Hik-ProConnect

Convergent Security Service Solution

Hik-ProConnect is a convergent, cloud-based security solution that helps manage services for your customers and expand your business by subscription offers.

You can monitor the system health status of your customers' sites – even resolving problems – remotely, using a simple and reliable platform.

Hik-ProConnect solution enables you to customize security solutions for customers with fully-converged Hikvision device, covering video, intrusion, access, intercom, and more.

- Easy to access with Portal and Mobile Client
- Centralized device management
- 24/7 continuous device status monitoring
- Multiple accounts with individual permissions
- Comprehensive device authority management mechanism
- Remote operation and maintenance capabilities for high quality and efficient services
- More efficient installation process
- Various cross-device linkage scenarios and timely pushing event and related videos to Hik-Connect Mobile Client
- Co-branding and brand promotion

Hik-ProConnect Portal

General

Supported Language	English, Arabic, Brazilian Portuguese, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovakian, Slovenian, Spanish, Swedish, Thai, Traditional Chinese, Turkish, Ukrainian, Uzbek, and Vietnamese.
Wizard	Guide user through the process of configurations and operations.
Feedback	- Submit feedback information, including Installation and Deployment, Linkage Rule, Maintenance, Company Management, Permission, Exception, and Other. - The words, a picture, and email address can be used for reply.
Demo	Experience general features of Hik-ProConnect without registering any accounts to promote further registration, use and purchase for Hik-ProConnect.
Deployment	Global server deployment for accessing Hik-ProConnect more quickly and stably.

System Requirements

Operating System	Microsoft® Windows 7/8.1/10 (32-bit and 64-bit).
Web Browser	Internet Explorer 11 (32-bit and 64-bit) and above, and version of Firefox (32-bit and 64-bit) and Google Chrome (32-bit and 64-bit) released in the last half year.

Account Management

Employee	Unlimited.
Account	- Register Installer Admin account using email. When registering account, select to subscribe to marketing communications about Hik-ProConnect. You can unsubscribe at any time. - Delete Installer Admin account. - Edit basic information or change password for current account. - Invite employee to register an Installer account.
Role	- Three default roles (including IT Manager, Site Manager, and Administrator) are supported. - Manage roles and customize role.

	Assign roles with different permissions, including Manage All Sites, Manage Assigned Site, Manage Account and Role, and Manage Company Information.
Company Information	- Bind company information, including company logo, business license number, VAT number, etc. - Display company logo on the Hik-Connect Mobile Client for brand promotion. - View comparison about the supported functions and manageable devices between basic package and health monitoring package.

Home Page

Contents	Include the banner, site overview, device overview, exception overview, frequently used functions, recently visited sites, employees in total, and help.
Quick Entries	Go to the module directly via quick entries.

Site Management

Number of Sites	Unlimited.
Manage Site	Add new/existing site, edit, and delete site. Different countries and regions are supported when adding new site, including time zone and phone area code.
Invite Site Owner	- Invite end user as Site Owner by email or phone number. The end user will receive the invitation email or message in email box or via short message with a download link of Hik-Connect Mobile Client, and can select whether to accept the invitation via Hik-Connect Mobile Client. - When inviting Site Owner, apply for permissions of site information management, configuration, and live view, and set validity period (1 to 8 hours, or permanent) for the permissions of configuration and live view.
Apply for Site Authorization	- Site Owner can select whether to grant the authorization. - Site Owner can select the devices, added in Hik-Connect Mobile Client, but not added and managed in the site, and

	authorize the permissions of the devices to the Installer. ● The Installer can release the permissions of configuration and live view actively.
Cancel Authorization	The end user can cancel the site authorization.

Device Management

Device	Unlimited.
Supported Device Type	Network camera, NVR, DVR, access control device, security control panel, video intercom device, and doorbell.
Cloud P2P	Support accessing device via Cloud P2P, applicable for different network environments.
Adding Mode	● Add one or multiple devices detected by SADP. ● Add device by Hik-Connect service. ● Add device by IP address or domain name. ● Add device in a batch by entering device parameters in a predefined template. ● Add a device to the site authorized to an Installer and set permissions for Installer on Hik-Connect Mobile Client. After that the Installer can manage this device on Hik-ProConnect.
Device Upgrade	● Upgrade one or multiple devices remotely. ● Detect the compatibility of devices' firmware versions with Hik-ProConnect when adding devices.
DDNS	For devices with invalid or old firmware version added by Hik-Connect service, configure DDNS for them to support Hik-ProConnect's functions properly, such as health monitoring, linkage rule, remote configuration, etc.

