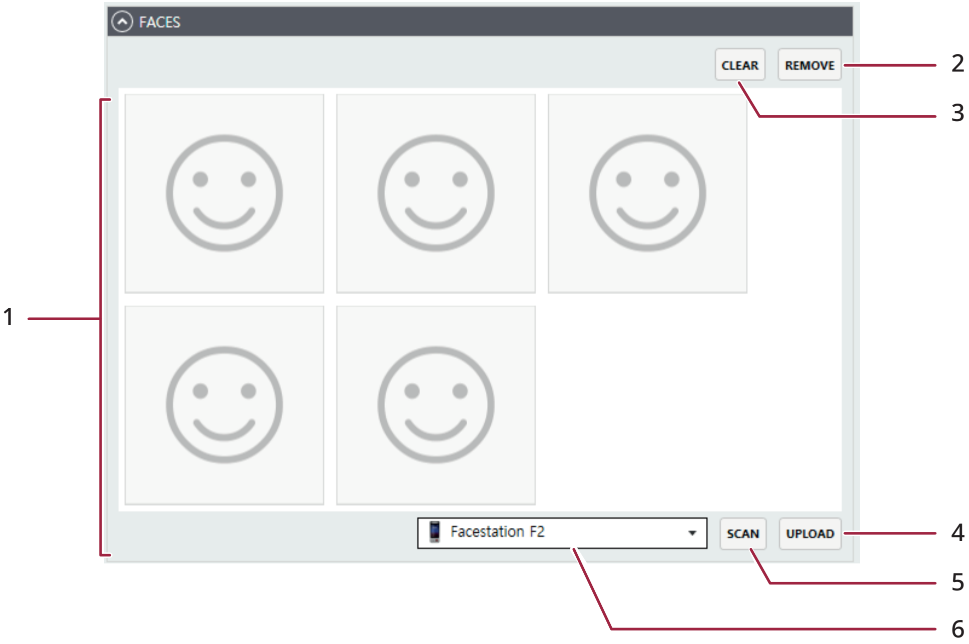
On the Suprema Integration with Genetec Security Center server, you can enroll user's face by selecting the device. Or, you can also select the user on the device with an LCD display to enroll the face directly.

Whether you enroll the face on a server or on a specific device, that user's information is synchronized in real time on all devices connected to Suprema Integration with Genetec Security Center.

- You can register up to 5 face templates per user. On FaceStation F2, you can register up to 2 face templates per user.
- When registering a face, maintain a distance of 60 cm to 100 cm between the device and the face.
- Do not change your face expression.
- Do not wear masks, hats, or eye patches.
- Do not raise head up or lower head.
- Do not close your eyes.
- Do not wear thick makeup.
- Be careful not to display two faces on the screen. Register one person at a time.
- If you do not follow the instructions on the screen, the face registration may take longer or may fail.

Server

1. Click .
2. Select a user and click **Manage Faces**.
3. Configure the settings.



No.	Item	Description
1	Face Image	Select the face.
2	REMOVE	Delete the selected face template.
3	CLEAR	Delete all registered face templates.
4	UPLOAD	Upload a user's picture.
5	SCAN	Click **SCAN** and then follow the instructions on the device screen to scan.
6	Device	Select a device to enroll the face with.

4. Click **APPLY** to enroll the face.

Device

You can view the added user in the user list of the device connected to Suprema Integration with Genetec Security Center.

- This section uses FaceStation F2 as an example. The user interface such as the name of functions and the shape of icons may be different for each device.
- For how to register the face of each device, refer to the user guide of the device.

1. Press and authenticate with the Admin level credential.
2. Select **USER** and select a user to enroll a face.
3. Press **Face**.
4. Press and enroll a face.

Erolling a visual face

Visual Face is a credential that captures the user's face with a visual camera. It is different from face information captured with an infrared camera and is only available on devices that support Visual Face.

- The devices that can use Visual Face are as follows.
  - FaceStation F2 FW v1.1.1 or later

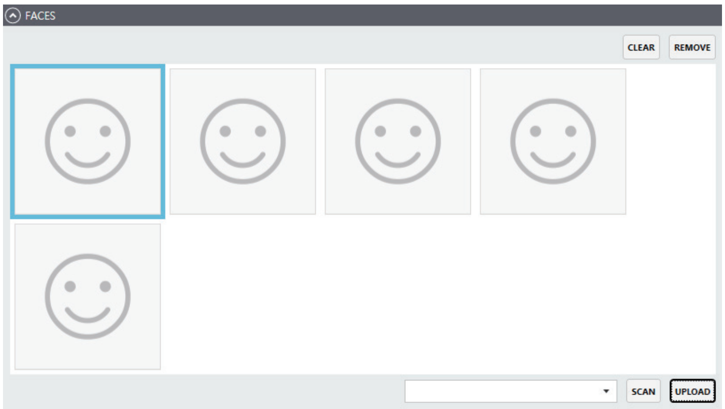
Enroll by uploading an image

You can upload the image to use as a visual face.

- FaceStation F2 must be connected when uploading an image.

1 Click 👥.

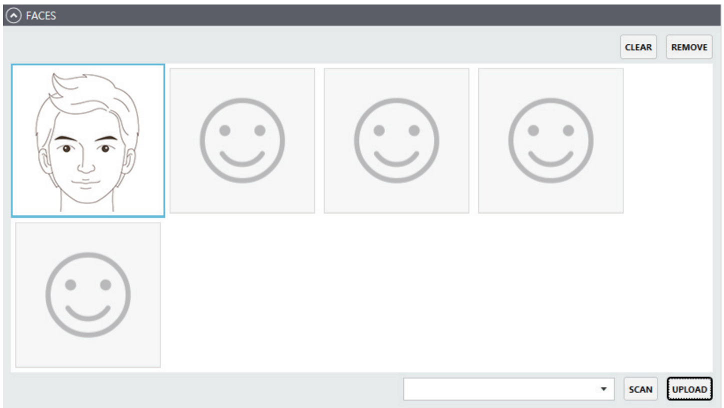
2 Select a user and click **Manage Faces**.



3 Click **UPLOAD** and select an image to be enrolled as the user's visual face.

- Supported image file size is up to 5MB.
- Supported image file formats are JPG, JPEG and PNG.
- Use an image with the user's face straight in the front. Do not use images taken with the user wearing a mask, hat, eye patch, etc., closing eyes, or frowning.

4 A visual face image will appear on the **Face** tab. Click **APPLY**. If the upload fails, check the device connection and the specifications of the image file. And then try again.



Enroll remotely

You can send the visual face remote enrollment link to users via email. Users can access the link from their mobile device and enroll their visual face directly.

An AWS account is required to use the visual face remote enrollment, and you need to register your AWS account and set the SMTP/POP.

Checking AWS account information

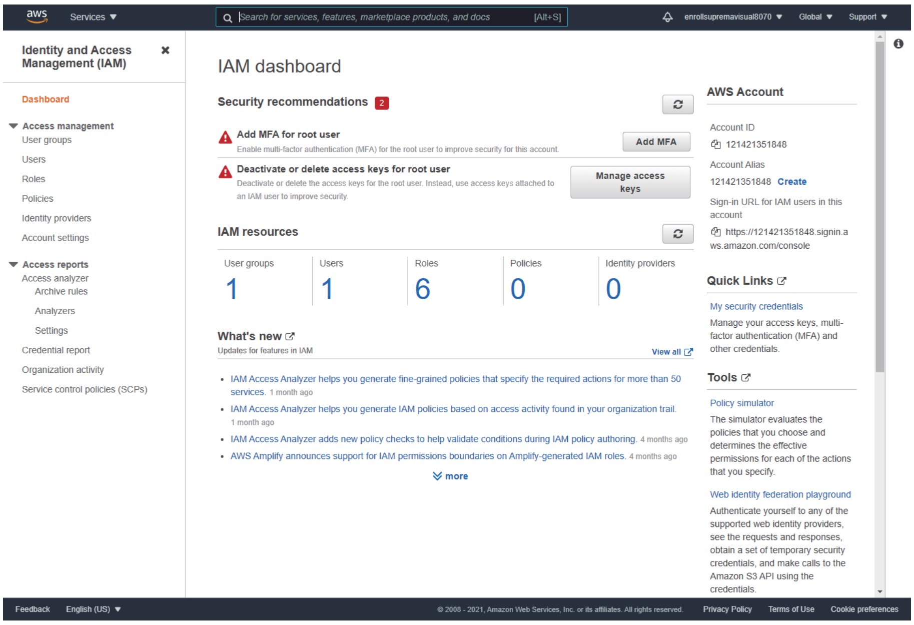
To use the visual face remote enrollment, the following information is required.

- AWS Account ID
- AWS Access Key ID
- AWS Secret Access Key
- Default region name
- Default output format

You can find this information on the AWS website (https://aws.amazon.com).

1 Log in to your AWS account. If you do not have an account, click **Create an AWS Account** to create one.

2 Click **Services** to access **Identity and Access Management (IAM)**.



IAM dashboard

Security recommendations 2

Add MFA for root user
Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Deactivate or delete access keys for root user
Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	6	0	0

What's new
Updates for features in IAM

- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 1 month ago
- IAM Access Analyzer helps you generate IAM policies based on access activity found in your organization trail. 1 month ago
- IAM Access Analyzer adds new policy checks to help validate conditions during IAM policy authoring. 4 months ago
- AWS Amplify announces support for IAM permissions boundaries on Amplify-generated IAM roles. 4 months ago

AWS Account

Account ID
121421351848

Account Alias
121421351848 Create

Sign-in URL for IAM users in this account
https://121421351848.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

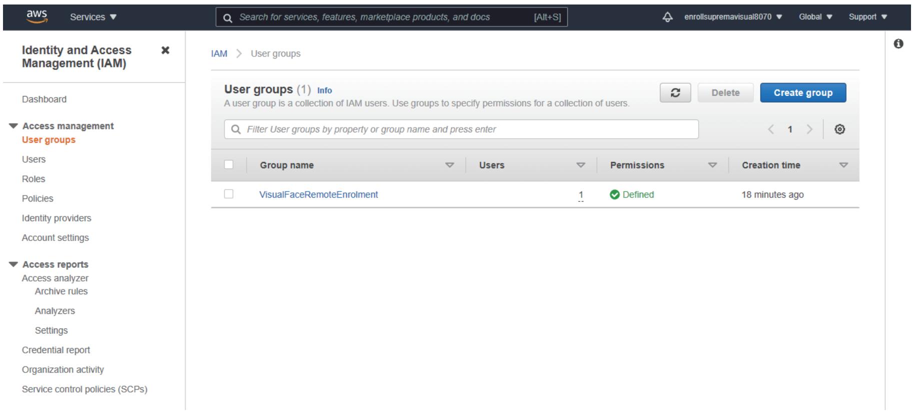
Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

