

1. Security Center 5.12 A&E Specifications
2. CSI MasterFormat Division 28
3. **July 12, 2024**
4. **Table of Contents**

[**Section 28 13 00 – Access Control Software and Database Management**](#_heading=h.30j0zll)  **7**

[Part 1 - General 7](#_heading=h.1fob9te)

[1.01](#_heading=h.3znysh7) Related Work 7

[1.02](#_heading=h.2et92p0) Definitions 7

[1.03](#_heading=h.tyjcwt) Qualifications 7

[Part 2 - Products 8](#_heading=h.3dy6vkm)

[2.01](#_heading=h.1t3h5sf) Electronic Access Control System General Requirements 8

[2.02](#_heading=h.4d34og8) Failover and Standby Requirements 9

[2.03](#_heading=h.2s8eyo1) ACS Access Management 10

[2.04](#_heading=h.17dp8vu) ACS Global Cardholder Management *(Specifier, additional license required and Enterprise only for the central site)* 10

[2.05](#_heading=h.3rdcrjn) ACS Hardware Compatibility List 11

[2.06](#_heading=h.26in1rg) Seamless Unification with VMS 13

[2.07](#_heading=h.lnxbz9) ACS Controller (Unit) Management 14

[2.08](#_heading=h.35nkun2) ACS Cardholder and Cardholder Group Management 14

[2.09](#_heading=h.1ksv4uv) ACS Credential Management 15

[2.10](#_heading=h.44sinio) ACS Custom Card Formats 16

[2.11](#_heading=h.2jxsxqh) ACS Badge Designer 16

[2.12](#_heading=h.z337ya) ACS Door Management 17

[2.13](#_heading=h.3j2qqm3) ACS Elevator Management 18

[2.14](#_heading=h.1y810tw) ACS Visitor Management 18

[2.15](#_heading=h.4i7ojhp) ACS People Counting & Area Presence Tracking (Mustering) 19

[2.16](#_heading=h.2xcytpi) ACS Custom Fields (User-Defined Fields) 21

[2.17](#_heading=h.1ci93xb) ACS Import Tool 21

[2.18](#_heading=h.3whwml4) General Client Software Requirements 22

[2.19](#_heading=h.2bn6wsx) Configuration User Interface (UI) 24

[2.20](#_heading=h.qsh70q) ACS Client User Interface (UI) 24

[2.21](#_heading=h.3as4poj) Server Administrator User Interface Requirements 28

[2.22](#_heading=h.1pxezwc) Unified Web Interface (UWI) General Requirements 29

[2.23](#_heading=h.49x2ik5) Smartphone and Tablet App General Requirements 31

[2.24](#_heading=h.2p2csry) Health Monitor 34

[2.25](#_heading=h.147n2zr) USP General Requirements 34

[2.26](#_heading=h.3o7alnk) USP Architecture 36

[2.27](#_heading=h.23ckvvd) USP Access Control, Video, and ALPR Unification 40

[2.28](#_heading=h.ihv636) USP Alarm Management 40

[2.29](#_heading=h.32hioqz) USP Threat Levels *(Specifier, Professional and Enterprise)* 41

[2.30](#_heading=h.1hmsyys) USP Advanced Task Management 42

[2.31](#_heading=h.41mghml) USP Reporting 42

[2.32](#_heading=h.2grqrue) USP Dashboards 44

[2.33](#_heading=h.vx1227) USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)* 44

[2.34](#_heading=h.3fwokq0) USP Zone Management 45

[2.35](#_heading=h.1v1yuxt) USP User and User Group Security, Partitions, and Privileges Management 46

[2.36](#_heading=h.4f1mdlm) USP Event/Action Management 47

[2.37](#_heading=h.2u6wntf) USP Schedules and Scheduled Tasks 48

[2.38](#_heading=h.19c6y18) USP Macros and Custom Scripts 48

[2.39](#_heading=h.3tbugp1) USP Dynamic Graphical Maps (DGM) 48

[2.40](#_heading=h.28h4qwu) USP Audit and User Activity Trails (Logs) 53

[2.41](#_heading=h.nmf14n) USP Incident Reports 53

[2.42](#_heading=h.37m2jsg) USP Data Ingestion 54

[2.43](#_heading=h.1mrcu09) USP Third Party Integration 55

[2.44](#_heading=h.46r0co2) USP Software Development Kit (SDK) *(Specifier, Professional and up, additional license required)* 60

