

Security Center 5.11 Ordering Guide

NOVEMBER 1, 2022

INTRODUCTION	5
OVERVIEW	5
PRODUCT CODES	6
PACKAGE SELECTION.....	7
<i>Security Center Base Package</i>	7
<i>Package selection</i>	7
SECURITY CENTER.....	9
BASE PACKAGE.....	9
BASE PACKAGE FEATURES	10
<i>Plan Manager</i>	10
<i>Plan Manager Standard</i>	10
<i>Plan Manager Advanced (Professional and Enterprise packages only)</i>	10
<i>Sipelia™</i>	10
<i>Alarm management</i>	11
<i>Advanced Reporting</i>	11
<i>System Partitioning</i>	11
<i>Zone Monitoring</i>	11
<i>Inputs and Outputs</i>	11
<i>Custom Fields</i>	11
<i>Email support</i>	11
<i>Incident Reports</i>	11
<i>Visitor Management Module</i>	12
<i>Import Tool</i>	12
<i>Max Occupancy</i>	12
<i>Mustering task</i>	12
<i>Archiving support</i>	12
<i>Media Router</i>	12
<i>Audio support</i>	12
<i>Camera sequence</i>	13
<i>Media Encryption</i>	13
<i>Camera Dewarping</i>	13
<i>Edge recording and archive transfer support</i>	13
<i>Keyboard and Joystick support</i>	13
<i>Time zone support</i>	13
<i>Access Manager</i>	13
<i>Intrusion Manager Role</i>	14
<i>Macros</i>	14
<i>Support for virtualization</i>	14
<i>KiwiVision Video Analytics</i>	14
<i>Camera Blocking (Professional and Enterprise package only)</i>	15
<i>Remote Security Desk (Professional and Enterprise package only)</i>	15
<i>Threat Levels (Professional and Enterprise package only)</i>	15
<i>Record Fusion Service (Professional and Enterprise package only)</i>	15
<i>Windows Active Directory (Professional and Enterprise package only)</i>	16
<i>Authentication (Professional and Enterprise package only)</i>	16
<i>Languages</i>	16
SECURITY CENTER STANDARD	17
OMNICAST™ STANDARD.....	17
SYNERGIS™ STANDARD	17
FEDERATION™ OPTION.....	18
UPGRADE TO PRO OR ENTERPRISE	18
SECURITY CENTER PROFESSIONAL	19

OMNICAST™ PROFESSIONAL	19
SYNERGIS™ PROFESSIONAL	20
FEDERATION™ OPTION.....	20
UPGRADE TO ENTERPRISE.....	20
SECURITY CENTER ENTERPRISE.....	21
OMNICAST™ ENTERPRISE	21
<i>Failover camera connection</i>	22
<i>Auxiliary Archiver</i>	22
<i>Hardware Matrix</i>	22
SYNERGIS™ ENTERPRISE	23
FAILOVER DIRECTORY	23
CONNECTION LICENSES	25
SECURITY DESK CLIENT, WEBAPP AND GENETEC MOBILE CONNECTION	25
CAMERA CONNECTION	25
<i>Video Import Profile</i>	25
<i>Camera connection for Bosch VRM</i>	25
ANALOG CAMERA CONNECTION	26
BODY WEARABLE CAMERA CONNECTION	26
DVR INPUT	26
READER CONNECTION	27
SHARPV CONNECTION	27
WIRELESS READER CONNECTION	27
JETWAY FUNCTIONNALITY	27
GLOBAL CARDHOLDER MANAGEMENT CONNECTION	27
EVACUATION ASSISTANT.....	27
SMARTCARD ENCODING MODULE	27
SOFTWARE FOR 2 TIER ARCHITECTURE	27
INTERCOM CONNECTION LICENSES.....	28
SDK CONNECTION.....	28
OPTIONAL FEATURES.....	29
OMNICAST CLOUD STORAGE	29
FEDERATION™	29
STRATOCAST™ FEDERATION™	29
GLOBAL CARDHOLDER MANAGEMENT	30
NEC AND WINDOWS CLUSTERING SUPPORT	30
PLUGINS	30
<i>Intrusion Panels</i>	30
<i>Access Control System</i>	32
<i>Access Control Ecosystem</i>	35
<i>Elevator Destination Dispatch</i>	37
<i>Asset and Key Management System</i>	38
<i>Videowalls</i>	40
<i>Shot Detection Systems</i>	40
<i>Industrial Internet of Things (IIoT)</i>	41
<i>Transaction Monitoring</i>	43
<i>Hexagon EDGEFrontier CAD</i>	44
<i>SPS Checkpoint</i>	44
<i>AdroneX</i>	44
<i>Hybrid Frameworks</i>	44
GENETEC MISSION CONTROL™	46
CONNECTION LICENSES	46
<i>Genetec Mission Control™ Operator License</i>	46
<i>Enterprise Operator Site License</i>	46

FEATURES ACTIVATED WITH THE OPERATOR LICENSE	46
<i>Genetec Mission Control™ Incident Manager role</i>	47
<i>Rules Engine</i>	47
<i>Manual trigger of Incidents</i>	47
<i>Automation Engine</i>	47
<i>Interactive Standard Operating Procedures</i>	47
<i>Dynamic Standard Operating Procedure (DSOP)</i>	47
<i>Document Management</i>	47
<i>Incident Queue Mirroring</i>	48
<i>Failover capability</i>	48
<i>Geolocation on Map</i>	48
<i>Reminders</i>	48
<i>TTR measurement and enforcement</i>	48
<i>Collaborative Incidents</i>	48
<i>Supervision</i>	48
<i>Alarm management</i>	48
<i>Profile</i>	48
<i>Email support</i>	49
<i>Incident Reports</i>	49
<i>Macros</i>	49
<i>Support for virtualization</i>	49
<i>Languages</i>	49
GENETEC MISSION CONTROL™ ADVANTAGE	49
<i>Advantage Operator</i>	49
<i>Advantage Site Operator</i>	49
GENETEC MISSION CONTROL™ PROFESSIONAL SERVICES	50
<i>PS-DS-BUNDLE</i>	50
GENETEC LIFECYCLE MANAGEMENT (GLM)	51
APPENDIX A – SERVER TYPE	51
APPENDIX B – WORKSTATION TYPE	51
APPENDIX D – PRICING	51

Introduction

Overview

The following ordering guide contains information about Security Center version 5.x; please refer to the cover page to ensure you have the latest ordering guide at hand.

The Security Center ordering guide explains the different part numbers of the price list and the interdependence between the part numbers. It also includes basic design guidelines and scalability figures.

For Autovu™ ordering information, please refer to the Autovu™ ordering guide.

For Security Center SaaS including Cloud storage, Federation as a Service and other cloud services, please refer to the Security Center SaaS Ordering Guide.

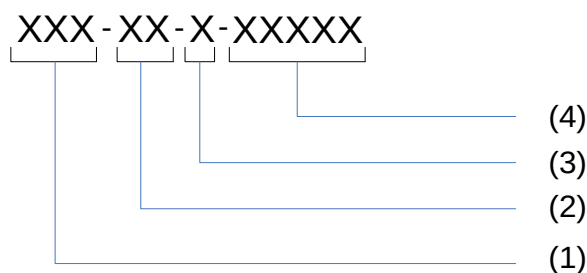
This ordering guide explains the different packages together with the different features (basic and optional) of each package.

Security Center – 5.11 will be available under three different Packages:

- Security Center™ Standard
- Security Center™ Professional
- Security Center™ Enterprise

Product codes

Product codes include 4 blocks, defined as follows:



(1) Platform identification - Alphabetical

GSC: Genetec Security Center

(2) Product identification - Alphabetical

Blank: Common or core functionality available to all sub-systems

Om: Omnicast™

Sy: Synergis™

(3) Package:

Blank: Functionality available in multiple packages

S: Standard

P: Professional

E: Enterprise

(4) Part identification:

Alphanumeric: when part number starts with a number, item can be ordered in quantities; otherwise it is a system wide option.

Version:

The version of the product must be specified on each order, by adding the no charge part number GSC-5.11.

GSC-Base-5.x is not required starting with Security Center 5.11.

Package selection

Security Center Base Package

The Security Center Base Package must be ordered every time a system is ordered, whether it is Omnicast™ video surveillance, Synergis™ access control or Autovu™ license plate recognition. The Security Center Base Package is used to specify the product version being purchased.

