Genetec Security Center.

What's New in Security Center 5.7

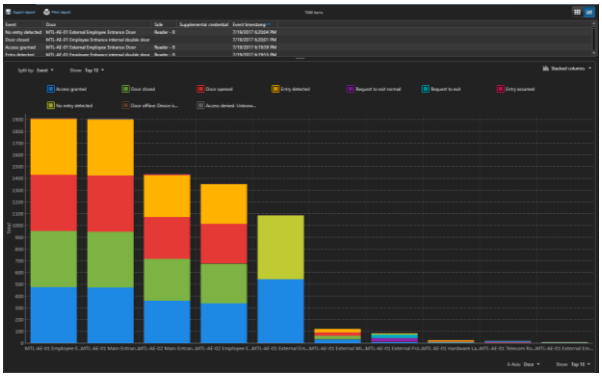
Security Center 5.7 introduces several new capabilities related to the core platform, video surveillance (VMS), access control (ACS) and automatic license plate recognition (ALPR).

Security Center platform features

USER EXPERIENCE

Visual reporting

Perform searches and run investigations that rely on visual and user-friendly reports. Security Center reporting tasks are now powered by dynamic charts and graphs that deliver insights you act on. This opens the door for deeper data analysis and identification of activity patterns that enhance your understanding.



Access control visual report in Security Desk

Layout entity

Design new layouts, save them and quickly access them at any moment to change the monitoring layout of any task. Layouts now appear as entities in the logical tree, alongside areas, cameras, and doors, so they are easily accessible. You can also position your newly created layout entities on a map that you then drag-and-drop onto a second monitor to quickly customize the view to your needs.

Email notification enhancements

Emails triggered by the event-to-action mechanism can now be customized to contain more relevant and timely information. You can configure the email notification's subject and body using fields (for example, entity name and status) pulled directly from event-specific information or its source. To further enhance readability, you can also customize the style and font of the email message.

MAPS

Camera coverage tool

This new tool makes sure you have eyes everywhere to maximize your security and video coverage. It shows the potential field of view of all your cameras within a map and takes into account the physical environment (for example, the height of walls and obstructions you have defined). This lets you quickly identify blind spots in any given location and make changes to expand coverage.

Usability and visualization

Enhanced usability streamlines the everyday use of maps:

- You can now zoom in on a section of the map by pressing Ctrl button and drawing a rectangle around that section
- Easily accessible command buttons overlaid on the map for zooming in an out, selecting a map preset, and using Smart click
- Save your favorite map locations as presets, and quickly navigate to them with a click
- Customize the color of inputs, zones, and intrusion detection areas according to their states
- Unclutter your map by showing inputs, zones, and intrusion detection areas only when they are in certain states
- Take the height of buildings and walls into consideration when showing cameras' field of views. When using the Smart click function, only the cameras that have visibility of the selected position are displayed

Easier configuration of maps

Boost your efficiency and decrease map setup time by copying map settings to multiple locations. Doing this eliminates the need to reconfigure all associated entities. A practical example is when you need to create several versions of the same map to account for different background languages. Rather than configuring the same map multiple times from scratch, you can now copy the map in a single step including all embedded entities, then simply change the background.

Note: 5.7 is the last version that will support the Plan Manager 10.3 plugin (legacy version). From 5.8, we will only support the native Plan Manager.

MOBILE AND WEB APPS

Alarm management (Web Client)

The Security Center web client now allows you to manage and monitor real-time alarms, easily acknowledge them, and trigger them.

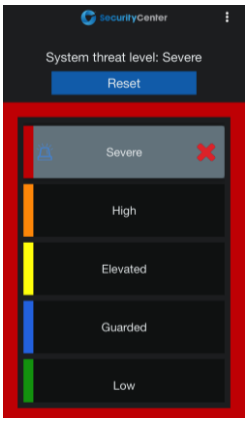
Threat level management (Web Client)

The Security Center web client now supports threat level management, allowing you to view system status and trigger threat levels from wherever you are.

New threat level mobile app

With the new Security Center Threat Level app, you can remotely trigger threat levels and instantly change the state your Security Center system no matter your location. Download the Security Center Threat Level app here.