[Part 3 - Execution 61](#_heading=h.2lwamvv)

[3.01](#_heading=h.111kx3o) Warranty 61

[3.02](#_heading=h.3l18frh) Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 61

[3.03](#_heading=h.206ipza) Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)* 63

[**Section 28 17 00 – Physical Access Management System 64**](#_heading=h.4k668n3)

[Part 1 - General 64](#_heading=h.2zbgiuw)

[1.01](#_heading=h.1egqt2p) Related work 64

[1.02](#_heading=h.3ygebqi) Definitions 64

[1.03](#_heading=h.2dlolyb) Qualifications 65

[Part 2 - Products 65](#_heading=h.sqyw64)

[2.01](#_heading=h.3cqmetx) Physical Access Management System (PAMS) 65

[2.02](#_heading=h.1rvwp1q) Architecture 66

[2.03](#_heading=h.4bvk7pj) Management 68

[Part 3 - Execution 73](#_heading=h.2r0uhxc)

[3.01](#_heading=h.1664s55) Execution 73

[**Section 28 19 00 – Access Control Vehicle Identification Systems 76**](#_heading=h.25b2l0r)

[Part 1 - General 76](#_heading=h.kgcv8k)

[1.01](#_heading=h.34g0dwd) Related Work 76

[1.02](#_heading=h.1jlao46) Definitions 76

[1.03](#_heading=h.43ky6rz) Qualifications 76

[Part 2 - Products 77](#_heading=h.2iq8gzs)

[2.01](#_heading=h.xvir7l) SharpV All in one Cameras 77

[2.02](#_heading=h.3hv69ve) Client Software Application 79

[2.03](#_heading=h.1x0gk37) Surveillance User Interface (UI) 79

[2.04](#_heading=h.4h042r0) Server Administrator User Interface Requirements 79

[2.05](#_heading=h.2w5ecyt) Unified Web Interface (UWI) General Requirements 80

[2.06](#_heading=h.1baon6m) Health Monitor 81

[2.07](#_heading=h.3vac5uf) USP General Requirements 82

[2.08](#_heading=h.2afmg28) USP Architecture 84

[2.09](#_heading=h.pkwqa1) USP ALPR, Video, and Access Control Unification 88

[2.10](#_heading=h.39kk8xu) USP Threat Levels *(Specifier, Professional and Enterprise)* 89

[2.11](#_heading=h.1opuj5n) USP Remote Task 89

[2.12](#_heading=h.48pi1tg) USP Advanced Task Management 90

[2.13](#_heading=h.2nusc19) USP Reporting 90

[2.14](#_heading=h.1302m92) USP Dashboards 91

[2.15](#_heading=h.3mzq4wv) USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)* 92

[2.16](#_heading=h.2250f4o) USP User and User Group Security, Partitions, and Privileges Management 93

[2.17](#_heading=h.haapch) USP Event/Action Management 94

[2.18](#_heading=h.319y80a) USP Schedules and Scheduled Tasks 96

[2.19](#_heading=h.1gf8i83) USP Macros and Custom Scripts 96

[2.20](#_heading=h.40ew0vw) USP Dynamic Graphical Maps (DGM) 96

[2.21](#_heading=h.2fk6b3p) USP Audit and User Activity Trails (Logs) 100

[2.22](#_heading=h.upglbi) USP Incident Reports 101

[2.23](#_heading=h.3ep43zb) USP Data Ingestion 101

[2.24](#_heading=h.1tuee74) USP Third Party Integration 102

[2.25](#_heading=h.4du1wux) USP Software Development Kit (SDK) 107

[Part 3 - Execution 108](#_heading=h.2szc72q)

[3.01](#_heading=h.184mhaj) Warranty 108

[3.02](#_heading=h.3s49zyc) Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 108

[3.03](#_heading=h.279ka65) Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)* 110

[**Section 28 23 00 – Video Management System 111**](#_heading=h.meukdy)

[Part 1 - General 111](#_heading=h.36ei31r)

[1.01](#_heading=h.1ljsd9k) Related Work 111

[1.02](#_heading=h.45jfvxd) Definitions 111

[1.03](#_heading=h.2koq656) Qualifications 111

[Part 2 - Products 112](#_heading=h.zu0gcz)