Live View

Window Division	1/4/9/16-window division for live view.
Display Time	Up to five minutes once for live view via Hik-Connect service.
Supported Operations	Capturing picture, recording, digital zoom, audio control, PTZ control (preset, zoom in/out, focus, iris, speed control, etc.), wiper, and switching image quality (high definition / standard definition / fluent) are supported during live view.

Linkage

Device Type	Configure linkage rule for the devices (including network camera, NVR/DVR, security control panel, access control device, video intercom device, and doorbell) in a site.
Template	Six pre-defined templates designed for typical applications and used for flexible linkage rule configuration, including Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling, and Perimeter Zone Alarm.
Linkage Mode	● The linkage of the device (if supported) will be triggered via LAN in priority. ● The linkage via Hik-ProConnect Cloud is active in different networks.
Linkage Schedule	Customize linkage schedule for activating the linkage in specified time and dates in each week.
Triggering Event	● For camera: Motion Detection, Face Detection, Intrusion, and Line Crossing Detection. ● For access control device: Tampering Alarm. ● For door linked to access control device: Door Opened Abnormally. ● For door station: Calling. ● For area of security control panel: Away Arming, Disarmed, Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered, and Stay Arming. ● For zone linked to security control panel: Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, and Sensor Tampered. ● For doorbell: Calling. ● For camera linked to doorbell: PIR detection.
Linkage Action	Up to 10 linked devices and 128 linkage actions (including up to 4 linkage actions of capturing and

recording) are supported.
- For camera: Capture, Recording, Call Preset, Call Patrol, Call Pattern, Arm, Disarm, Enable Privacy Mask, and Disable Privacy Mask.
- For alarm output: Alarm Output.
- For door linked to access control device: Open Door, Remain Open, and Remain Closed.
- For area of security control panel: Stay Arm, Away Arm, and Disarm.
- For door station: Open Door.
- For alarm input: Arm Alarm Input and Disarm Alarm Input.

Enable/Disable Linkage Rule	Enable or disable linkage rule to allow the linkage rule to be active or inactive (if abnormal).

Health Status

Locate Device	• According to device types, locate the abnormal device(s) quickly. • Search device by entering keywords.
Status Display	Show device list of each site and status information. Refresh status for the first time login and entering Health Status page.
Automatically Inspect	Inspect the working status of the devices automatically and display the last inspected time.
Manually Inspect	Inspect the status information of the devices manually.
Remote Configuration	Remotely configure device parameters.
Status of Encoding Device	Show status information, including network status, storage status of HDD or SD card, IP channel status of NVR, S.M.A.R.T. information of HDD, overwritten recording status, HDD usage, etc.
Status of Security Control Panel	Show status information, including network status, low battery, mobile network/wireless network/wired network/disconnected, and remaining battery power.
Status of Access Control Device	Show network status.
Status of Video Intercom Device	Show network status.
Status of Doorbell	Show network status and SD Card status.

Exception Rule

Exception Type	• Device Exception: Offline (duration configurable), SD Card Full, SD Card Error, HDD Full, HDD Error, No HDD, Invalid Property

of HDD, Abnormal HDD Temperature, HDD Self-Test Exception, HDD All-Test Exception, Weak Wi-Fi Signal, No Network Connection, Low Battery, Network Exception, and Zone Tampered.
- Channel Exception: Offline (duration configurable), Low Battery, Network Exception, Weak Signal for Connecting, Zone Tampered, and Video Loss.

Received by	Portal, Mobile, and Email.
Recipient	Site Manager (by default), or Installer Admin.
Time	Receive the exception always or in specified time and dates in each week.
Batch Configuration	Enable or set exception rules in a batch.
Copy Rule	Copy rule settings to other devices or channels.

Exception Center

Notification Retention Days	Up to 7 days.
Real-Time Display	Display the exceptions of devices in all sites or assigned site(s) in real time, including time, site name, source, exception type, Site Owner, etc.
Filter Exception	Filter the exceptions by exception type, time period, and source.
Open in New Window	Open a new window of the browser to view the Exception Center.
Export Records	Export exception records in CSV, Excel, or PDF format.

Logs

Log Retention Days	Up to 90 days.
Log Search	Search operation logs by operator and time.
Log Information	Including operator, operating time, client, site, target, result, etc.