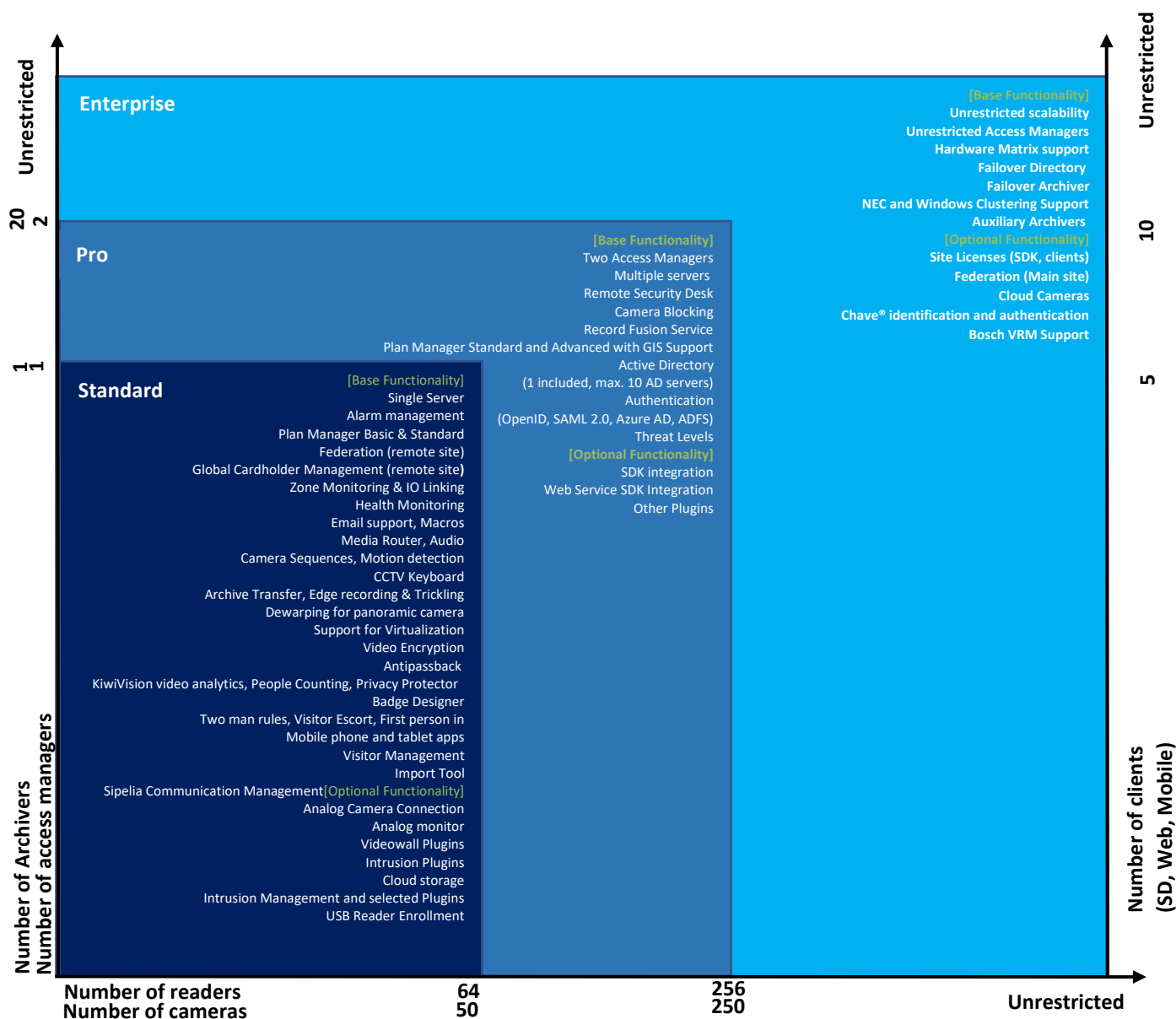
Package selection

The base package must be selected based on the:

- Overall camera/analog monitor count
- Number of Archivers
- Number of client connections
- Failover
- Federation™
- Third-party integration (SDK)
- Overall reader count
- Number of Access Managers
- Number of cardholders

Package and Feature Breakdown

Security Center (Unified Package)



Security Center

Base Package

Product Code [GSC-5.11]

The Security Center Base package must be ordered every time a system is ordered whether it is an Omnicast™, Synergis™ or Autovu™ system that is being installed. The Security Center Base package is used to specify the product version being purchased.

The Security Center Base package, which includes functionality common to all systems, is defined as follows:

One Genetec Security Center (GSC) Base Package includes:

- One (1) GSC Directory
- Five (5) Security Desk client connections and five (5) Web client or Mobile App connections
- Plan Manager Basic (Standard Package)
- Plan Manager Advanced (Pro and Enterprise Package)
- Alarm Management
- Advanced Reporting
- System Partitioning
- Zone Monitoring
- IO Modules Support
- Import Tool
- Intrusion Manager Role
- Sipelia base package, Sipelia Public Announcement, & Sipelia Trunking
- Synergis Import Tool, Synergis Max Occupancy, Synergis Mustering, Synergis Visitor Management Module
- KiwiVision Video Analytics: Camera Integrity Monitor, People Counter, Privacy Protector, Security Video Analytics
- Custom Fields
- Email Support
- Incident Reports
- Macros Support (actual macros sold separately)
- Support for server virtualization
- All supported languages

A Security Center Standard, Professional, or Enterprise base package is required in addition to the Security Center Base package to enable access control, video surveillance, or license plate recognition.

Base Package Features

Below is the description of the Security Center Base Package.

Plan Manager

Plan Manager adds image-based mapping capabilities to the Security Center system. We support JPG, PNG and BMP image formats as map backgrounds and the display of cameras, doors, LPR units, intrusion areas, industrial IoT devices and custom entities.

Plan Manager Standard

Plan Manager Standard allows map design with dynamic content, multi-level map support, zooming capabilities for cameras.

Plan Manager Standard supports the following functionality:

- PDF based vector image maps
- AutoCAD image maps (and object positioning)
- Map configuration import (from CSV, XLSX, JSON, KML/KMZ)
- PTZ control and orientation feedback
- Additional contextual actions when right-clicking on entities
- Alarm management

Plan Manager Advanced (Professional and Enterprise packages only)

Plan Manager Advanced provides advanced mapping capabilities to the Security Center system through the integration of external geographical information systems (GIS) and overlaid data layers (KML layers).

Plan Manager Advanced supports the following functionality:

- GIS maps
 - ESRI ArcGIS as map backgrounds & data layers
 - Google Maps as map backgrounds
 - Bing Maps for map background
 - WMS / WMTS Maps for map background
- Geocoded searches (ESRI, Google, Bing)
- KML objects data layer

GIS support for Plan Manager is available in the Pro and Enterprise packages.

Sipelia™

Sipelia™ delivers Communication Management features into Security Center for voice and video communications with and between SIP devices. It enables voice and video communication between Security Desk users.

The Security Center base package provides the ability to set voice and video communication between Security Desk users. To communicate with other SIP devices it is required to add connection Licenses [GSC-Sipelia-1SIP].

Trunk functionality

Trunk is a technology part of SIP standard that allows to interconnect 2 SIP servers (IPBX). It is most often required to connect Sipelia™ to an Intercom Exchange Server. Intercom Exchange Servers are used to connect analog and non-SIP Intercoms.

Intercoms behind a trunk configured in Sipelia™ requires a connection license [GSC-Sipelia-1SIP]

Important: *This item requires ordering a minimum one year of Genetec Advantage.*

Public address

The public address functionality allows to broadcast a live or a pre-recorded message to any SIP entity managed by Sipelia.

Alarm management

This feature enables the usage of the alarm management functionality which includes the ability to trigger alarms manually or automatically based on system events, to send alarms to specific recipients, to acknowledge alarms, to forward alarms, to snooze alarms and to assign a procedure to an alarm.

The alarm management runs on the Directory Role.

Advanced Reporting

Allows users to create reports and report templates.

Automatically sending a report by email required the Report Manager Role (*installed by default*).

System Partitioning

Allows administrators to segment the Security Center solution into logical partitions and control user access to specific entities. User access to a partition includes operation and administration access rights.

Zone Monitoring

Allows administrators to create zones and associate inputs from access control devices and/or video cameras or encoders for monitoring. IO linking is also possible through the use of zones.

Zone Monitoring runs on the Zone Manager Role (*installed by default*).

Inputs and Outputs

This feature enables the use of I/O modules such as HID VertX V200, VertX V300, Axis P8221 and HWg-Juno 101/404.

Custom Fields

Supports the ability to assign custom fields to various entities in the Security Center, including cardholders, credentials, zones, and more.

Email support

Supports the ability to send an email to a user or user group or cardholder. An email can contain a report (PDF or Excel format) or can be triggered following any event in the system.

Incident Reports

Supports the ability to create an incident in the Security Desk. Administrators can also make it mandatory that an operator enter an incident upon acknowledgement of an alarm.

Incident Reports runs on the Directory Role.

Visitor Management Module

The Visitor Management Module is a specific task of the Security Desk task allows you to check in, check out, and modify visitors, as well as manage their credentials, including temporary replacement cards.

Import Tool

The import tool allows to import cardholders, cardholder groups, and credentials from a CSV file.

Max Occupancy

This feature set a limit of cardholders that can be in an area simultaneously. There are two modes of operation, one will only raise an event when the maximum is reached while the second will raise the event and deny the access.

Mustering task

This feature allows the use of Security Desk instance to be used as mustering station using a USB reader. This can't be used with the Evacuation Assistant. One license is required per workstation.

Archiving support

Archiver support is the capacity for the system to record cameras and index video files in a database. Additional Archivers can be added to a system as the number of cameras increases and also for distributed systems. The number of Archivers in the system is not licensed.

Performance

The number of cameras that can be handled by a single archiver will vary depending on the performance of the hardware where the Omnicast™ application is running. A high end server can handle a maximum of 300 cameras or 500 Mbps of throughput; whichever comes first.

The performance on Genetec Streamvault appliances goes up to 1,000 cameras with 2.0Gbps throughput. Please refer to the system requirements and Streamvault catalog for additional configurations.

Media Router

The Media Router along with the redirection agents are responsible for all the video streaming and routing in the system. There is usually only one (1) Media Router Role per system. An additional Media Router Role can be deployed for redundancy purposes. Not additional license is required for additional Media Router Roles.

Multiple redirection agents can be deployed in order to optimize the video streaming. Each Archiver Role include a redirection agent which is used to for multicast by Archiver scenario for example.

The Media Router Role support load balancing. Adding multiple redirection agents on the same network will provide round-robin load balancing across all redirection agents.

Performance

On a high end server, one (1) redirection agent can handle a maximum video redirection throughput of 480 Mbps (ex. 240 Mbps IN / 240 Mbps OUT).

Audio support

This feature enables system wide 2-way audio for both listening and recording. Audio is supported using the microphone and speaker ports (or built-in) of video units (IP cameras, encoders, decoders, etc.). The feature is hardware dependant. The video units must have audio capability and it must be supported by Omnicast™ for this specific model/manufacturer.

Camera sequence

Camera sequence allows users to configure a list of cameras to be displayed in cycle in a single tile within the Security Desk.

Camera sequences are cycled by the Security Desk. No additional role is required to host/cycle camera sequences.

Media Encryption

The Archiver is able to encrypt the media at rest and when transmitting it. Media includes video, audio and metadata. This is a system wide feature and is included in all package.

Starting from 5.5 SR1, encryption from the camera is supported (with selected camera manufacturers and models only, see SDL).

Performance

The performance of the Archiver will be affected when encryption is turned on especially if more than one (1) certificate is used for encryption. See system requirements for more details.

Camera Dewarping

This features provides the ability to dewarp panaromic camera stream in the Security Desk.