Note: the application is currently only available on iOS devices. It is included with the Threat Levels module.



Threat Level mobile app

CYBERSECURITY

Enhanced Privileges

You can now grant configuration operations (for example, event-to-actions, user management, and role configuration) to non-admin users. It allows for greater control and flexibility of the Security Center configuration and improves security, since users only have access to what they need.

Plan Manager security

Connections to the Map Manager role are now authenticated using claim-based authentication, preventing unauthorized access to map data. Additionally, federated maps are now available to the users at the Federation level. This reduces the surface of attack of a Security Center installation by preventing access to the federated sites.

Firmware recommendation

It is now easier to manage the firmware running on your cameras. The system reviews your firmware via the Genetec Update Service (GUS) and recommends upgrades, or notifies you of vulnerabilities.

Omnicast Video Management

PRIVACY PROTECTION

A new, embedded KiwiVision Privacy Protector module (will be available with Security Center 5.7 SR1)

The KiwiVision Privacy Protector® module allows you to maintain the privacy of individuals within view of surveillance cameras. It automatically anonymizes individuals in live and recorded video by first detecting them, followed by blurring or masking them as they move throughout a scene. It can be used indoors and outdoors, in confined and public areas.

KiwiVision Privacy Protector is now a native role in Security Center and is fully unified at the server and client application level. The module is configured using the Config Tool and settings are applied to video from cameras that need privacy protection. Authorized operators can easily unlock the original video within the video monitoring tile. Unauthorized operators only see the privatized stream. The Privacy Protector can be configured together with encryption for situations where access to the original stream requires authenticated access using a smart card and a PIN code.

Note: the KiwiVision Privacy Protector does not require an SDK license nor extra camera connections for the pixelated stream. Only the new part number needs to be quoted. You now perform licensing, configuration and stream selection operations for KiwiVision Privacy Protector directly in Security Center.

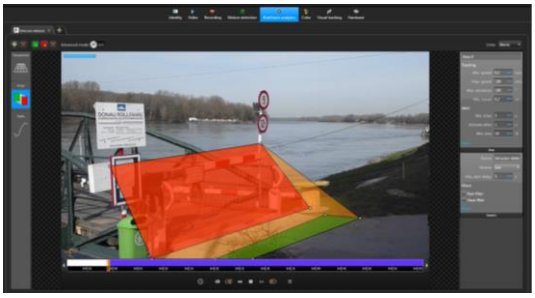
INTELLIGENCE

KiwiVision Intrusion Detector plugin

Automatically detect people or vehicles in designated or important areas. The KiwiVision Intrusion Detector plugin automates security by generating real-time alarms when individuals or vehicles enter sensitive areas, secured perimeters, or restricted zones.

KiwiVision Intrusion Detector is now unified with Security Center. This simplifies the setup because it can be performed entirely within the Config Tool. Operators receive automated intrusion detection alarms and events in Security Desk event monitoring and alarm management tasks. A new KiwiVision intrusion detector report allows you to search intrusion events in a list view, which includes video thumbnails.

Note: the Intrusion Detector plugin is included in the Security Center 5.7 installer; you only need to activate it.



KiwiVision configuration in the Config Tool

Quick search forensics tool

Target your video search to get quicker results with the Quick search tool. Accessed from the Security Desk Monitoring task, the tool lets you define an area of interest within a video segment. It automatically identifies relevant changes in the area and presents a visual timeline that lets you further refine your search. This allows you to find the video you are looking for in a couple of clicks.

Quick search visual timeline

ALWAYS RECORDING

To enhance your awareness of video recording status and potential issues, new notifications have been added. Users are informed immediately when there is a discrepancy between the expected recording state vs. the actual recording state. For example:

- If a camera stops recording for normal reasons (e.g. no more motion detected), Security Desk simply notifies you that the recording has stopped.
- If a camera stops recording for abnormal reasons (e.g. due to database issues), Security Desk notifies you of a recording problem.

Given that recording problems can be triggered by various conditions (database, camera, or environmental issues), the notification includes additional detail to better guide your subsequent corrective actions.