Security

Channel Encryption	HTTPS and TLS/SSL are used to ensure the security of the transmission process.
Signal Encryption	AES 128 and RSA are used to ensure the security of data content.
Protection Against Account Attacks	Once the platform discovers account-hacking attacks, it will ban IPs.
Verification Code Encryption	Ensure the security of streaming during remote preview and download.
P2P	Establish secure link without port mapping and avoid exposing ports to the public network.
Unique Serial Number	The unique serial number can only be bound by one account to prevent the device from being added by an

	attacker.
AX Pro Compatible	
Device Settings	● Reset AX Pro. ● Set Wi-Fi parameters and GPRS/3G/4G network parameters. ● Set Entry Delay duration and Exit Delay duration for area. ● Set arming/disarming schedule for area. You can set weekend exception and holiday exception for the schedule. ● Set ARC parameters. ● Link network camera and set stream parameters.
Remote Maintenance	● Reboot device. ● Configure device parameters remotely. ● Upgrade device. ● Switch device language. ● Search logs by event type, time, etc. ● Perform arming and disarming.
User Management	● User management system compliant with EN50131 standards for avoiding second login. ● Card management, including adding card, deleting card, setting card type (e.g., patrol card), and linking area with card.
Health Check	Check the health status of the devices remotely (including network status, battery, signal strength, ARC connection status, peripherals status, RF signal strength, chassis status, and average wireless noise), and export a report showing the results: Pass or Not Pass.
Linkage	● The triggering event types for area: Away Arming, Disarmed, Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered, Stay Arming, Area Follow Zone Alarm, Area Panic Zone Alarm, Area Gas Zone Alarm, Area Medical Zone Alarm, and Area Timeout Zone Alarm. ● The triggering event types for zone: Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered, Bypass Restored, Follow Zone Alarm, Panic Zone Alarm, Gas Zone Alarm, Medical Zone Alarm, and Timeout Zone Alarm. ● Linkage actions: Stay Arming, Away Arming, and Disarm.
Exception Center	The Installers can check the received notifications in Exception Center (including offline, zone tampered, weak Wi-Fi signal, low battery, etc.) and take timely actions.

Hik-ProConnect Mobile Client

General

Supported Language	English, Arabic, Brazilian Portuguese, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovakian, Slovenian, Spanish, Swedish, Thai, Traditional Chinese, Turkish, Ukrainian, Uzbek, and Vietnamese.
Feedback	● Submit feedback information, including Installation and Deployment, Linkage Rule, Maintenance, Company Management, Permission, Exception and Other. ● The words, a picture, and email address can be used for reply.
Deployment	● Global server deployment for accessing Hik-ProConnect more quickly and stably.

System Requirements

iOS	iOS 10 or later versions (since iPhone 6 or iPad Air).
Android	Android 5.0 or later versions. * *The latest version of Hik-ProConnect Mobile Client can be detected and you can select whether to upgrade it when a prompt pops up.*

Account Management

Account	● Register Installer Admin account using email. When registering account, select to subscribe to marketing communications about Hik-ProConnect. You can unsubscribe at any time via Hik-ProConnect Portal. ● Change password for current account.
Company Information	Bind company information, including company logo, business license number, VAT number, etc.

Home Page

Contents	Include the shortcut, banner, site overview, exception overview, and recently visited sites.
Quick Entries	Go to the module directly via quick entries.

Site Management

Number of Sites	Unlimited.
Manage Site	Add new/existing site, edit, and delete site. Different countries and regions are supported when adding new site, including time zone and phone area code.
Invite Site Owner	● Invite end user as Site Owner by email or phone number. The end user will receive the invitation email or message in email box or via short message with a download link of Hik-Connect Mobile Client, and can select whether to accept the invitation via Hik-Connect Mobile Client. ● When inviting Site Owner, apply for permissions of site information management, configuration, and live view, and set validity period (1 to 8 hours, or permanent) for the permissions of configuration and live view.
Apply for Site Authorization	● Site Owner can select whether to grant the authorization. ● Site Owner can select the devices, added in Hik-Connect Mobile Client, but not added and managed in the site, and authorize the permissions of the devices to the Installer. ● The Installer can release the permissions of configuration and live view actively.
Cancel Authorization	The end user can cancel the site authorization.