Edge recording and archive transfer support

Edge recording support provides the ability to retrieve recorded video from the edge devices using the Security Desk. This feature can be used to protect recorded video during a network outage. Archive transfert support adds the ability to automate the transfer of the edge recorded video to the Omnicast™ Archiver. Consult the SDL for the list of all video units supporting this fonctionality.

Keyboard and Joystick support

Keyboard and Joystick support allows operator to control the local or a remote Security Desk using a CCTV Keyboard or a USB Joystick connected to the local workstation PC.

Time zone support

This feature allows the Omnicast™ system to run in a multi time zone environment where the cameras, the clients and/or the servers are located in multiple different time zones.

Access Manager

Additional Access Manager are necessary when the system expands beyond the number of readers supported by one Access Manager or if the system is geographically distributed.

Performance

The number of readers that can be handled by a single Access Manager will vary depending on the performance of the hardware where the Synergis™ application is running. One high-end server running the access manager can support up to 2,048 readers when deployed with Synergis™ Cloud Link appliances. This scalability number will vary depending on the hardware connected to the Synergis™ Cloud Link appliance.

Intrusion Manager Role

The Intrusion Manager is necessary to allow specific intrusion alarm panels to be enrolled into the system and benefit from the native intrusion functions and reporting available within Security Center.

Macros

This feature enables the usage of macros in the system.

The macros runs on the Directory Role.

Support for virtualization

Virtualization support is intended for Omnicast™ or Synergis™ systems running in a virtual environment. The support for virtual environment is for Security Center servers only. The virtual environment supported by Omnicast™ and Synergis™ are VMware and HyperV. Please refer to the Server and OS Requirements document for supported versions as well as the system design guidelines available on TechDoc Hub.

Note that running in a virtual environment may have performance implications which can invalidate certain design guidelines recommended by Genetec.

KiwiVision™ Video analytics

Each base package includes up to a count of 300 channels for each KiwiVision™ Video analytics module (Privacy Protector, Security Video Analytics, or People Counter). If more than 300 channels are required to run analytics, additional ones can be purchased through their respective part numbers.

NOTE: The KiwiVision™ Camera Integrity Monitor module is part of the base license and can be included on an unlimited amount of cameras.

For example, with a base license, you can have 300 channels running the Security Video Analytics module, 135 channels running the Privacy Protector™ module, 50 channels running the People Counter module, and 460 channels running the Camera Integrity Monitor module.

Privacy Protector

Privacy Protector™ avoids unnecessary intrusion into personal privacy without compromising security. The feature automatically hides all persons in surveillance videos in real-time, and in the meantime, actions remain recognizable. Access to unpixelated video streams can be controlled based on privilege.

Enables the KiwiVision™ Privacy Protector™ module for one camera connection.

Important: One year of Genetec Advantage is highly recommended if it's enabled on a system. If more than 300 channels are running analytics, each extra channel for Privacy Protector requires the GSC-OM-1PP300+ part number.

Security Video Analytics

Security Video Analytics offers various scenarios to automatically detect defined events of interest. Scenarios include Perimeter protection, Area protection, Direction control, Object detection, Stopped vehicle detection, Tailgating detection, Positional tracking.

As soon as the defined conditions are met, an event is generated in Security Desk.

Enables the KiwiVision™ Security video analytics module, and provides access to configure one camera connection the following scenarios: Perimeter protection, Area protection, Direction control, Object detection, Stopped vehicle detection, Tailgating detection, Positional tracking.

Important: One year of Genetec Advantage is highly recommended if it's enabled on a system. If more than 300 channels are running analytics, each extra channel for Security Video Analytics requires the GSC-OM-1VAS300+ or GSC-OM-1VASU300+ part number.

GSC-OM-1VAS300+ > provides access to configure one camera connection for one of the available scenarios

GSC-OM-1VASU300+ > provides access to configure one camera connection for any number of the available scenarios

Camera Integrity Monitor

Camera Integrity Monitor automatically checks each licensed camera in regular intervals to detect tampering (e.g. covering), out of focus, and if has been turned. If such a case is detected, an event is raised. It is mainly designed to be used as a maintenance feature

People Counter

The People Counter module adds people counting and crowd estimation video analytics capabilities to Security Center, using the People counting scenario.

Enables the KiwiVision™ People Counter module and provides access to configure people counting and crowd estimation scenarios for one camera connection.

Important: One year of Genetec Advantage is highly recommended if it's enabled on a system. If more than 300 channels are running analytics, each extra channel for People Counter requires the GSC-OM-1PC300+ part number.

Camera Blocking (Professional and Enterprise package only)

This feature allows operators to block the transmission of the live/playback video streams or a segment of recorded video streams on demand and for only of specific cameras. The blocking is based on the user security level.

Remote Security Desk (Professional and Enterprise package only)

This feature allows Security Desk operator to control the content of other Security Desk workstations connected to the same system through a graphical representation of the remote workstations and monitors. The feature is used to create video wall applications using the Security Desk.

Threat Levels (Professional and Enterprise package only)

This feature allows operators to dynamically change to state of the entire Security Center system when a critical event happens or operations changes on how we would the system to behave.

This is a system wide feature.

Record Fusion Service (Professional and Enterprise package only)

This feature allows importing data from external sources as a record and reusing these records in the platform through visual reports, dashboards & maps. Records can be imported through the Record Fusion Caching Service role from:

The following format are supported:

- Flat files.
 - CSV (comma separated values), TSV (tab separated values), SSV (semicolon separated values)
 - JSON, BSON
 - KML, KMZ
 - GPX (GPS Exchange Format)

- A REST interface.

Windows Active Directory (Professional and Enterprise package only)

Product Code [GSC-1AD-USCH] [GSC-1AD]

This feature allows system administrators to integrate to Windows Active Directory. The Windows Active Directory integration allows the synchronization of an Active Directory Windows user database with the Security Center users, user groups, cardholders and cardholder groups. The Active Directory role also support the synchronization over Active Directory Universal Groups and Global Catalogs.

One (1) Active Directory connection is enabled by default in the Professional and in the Enterprise base packages. In the case where Security Center needs to connect to multiple Active Directory servers, up to an additional 9 Active Directory connections can be ordered for a maximum of 10 Active Directory connections.

Authentication (Professional and Enterprise package only)

Product Code [GSC-1AUTH]

This feature enables 1 Authentication Role. The Authentication Role enables using an external identity provider for user authentication into Genetec Security Center™. The external identity provider supported are:

- Windows Active Directory Federation Services (ADFS)
- Azure Active Directory (through OpenID Connect)
- Other Open ID Connect / SAML2 authentication agents such as:
 - Ping Identity
 - KeyCloak
 - OKTA

One (1) Authentical role connection is enabled by default in the Professional and in the Enterprise base packages. In the case where Security Center needs to more authentication roles, additional connections can be ordered.

Languages

Security Center supports the following languages:

English, French, Arabic, Czech, Dutch, German, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Persian (Farsi), Polish, Portuguese (Brazilian), Simplified and Traditional Chinese, Russian, Spanish, Swedish, Thai, Turkish, Vietnamese.

Security Center Standard

Product Code [GSC-Base-S]

The Security Center Standard base package includes the licenses to :

- Omnicast™ Standard
- Synergis™ Standard
- Autovu™ Standard

The Security Center Standard Base package is limited to a maximum of 50 cameras, 1 archiver, 64 readers, 1 access manager and 5 clients. The maximum of five (5) clients connections includes five (5) Security Desk AND five (5) Web Clients OR five (5) Mobile Clients.

For detailed information about each individual inclusion, please refer to their respective section within the document.

Omnicast™ Standard

The Omnicast™ Standard package is the entry level package targeted for system with a low camera count which requires a cost effective solution. The Standard package includes the typical functionalities of a video management system all included in a single base package. The Standard package is intended to work on a single server installation.

A base package is mandatory for every Omnicast™ system.

The Omnicast™ Standard system can be federated by an Enterprise system.

The Archiver included in the base package cannot be installed on a separate server (single server operation only in the Standard package).

- Archiving support (Max. 50 cameras)
- Media Router
- Audio
- Camera Sequences
- Camera Dewarping
- Keyboard and Joystick
- Edge recording and trickling
- Time Zone

Synergis™ Standard

The Synergis™ Standard package is the entry level package targeted for systems with a lower reader count which requires a cost effective solution. The Standard package is intended to work on a single server installation. The base package includes the following functions at no additional cost:

- Badge designer

- Elevator control
- People counting
- Antipassback
- Two man rules
- First person in
- To set unlocking schedule
- To enable access rule
- Support for USB enrolment reader
- Mobile credential management task
- HID Mobile credential support (Origo)

A base package is mandatory for every Synergis™ system.

The Synergis™ Standard system can be federated by an Enterprise system.

The Synergis™ Standard system can connect to a Synergis™ Enterprise system for Global Cardholder Management.

The Access Manager included in the base package cannot be installed on a separate server (single server operation only in the Standard package).

Federation™ option

All Standard systems can be federated into an Security Center™ Enterprise system. No cost is associated to this option for the Standard system.

Upgrade to Pro or Enterprise

Product Code [GSC-S2P-UP] [GSC-S2E-UP]

Upgrading from Security Center™ Standard to Pro or Enterprise is available. Specific part numbers are available to upgrade from Standard to Pro or Enterprise.

Security Center Professional

Product Code [GSC-Base-P]

The Security Center Professional base package includes the licenses to :

- Omnicast™ Professional
- Synergis™ Professional
- Autovu™ Standard
- Plan Manager Advanced with unrestricted entity count
- Threat Levels
- Record Fusion Service
- 1 Active Directory connection
- 1 Authentication role

The Security Center Professional Base Package is limited to a maximum of 250 cameras, 20 archivers, 256 readers, 2 Access Managers, and 10 clients. The maximum of ten (10) clients connections includes ten (10) Security Desk AND ten (10) Web Clients OR ten (10) Mobile Clients.

For detailed information about each individual inclusion, please refer to their respective section within the document.

Omnicast™ Professional

The Professional package is the ideal choice for small system which requires a cost effective solution. The Professional package includes the standard functionalities of a video management system. More advanced functionalities are offered in option.