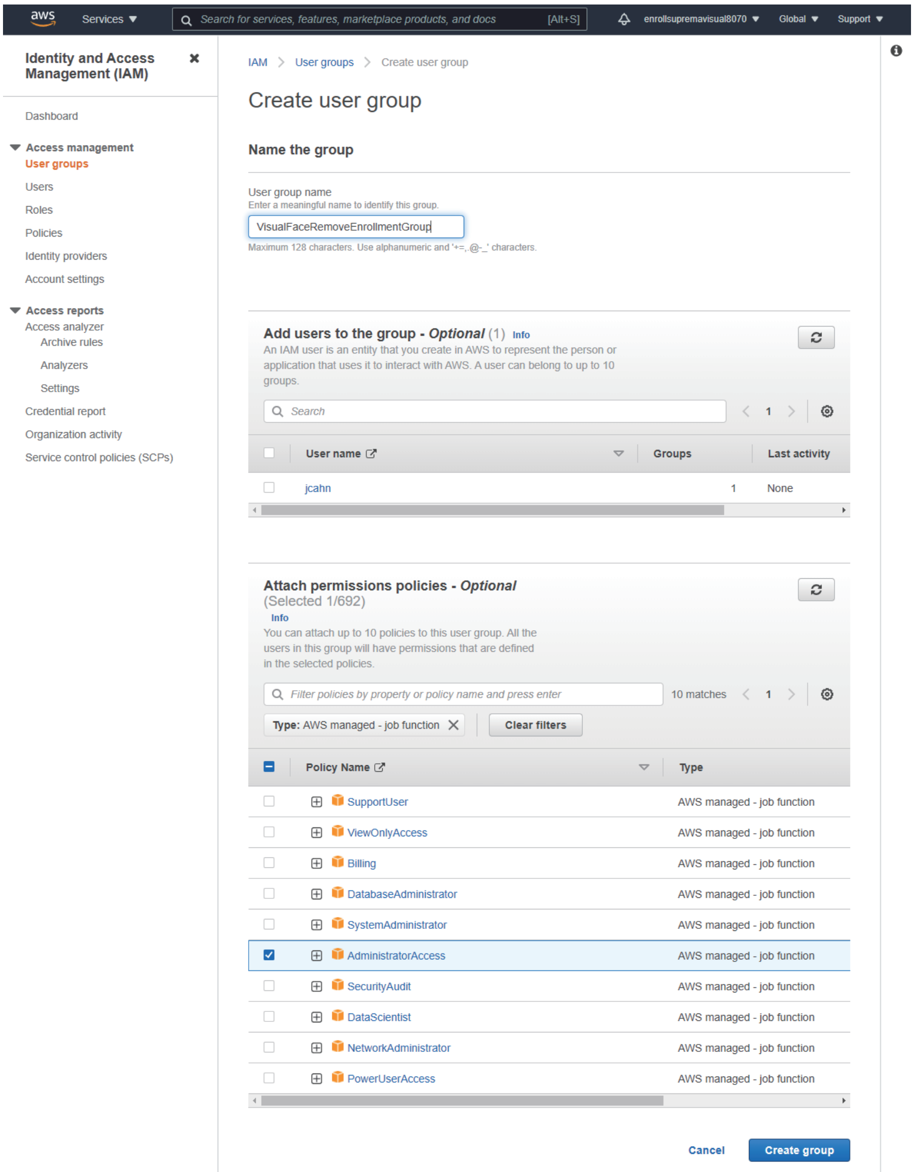
3 Select **User groups** under **Access management** and click **Create group**.



User groups (1)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	VisualFaceRemoteEnrolment	1	✓ Defined	18 minutes ago

4 Enter the user group name and select **AdministratorAccess** for the permissions policies. And then click **Create group**.



IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
VisualFaceRemoveEnrollmentGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

□	User name	Groups	Last activity
□	jcahn	1	None

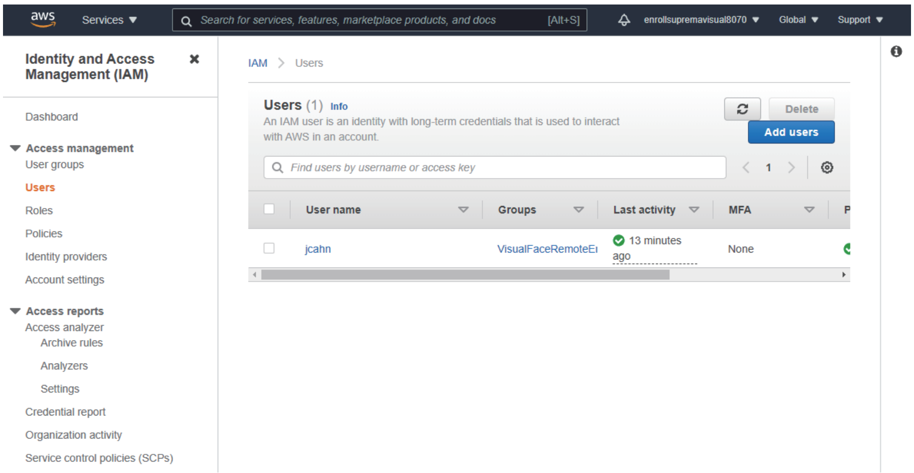
Attach permissions policies - *Optional* (Selected 1/692) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter
10 matches
Type: AWS managed - job function ✕
Clear filters

☐	Policy Name	Type
□	SupportUser	AWS managed - job function
□	ViewOnlyAccess	AWS managed - job function
□	Billing	AWS managed - job function
□	DatabaseAdministrator	AWS managed - job function
□	SystemAdministrator	AWS managed - job function
☑	AdministratorAccess	AWS managed - job function
□	SecurityAudit	AWS managed - job function
□	DataScientist	AWS managed - job function
□	NetworkAdministrator	AWS managed - job function
□	PowerUserAccess	AWS managed - job function

Cancel
Create group

5 Select **Users** under **Access management** and click **Add users**.



IAM > Users

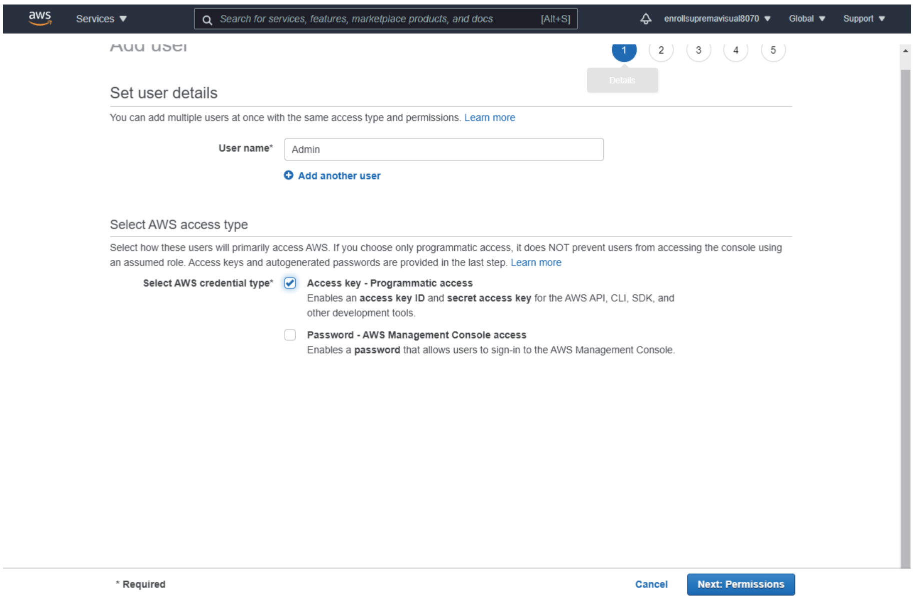
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Delete
Add users

Find users by username or access key

□	User name	Groups	Last activity	MFA	P
□	jcahn	VisualFaceRemoteE	13 minutes ago	None	

6 Enter the user name and Select **Access key - Programmatic access** on the **Select AWS access type** tab. And then click **Next:Permissions**.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
enrollsupremavisual8070 ▼
Global ▼
Support ▼
Add user
1
2
3
4
5
Details

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Admin

Add another user

Select AWS access type

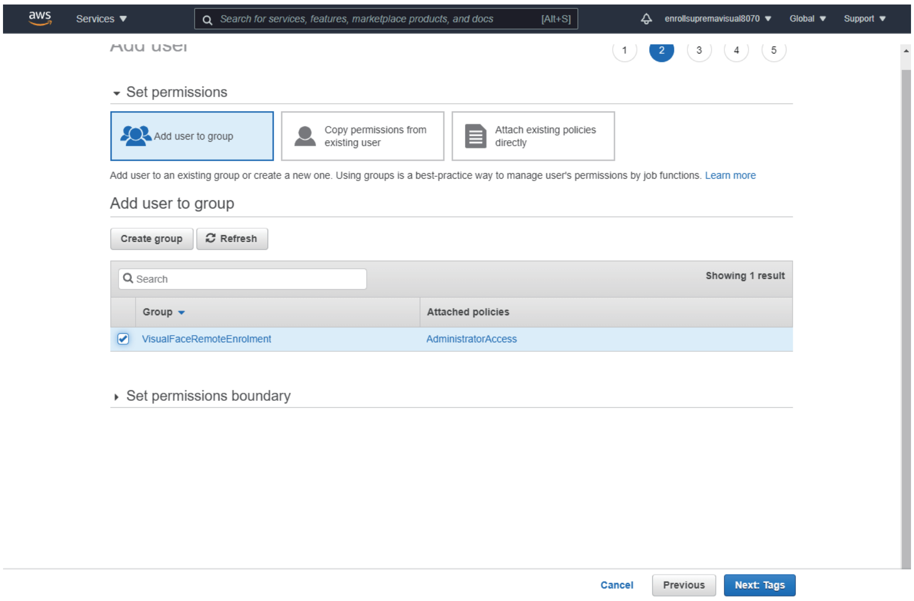
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* ☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

7 Select the group and click **Next:Tags**.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
enrollsupremavisual8070 ▼
Global ▼
Support ▼
Add user
1
2
3
4
5

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Create group
Refresh
Search

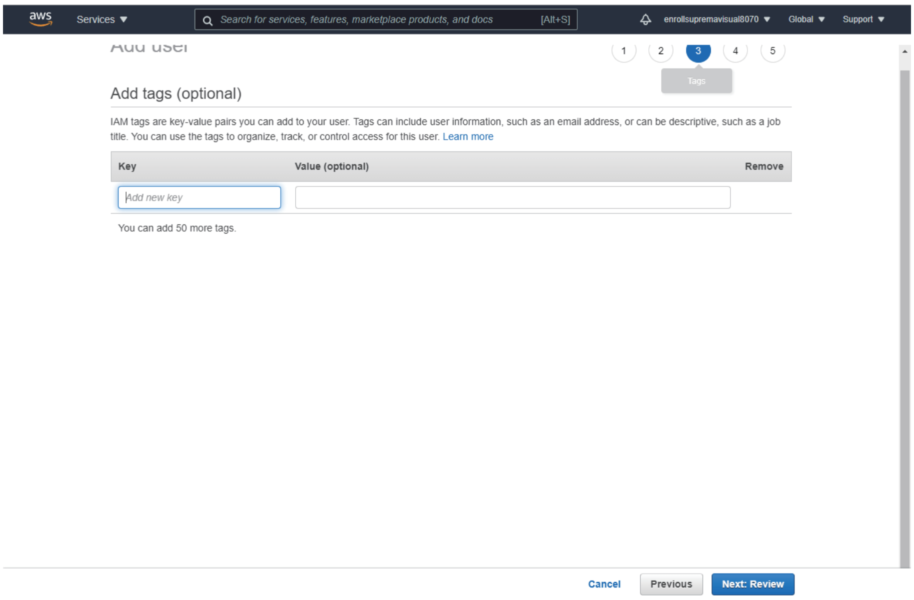
Showing 1 result

	Group	Attached policies
☑	VisualFaceRemoteEnrolment	AdministratorAccess

Set permissions boundary

Cancel
Previous
Next: Tags

8 Add tags. This step is optional. Click **Next:Review**.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
enrollsupremavisual8070 ▼
Global ▼
Support ▼
Add user
1
2
3
4
5
Tags
Cancel
Previous
Next: Review