BODY-WORN CAMERAS

Offloading video from body-worn cameras (will be available with Security Center 5.7 SR1)

Review video captured with body-worn cameras, and centrally store and manage all archives in Security Center. Recordings from these devices can now be automatically imported into Security Center, when docked at the end of a shift. Body-worn cameras can be assigned to officers within Security Center, in order to search for recordings based on the individual a camera is assigned to.

Note: the integration is currently available with Point Blank IRIS cameras and equipment.

MAINTENANCE & CONFIGURATION

Camera maintenance

Event-to-actions are now suspended if a camera is in maintenance mode. A camera in maintenance mode will display an orange color. For example, a transmission lost event will trigger an alarm. It makes no sense to trigger the alarm if the transmission lost event is coming from a camera that is in maintenance mode.

Visual tracking configuration

You can now copy your Visual Tracking settings from one camera to another, speeding up the configuration of devices that require similar settings.

Security Center Synergis Access Control

HID MOBILE ACCESS PORTAL INTEGRATION

With the new HID Mobile Access portal integration, you can now assign mobile credentials to cardholders through the Cardholder management and Credential management tasks in Security Center. Customers can efficiently move to mobile credentials without having to enroll credentials in both HID Mobile Access Portal and in Security Center Synergis™.

ACCESS MANAGER FAILOVER FOR BUSINESS CONTINUITY

Take advantage of continuous monitoring of access control (ACS) devices and events, even during server failures. Failover capabilities are now available for the Synergis Access Manager role. It ensures that the Access Manager role is up and running at all times and critical information is always available. Your system automatically detects failure with the primary Access Manager server and quickly redirects connectivity to a designated standby Access Manager server for disaster recovery*.

We now offer comprehensive, unified failover for both ACS and video, which is more cost-effective when compared to third-party failover options like NEC and MS Windows Clustering.

* The Access Manager should be pointing to a database capable of failover.

ENHANCED SCALABILITY

Access Manager scalability enhancements with HID devices
Manage more HID devices per Access Manager:

- Up to 100 HID VertX V1000 controllers per Access Manager (up from 80 controllers)
- Up to 2,000 readers managed by HID VertX V1000 controllers (up from 1,400 readers)
- Up to 700 readers managed by HID EDGE EVO and HID V2000 controllers per Access Manager (up from 350 readers)

Global Cardholder Management scalability
Synergis now supports up to 250,000 cardholders with Global cardholder management.

REPORTING ENHANCEMENTS

Visual reports
You can now view access control events and alarms with graphs and charts. This brings more clarity on the flow of cardholders and the frequency of events and alarms. For example, you can easily identify and compare which doors and areas are being accessed more often during peak business hours.

Wireless lock battery reports
You can now run reports on the battery status of all wireless ASSA ABLOY locks managed by Synergis. This allows you to quickly determine which locks are running low on power and take corrective measures before failure occurs.

Remove specific cardholders from an area (will be available with Security Center 5.7 SR1)
If a cardholder leaves an area without presenting their badge to exit, you can now manually remove that cardholder from that area to correct the presence report.

INTEGRATION ENHANCEMENTS – Requires Softwire 10.5

New Mercury Security EP panel capabilities*
New capabilities have been enabled for Mercury EP panels including OSDP 2.0 (secure channel), duress PIN, elevator management, and visitor escort. All of these features are now supported on standalone Mercury EP panels and work even when disconnected from Synergis Cloud Link.

New ASSA ABLOY IP lock capabilities*
New capabilities have been enabled on ASSA ABLOY IP locks including privacy mode, and escape and return mode.

*Please see the Softwire 10.5 General Availability announcement for more details.

AutoVu Automatic License Plate Recognition (ALPR)

USER EXPERIENCE

Visual reporting
It is now easier to understand the vehicle traffic in your environment by running rich visual reports that leverage graphs and charts. You can see all the reads and hits of your ALPR system on a single dynamic graph. You can now narrow down your research and see the activity of certain vehicles, or parking lot activity over a specific period of time.

Audit tracking
This new functionality allows you to add a mandatory field for report generation. When operators run ALPR reports, they will need to type in the reason as to why the report was run. This new field is tracked along with everything else we currently track in the activity trail.

Need more details? Please contact your local Genetec Channel Partner, or Sales@Genetec.com