A base package is mandatory for every Omnicast™ system.

The Omnicast™ Professional system can be federated by an Enterprise system.

One Omnicast™ Professional 5.x Base Package is required per Omnicast™ system

- Archiving support (Max. 250 cameras)
- Media Router
- Audio
- Remote Security Desk
- Camera Sequences
- Camera Blocking
- Camera Dewarping
- Keyboard and Joystick
- Edge recording and trickling

- Time Zone

Synergis™ Professional

The Professional package is the ideal choice for smaller to mid-sized systems which require a cost effective solution. More advanced functionalities are optional. The base package includes the following functions at no additional cost

- Badge designer
- Elevator control
- People counting
- Antipassback
- Two man rules
- First person in
- To set unlocking schedule
- To enable access rules
- Support for USB enrolment reader
- Mobile credential management task
- HID Mobile credential support (Origo)

A base package is mandatory for every Synergis™ system.

The Synergis™ Professional system can be federated by an Enterprise system.

The Synergis™ Professional system can connect to a Synergis™ Enterprise system for Global Cardholder Management.

Federation™ option

All Professional systems can be federated into an Security Center™ Enterprise system. No cost is associated to this option for the Professional system.

Upgrade to Enterprise

Product Code [GSC-P2E-UP]

Upgrading from Security Center™ Professional to Enterprise is available. Specific part numbers are available to upgrade from Pro to Enterprise.

Security Center Enterprise

Product Code [GSC-Base-E]

The Security Center Enterprise base package includes the licenses to :

- Omnicast™ Enterprise
- Synergis™ Enterprise
- Autovu™ Standard
- Plan Manager Advanced with unrestricted entity count
- Threat Levels
- 1 Active Directory connection
- Failover Directory

The Security Center Enterprise Base Package has no restriction for the number of cameras, archivers, readers, Access Managers, and clients connections.

For detailed information about each individual inclusion, please refer to their respective section within the document.

Omnicast™ Enterprise

Enterprise package is the ideal choice if you plan on benefiting from the full power of Omnicast™, as all the software options are available, as well as the ability to scale to hundred of thousands of cameras and the optional failover capabilities.

A base package is mandatory for every Omnicast™ system.

The Omnicast™ Enterprise package is also required for the head end of a Federation™ system. The Omnicast™ Enterprise Package can federate Omnicast™ Enterprise, Professional or Standard systems.

Omnicast™ Enterprise 5.x base package includes the following features:

- Archiving support (Max. 1,000 cameras per Archiver / 100 on Directory Machine)
- Auxiliary Archiving
- Media Router
- Audio
- Remote Security Desk
- Camera Sequences
- Camera Blocking
- Camera Dewarping
- Keyboard and Joystick

- Edge recording and trickling
- Hardware Matrix
- Time Zone

Failover camera connection

Failover cameras is included with Security Center starting at version 5.11, each camera license purchased include a failover camera.

Additional archiver servers may need to be deployed in order to failover the cameras.

Starting from 5.5, it is possible to configure up to three (3) archive roles to protect a single camera. This configuration allows to support disaster recovery scenarios where local archiver failover is required in addition to a central failover archiver in case the local site is completely offline but the camera can still reach the central site.

Performance

The number of cameras that can be handled by a single archiver will vary depending on the performance of the hardware where the Omnicast™ application is running. The Failover Archiver, on a high end server, can secure up to 3 archivers, and up to 900 cameras but like the regular archiver can handle the simultaneous failover of maximum 300 cameras or 300 Mbps of throughput; whichever comes first.

Important: This item requires ordering a minimum one year of Genetec Advantage.

Auxiliary Archiver

Auxiliary Archiving provides the capability to protect video archiving by recording a camera already managed by an archiver on a different schedule with a different video quality. This option is not a replacement of the Archiver. It is a complementary option.

This option is included in the Enterprise base package only.

Performance

The number of cameras that can be handled by a single Auxiliary Archiver will vary depending on the performance of the hardware where the Omnicast™ application is running. Like a regular archiver, the Auxiliary Archiver, on a high end server, can handle a maximum of 300 cameras or 150 Mbps of throughput; whichever comes first.

Hardware Matrix

This features allows controlling a hardware matrix from Security Center using virtual cameras to switch cameras on the hardware matrix. An Omnicast™ 4.x system is required to be used as the driver for the hardware matrix. The Omnicast™ 4.x must be federated by Security Center in order to get access to the virtual cameras created by the hardware matrix driver. The license for the Omnicast™ 4.x system and the federation connection are included with the hardware matrix connection.

Hardware Matrix support is only available in Enterprise.

Synergis™ Enterprise

Enterprise package is the ideal choice if you plan on benefiting from the full power of Synergis™ with the ability to scale to tens of thousands of doors and the optional failover components. The base package includes the following functions at no additional cost

- Badge designer
- Elevator control
- People counting
- Antipassback
- Two man rules
- First person in
- To set unlocking schedule
- To enable access rules
- Support for USB enrolment reader
- Mobile credential management task
- HID Mobile credential support (Origo)

A base package is mandatory for every Synergis™ system.

The Synergis™ Enterprise package is required for the head end of a Federation™ system. The Synergis™ Enterprise Package can federate Synergis™ Enterprise, Professional or Standard systems.

The Synergis™ Enterprise package is required to support Global Cardholder Management of remote independent Synergis™ systems. Remote systems can be Synergis™ Standard, Professional, or Enterprise systems.

One Synergis Enterprise 5.x Base Package is required per Synergis™ system and includes unlimited Access Managers.

A Synergis™ Enterprise system is required to support site licenses for Security Desk client applications, mobile app connections, or web client connections.

Failover Directory

In Backup/Restore mode, the Failover Directory works as a master to slave configuration. The Directory designated as the master will be responsible to push the system configuration to the slave directories after a failover. This can be automated or configured as a manual action. In this mode, configuration changes done on the secondary Directories will be lost after fail back unless the manual mode is selected to restore the changes first.

In SQL Mirroring and AlwaysOn mode, the configuration will be fully synchronized between all Directories. No loss in configuration will happen after fail back.

Failover Directory is only available in Enterprise.

Starting from 5.5, it is now possible to configure a Failover Directory role located in another geographic area (or building) to act as a disaster recovery server. A Failover Directory role now configured for disaster recovery only becomes available when all other Directories go offline or fail.

Performance

The maximum number of cameras in a Failover Directory configuration is the same as the maximum number of cameras supported by the Directory. This is valid for all modes.

The total number of Directories in a system should not exceed five (5).

Important: *This item requires ordering a minimum of one year of Genetec Advantage.*

Connection Licenses

Security Desk Client, WebApp and Genetec Mobile connection

Product Code [GSC-1Login]

A client connection is needed for each Security Desk client, Web client station, or Genetec Mobile app that connects to Security Center regardless of the number of client application running on the station. The Security Center client connection license is for concurrent connections and combined connections with web app or mobile. The Config Tool client application doesn't require a client connection license. One (1) client connection will provide a license for Security Desk and the Web App or Genetec mobile app.

User site license

Product Code [GSC-Login-Site]

Site license for client connection is available. The site license allows unrestricted concurrent client connections to the system.

Camera connection

Product Code [GSC-OM-S-1C] [GSC-OM-P-1C] [GSC-OM-E-1C]

A camera connection license is required for each video channel connected to the system (e.g. IP camera, video encoder or video decoder).

For multi-channel video units, a camera connection license is required for each video channel unless the video unit has the functionality of disabling the video channel at the source. This is valid for both multi-channel encoders and decoders.

Multi-sensor cameras require only one (1) camera connection as of the initial Security Center version the camera was certified with.

No camera connection is included in the base package.

Video Import Profile

The Video Import Profile connection is intended for the use of Offline Camera Devices in Security Center. A Video Import Profile allows the configuration of an Offline Camera that creates a repository for the import of G64, MOV, AVI and MP4 video files in Security Center. It offers the ability to import the video from Body Worn Cameras (BWC) and can be extended to any video source. This connection is certified with selected video offline unit (consult the SDL for the exact list).

Camera connection for Bosch VRM

The camera connection for Bosch VRM is required when Omnicast™ is installed with the Bosch VRM solution. The video recording is managed by the Bosch VRM system and seen as edge recording for Omnicast™.

The camera connection for Bosch VRM license is order instead of the regular camera connection license. This is not an add-on to the regular camera connection license.

Failover camera connections can also be ordered using the Bosch VRM solutions in order to protect the command and control of the camera. The recording of the camera is not protected by Omnicast™ in this case since it is managed by Bosch. It is also possible to have a redundant archiving by enabling the recording on the archiver and on the VRM in the same time

Performance

The following performance capabilities apply for the design when the video is recorded exclusively on the VRM. The Archiver for Bosch VRM is required when Omnicast™ is installed with the Bosch VRM solution. Using the Bosch VRM solution, the video recording is done at the edge using Bosch IP video units and iSCSI storage units. This part number will enable to Archiver to go up to 1,000 cameras per Archiver.

Because this Archiver doesn't record video, it has the ability to manage up to 1,000 cameras for command and control on a high end server. No live video redirection shall be done by the Archiver when managing 1,000 cameras. The network should be fully multicast and live streaming should be multicast from the camera/encoder to the Live Viewer.

Playback video will transit through the Omnicast™ Archiver. A maximum of 100 Mbps (50 Mbps IN / 50 Mbps OUT) of playback redirection is supported by the Archiver when managing 1,000 cameras.

Analog camera connection

Product Code [GSC-OM-S-1PAC] [GSC-OM-P-1PAC] [GSC-OM-E-1PAC]

The analog camera connection is intended for specific IP video encoders. The analog camera connection is at a lower price than the regular camera connection and is only compatible with some entry-level encoders (less functionality). This connection is valid with selected encoders only (consult the SDL for the exact list).

The analog camera connection is compatible with 5.2 SR3 and up.

No analog camera connection is included in the base package.

The analog camera connection for Enterprise system is supported for system up to 300 cameras.