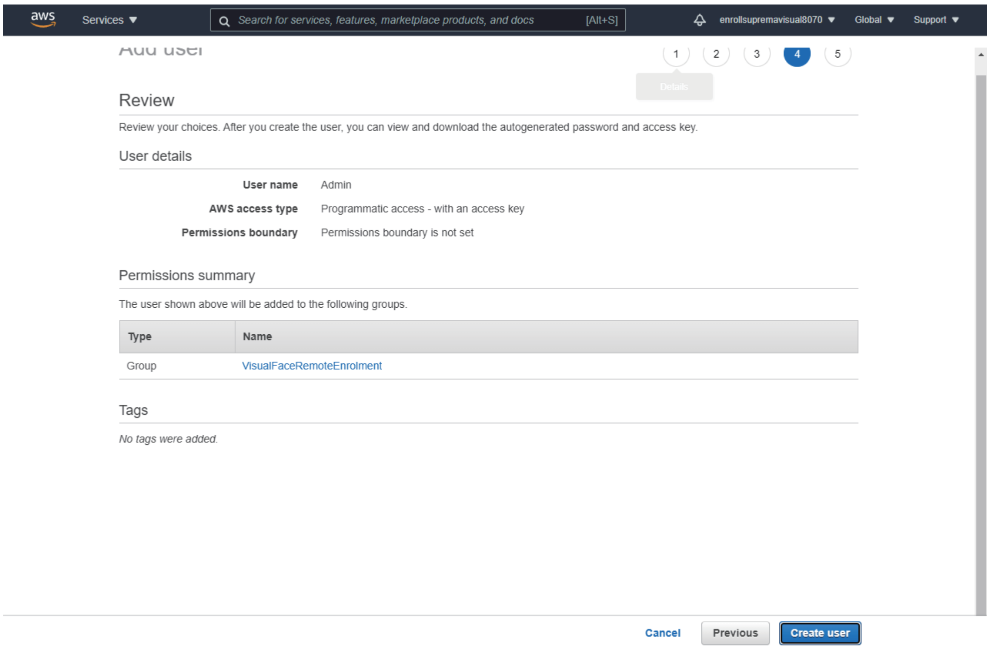
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

9 Check the user details you have set and click **Create user**.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
enrollsupremavisual8070 ▼
Global ▼
Support ▼
Add user
1
2
3
4
5
Details
Cancel
Previous
Create user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name Admin

AWS access type Programmatic access - with an access key

Permissions boundary Permissions boundary is not set

Permissions summary

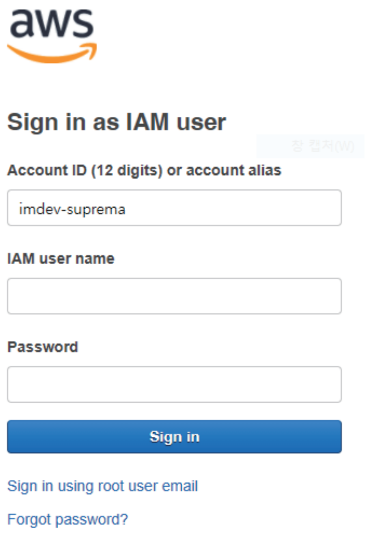
The user shown above will be added to the following groups.

Type	Name
Group	VisualFaceRemoteEnrolment

Tags

No tags were added.

10 Sign in again with the created IAM user account.



Sign in as IAM user

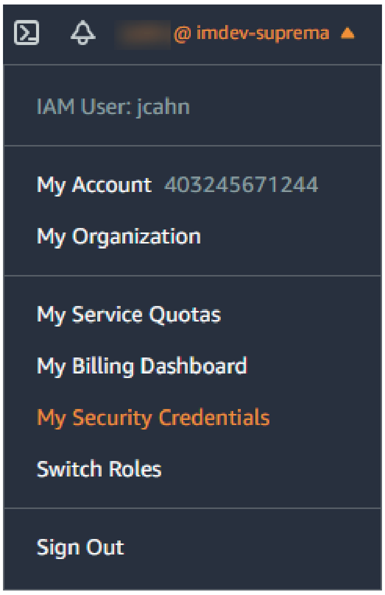
Account ID (12 digits) or account alias

imdev-suprema

IAM user name

Password

11 Click your email address in the upper right corner of the screen and then click **My Security Credentials**.

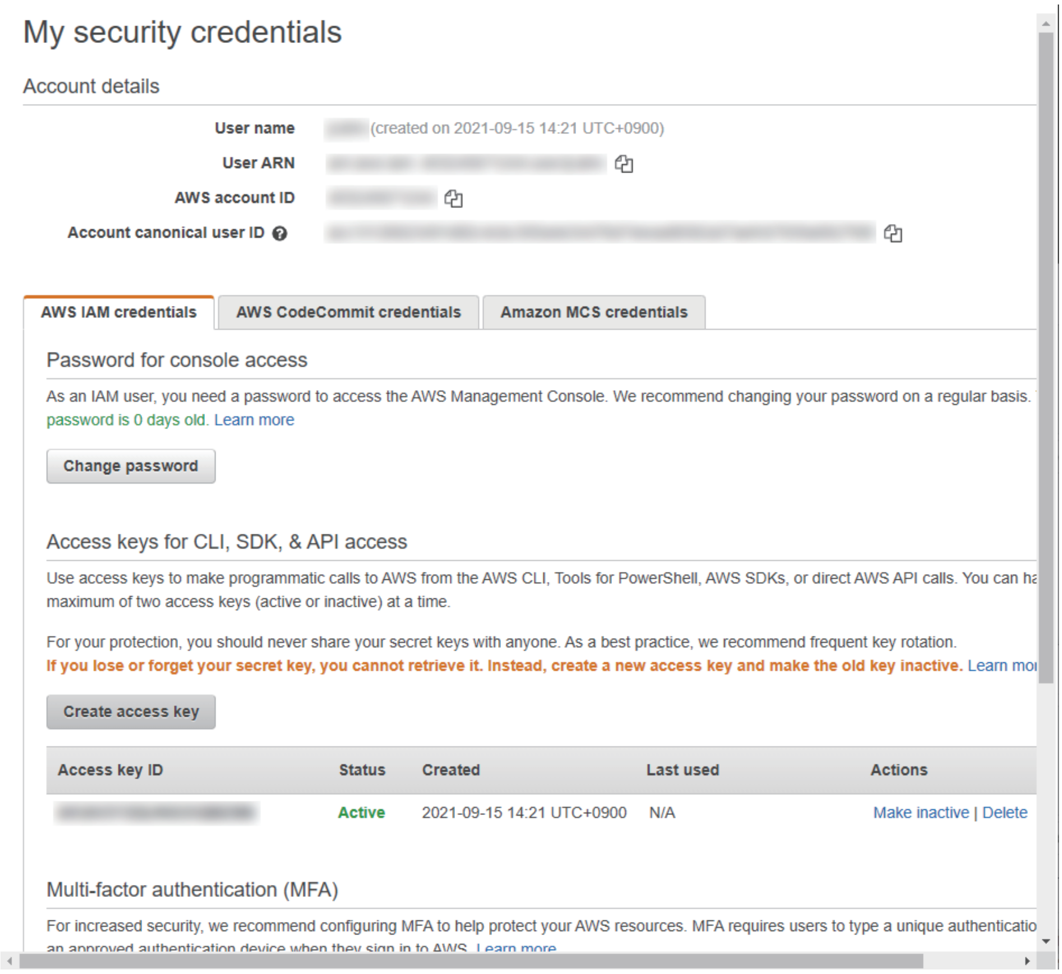


[redacted] @ imdev-suprema

IAM User: jcahn

My Account 403245671244

12 Check your **AWS Account ID**. Then, click **Create access key** on the **AWS IAM credentials** tab.



My security credentials

Account details

User name	[redacted] (created on 2021-09-15 14:21 UTC+0900)
User ARN	[redacted]
AWS account ID	[redacted]
Account canonical user ID	[redacted]

Password for console access

As an IAM user, you need a password to access the AWS Management Console. We recommend changing your password on a regular basis. password is 0 days old. Learn more

Access keys for CLI, SDK, & API access

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can ha maximum of two access keys (active or inactive) at a time.

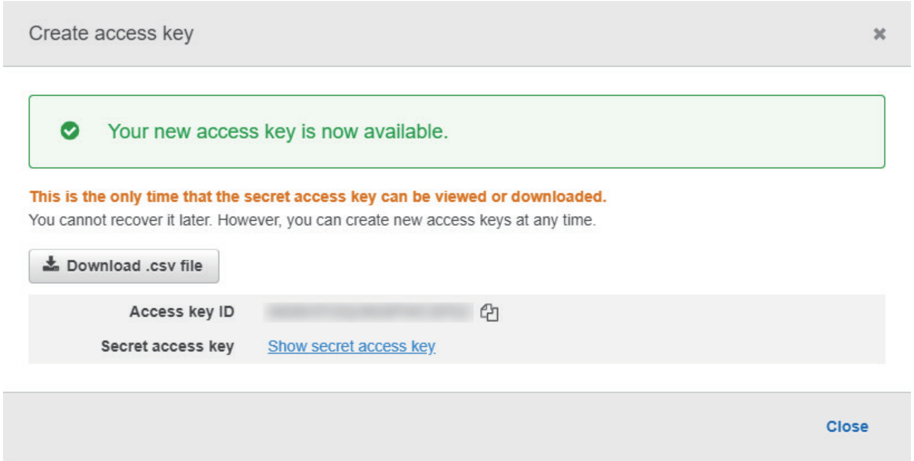
For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn mor

Access key ID	Status	Created	Last used	Actions
[redacted]	Active	2021-09-15 14:21 UTC+0900	N/A	Make inactive | Delete

Multi-factor authentication (MFA)

For increased security, we recommend configuring MFA to help protect your AWS resources. MFA requires users to type a unique authenticatio an approved authentication device when they sign in to AWS. Learn more

13 Click **Show secret access key**.



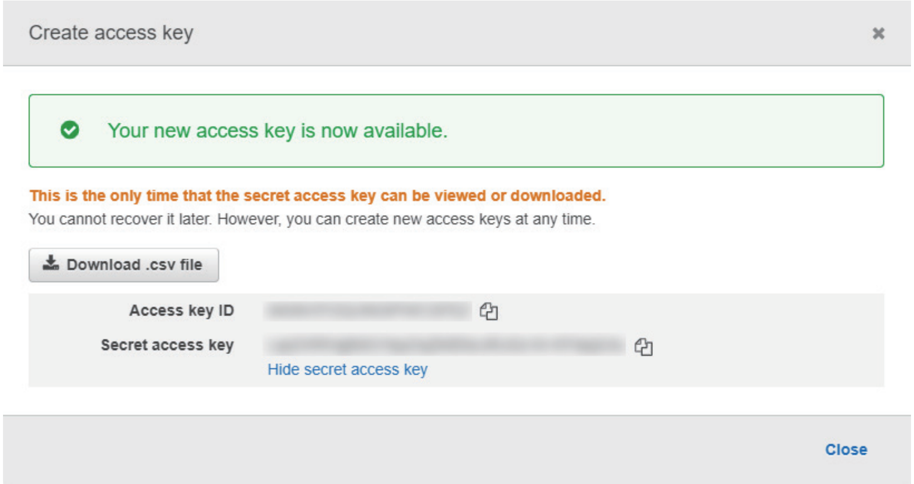
Create access key

Your new access key is now available.