[2.01](#_heading=h.3jtnz0s) VMS General Requirements 112

[2.02](#_heading=h.1d96cc0) Cyber Security Requirements 114

[2.03](#_heading=h.3x8tuzt) Failover and Standby Requirements 116

[2.04](#_heading=h.2ce457m) Archiving 116

[2.05](#_heading=h.rjefff) Auxiliary Archiver *(Specifier, Enterprise only)* 121

[2.06](#_heading=h.3bj1y38) Standby Archiver *(Specifier, Enterprise only)* 121

[2.07](#_heading=h.1qoc8b1) Cloud Archiving 122

[2.08](#_heading=h.4anzqyu) VMS Media Streaming 123

[2.09](#_heading=h.2pta16n) VMS Video Archives Transfer capabilities 124

[2.11](#_heading=h.14ykbeg) Security Video Analytics 126

[2.12](#_heading=h.3oy7u29) Camera Integrity Monitor 127

[2.13](#_heading=h.243i4a2) Privacy Protector 128

[2.14](#_heading=h.j8sehv) People Counter 129

[2.15](#_heading=h.338fx5o) General Client Software Requirements 130

[2.16](#_heading=h.1idq7dh) Configuration User Interface (UI) 132

[2.17](#_heading=h.42ddq1a) VMS Client User Interface (UI) 134

[2.18](#_heading=h.2hio093) Server Administrator User Interface Requirements 140

[2.19](#_heading=h.wnyagw) Unified Web Interface (UWI) General Requirements 141

[2.20](#_heading=h.3gnlt4p) Smartphone and Tablet App General Requirements 143

[2.21](#_heading=h.1vsw3ci) Health Monitor 145

[2.22](#_heading=h.4fsjm0b) Session Initiation Protocol (SIP) Communication Management (CM) 146

[2.23](#_heading=h.2uxtw84) USP General Requirements 151

[2.24](#_heading=h.1a346fx) USP Architecture 153

[2.25](#_heading=h.3u2rp3q) USP Access Control, Video, and ALPR Unification 156

[2.26](#_heading=h.2981zbj) USP Threat Levels *(Specifier, Professional and Enterprise)* 158

[2.27](#_heading=h.odc9jc) USP Remote Task 158

[2.28](#_heading=h.38czs75) USP Advanced Task Management 159

[2.29](#_heading=h.1nia2ey) USP Reporting 159

[2.30](#_heading=h.47hxl2r) USP Dashboards 161

[2.31](#_heading=h.2mn7vak) USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)* 162

[2.32](#_heading=h.11si5id) USP Zone Management 162

[2.33](#_heading=h.3ls5o66) USP User and User Group Security, Partitions, and Privileges Management 163

[2.34](#_heading=h.20xfydz) USP Event/Action Management 164

[2.35](#_heading=h.4kx3h1s) USP Schedules and Scheduled Tasks 166

[2.36](#_heading=h.302dr9l) USP Macros and Custom Scripts 167

[2.37](#_heading=h.1f7o1he) USP Dynamic Graphical Maps (DGM) 167

[*2.38*](#_heading=h.3z7bk57) USP Digital Evidence Management System (DEMS) *(Specifier, Genetec Clearance, separate subscription required)* 172

[2.39](#_heading=h.2eclud0) USP Audit and User Activity Trails (Logs) 173

[2.40](#_heading=h.thw4kt) USP Incident Reports 173

[2.41](#_heading=h.3dhjn8m) USP Data Ingestion 174

[2.42](#_heading=h.1smtxgf) USP Third Party Integration 175

[2.43](#_heading=h.4cmhg48) USP Software Development Kit (SDK) 180

[Part 3 - Execution 181](#_heading=h.2rrrqc1)

[3.01](#_heading=h.16x20ju) Warranty 181

[3.02](#_heading=h.3qwpj7n) Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 181

[3.03](#_heading=h.261ztfg) Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)* 183

[**Section 28 51 00 – Information Management & Presentation 184**](#_heading=h.l7a3n9)

[Part 1 - General 184](#_heading=h.356xmb2)

[1.01](#_heading=h.1kc7wiv) Related Work 184

[1.02](#_heading=h.44bvf6o) Definitions 184

[1.03](#_heading=h.2jh5peh) Qualifications 184

[Part 2 - Products 185](#_heading=h.ymfzma)