Body wearable camera connection

Product Code [GSC-OM-S-1BWC] [GSC-OM-P-1BWC] [GSC-OM-E-1BWC]

The Body Wearable Camera connection is intended for the use of body wearable cameras in Security Center. It allows the creation of an evidence repository for the import of body wearable files into Security Center. One BWC Camera connection is required per holder (refer to SDL for certified body wearable cameras).

No body wearable camera connection is included in the base package

The body wearable camera connection is compatible with 5.7 SR1 and up.

DVR Input

Product Code [GSC-OM-P-1DV] [GSC-OM-E-1DV]

The GE DVMRe/StoreSafe is the only equipment for which the DVR input can be ordered. The DVR input license needs to be ordered for each video input on the DVR (NOT per DVR unit).

The DVR input license allows for live streaming and retrieval of the recorded video on the DVR, but doesn't allow recording of the DVR camera on the Archiver.

No DVR Input is included in the base package.

Reader connection

Product Code [GSC-Sy-S-1R] [GSC-Sy-P-1R] [GSC-Sy-E-1R]

One (1) reader connection license is required for each door reader connected to the system. A reader connection is only required if the hardware is NOT purchased with the software. No reader connections are included in the base package.

SharpV connection

Product Code [GSC-Sy-S-1S] [GSC-Sy-P-1S] [GSC-Sy-E-1S]

One (1) reader connection license is required for each SharpV reader connection for license plate as a credential

Wireless Reader connection

Product Code [GSC-Sy-S-1WR] [GSC-Sy-P-1WR] [GSC-Sy-E-1WR]

One (1) reader connection license is required for each reader embedded in lockset, cylinder or padlock connected to the system.

Jetway functionality

Product Code [GSC-SY-P-JETWAY] [GSC-SY-E-JETWAY]

System wide setting to support the Jetway functionality on the Synergis CloudLink™

Global Cardholder Management connection

Product Code [GSC-Sy-E-1GCHM]

One (1) Global Cardholder Management connection license is required at the central site for each remote site that connects back to a central Synergis™ Enterprise system to synchronize cardholders, credentials, and badge templates.

Evacuation Assistant

Product Code [GSC-SY-EVACUATION]

Manage evacuations and mustering areas using a web dashboard. Use reader activity and to automatically mark cardholder as safe and allow mustering captain to check-in, mark as unsafe or safe. Monitor live status of different evacuations through dashboards which show who is missing, unsafe or safe.

Smartcard Encoding module

Product Code [GSC-Sy-S-SCE] [GSC-Sy-P-SCE] [GSC-Sy-E-SCE]

Smart Card Encoding module to program Desfire EV1 cards from Security Desk™ using the STid USB readers.

Softwire for 2 tier architecture

Product Code [GSC-SY-S- S2TI] [GSC-SY-P- S2TI] [GSC-SY-E-S2TI]

Genetec™ System wide Softwire integration pack for VM or server (2 tier architecture). Not required on the SV300 appliances.

Intercom Connection licenses

Product Code [GSC-Sipelia-1SIP]

A connection license is required for each Communication Devices such as intercom that is configured in Sipelia including intercom connected through an Intercom Exchange Server (behind a trunk). Each connection enables failover as well as audio and video recording features as of Security Center 5.11.

Security Desk users associated with a SIP extension don't require connection licenses.

SDK connection

A SDK connection is required for an application that has been created using the Security Center SDK. One (1) SDK connection is needed per concurrent application connection.

Ex.: One SDK application running on five (5) stations simultaneously will require five (5) SDK connections.

There is no longer a generic part number for SDK connections. SDK connections are assigned on a per partner and/or project basis and have a specific certificate assigned to it. You must contact Genetec to obtain a specific SDK connection part number specific to your company and/or project.

Site License for SDK connection is possible, but it has to be requested on demand.

Optional Features

Omnicast Cloud storage

Omnicast Cloud storage provides an extension to on premise storage for Security Center Omnicast. It allows longer term retention, secure and redundant storage, and seamless retrieval from Security Desk.

This option is compatible with Security Center Omnicast on-premise and SaaS Edition, and it is sold on a subscription basis. Please refer to the Security Center as a Service (SCaaS) Ordering Guide for the feature description and ordering options.

Federation™

Product Code [GSC-1SCFED-20] [GSC-1SCFED] [GSC-1OM4FED-20] [GSC-1OM4FED]

The Federation™ offers the possibility of bridging several independent access control, video and/or license plate recognition systems located in remote or regional sites into a single virtual system.

An Enterprise base package is required to order the federation options. The Federated systems can be any package (Standard, Pro, Enterprise, SV line).

If one of the Federated system is an Omnicast™ system, the Federation™ must include an Omnicast™ Enterprise base package and vice-versa with Synergis™.

The Federation™ options depend on the number of entities to be federated. Two options exist:

Small site with less than 20 entities [GSC-1SCFED-20] [GSC-1OM4FED-20]

Sites with unrestricted number of entities [GSC-1SCFED] [GSC-1OM4FED]

Performance

The number of systems and entities that can be handled by a single Federation™ Role on a high-end server is the following:

Maximum 100x Omnicast™ 4.x systems with 150 entities each

Maximum 500x Security Center systems with 150 entities each

Video streams are NOT redirected by the Federation™ server.

Stratocast™ Federation™

Product Code [GSC-OM-E-1CCFED]

Stratocast™ Federation™ offers the possibility of bridging several independent Stratocast™ systems located in remote or regional sites into a single virtual Security Center system.

An Security Center Enterprise base package is required to order the federation Stratocast™ Federation™ option.

The Federation™ licence is waived for sites within the same legal entity as the owner of the Security Center Enterprise base package.

Global Cardholder Management

This feature allows the synchronization of cardholders, credentials, and badge templates between remote independent Synergis™ sites and a central Synergis™ site, or between remotes Synergis™ sites (via the central site). The global cardholder synchronization role runs on the remote site(s), however the connection licenses must be purchased at the central site, there is no special license need at the remote site(s).

The central site must be a Enterprise system.

NEC and Windows Clustering Support

Product Code [GSC-StandbyServer]

NEC and Windows Clustering support licensing is intended for systems which use NEC or Microsoft Windows Clustering for the failover mechanism. This licensed option provides an additional Security Center Directory license for one additional node in the cluster.

Clustering support is only available in Enterprise.

Important: This item requires ordering a minimum one year of Genetec Advantage.

Plugins

The listed plugins might not work with all the service releases of the current Genetec Security Center version, please refer to the Security Center Supported Plugins document on TIP for version compatibility and supported hardware.

Intrusion Panels

Bosch

Product Code [GSC-1AP-Bosch]

A Bosch B & G Series intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported Bosch panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

Bosch Map 5000

Product Code [GSC-1AP-BoschMap5000]

A Bosch MAP 5000 series intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported Bosch panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

Honeywell Galaxy & Flex

Product Code [GSC-1AP-CDC3-HW]

A Honeywell Galaxy Dimension intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for

supported Honeywell Galaxy Dimension panels. The new integration ordered using GSC-1AP-CDC3-HW replaces the previous GSC-1AP-HIGalaxy for any new systems starting at SC 5.7.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

DSC

Product Code [GSC-1AP-DSC]

A DSC PowerSeries intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported DSC PowerSeries panels.

Important: This item requires either Standard, Professional or Enterprise package (and the Alarm panel Advantage to be added to system's Genetec Advantage.

DMP

Product Code [GSC-1AP-DMP]

A DMP intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported DMP panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

SPC

Product Code [GSC-1AP-CDC2-SPC]

A SPC intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported SPC panels

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

Aritech ATS Master and Advance

Product Code [GSC-1AP-CDC3-UTCMaster]

A Aritech ATS Master and Advance intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported Aritech panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

SATEL

Product Code [GSC-1AP-SATEL]

A SATEL intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported UTC panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

TELENOT

Product Code [GSC-1AP-TELENOT]

A TELENOT intrusion panel part is required for each intrusion panel connected to the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported UTC panels.

Important: This item requires either Standard, Professional or Enterprise package and the Alarm panel Advantage to be added to system's Genetec Advantage.

Alarm Panel Receiver

Product Code [GSC-1PAP-Receiver]

This plugin requires one Receiver part for every set of 100 intrusion panel connected to the receiver and monitored by the system. Please refer to the Supported Plugin in Security Center guide and release notes for supported Receivers. Plugin supports DMP Serial 3, Bosch Contact ID, and DSC Sur-Gard SIA protocols.

Important: This item requires either Standard, Professional or Enterprise package

Buy-Time

Product Code [GSC-1PAP-BuyTime]

This plugin allows specific cardholder to delay, by a set interval, the scheduled auto-arming of intrusion areas using local door readers. One part required per system to manage arming delays of intrusion areas. Please refer to the Security Center user guides and release notes for supported panels.

Southwest Microwave RPM II

Product Code [GSC-1PSWM-RPMII]

New installation of southwest Microwave will be delivered using their new RPMII unit. The Southwest Microwave RPM II Plugin, via the RPMII unit, provides interface to 1)SWMW INTREPID MicroPoint™ II Fence Detection System, 2)MicroTrack™ II Buried Cable Detection System and 3)MicroWave 330 Digital Microwave Sensor.

This MicroPoint RPMII Plugin is only compatible with Southwest Microwave RPMII unit.

The MicroPoint RPMII Plugin is hosted on the Plugin Role.

Important: This item requires either Professional or Enterprise package.

Access Control System

Lenel OnGuard

Product Code [GSC-1PLEN]

The Lenel OnGuard Plugin provides integration between Security Center and Lenel OnGuard access control solution. The plugin imports access control, cardholders and intrusion entities as well as

events and alarms to Security center. It enables operators to manage OnGuard events and alarms within Security Center, and monitor associated video from live access control events. A Security Center operator can also perform some tasks from Security Desk into the Lenel system (Deactivate CH, unlock doors)

The Lenel OnGuard Plugin is hosted on the Plugin Role.

Important: This item requires either Professional or Enterprise package

Performance

One (1) plugin part is required for every 750 Lenel readers on the system.

Third Party Software requirement

Lenel OpenAccess License fee (third party license) is required. This Lenel components must be purchased directly from Lenel.