This is the only time that the secret access key can be viewed or downloaded.
You cannot recover it later. However, you can create new access keys at any time.

Access key ID	[redacted]
Secret access key	Show secret access key

14 Check the **Access Key ID** and **Secret access key**. Keep your access key in a safe place to avoid losing it.



Create access key ×

Your new access key is now available.

This is the only time that the secret access key can be viewed or downloaded.
You cannot recover it later. However, you can create new access keys at any time.

Download .csv file

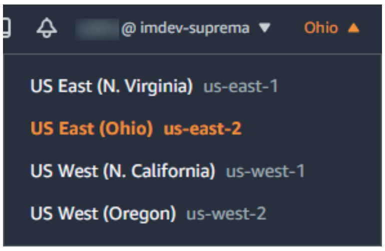
Access key ID [redacted]

Secret access key [redacted]

Hide secret access key

Close

15 Click **Global** in the upper right corner of the screen to select a region.



[redacted]@ imdev-suprema ▼ Ohio ▲

US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

US West (N. California) us-west-1

US West (Oregon) us-west-2

Checking SMTP/POP3 information

Visual face remote enrollment links are emailed to individual users. When a user accesses the link and registers a face using a mobile device, the visual face data is sent back to the system via email. Incoming Mail (POP) Server and Outgoing Mail (SMTP) Server are required for this process.

This document describes how to set up the SMTP/POP server using Gmail as an example. If you are using another email service, refer to the guidance of the email service provider.

1 Log in with a gmail account to use as an SMTP and POP server.

2 Click ⠿ → Account.

3 Select **Security** in the navigation panel.

4 Click **Less secure app access** and set **Allow less secure apps** to **ON**.

5 Under **Signing in to Google**, click **2-Step Verification** → **GET STARTED**.

6 Follow the on-screen instructions to create an app password.

7 Click ⠿ → **Gmail**.

8 Click ⚙ → **See all settings**.

9 Click the **Forwarding and POP/IMAP** tab.

10 In the **POP download section**, select **Enable POP for all mail** or **Enable POP for mail that arrives from now on**.

11 Click **Save Changes**.

If you set up the SMTP/POP servers with gmail as above, you can enter each field of SMTP and POP3 in the visual face settings on Settings as follows.

Item	Description
Outgoing Mail (SMTP) Server	• **Server Address**: smtp.gmail.com • **Port**: 587 • **User Name**: Email sender name • **Password**: The app password created in step 6 above
Incoming Mail (POP) Server	• **Server Address**: pop.gmail.com • **Port**: 995 • **User Name**: Email recipient name • **Password**: The app password created in step 6 above

- When using the SMTP server as an email account with two-factor authentication and change the password of the account, note the following: Once you set up two-factor authentication, the SMTP password is the same as the app password generated using two-factor authentication, not the password of the email account. At this time, if the password of the email account is changed, the app password is automatically deleted, and the SMTP password is no longer available. When changing the password for the email account, regenerate the app password and then set the SMTP password again.

Enrolling a visual face remotly

You can send the visual face remote enrollment link to users via email.

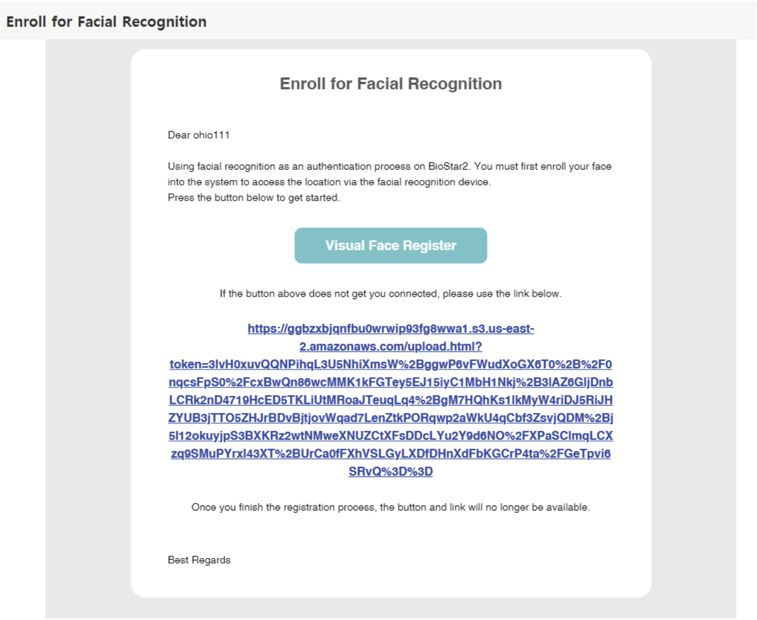
If all settings for using remote enrollment are completed and email address is registered to the user, a remote enrollment link will be automatically sent to the user by email. Users can access the link from their mobile device and enroll their visual face directly.

You can also manually send emails to users if automatic delivery fails.

1 Click 👥.

2 Select a user and click **Resend Mail**.

3 The visual face enrollment link will be sent to the email of the selected user.



Enroll for Facial Recognition

Enroll for Facial Recognition

Dear ohio111

Using facial recognition as an authentication process on BioStar2. You must first enroll your face into the system to access the location via the facial recognition device.
Press the button below to get started.

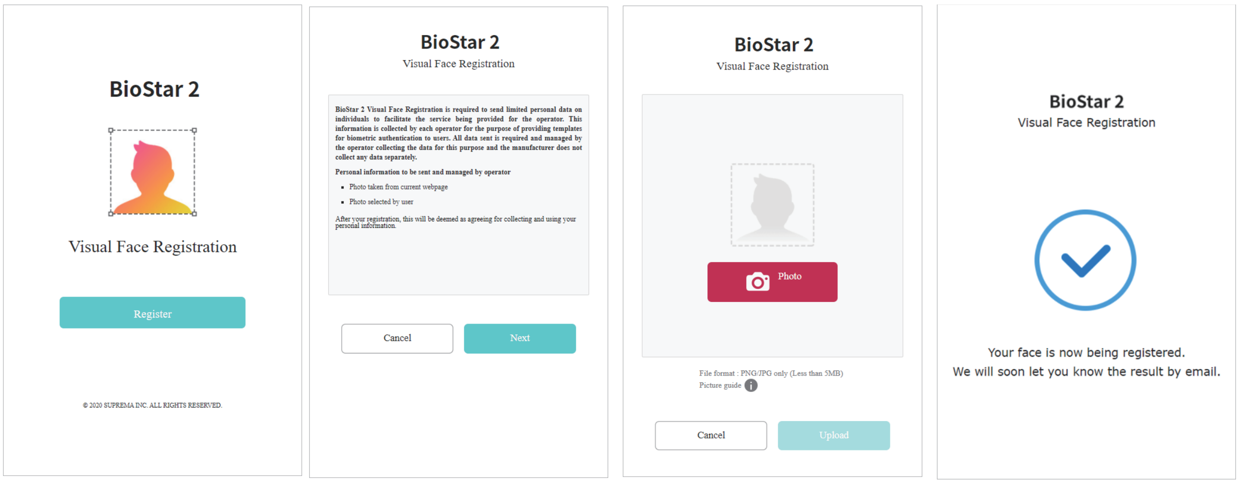
If the button above does not get you connected, please use the link below.

https://ggbzxbjqnfbu0wrwip93fg8wwa1.s3.us-east-2.amazonaws.com/upload.html?token=3lvH0xuvQQNPihqL3U5NhiXmsW%2BggwP6vFWudXoGX6T0%2B%2F0nqcsFpS0%2FcxBwQn86wcMMK1kFGTey5EJ15iyC1MbH1Nkj%2B3lAZ6GljDnbLCRk2nD4719HcED5TKLiUtMRoaJTeuqLq4%2BgM7HQhKs1lkMyW4riDJ5RiJHZYUB3jTTO5ZHJrBDvBjtjovWqad7LenZtkPORqwp2aWkU4qCbf3ZsvjQDM%2Bj5l12okuyjpS3BXKRz2wtNMweXNUZCtXFsDDcLYu2Y9d6NO%2FXPaSClmqLCXzq9SMuPYrxl43XT%2BUrCa0fFXhVSLGyLXDfDHnXdFbKGCrP4ta%2FGeTpvi6SRvQ%3D%3D

Once you finish the registration process, the button and link will no longer be available.

Best Regards

When the user taps on **Visual Face Register** button on the email, the visual face enrollment is executed as follows.



BioStar 2

Visual Face Registration

Register

© 2020 SUPREMA INC. ALL RIGHTS RESERVED.

BioStar 2

Visual Face Registration

BioStar 2 Visual Face Registration is required to send limited personal data on individuals to facilitate the service being provided for the operator. This information is collected by each operator for the purpose of providing templates for biometric authentication to users. All data sent is required and managed by the operator collecting the data for this purpose and the manufacturer does not collect any data separately.

Personal information to be sent and managed by operator

- Photo taken from current webpage
- Photo selected by user

After your registration, this will be deemed as agreeing for collecting and using your personal information.

Cancel Next

BioStar 2

Visual Face Registration

Photo

File format : PNG/JPG only (Less than 5MB)

Picture guide

Cancel Upload

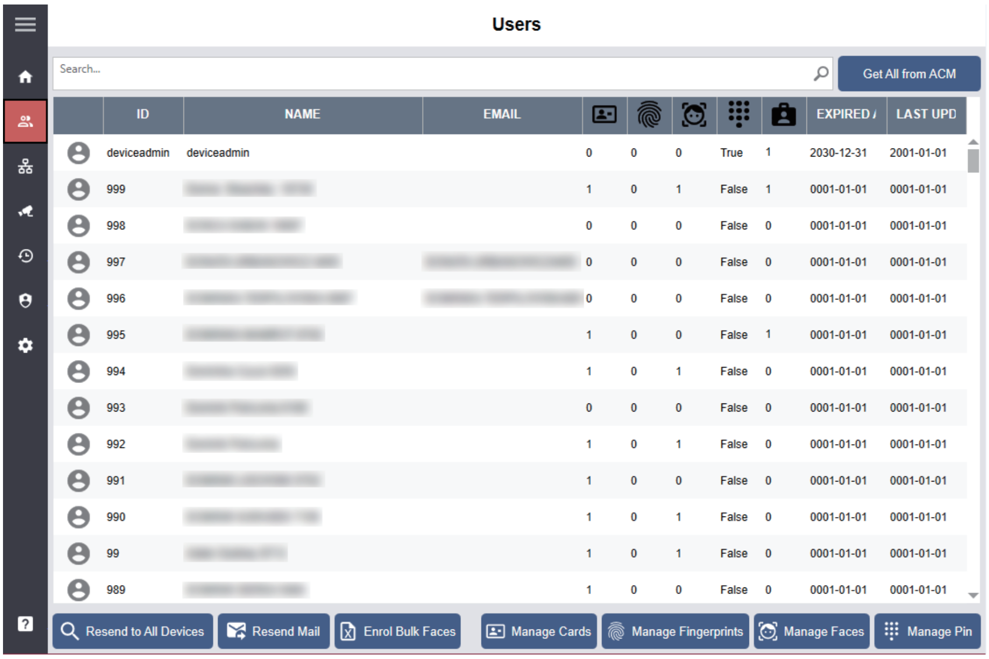
BioStar 2

Visual Face Registration

Your face is now being registered.
We will soon let you know the result by email.