Device Management

Number of Devices	Unlimited.
Supported Device Type	Network camera, NVR, DVR, access control device, security

	control panel, video intercom device, and doorbell.
Cloud P2P	Support accessing device via Cloud P2P, applicable for different network environments.
Adding Mode	● Add a device by scanning QR code. ● Add a device by Hik-Connect service. ● Add a device by IP address or domain name. ● Connect wired offline device to network by setting AP.
Device Upgrade	● Upgrade device remotely. ● Detect the compatibility of devices' firmware versions with Hik-ProConnect when adding devices.
DDNS	For devices with invalid or old firmware version added by Hik-Connect service, configure DDNS for them to support Hik-ProConnect's functions properly, such as health monitoring, linkage rule, remote configuration, etc.
Remote Configuration	Configure the parameters of network camera / NVR / DVR remotely, including video/audio parameters, event settings, storage settings, image parameters, etc.
Live View	
Window Division	1-window division for live view.
Display Time	Up to five minutes once for live view via Hik-Connect service.
Supported Operations	PTZ control (preset, zoom in/out, focus, iris, speed control, etc.), wiper, and switching image quality ((high definition / standard definition / fluent)) are supported during live view.
Linkage	
Device Type	Configure linkage rule for the devices (including network camera, NVR, DVR, access control device, security control panel, video intercom device, and doorbell) in a site.
Template	Six pre-defined templates designed for typical applications and used for flexible linkage rule configuration, including Intrusion, Forced Entry Alarm, Back to Home/Office, Away,
	Visitor Calling, and Perimeter Zone Alarm.
Linkage Mode	● The linkage of the device (if supported) will be triggered via LAN in priority. ● The linkage via Hik-ProConnect Cloud is active in different networks.
Linkage Schedule	Customize linkage schedule for activating the linkage in specified time and dates in each week.
Triggering Event	● For camera: Motion Detection, Face Detection, Intrusion, and Line Crossing Detection. ● For access control device: Tampering Alarm. ● For door linked to access control device: Opening Door Abnormally. ● For door station: Calling. ● For area of security control panel: Away Arming, Disarmed, Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered, and Stay Arming. ● For zone linked to security control panel: Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, and Sensor Tampered. ● For doorbell: Tampering Alarm. ● For camera linked to doorbell: PIR detection.
Linkage Action	Up to 10 linked devices and 128 linkage actions (including up to

4 linkage actions of capturing and recording) are supported.
- For camera: Capture, Recording, Preset, Patrol, Pattern, Arm, Disarm, Enable Privacy Mask, Disable Privacy Mask.
- For alarm output: Alarm Output.
- For door linked to access control device: Open Door, Remain Open, and Remain Closed.
- For area of security control panel: Stay Arming, Away Arming, and Disarm.
- For door station: Open Door.
- For alarm input: Arm Alarm Input and Disarm Alarm Input.

Enable/Disable Linkage Rule	Enable or disable linkage rule to allow the linkage rule to be active or inactive (if abnormal).

Exception

Exception Type	• Device Exception: Offline (duration configurable), SD Card Full, SD Card Error, HDD Full, HDD Error, No HDD, Invalid Property of HDD, Abnormal HDD Temperature, HDD Self-Test Exception, HDD All-Test Exception, Weak Wi-Fi Signal, No Network Connection, Low Battery, Network Exception, and Zone Tampered. • Channel Exception: Offline (duration configurable), Low Battery, Network Exception, Weak Signal for Connecting, Zone Tampered, and Video Loss.
Received by	Portal, Mobile, and Email.
Recipient	Site Manager (by default), or Installer Admin.
Time	Receive the exception notifications always or in specified time and dates in each week
Batch Configuration	Enable or set exception rules in a batch.
Copy Rule	Copy rule settings to other devices or channels.

Exception Center

Notification Retention	Up to 7 days.

Days	
Real-Time Display	Display the exceptions of the devices in all sites or assigned site(s) in real time, including time, site name, source, exception type, Site Owner, etc.
Filter Exception	Filter the exceptions by exception type, time period, and source.
Open in New Window	Open a new window of the browser to view the Exception Center.

Security

Channel Encryption	HTTPS and TLS/SSL are used to ensure the security of the transmission process.
Signal Encryption	AES 128 and RSA are used to ensure the security of data content.
Protection Against Account Attacks	Once the platform discovers account-hacking attacks, it will ban IPs.
Verification Code Encryption	Ensure the security of streaming during remote preview and download.
P2P	Establish secure link without port mapping and avoid exposing ports to the public network.
Unique Serial Number	The unique serial number can only be bound by one account to prevent the device from being added by an attacker.