Lenel OnGuard Video Translator

Product Code [GSC-1VLEN]

The Lenel OnGuard Video Translator plugin provides the ability to view Security Center video from the OnGuard client application.

Important: This item requires either Professional or Enterprise package

Performance

One (1) Lenel Video Translator must be ordered per Lenel server.

Third Party Software requirement

Third Party software is required. This Lenel components must be purchased directly from Lenel, additional cost is involved.

Software House C•CURE 9000 Access Control

Product Code [GSC-1PSHCC]

The Software House C•CURE 9000 Plugin provides integration between Security Center and Software House C•CURE 9000 access control solution, enabling operators to view and manage C•CURE events, alarms and causes, import cardholder information within Security Center, and monitor associated video from live access control events as well as execute some actions (lock/unlock doors) and other manual actions to CCure entities.

The Software House C•CURE 9000 Plugin is hosted on the Plugin Role.

Important: This item requires either Professional or Enterprise package

Performance

One (1) C•CURE 9000 access control plugin part is required for every 750 C•CURE readers on the system.

Third Party Software requirement

Third party software is required. The C•CURE components must be installed on a separate server, additional cost is involved.

Product Code [CC9000-GENS1] C•CURE 9000 system license is required for the access control integration plugin option with Genetec Security Center.

Software House C•CURE 9000 Video Integration

Product Code [GSC-1PVSHCC]

The Software House C•CURE 9000 video integration plugin provides the ability to view Security Center video from the C•CURE client application.

The C•CURE Video integration component reside on a C•CURE client and server computers.

Important: This item requires either Professional or Enterprise package

Performance

One (1) C•CURE 9000 video integration plugin is required per system regardless of the number of C•CURE workstations.

Third Party Software requirement

Third party software is required. The C•CURE components must be installed on a separate server, additional cost is involved.

Product Code [CC9000-GENSECCTR] C•CURE 9000 video integration option with Genetec Security Center is required within the C•CURE 9000 system licence for the video integration plugin.

Siemens Sipass

Product Code [GSC-1PSIPASS]

The Sipass plugin provides an integration between Security Center and Sipass access control solution. The plugin synchronizes access control entities, carholders, events and alarms to Security center. It is also possible to control doors locks and outputs from Security Center.

The Sipass plugin is hosted on the Plugin Role

Important: This item requires either Professional or Enterprise package

Performance

One (1) SiPass access control plugin part is required for every 750 SiPass readers on the system.

Third Party Software requirement

Third party software is required. The Sipass components must be installed on a separate server and configured separately, additional cost is involved.

AMAG Symmetry

Product Code [GSC-1PAMAG-SYM]

The AMAG Symmetry plugin provides an integration between Security Center and AMAG Symmetry access control solution. The plugin synchronizes access control entities, carholders, events and alarms to Security center. It will be also possible to control doors locks and outputs from Security Center in a later phase.

The AMAG Symmetry plugin is hosted on the Plugin Role

Important: This item requires either Professional or Enterprise package

Performance

One (1) AMAG access control plugin part is required for every 750 AMAG readers on the system.

Third Party Software requirement

Third party software is required. The AMAG Symmetry components must be installed on a separate server and configured separately, additional cost is involved.

Assa Abloy ARX

Product Code [GSC-1PCDC2-ASSA-ARX-25]

The Assa Abloy ARX plugin provides an integration between Security Center and Assa Abloy ARX access control solution. The plugin synchronizes access control entities, carholders, doors, controllers, monitors door states and cardholder events in Security Center. It is also possible to control doors locks from Security Center. One part per 25 doors connected and monitored by the system is required.

The ARX plugin is hosted on the Plugin Role

Important: This item requires either Professional or Enterprise package

Third Party Software requirement

Third party software is required.

Access Control Ecosystem

Document Scanner

Product Code [GSC-1PIDSCANNER]

The Document Scanner plugin gives the ability to use official document scanners for ease of cardholder and visitor enrollment.

This plugins supports a limited amount of document scanners, please consult the documentation for more information.

Performance

One plugin is required per enrollement workstation.

Third Party Software requirement

IDScann.net 3rd party license, or scanner Hardware may be needed.

Morpho Biometrics Scanner

Product Code [GSC-1PMORPHOBIOMETRICS]

The Morpho Biometrics plugin gives the ability to enroll Morpho Biometrics readers with Synergis.

Performance

One plugin is required per Security Center system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

SALTO SVN

Product Code [GSC-1PSALTOSVN] : Plugin base including 10 doors

Device Product Code [GSC-1PSALTOSVN-1D] : 1 Salto door (escutcheon)

Device Product Code [GSC-1PSALTOSVN-1L] : 1 Salto lock

The SALTO SVN Plugin integrates the SALTO Virtual network offline and online devices. This plugin gives the ability to synchronize, monitor and do after-the-fact investigation of the SALTO offline and online doors and locks. This is a software-to-software integration, even if the hardware is bought through Genetec, this plugin license and the device licenses are required to have the integration working. No need for reader licenses when the hardware is purchased from Genetec.

The base product code includes 10 doors. If locks or additional and doors are required, additional device product code are needed.

Important: This item requires ordering a reader Genetec Advantage per Salto doors to be added to system's Genetec Advantage.

CARD Synchronisation

Product Code [GSC-1PSingleCard]

The Card Synchronization plugin gives the ability to connect to external sources of cardholder data, map the data fields with cardholder data and keep Security Center synchronized with the value changes from the source. We can support multiple data source like CSV, SQL and Oracle databases. The plugin is also available in a hosted SaaS system with different data sources.

Performance

One part is required per maximum of 2 data sources

Third Party Software requirement

No need for 3rd party software

MedecoXT

Product Code [GSC-1PMEDECOBASE]: Plugin base

Product Code [GSC-1P-OFFLINELOCK-1L]: Individual intelligent lock

The Medeco XT plugin provides an integration between Security Center and the MedecoXT products. This plugin gives the ability to assign access rules of cardholders to MedecoXT locks. It also allows programming of MedecoXT keys with proper access rules and MedecoXT locks.

Important: This item requires either Professional or Enterprise package

Performance

1 base part per system and requires Offline lock parts to be added for every cylinder on the MedecoXT codebook.

Assa Abloy CLIQ

Product Code [GSC-1PCLIQBASE]: Plugin base

Product Code [GSC-1P-OFFLINELOCK-1L]: Individual intelligent lock

The CLIQ plugin provides an integration between Security Center and the CLIQ products. This plugin gives the ability to assign access rules of cardholders to CLIQ locks. It also allows programming of CLIQ keys with the proper access rules. The AssaAbloy CLIQ plugin is compatible with all of AssaAbloy group companies (Medeco, Abloy, Ikon, Mul-T-Lock)

Important: This item requires either Professional or Enterprise package

Performance

1 base part per system and requires Offline lock parts to be added for every cylinders on the CLIQ system.

ADVANCED ENROLLMENT**Product Code [GSC-1PAdvanceEnroll]**

With the Advanced Enrollment plugin, you can now use the HID Fargo Printer to batch produce, print and encode cards in a single operation. The plugin allows creation of badge templates. You can also print and encode using QR code, Barcode and Magstripe.

Important: This item requires either Professional or Enterprise package

Performance

One plugin is required per Security Center system.

Elevator Destination Dispatch**OTIS Compass****Product Code [GSC-1POTIS-COMPASS]**

The OTIS Compass Plugin integrates the OTIS destination dispatch solution. This plugin gives the ability to control the Compass solution using the Synergis access rules.

This plugins supports version 1, 2 and 3 of the OTIS Compass solution. Multiple building layout requires special configuration, please refer to plugin guide version 3.2 or later.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per OTIS facility network.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

ThyssenKrupp**Product Code [GSC-1P-TKDispatch]**

The ThyssenKrupp Plugin integrates the TK destination dispatch solution. This plugin gives the ability to manage elevator system units and events. Please consult the plugin guide for more information.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per building system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

MCE

Product Code [GSC-1P-MCESentry]

The MCE (Motion Control Engineering) Plugin integrates the MCE Sentry destination dispatch solution. This plugin gives the ability to manage elevator system units and events. It is currently available in LA mode only. Please consult the plugin guide for more information.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per building system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Schindler

Product Code [GSC-1PSCHINDLER-PORT]

The Schindler Plugin integrates the Schindler Port destination dispatch solution. This plugin gives the ability to manage elevator system units and events. Please consult the plugin guide for more information.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per building system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

KONE Destination Dispatch

Product Code [GSC-1P-KONE]

The KONE Plugin integrates the KONE destination dispatch solution. This plugin gives the ability to manage elevator system units and events. Please consult the plugin guide for more information.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per directory.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Asset and Key Management System

Deister proxSafe Key Management

Product Code [GSC-1PProxSafeKey]

The Deister ProxSafe Key Management System plugin integrates Security Center central cardholder management and access rules with the Deister ProxSafe system. It allows to synchronize key access between Security Center and ProxSafe. This Plugin requires the GSC-1P-KeyCabinetBase.

Important: This item requires Professional or Enterprise package)

Performance

One plugin is required per 1 ProxSafe physical cabinet. This Plugin requires the **GSC-1P-KeyCabinetBase** per Genetec system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Traka Asset Management

Product Code [GSC-1PTRAKA]

The Traka Asset Management System plugin integrates Security Center central cardholder management and access rules with the ASSA ABLOY Traka key system. It allows to synchronize key access between Security Center and TRAKA. This Plugin requires the GSC-1P-KeyCabinetBase.

Important: This item requires Professional or Enterprise package

Performance

One plugin is required per 1 TRAKA physical cabinet. This Plugin requires the **GSC-1P-KeyCabinetBase** per Genetec system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

MorseWatchmans KeyWatcher

Product Code [GSC-1PKeyWatcher]

The MorseWatchman KeyWatcher Management System plugin integrates Security Center central cardholder management and access rules with the MorseWatchman key system. It allows to synchronize key access and profiles between Security Center and KeyWatcher. This Plugin requires the GSC-1P-KeyCabinetBase.