- If the user receiving the visual face remote enrollment link uses an external email application, the language of the email application must be set to the language of their country. If the language does not support Unicode, the text in the email may be broken.
- Supported image file size is up to 5MB.
- Supported image file formats are JPG, JPEG and PNG.
- Once the visual face remote enrollment process is complete, users will receive an email notifying them of successful registration. If registration fails, a new link for the visual face remote enrollment will be sent and the user can retry the registration. At this time, the existing registration link will automatically expire.

4 When the user completes the upload, a number is displayed in the column. Select that user and click **Manage Faces**.



Users

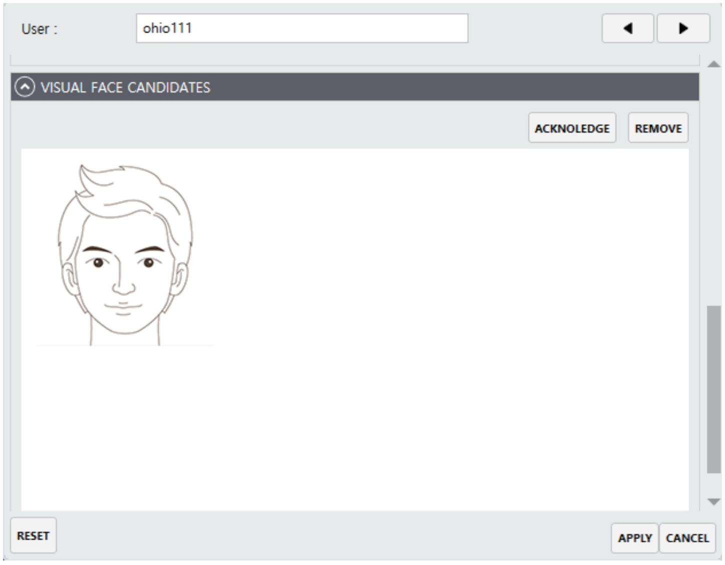
Search...

Get All from ACM

ID	NAME	EMAIL						EXPIRED /	LAST UPD
deviceadmin	deviceadmin		0	0	0	True	1	2030-12-31	2001-01-01
999	[redacted]		1	0	1	False	1	0001-01-01	0001-01-01
998	[redacted]		0	0	0	False	0	0001-01-01	0001-01-01
997	[redacted]	[redacted]	0	0	0	False	0	0001-01-01	0001-01-01
996	[redacted]	[redacted]	0	0	0	False	0	0001-01-01	0001-01-01
995	[redacted]		1	0	0	False	1	0001-01-01	0001-01-01
994	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
993	[redacted]		0	0	0	False	0	0001-01-01	0001-01-01
992	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
991	[redacted]		1	0	0	False	0	0001-01-01	0001-01-01
990	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
99	[redacted]		1	0	1	False	0	0001-01-01	0001-01-01
989	[redacted]		1	0	0	False	0	0001-01-01	0001-01-01

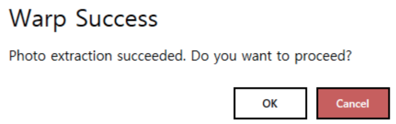
- If **Use Auto Acknowledge** is set in Settings, the process below will be omitted when the user completes visual face enrollment, and the user's visual face will be automatically enrolled. For more information, refer to Visual Face.

5 Check the visual face in the **VISUAL FACE CANDIDATES** tab and click **ACKNOLEDGE**.



User : ohio111

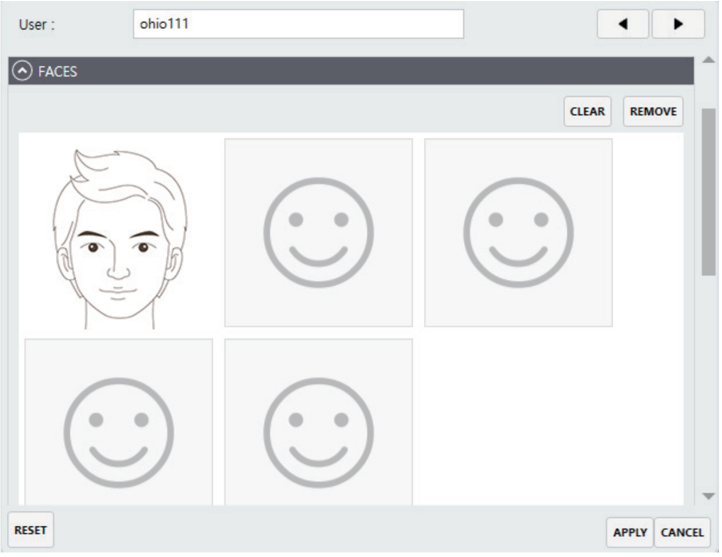
6 If the image extraction is successful, the following message is displayed. Click **OK** to continue.



Warp Success

Photo extraction succeeded. Do you want to proceed?

7 The extracted visual face is enrolled in the **FACES** tab. Click **APPLY** to complete the enrollment of the visual face, and the visual face is synchronized with devices so that the user can authenticate the face.



User : ohio111

Enroll by CSV Import

You can enroll user's visual face by importing CSV.

- FaceStation F2 must be connected when importing the CSV file.
- Each column setting in the CSV file is as follows.
  - **user_id**: Enter the user ID.
  - **face_image_file1**: Enter the image file name including the extension.
  - **face_image_file2**: Enter the image file name including the extension.
- It is recommended to use the same path for the CSV file and visual face image files to be loaded.

1 Enter the file name of visual face image, including the extension in visual face column (**face_image_file1**, **face_image_file2**) of CSV file, and then save it.

2 Click → **Enroll Bulk Faces**.

3 Select the csv file to import and click **Open**.

4 Data of the selected CSV file is displayed. Set the necessary items.

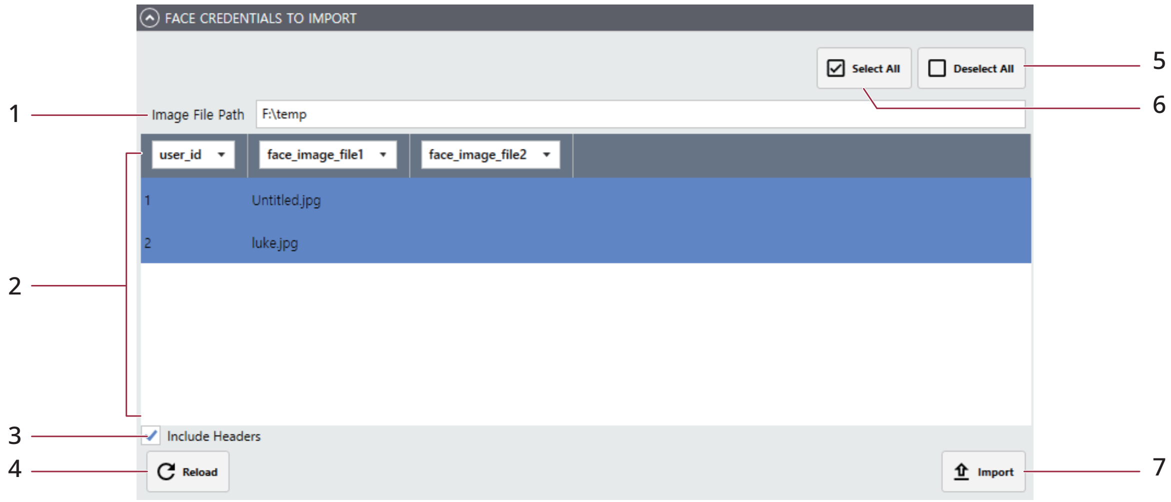
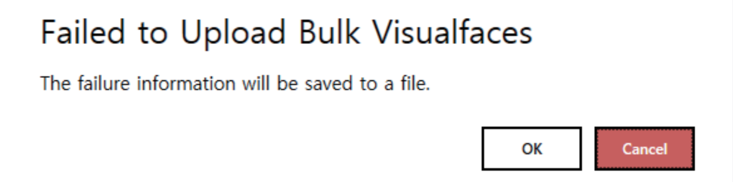


Image File Path: F:\temp

user_id	face_image_file1	face_image_file2
1	Untitled.jpg	
2	luke.jpg	

No.	Item	Description
1	Image File Path	Set the path of image files. It is recommended to use the same path for the CSV file and visual face image files to be loaded.
2	User data	A list of loaded users is displayed.
3	Include Headers	If there is a header in the csv, click this option.
4	Reload	Load the csv file again.
5	Deselect All	Deselect selected users.
6	Select All	Select all users.
7	Import	Select users to import and click **Import**.

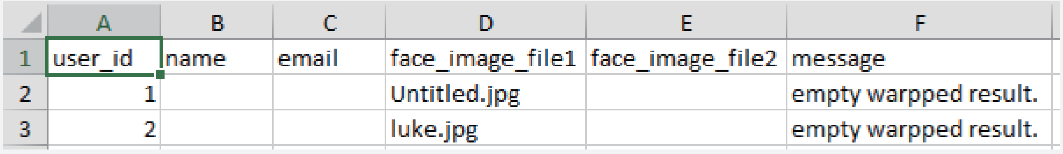
- If an error occurs during the import of CSV file information, you can upload it again after checking only the erroneous CSV data.



Failed to Upload Bulk Visualfaces

The failure information will be saved to a file.

If you see the error message, click **OK** and download the import failure result file.



	A	B	C	D	E	F
1	user_id	name	email	face_image_file1	face_image_file2	message
2	1			Untitled.jpg		empty warpped result.
3	2			luke.jpg		empty warpped result.

Resending user data to connected devices

You can send users to all devices connected to Suprema Integration with Genetec Security Center.