AX Pro Compatible

Device Settings	• Reset AX Pro. • Set Wi-Fi parameters and GPRS/3G/4G network parameters. • Set Entry Delay duration and Exit Delay duration for area. • Set arming/disarming schedule for area. You can set weekend and holiday exception for the schedule. • Set ARC parameters. • Link network camera and set stream type. • Scan QR code to add wireless detectors and peripherals, and set related parameters, including door magnetic detector, door magnetic and shock detector, infrared detector, dual-technology detector, water

		leak detector, panic button, PIRCAM detector, smoke detector, siren, relay output, wireless keypad, wireless repeater, wireless card reader, etc.
Remote Maintenance	● Reboot device. ● Configure device parameters remotely. ● Upgrade device. ● Switch device language. ● Perform arming and disarming.	
User Management	● User management system compliant with EN50131 standards for avoiding second login. ● Card management, including adding card, deleting card, setting card type (e.g., patrol card), and linking area with card.	
Linkage	● The triggering event types for area: Away Arming, Disarmed, Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered,	

Stay Arming, Area Follow Zone Alarm, Area Panic Zone Alarm, Area Gas Zone Alarm, Area Medical Zone Alarm, and Area Timeout Zone Alarm.
● The triggering event types for zone: Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, Delayed Zone Alarm, Internal Delayed Zone Alarm, Fire Alarm Zone Alarm, Perimeter Zone Alarm, 24-Hour Silent Alarm Zone Alarm, 24-Hour Auxiliary Zone Alarm, 24-Hour Shock Alarm Zone Alarm, Sensor Tampered, Bypass Restored, Follow Zone Alarm, Panic Zone Alarm, Gas Zone Alarm, Medical Zone Alarm, and Timeout Zone Alarm.
● Linkage actions: Stay Arming, Away Arming, and Disarm.

Exception Center	The Installers can check the received notifications in Exception Center (including offline, zone tampered, weak Wi-Fi signal, low battery, etc.) and take timely actions.

HIKVISION®

Distributed by

HIKVISION®

Hikvision Europe
Dirk, Storklaan 3, 2132 PX Hoofddorp,
The Netherlands
T +31-23-5542770
sales.eu@hikvision.com

Headquarters T +86-571-8807-5998 overseasbusiness@hikvision.com	**Hikvision USA** T +1-909-895-0400 sales.usa@hikvision.com	**Hikvision UK & Ireland** T +01628-902140 sales.uk@hikvision.com	**Hikvision UAE** T +971-4-4432090 salesme@hikvision.com	**Hikvision Russia** T +7-495-669-67-99 saleru@hikvision.com
Hikvision Australia T +61-2-8599-4233 salesau@hikvision.com	**Hikvision Italy** T +39-0438-6902 info.it@hikvision.com	**Hikvision South Africa** Tel: +27 (10) 0351172 sale.africa@hikvision.com	**Hikvision Singapore** T +65-6684-4718 sg@hikvision.com	**Hikvision Korea** T +82-(0)31-731-8817 sales.korea@hikvision.com
Hikvision India T +91-22-28469900 sales@pramahikvision.com	**Hikvision Brazil** T +55 11 3318-0050 Latam.support@hikvision.com	**Hikvision France** T +33(0)1-85-330-450 info.fr@hikvision.com	**Hikvision Spain** T +34-91-737-16-55 info.es@hikvision.com	**Hikvision Poland** T +48-22-460-01-50 info.pl@hikvision.com
Hikvision Canada T +1-866-200-6690 sales.canada@hikvision.com	**Hikvision Turkey** T +90 (216)521 7070- 7074 sales.tr@hikvision.com	**Hikvision Kazakhstan** T +7-727-9730667 nikia.panfilov@hikvision.ru	**Hikvision Tashkent** T +99-87-1238-9438 uzb@hikvision.ru	**Hikvision Indonesia** T +62-21-2933759 Sales.Indonesia@hikvision.com
Hikvision Thailand T +662-275-9949 sales.thailand@hikvision.com	**Hikvision Malaysia** T +601-7652-2413 sales.my@hikvision.com	**Hikvision Vietnam** T +84-974270888 sales.vt@hikvision.com	**Hikvision Hong Kong** T +852-2151-1761 info.hk@hikvision.com	**Hikvision Colombia** sales.colombia@hikvision.com