Important: This item requires Professional or Enterprise package

Performance

One plugin part is required per 1 MorseWatchman physical cabinet. This Plugin requires the **GSC-1P-KeyCabinetBase** per Genetec system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

KeySystems SAM

Product Code [GSC-1PKeySystems-SAM]

The KeySystem SAM plugin integrates Security Center central cardholder management and access rules with the KeySystem solution. It allows to synchronize key access and profiles between Security

Center and KeySystem. This Plugin requires the GSC-1P-KeyCabinetBase. The plugin is not fully released at the time of the ordering guide release.

Important: This item requires Professional or Enterprise package

Performance

One plugin part is required per 1 KeySystem physical cabinet. This Plugin requires the **GSC-1P-KeyCabinetBase** per Genetec system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Videowalls

Barco CMS

Product Code [GSC-1PBARCOCMS]

The Barco CMS Plugin is a video wall plugin that integrates Barco Video Wall Displays through the CMS (Control Room Management Suite) SDK. The Barco CMS Plugin allows controlling the video content displayed on the video wall.

The Barco CMS Plugin is compatible with the Barco Transform A and Transform N controllers.

The Barco CMS Plugin is hosted on the Plugin Role.

Performance

A plugin is required per Barco CMS server.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Videowall – EIZO

Product Code [GSC-1PVW-EIZO]

The EIZO videowall Plugin is a videowall plugin that integrates EIZO Video displays through the Genetec Videowall framework. The EIZO videowall plugin allows controlling the video content displayed on the video wall.

Performance

1 Part is required per monitor controlled by the videowall framework.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Shot Detection Systems

Shot spotter

Product Code [GSC-1PCDC0-SHOTSPOTTER]

The ShotSpotter Gunshot Detection plugin integrates alerts received from the ShotSpotter service into Security Center using the ShotSpotter Gunshot Detection plugin role.

Important: This item requires either of Professional or Enterprise packages and ordering a minimum one year of Genetec Advantage.

Performance

One plugin is required per Security Center system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

SDS Guardian Gunshot

Product Code [GSC-1PSDS-GUARDGUNSHT]

The SDS Guardian Gunshot Detection plugin integrates alerts received from the Shooter detection service into Security Center using the Guardian Gunshot Detection plugin role.

Important: This item requires either of Professional or Enterprise packages and ordering a minimum one year of Genetec Advantage.

Performance

One plugin is required for every 100 SDS sensors monitored by Security Center system.

Third Party Software requirement

Third party software and hardware is required, additional cost is involved.

Industrial Internet of Things (IIoT)

Product Code [GSC-IIoT]

The plugins gives the ability to ingest external devices statuses and bring them into Genetec Security Center as custom events, monitor and do after-the-fact investigation through the device statuses.

The plugins can support many device protocols, and adapt to many devices in these different protocols. Depending on the devices and the protocol, some deployment may be complex for certain type of devices.

This part number allow you unrestricted quantity of data point for ONE protocol can be selected within the configuration. If more than ONE protocol is required within the same Genetec Security Center licence, a second or multiple parts will need to be added.

Important: This item requires Standard, Professional or Enterprise packages.

OPC UA Client

The OPC UA Client plugin gives the ability to ingest OPC UA devices statuses. OPC can be seen in the field through 4 different protocols : OPC DA, OPC EA, OPC HA and OPC UA. These 4 protocols are not compatible with each other. This plugin only support OPC UA. An OPC DA/EA/HA device can be connected to our plugin through an external OPC DA/EA/HA to UA gateway at additional cost, but not provided by Genetec.

BACnet

The BACNet plugin integrates Building Automation and Control (BAC) network devices and sensors in Security Center. The plugin monitors heating and ventilating sensors, air-conditioning, lighting and accesses controls, and fire detection systems and associated equipment. When sensor status are

received, it automatically generates an events in Security Center. It is also possible to send BACnet commands back to BACnet devices through the plugin.

ModBus

The Modbus plugin allows compatible industrial devices and sensors, that are connected over an IP network, to be supervised by Security Center. The plugin will monitor the Modbus device's input values or update the device register. When sensor's status and values are received, the plugin captures the value and, using the rule engine, you can trigger custom events in Security Center. The plugin also allows to write from Security center into Modbus registers. The plugin also allows to create custom "actions" by writing from Security center into Modbus a registers.

SNMP Manager

The SNMP Manager plugin integrates SNMP network devices in Security Center. The plugin allows to enroll, poll and monitor SNMP equipment states by reading its OID register or receiving SNMP traps. The plugin also contains an engine rule that allows users to configure specific actions when it detects conditions of data changes of the monitored SNMP properties.

TCP Server

The TCP Server plugin replaces the ASCII custom solution. The TCP Server plugin integrates systems sending TCP data to the TCP Server plugin into Security Center. Devices are identified using a Device ID regex. When TCP Server arguments are received, the plugin captures the values and, using conditions settings in the rule engine, you can trigger alarms/events/state changes in Security Center.

HTTPS Server

The HTTPS Server plugin establish a connection using HTTP connectors with systems that can send POST messages using a device URL into Security Center. When HTTP arguments are received, the plugin captures the values and, using conditions settings in the rule engine, you can trigger alarms/events/state changes in Security Center.

MQTT Client

The MQTT Client plugin integrates systems sending device data using JSON Paths to the MQTT Client plugin into Security Center. When MQTT Client arguments are received, the plugin captures the values and, using conditions settings in the rule engine, you can trigger alarms/events/state changes in Security Center.

OPC Server – UA

Product Code [GSC-1POPC-S]

The OPC Server plugin gives the ability to export and expose the logical identifiers of camera, area, and door entities as OPC UA objects and update their state values.

Important: This protocol requires the part to be purchased. It is not included within the general IIoT part number.

Industrial Protocol Interface

Product Code [GSC-1PES-INDUSTRIAL-PROTCL-IF]

Optional:

Product Code [GSC-1PES-IPIEVENTS] – To enable IPI events for SNMP

The Industrial Protocol Interface plugin gives the ability to expose Security Center entities as protocol object values. Currently, BACnet and SNMP protocols are supported through this plugin.

Performance

Starting from Security Center 5.11, one part provides unrestricted data points monitored in Security Center system.

Transaction Monitoring

ATM: Diebold

Product Code [GSC-1PATMDIEBOLD]

The ATM Plugin is an integration that allows receiving ATM transaction print & Journal data from ATM machine and consolidate the transaction events, data and associated video in Security Center for event storage. The ATM Plugin allows doing event monitoring, report and individual transaction export.

The ATM: Diebold Plugin is compatible with the ATM Diebold using Agilis interface

The ATM Plugin is hosted on the Plugin Role.

Transaction Finder

Product Code [GSC-1P-TRANSACFINDER-BASE]: Plugin Base

Product Code [GSC-1P-TRANSACFINDER-1R]: 1 cash register

Product Code [GSC-1P-TRANSACFINDER-5R]: 5 cash registers

Product Code [GSC-1P-TRANSACFINDER-10R]: 10 cash registers

Product Code [GSC-1P-TRANSACFINDER-20R]: 20 cash registers

Product Code [GSC-1P-TRANSACFINDER-*PARSER*]: Parser

The Transaction Finder Plugin is an integration that allows receiving and consolidating the POS transaction events, data and associated video in Security Center for event storage. The Transaction Finder Plugin allows doing event monitoring, exception reporting, and transaction evidence exporting. The parser receives, standardizes and formats data from the point-of-sale system, so it can be pushed to the REST API.

Important: This item requires either of Professional or Enterprise packages and ordering a minimum one year of Genetec Advantage.

Performance

1 base part per system, requires at least 1 parser/client and individual register parts.

TagTracker

Product Code [GSC-1PTagTracker]

The Plugin allows integration of barcode readers to connect with Security Center and collect, store and allow reporting and searching of barcode items with associated video. One part is required for each barcode reader. Please refer to the Security Center user guide and release notes for details.

Important: This item requires either of Professional or Enterprise packages

Hexagon EDGEFrontier CAD

Product Code [GSC-1PHEXAGONCAD]

The Plugin allows integration with Hexagon EdgeFrontier CAD system. One part is required for each Edgefrontier system it is connecting to. Please refer to the Security Center user guide and release notes for details.

Important: This item requires ordering a minimum one year of Genetec Advantage.

SPS Checkpoint

Product Code [GSC-1PSPSCheckpoint]

The Plugin allows creation and tracking of guard tours using any Security center inputs like door readers, intrusion points, motion detection, etc. One part is required per system. Please refer to the Security Center user guide and release notes for details.

Important: This item requires either of Professional or Enterprise packages

AdroneX

Product Code [GSC-1P-ADRONEX]

The Plugin allows operators to dispatch Skeyetech's autonomous drones directly from Security Center manually or based on system events. Please refer to the Security Center user guide and release notes for details.

Important: This item requires either of Professional or Enterprise packages and the Drone Advantage to be added to system's Genetec Advantage

Performance

One part is required per system

Hybrid Frameworks

Videowall Framework

Product Code [GSC-1PVIDEOWALL]

The Plugin allows to connect to an integration developed through the Videowall framework. Requires the specific SDK integration part.

Performance

One part per video wall unit. Requires the specific SDK integration part.

Third party requirements

Third party software and hardware is required, additional cost is involved.

DYNAMIC LOG BOOK

Product Code [GSC-1P-DYNLOGBOOK-BASE & GSC-1P-DYNLOGBOOK-CLIENT]:

The plugin allows custom template creation to replace paper forms and allows an operator to fill, save and search on completed forms. The plugin contains an extensive form designer to allow the use of multiple field types, list of values, layouts, images, etc. We can set automatic triggers based on SC events using a specific Macro.

Important: This item requires either Professional or Enterprise

Performance

One base plugin is required per Security Center system for up to 5 client stations. One client part is required per each additional client stations using the plugin.

Genetec Mission Control™

Mission Control™ is a collaborative decision management system, integrated into Security Center, that provides new levels of situational intelligence, visualization, and complete incident management capabilities. It helps security personnel make quick decisions when faced with routine tasks or unanticipated situations, by ensuring a timely flow of information. Mission Control moves organizations beyond simple event and alarm management. By collecting and qualifying data from thousands of sensors and security devices (SCADA, OPC, RADAR, cameras, readers etc.), Mission Control can spot the most complex situations and incidents, and guide security teams in their response, following organization-specific processes and compliancy requirements.