1 Click 👥.

2 Select users to send and click **Resend to All Devices**.

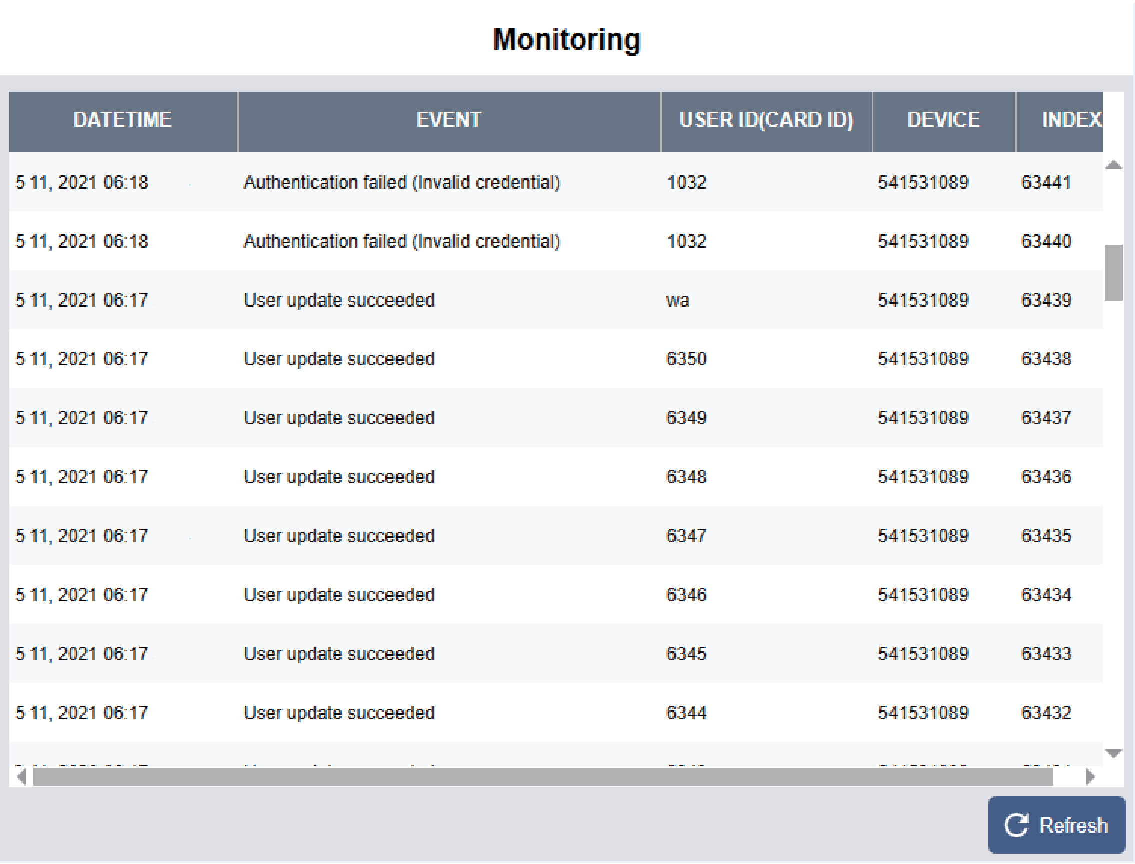
3 Check the list of users on the device.

Monitoring

You can use the Monitoring menu to view logs.

1 Click 📹.

2 Check the logs.
To delete the logs, click **Clear**.



Monitoring

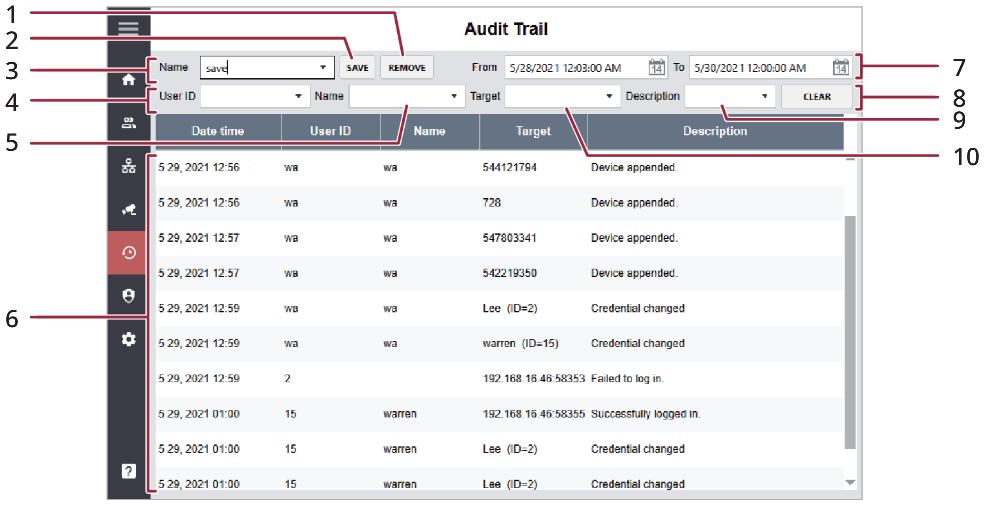
DATETIME	EVENT	USER ID(CARD ID)	DEVICE	INDEX
5 11, 2021 06:18	Authentication failed (Invalid credential)	1032	541531089	63441
5 11, 2021 06:18	Authentication failed (Invalid credential)	1032	541531089	63440
5 11, 2021 06:17	User update succeeded	wa	541531089	63439
5 11, 2021 06:17	User update succeeded	6350	541531089	63438
5 11, 2021 06:17	User update succeeded	6349	541531089	63437
5 11, 2021 06:17	User update succeeded	6348	541531089	63436
5 11, 2021 06:17	User update succeeded	6347	541531089	63435
5 11, 2021 06:17	User update succeeded	6346	541531089	63434
5 11, 2021 06:17	User update succeeded	6345	541531089	63433
5 11, 2021 06:17	User update succeeded	6344	541531089	63432

Audit Trail

Audit trail tracks user access information as well as all the information changed in the system. You can extract data using filters for each item.

1 Click 🕘.

2 Set filters.



Audit Trail

Name: save

From: 5/28/2021 12:03:00 AM To: 5/30/2021 12:00:00 AM

User ID: Name: Target: Description:

Date time	User ID	Name	Target	Description
5 29, 2021 12:56	wa	wa	544121794	Device appended.
5 29, 2021 12:56	wa	wa	728	Device appended.
5 29, 2021 12:57	wa	wa	547803341	Device appended.
5 29, 2021 12:57	wa	wa	542219350	Device appended.
5 29, 2021 12:59	wa	wa	Lee (ID=2)	Credential changed
5 29, 2021 12:59	wa	wa	warren (ID=15)	Credential changed
5 29, 2021 12:59	2		192.168.16.46:58353	Failed to log in.
5 29, 2021 01:00	15	warren	192.168.16.46:58355	Successfully logged in.
5 29, 2021 01:00	15	warren	Lee (ID=2)	Credential changed
5 29, 2021 01:00	15	warren	Lee (ID=2)	Credential changed

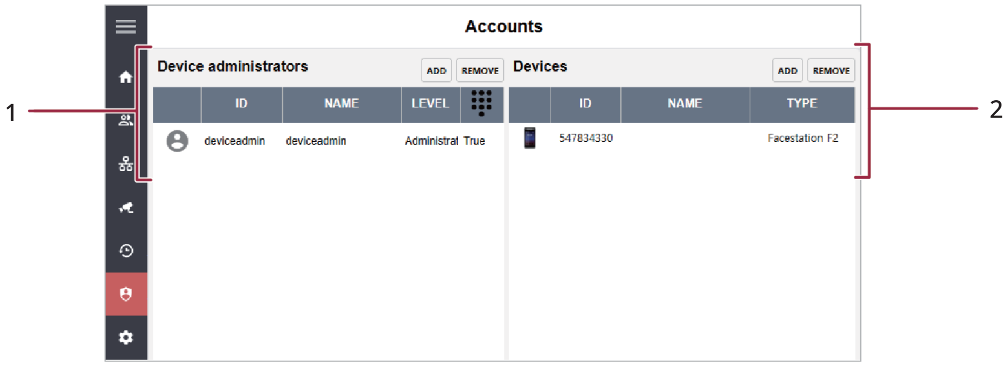
No.	Item	Description
1	REMOVE	Remove the preset filter.
2	SAVE	Save the current filter values.
3	Name	Select a preset filter.
4	User ID	Select a user ID.
5	Name	Select a username.
6	Audit List	Shows the audit list.
7	Period	Set the period.
8	CLEAR	Clear the current filter values.
9	Description	Select a description.
10	Target	Select a target.

Accounts

You can assign administrator account levels to registered users.

1 Click 🛡.

2 Configure the settings.



Accounts

Device administrators ADD REMOVE

ID	NAME	LEVEL	
deviceadmin	deviceadmin	Administrat	True

Devices ADD REMOVE

ID	NAME	TYPE
547834330		Facestation F2

No.	Item	Description
1	Device administrators	A list of administrators registered with Suprema Integration with Genetec Security Center is displayed. If a PIN is set in the administrator account, the administrator can log in directly to Suprema Integration with Genetec Security Center. • **ADD**: Assign the administrator level by selecting a user. Select an account level type, then click on the user to whom you want to assign that level. **NOTE** • The administrator account levels are as follows: • **Administrator**: Users can access and use all menus. • **Device Operator**: If a PIN is registered with the user, the user can log in to Suprema Integration with Genetec Security Center. Also, users can register user accounts in the client system and configure device settings by accessing devices. • **User Operator**: If a PIN is registered with the user, the user can log in to Suprema Integration with Genetec Security Center. Also, users can register user accounts in the client system and enroll users in devices. • **REMOVE**: Remove an administrator.
2	Devices	The list of devices that can be managed by the user selected in the Device administrator list is displayed. • **ADD**: Add devices to the selected administrator. • **REMOVE**: Remove the device from the selected administrator.

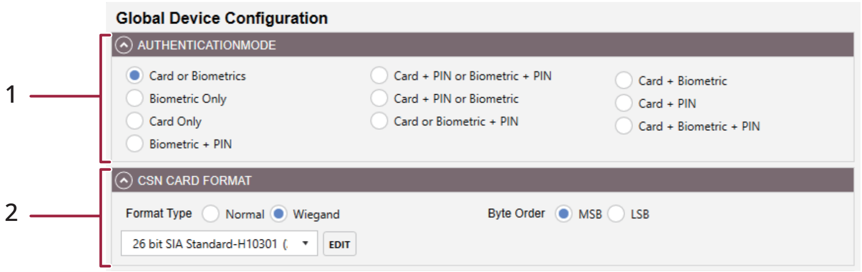
Settings

Global Device Configuration

You can edit settings of registered devices.

1 Click ⚙.

2 Configure the settings.



Global Device Configuration

AUTHENTICATIONMODE

● Card or Biometrics
○ Biometric Only
○ Card Only
○ Biometric + PIN
○ Card + PIN or Biometric + PIN
○ Card + PIN or Biometric
○ Card or Biometric + PIN
○ Card + Biometric
○ Card + PIN
○ Card + Biometric + PIN

CSN CARD FORMAT

Format Type ○ Normal ● Wiegand

Byte Order ● MSB ○ LSB

26 bit SIA Standard-H10301 (▾ EDIT

No.	Item	Description
1	AUTHENTICATION MODE	Configure the authentication modes of the device. Suprema Integration with Genetec Security Center can use any combinations of biometric credentials, card, and PIN as authentication modes.
2	CSN CARD FORMAT	Set the CSN card format used by the device. • **Format Type**: If Format Type is set to **Normal**, the device will read the card serial number (CSN). If the option is set to **Wiegand**, the device will read the card serial number in a Wiegand format that the user has defined. If Format Type is set to **Wiegand**, you can set the Wiegand format to be used in the device. Click **EDIT** to edit the Wiegand format. You can configure the number of bits and rules for the Wiegand format directly in Suprema Integration with Genetec Security Center, as in Genetec Security Center. • **Byte Order**: When Byte Order is set to **MSB**, the device reads a card ID from the highest byte to the lowest byte. When the option is set to **LSB**, the device reads a card ID from the lowest byte to the highest byte.

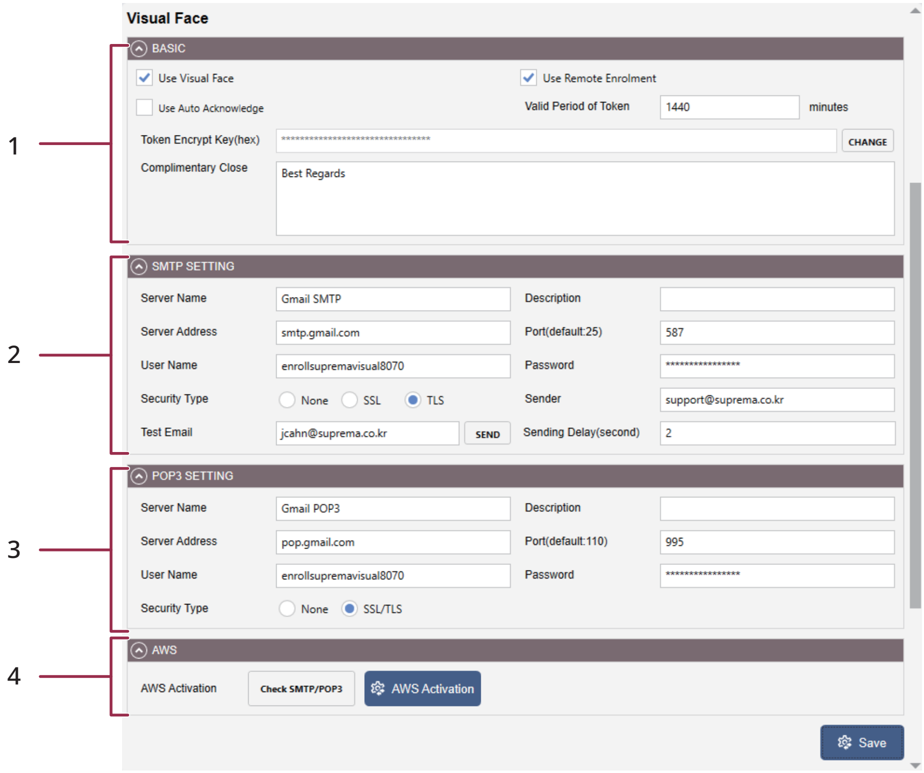
3 Click **Save** to save the settings.

Visual Face

You can set whether to use visual face and remote enrollment. And you can also enter the SMTP/POP3 settings and activate AWS.

1 Click ⚙.

2 Configure the settings.



Visual Face

BASIC

☑ Use Visual Face ☑ Use Remote Enrolment

□ Use Auto Acknowledge Valid Period of Token 1440 minutes

Token Encrypt Key(hex) ******************************** CHANGE

Complimentary Close Best Regards

SMTP SETTING

Server Name Gmail SMTP Description

Server Address smtp.gmail.com Port(default:25) 587

User Name enrollsupremavisual8070 Password ***************

Security Type ○ None ○ SSL ● TLS Sender support@suprema.co.kr

Test Email jcahn@suprema.co.kr SEND Sending Delay(second) 2

POP3 SETTING

Server Name Gmail POP3 Description

Server Address pop.gmail.com Port(default:110) 995

User Name enrollsupremavisual8070 Password ***************

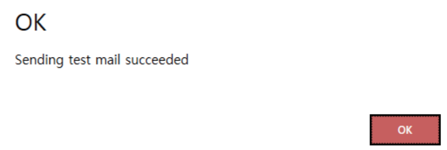
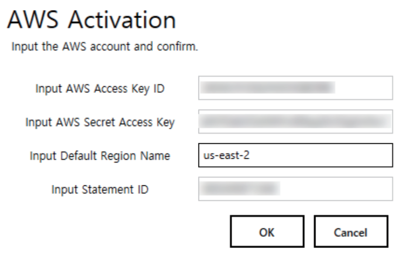
Security Type ○ None ● SSL/TLS

AWS

AWS Activation Check SMTP/POP3 AWS Activation

Save

No.	Item	Description
1	BASIC	You can make basic settings related to visual face. • **Use Visual Face**: Click to use the visual face as a credential. • **Use Remote Enrollment**: Click to use the visual face remote enrollment. • **Use Auto Acknowledge**: Click to automatically enroll a visual face as a user's credential when that is received by email. If this option is not selected, the administrator must enroll it manually. • **Valid Period of Token**: Set the time for the visual face remote enrollment link to expire. You can enter numbers from 30 to 10080. If you enter an invalid value and save it, it will be changed to 1440. • **Token Encrypt Key(hex)**: Enter the token encrypt key. If there is no token encryption key, it is automatically generated. If the key is exposed, click **CHANGE** to change the key. • **Complimentary Close**: Enter the complimentary close in the email.

2	SMTP SETTING	Set up SMTP to send emails including remote enrollment link. • **Server Name**: Enter the SMTP server name. • **Description**: Enter the description. • **Server Address**: Enter the SMTP server address. SMTP server address is the same form as 'smtp. Email Service Provider.com'. • **Port(default: 25)**: Enter the port number of the email used as the SMTP server. • **User Name**: Enter the name or email address of the email sender. • **Password**: Enter the app password for the email account used as the SMTP server. • **Security Type**: Select security type. • **Sender**: Enter the email address of the email sender. • **Test Email**: Enter an email address to receive the test email and click **SEND**. If the test email is sent successfully, the message below will be displayed.  OK Sending test mail succeeded • **Sending Delay**: Enter the sending delay time. It is recommended to set 3 to 5 seconds. **NOTE** • For each SMTP information, refer to Checking SMTP/POP3 information.
3	POP3 SETTING	Set up POP3 to receive emails from users with remote enrollment information. • **Server Name**: Enter the POP3 server name. • **Description**: Enter the description. • **Server Address**: Enter the POP3 server address. POP3 server address is the same form as 'pop. Email Service Provider.com'. • **Port(default: 110)**: Enter the port number of the email used as the POP server. • **User Name**: Enter the Email recipient name. • **Password**: Enter the app password for the email account used as the POP server. • **Security Type**: Select security type. **NOTE** • For each POP3 information, refer to Checking SMTP/POP3 information.
4	AWS Activation	Activate AWS to use the visual face remote enrollment. Click **AWS Activation**. Enter the value of AWS Access Key ID, AWS Secret Access Key, Default region name, and AWS Statement ID (AWS Account ID).  AWS Activation Input the AWS account and confirm. Input AWS Access Key ID Input AWS Secret Access Key Input Default Region Name: us-east-2 Input Statement ID **NOTE** • For each AWS account information, please refer to Checking AWS account information.

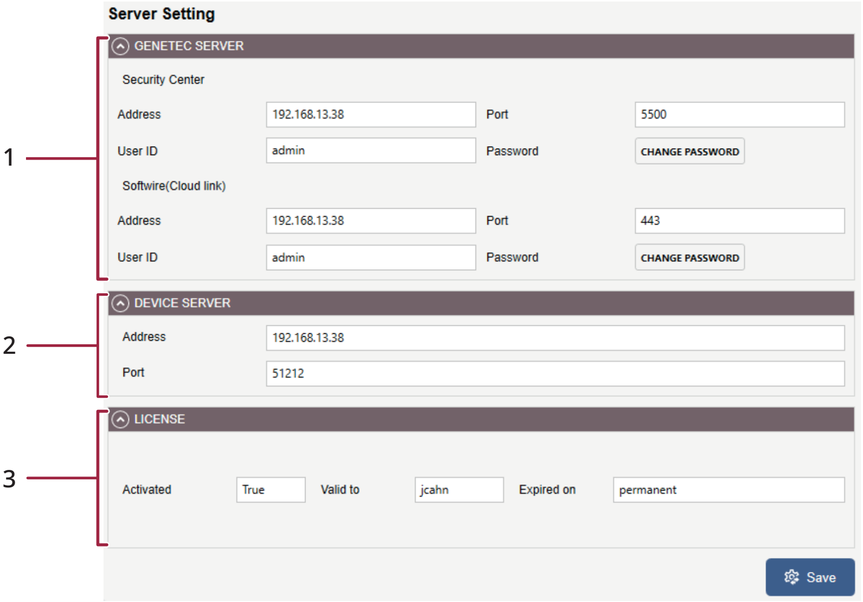
3 Click **Save** to save the settings.

Server Setting

You can set up the network for connecting with Genetec Security Center and devices. You can also activate the purchased license.

1 Click ⚙.

2 Configure the settings.



Server Setting

GENETEC SERVER

Security Center

Address: 192.168.13.38 Port: 5500

User ID: admin Password: CHANGE PASSWORD

Softwire(Cloud link)

Address: 192.168.13.38 Port: 443

User ID: admin Password: CHANGE PASSWORD

DEVICE SERVER

Address: 192.168.13.38

Port: 51212

LICENSE

Activated: True Valid to: jcahn Expired on: permanent

No.	Item	Description
1	GENETEC SERVER	• **Address**: Enter the IP address of both the Genetec Security Center server and Softwire. • **Port**: Enter the port number of both the Genetec Security Center server and Softwire. • **User ID**: Enter the operator ID of Suprema Integration with Genetec Security Center. • **Password**: Click CHANGE PASSWORD to change the current password.
2	DEVICE SERVER	• **Address**: Enter the IP address to use in the device. • **Port**: Enter the port number to use in the device.
3	LICENSE	• **Activated**: It shows the current license status. If the license is activated, it shows **True**. If the license is deactivated, it shows **False**. • **Valid to**: It indicates who has the license. • **Expired on**: It indicates the valid date of the license. **NOTE** • You can find contact details of your local distributor on the Suprema website (https://www.supremainc.com/en/wheretobuy/list.asp).

3 Click **Save** to save the settings.

Enrollment Helper

You can enroll fingerprints and faces by opening a window for enrollment directly from Config Tool by using Enrollment Helper.

- You can choose whether to install the Enrollment Helper when you install the Suprema Integration with Genetec Security Center.

Enrolling credentials with Enrollment Helper

You can enroll fingerprints and faces for both existing and new users.