It can also execute automated tasks without the need of involving an operator. System could automatically advise through email any abnormal activities related to video, access control, ALPR or any Security Center abnormal events. Through the automated task, it will help getting extra security functions that are engage only on specific situations from different devices or events that gets repeated within a programmed interval.

Genetec Mission Control™ 3.x is available under two different Packages:

- Genetec Mission Control™ Perpetual License
- Genetec Mission Control™ Subscription

Important: Genetec Mission Control™ is available with Standard, Professional and Enterprise versions of Security Center.

Connection licenses

Genetec Mission Control™ Operator License

Product Code [GSC-MC-10PP]

An operator connection is required for each Security Desk client station or Genetec™ mobile app connection that have the privilege to connects to Genetec Mission Control™. The operator connection license is for concurrent connections. The Config Tool client application does not require an operator connection license.

Note:

Genetec Mission Control™ functionality in the Genetec™ mobile app will be added to existing mobile app licenses. Therefore, they must be purchased separately and require Mobile Server role installation.

Enterprise Operator Site License

Product Code [GSC-MC-OPPSITE]

Site license for operator connection is available. The site license allows unrestricted concurrent operator connections to the system from the Security Desk client station or Genetec™ mobile application.

The site license does not restrict the number of active incidents or incident types.

Features activated with the Operator License

Genetec Mission Control™ features available with an Operator License are as follows:

For information on core platform and other component functionalities, refer to the relevant sections of the *Security Center Ordering Guide*.

Genetec Mission Control™ Incident Manager role

The Incident Manager is the central role that recognizes situational patterns, and triggers incidents in the Genetec Mission Control™ system. This role manages the incident automation workflows and keeps track of all user activities related to incidents. The Incident Manager role is automatically created when you upgrade your Security Center system to Genetec Mission Control™ and is hosted by default on your main server. There can be only one instance of this role on your system.

Rules Engine

The Rules Engine is the component of Genetec Mission Control™ that analyzes and correlates the data (events) collected by Security Center, based on predefined rules. The Rules Engine uses this data to detect and trigger incidents in Genetec Mission Control™.

An incident trigger is a sequence of rules that are applied by the Genetec Mission Control™ Rules Engine to automatically detect and trigger incidents. The Rules Engine looks for specific combinations of events (type, time, correlation, and frequency) in the system in order to determine whether an incident must be triggered.

Manual trigger of Incidents

Incidents can be configured for the user to trigger them directly from either the dedicated Incident monitoring task, the generic Monitoring task or Plan Manager.

Automation Engine

An incident automation is a series of activities associated with an incident type. These activities are performed by the system during the life cycle of an incident. The activities can change the incident state and properties, affect other entities in the system, or simply wait for a condition to become true. The incident automation helps automate the simple tasks, such as exporting the incident when it is resolved, so operators can focus on more complex ones.

Interactive Standard Operating Procedures

A standard operating procedure (SOP), or incident procedure, is a series of steps that the operator must follow before changing an incident state to Resolved. Each step can range from a very simple task, such as Call 911, to a complex task that requires support documents to accomplish. All actions taken by the operator are logged by the system in the incident history for audit purposes. A simple incident procedure is an ordered list of steps that do not involve multiple-choice questions. Operators might be allowed to resolve the incident without validating all the steps, or to complete the steps out of sequence, depending on the configuration.

Dynamic Standard Operating Procedure (DSOP)

This feature works in conjunction with the Standard Operating Procedure functionality to augment the capabilities of an operator in handling a situation or incident within the given environment. DSOPs allow for interrogatory procedure to be used with defined responses which then direct the flow of the procedures presented to an operator as the situation is managed. Use of DSOPs does not now show the operator the full list of steps available but rather only the ones justified by the operator response and in a singular manner keeping the operator focused on the procedure at hand.

Document Management

The Genetec Mission Control™ document library folder is used to store relevant documents that can be attached to incidents based on type, time and location of occurrence, and recipients. Users can

attach a document to the incident itself, or to a specific step within the standard operating procedure (SOP).

Incident Queue Mirroring

For high availability, user must first configure a RabbitMQ cluster with a master node (primary server) and a secondary node (secondary server). After a working cluster is created, nodes can be mirrored. This ensures that when the master node is unavailable, the secondary node can be reached so no data is lost.

Failover capability

The Genetec Mission Control™ Incident Manager role can be configured to failover on a secondary server to the Incident Manager role to support failover. For more information on role failover, see the *Security Center Administrator Guide*.

Geolocation on Map

Monitoring incidents on maps provides a global assessment of a situation. On the map, users can see the incident location, overview details, and the status of all incidents within the area.

This functionality relies on the availability of the Plan Manager Advanced component.

Reminders

To make sure no incidents are overlooked, users can set up reminders that are displayed in the notification tray of all incident recipients at regular intervals for as long as the incidents are not *Closed*.

TTR measurement and enforcement

Time To Response (the time it took for an incident to transition to the *In progress* state for the first time, after it was triggered) and Time To Resolution (the time it took for an incident to transition to the Resolved state for the first time, after it was triggered) are provided for each incident. Thresholds can be defined for time associated with Time To Response, Time To Resolution and time associated with each step of the incident procedure. Events will be generated when thresholds are met, triggering actions in the incident automation workflow.

Collaborative Incidents

A collaborative incident is an incident type that requires the collaboration of multiple teams to resolve. Each team has specific tasks to follow, which are represented by sub-incidents. The collaborative incident is resolved when all its sub-incidents are resolved.

Supervision

An incident supervisor is a user who sees an incident in the Incident monitoring task because they supervise the incident recipients.

Alarm management

This feature enables the ability to trigger alarms manually or automatically based on system events, to send alarms to specific recipients, to acknowledge alarms, to forward alarms, to snooze alarms, and to assign a procedure to an alarm.

Alarm workflows introduced in Security Center 5.2 is included. No additional license is required for this functionality. The alarm management runs on the Directory Role.

Profile

The Profile feature provides a configurable operator role for use in a Genetec Mission Control™ environment. A profile dictates what region, incident type and location an operator can manage with regards to Genetec Mission Control™ incidents. An authenticated Security Center operator can have one or several Profiles assigned to them. Supervisors can manually or automatically reallocate Profile responsibilities based on conditions within the environment, providing simple management of situational conditions.

Email support

Supports the ability to send an email to a user or user group. An email can be triggered following any event in the system.

Incident Reports

Supports the ability to execute report queries within the incident role database. Multiple filters are available including date, incident type, state, owner, location, time for resolution to customize incident reports.

Macros

This feature enables the usage of macros in the system. The macros run on the Directory Role.

Support for virtualization

Virtualization support is intended for Genetec Mission Control™ systems running in a virtual environment. The support for virtual environment is for Genetec Mission Control™ servers only. The virtual environment supported by Genetec Mission Control™ are VMware and HyperV. Please refer to the Server and OS Requirements document for supported versions as well as the system design guidelines available on TechDoc Hub.

Note: Operating in a virtual environment may have performance implications which can invalidate certain design guidelines recommended by Genetec™.

Languages

Genetec Mission Control™ supports the following languages:

English, French, Dutch, Spanish, German, Turkish, Japanese, Korean.

Genetec Mission Control™ Advantage

The Advantage Lifecycle Management of Genetec Mission Control™ is dependent on the number of Genetec Mission Control™ operators. As with all Advantage programs, it provides expedited support, product upgrades during the term of compliance. It can be procured in single or multiple year configurations.

Advantage Parts are only available for perpetual licenses as it is included in subscription licenses.

Advantage Operator

Product Code [ADV-MC-1OPP-(x)Y] [(x) can be 1 to 5 years]

This is to be aggregated to the number of Genetec Mission Control™ Operator (GSC-MC-1OPP) present in the system.

Advantage Site Operator

Product Code [ADV-MC-OPPSITE-(x)Y] [(x) can be 1 to 5 years]

This applies to one Genetec Mission Control™ Site licence (GSC-MC-OPPSITE) present in the system.

Genetec Mission Control™ Professional Services

The scope of services that will be provided by the Genetec Mission Control™ Professional Services team is specified at the beginning of the project. It generally includes assistance on the following:

- Migration of existing incident management procedures into Genetec Mission Control™ automation workflows and standard operating procedures (SOPs).
- Knowledge transfer during Genetec Mission Control™ deployment.

You must have the following to ensure optimum levels of support:

- Latest major version of Security Center.

Having the latest version of Security Center ensures that all Genetec Mission Control™ features will work as intended. This also allows the Professional Services team to optimize Genetec Mission Control™ deployment rather than spending time on updates to Security Center.

- Details of situations that need to be monitored including incident triggers, incident procedures for automation and Standard Operating Procedures (SOPs) to be migrated to Genetec Mission Control™.

PS-DS-BUNDLE

The Genetec Professional Services team will assist with the following:

- Onsite or remote consulting with integrator regarding installation and configuration of Security Center and Genetec Mission Control™
- Project Statement of Work (SOW), risk management, communications, issues, action items, and project status updates
- Genetec Mission Control™ deployment strategy
- Translating existing Standard Operating Procedures (SOPs) into Genetec Mission Control™ SOPs and defining automation workflows for deployment
- Testing Genetec Mission Control™ incidents as need by the client
- Knowledge transfer
- Detailed reporting that includes:
 - Genetec Mission Control™ design
 - Best practices & recommendations
 - List of automation workflows

In order to get the most accurate evaluation of the time required for deployment and associated costs, an evaluation meeting would be required. Please send request to the Professional Services team at Proservices@genetec.com.

Genetec Lifecycle Management (GLM)

Please refer to the GLM document on the Channel Partner Portal for the different:

GLM policies

Upgrade packages

Warranty issues

Appendix A – Server type

See Security Center System Requirements on Genetec's Website at <http://www.genetec.com>

Appendix B – Workstation type

See Security Center System Requirements on Genetec's Website at <http://www.genetec.com>

Appendix D – Pricing

Download the Genetec Security Center price list on the Channel Partner Portal to get the latest pricing.