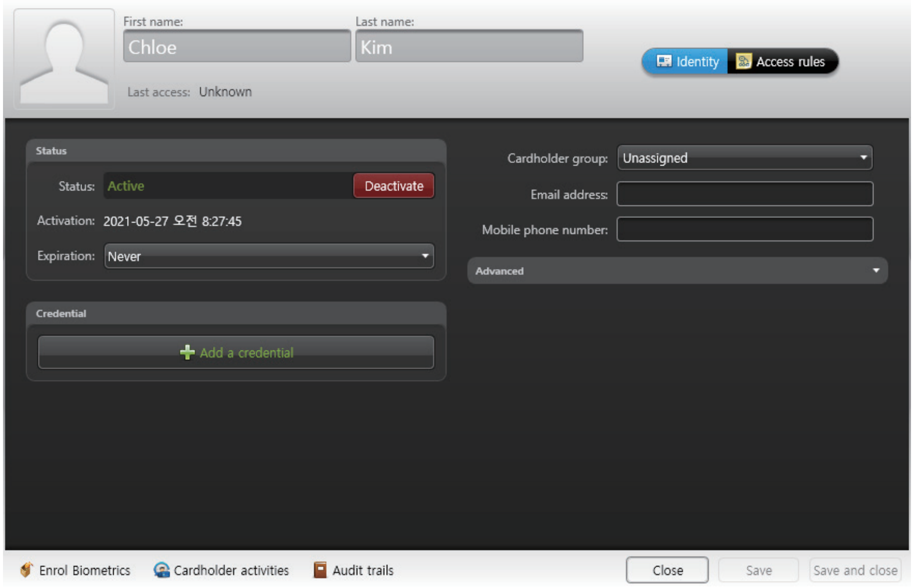
Enrolling credentials to existing users

1 Run **Config Tool**.

2 Click **Config Tool** > **Tasks** > **Cardholder management**.

3 Select a user from the list and click **Modify** at the bottom left corner of the window.

4 Click **Enroll Biometrics**.



First name: Chloe

Last name: Kim

Last access: Unknown

Status

Status: Active

Activation: 2021-05-27 오전 8:27:45

Expiration: Never

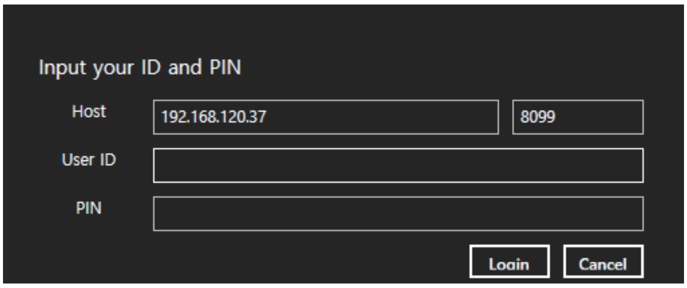
Credential

Cardholder group: Unassigned

Email address:

Mobile phone number:

5 Enter the user ID and PIN that you are using in Suprema Integration with Genetec Security Center and click **Login**.



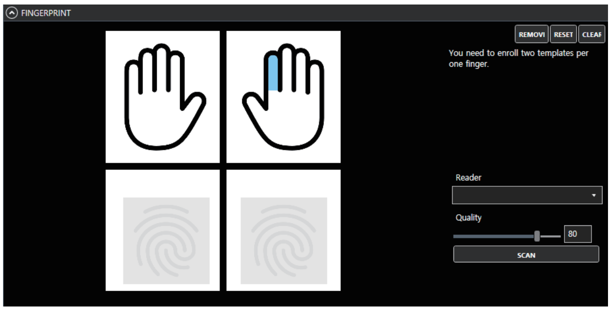
Input your ID and PIN

Host: 192.168.120.37 : 8099

User ID:

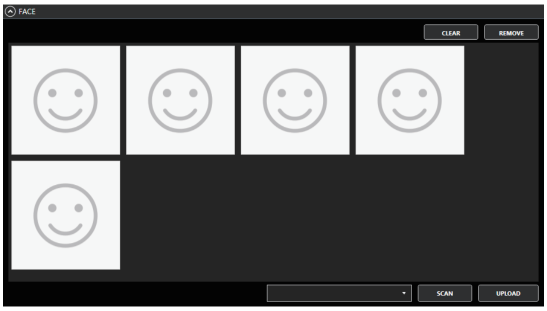
PIN:

6 Enroll fingerprints by referring to Enrolling a face. Or, Enroll faces by referring to Enrolling a face.



You need to enroll two templates per one finger.

Quality: 80



7 Click **APPLY** to save the settings.

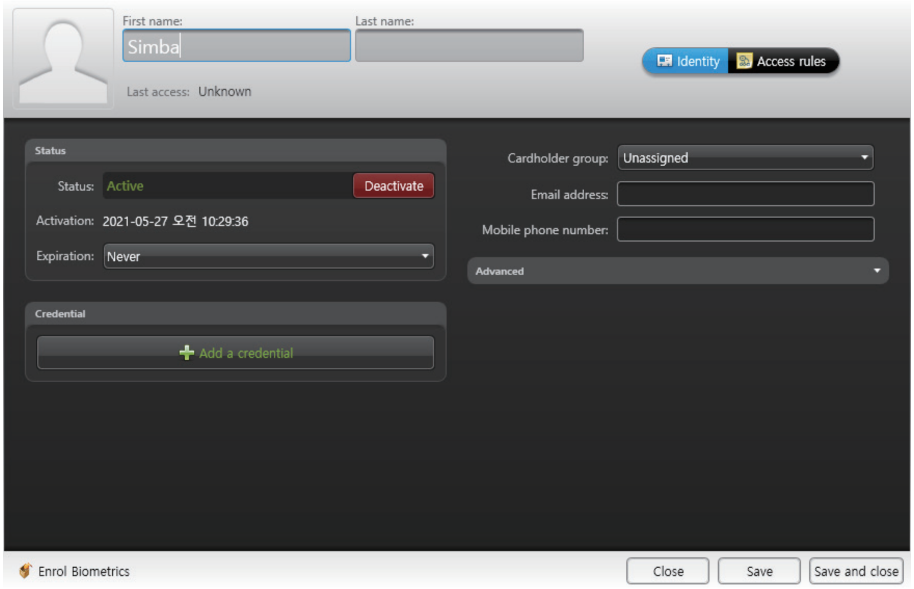
Enrolling credentials to new users

1 Run Config Tool.

2 Click **Config Tool** > **Tasks** > **Cardholder management**.

3 Click **New** at the bottom left corner of the window.

4 Enter user information and click **Save**.



First name: Simba

Last name:

Last access: Unknown

Status: Active

Activation: 2021-05-27 오전 10:29:36

Expiration: Never

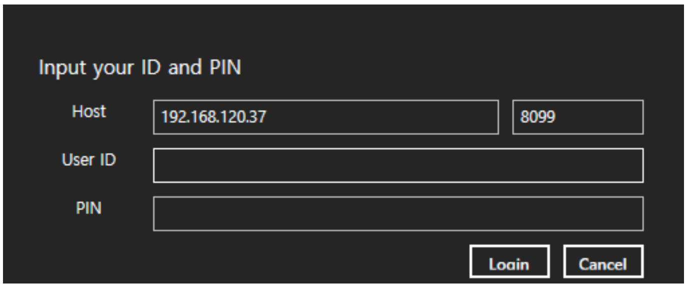
Cardholder group: Unassigned

Email address:

Mobile phone number:

5 Click **Enroll Biometrics**.

6 Enter the user ID and PIN that you are using in Suprema Integration with Genetec Security Center and click **Login**.



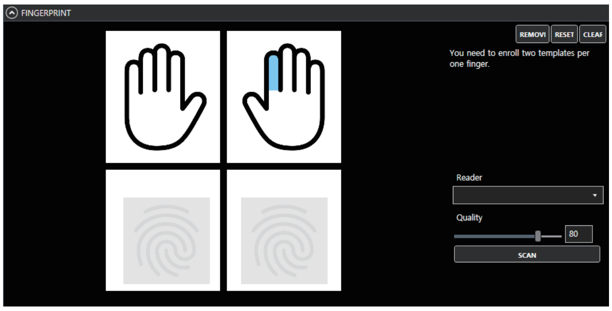
Input your ID and PIN

Host: 192.168.120.37 8099

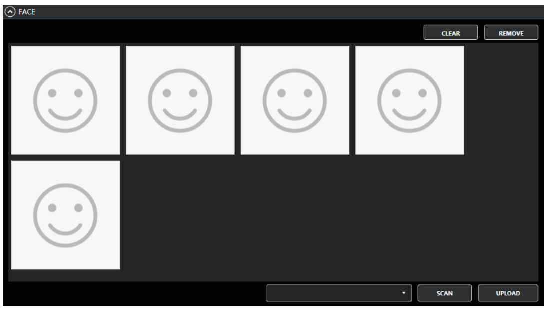
User ID:

PIN:

7 Enroll fingerprints by referring to Enrolling fingerprint. Or, Enroll faces by referring to Enrolling a face.



You need to enroll two templates per one finger.



8 Click **APPLY** to save the settings.

Troubleshooting

This troubleshooting provides information to solve unexpected issues that you may encounter when using Suprema Integration with Genetec Security Center.

Classification	Problem	Solution
License	I cannot create an access control unit due to a license error.	Enter "localhost" for Hostname instead of an IP address.
Visual Face	AWS activation failed, and logs occurred as 'aws is not recognized as an internal or external command, operable program or batch file'.	If AWSCLIV2.msi is not installed, you cannot activate AWS. Install AWSCLIV2.msi of the installation path and try to activate AWS again.
	AWS activation failed, and logs occurred as 'An error occurred (EntityAlreadyExists) when calling the CreateRole operation: Role with name tokenValid-role already exists'.	If there are already created IAM Roles, Lambda, and API Gateway, you cannot create duplicates. Delete the existing IAM Roles, Lambda, and API Gateway as described below and try again. 1 Sign in to your AWS account. 2 Click **Services** → **Identity and Access Management (IAM)**. 3 Select **Roles** under **Access management**. 4 Select **faceDetect-role**, **sendMail-role**, and **tokenValid-role** on the **Roles** list and click **Delete**. 5 Click **Services** → **Lamda** → **Functions**. 6 Select **tokenValidLambda**, **sendMailLambda**, and **faceDetectLambda** on the **Functions** list and click **Actions** → **Delete**. 7 Click **Services** → **API Gateway** → **APIs**. 8 Select **faceDetectLambda-API**, **sendMailLambda-API**, and **tokenValidLambda-API** on the **APIs** list and click **Actions** → **Delete**.
	AWS activation failed, and logs occurred as 'An error occurred (AccessDenied) when calling the CreateRole operation: User: arn:aws:iam::121421351848:user/jcahn is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::121421351848:role/tokenValid-role'.	If you do not have IAM user permissions, you cannot create IAM Roles. Refer to Checking AWS account information and add **AdministratorAccess** to the AWS user's Permission Policy and try again.

Appendices

Disclaimers

- Information in this document is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this document.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema's products that are not within Suprema's direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold “as is”.
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

Suprema has the copyright of this document. The rights of other product names, brands, and trademarks belong to individuals or organizations who own them.

Open Source License

gin-gonic/gin

whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Gorm

The MIT License (MIT)

Copyright (c) 2013-NOW Jinzhu <wosmvp@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Go-ps

The MIT License (MIT)

Copyright (c) 2014 Mitchell Hashimoto

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

google/uuid

Copyright (c) 2009,2014 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following

disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

gorilla/websocket

Copyright (c) 2013 The Gorilla WebSocket Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CommandLineParser

The MIT License (MIT)

Copyright (c) 2005 - 2015 Giacomo Stelluti Scala & Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MahApps Metro

MIT License

Copyright (c) .NET Foundation and Contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MahApps Metro IconPacks

The MIT License (MIT)

Copyright (c) 2016-2019 MahApps, Jan Karger

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Newtonsoft.Json

The MIT License (MIT)

Copyright (c) 2007 James Newton-King

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

Aphache/log4net

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

CovenantSQL/go-sqlite3-encrypt

The MIT License (MIT)

Copyright (c) 2014 Yasuhiro Matsumoto

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

mattn/go-sqlite3

tdewolff/Minify

go-ole/go-ole

ControlzEx/ControlzEx

The MIT License (MIT)

Copyright (c) 2015-2019 Jan Karger, Bastian Schmidt

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA
Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
http://www.supremainc.com/en/about/contact-us.asp