[2.01](#_heading=h.3im3ia3) General Requirements 185

[2.02](#_heading=h.1xrdshw) CDMS Graphical User Interface 186

[2.03](#_heading=h.4hr1b5p) CDMS Incident Management 188

[2.04](#_heading=h.2wwbldi) CDMS Incident Report 192

[2.05](#_heading=h.1c1lvlb) CDMS Dynamic Document Management 193

[2.06](#_heading=h.3w19e94) CDMS Rules Engine 194

[2.07](#_heading=h.2b6jogx) CDMS Automation Workflow Engine 194

[2.08](#_heading=h.qbtyoq) CDMS Standard Operating Procedure 197

[2.09](#_heading=h.3abhhcj) Electronic Access Control System *(Specifier, select one of the following)* 198

[2.10](#_heading=h.1pgrrkc) Video Management System *(Specifier, select one of the following)* 198

[2.11](#_heading=h.49gfa85) Server Administrator User Interface Requirements 198

[2.12](#_heading=h.2olpkfy) Smartphone and Tablet App General Requirements 199

[2.13](#_heading=h.13qzunr) Health Monitor 202

[2.14](#_heading=h.3nqndbk) USP General Requirements 203

[2.15](#_heading=h.22vxnjd) USP Architecture 204

[2.16](#_heading=h.i17xr6) USP Access Control, Video, and ALPR Unification 208

[2.17](#_heading=h.320vgez) USP Threat Levels *(Specifier, Professional and Enterprise)* 209

[2.18](#_heading=h.1h65qms) USP Remote Task 210

[2.19](#_heading=h.415t9al) USP Advanced Task Management 211

[2.20](#_heading=h.2gb3jie) USP Reporting 211

[2.21](#_heading=h.vgdtq7) USP Dashboards 212

[2.22](#_heading=h.3fg1ce0) USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)* 213

[2.23](#_heading=h.1ulbmlt) USP Zone Management 214

[2.24](#_heading=h.4ekz59m) USP User and User Group Security, Partitions, and Privileges Management 215

[2.25](#_heading=h.2tq9fhf) USP Event/Action Management 216

[2.26](#_heading=h.18vjpp8) USP Schedules and Scheduled Tasks 217

[2.27](#_heading=h.3sv78d1) USP Macros and Custom Scripts 218

[2.28](#_heading=h.280hiku) USP Dynamic Graphical Maps (DGM) 218

[2.29](#_heading=h.n5rssn) USP Audit and User Activity Trails (Logs) 222

[2.30](#_heading=h.375fbgg) USP Incident Reports 223

[2.31](#_heading=h.1maplo9) USP Data Ingestion 223

[2.32](#_heading=h.46ad4c2) USP Third Party Integration 224

[2.33](#_heading=h.2lfnejv) USP Software Development Kit (SDK) 229

[Part 3 - Execution 230](#_heading=h.10kxoro)

[3.01](#_heading=h.3kkl7fh) Warranty 230

[3.02](#_heading=h.1zpvhna) Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 230

[3.03](#_heading=h.4jpj0b3) Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)* 232

1. **Section 28 13 00 – Access Control Software and Database Management**
   1. **General**
      1. Related Work
         1. Division 08 - Door Hardware
         2. Division 14 - General Elevator Requirements
         3. Section 28 23 00 – Video Surveillance
      2. Definitions
         1. ACS – Access Control System
         2. CSA – Client Software Application
         3. DGM – Dynamic Graphical Maps
         4. ALPR – Automatic License Plate Recognition
         5. SDK – Software Development Kit
         6. GLM – Genetec Lifecycle Management
         7. SSM – Server Software Module
         8. UI – User Interface
         9. USP – Unified Security Platform
         10. UWI – Unified Web Interface
         11. VMS – Video Management System
      3. Qualifications
         1. The system programmer shall have attended manufacturer training and obtained certification in Genetec™ Security Center - Synergis™ Technical Certification.
         2. Optionally, the system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Enterprise Technical Certification.
         3. The system programmer shall be a Genetec certified partner with the following level of qualification: *(Specifier, select one of the following)*
            1. Certified Reseller or up
            2. Elite Reseller or up
            3. Unified Elite Reseller
         4. The system programmer shall submit proof of certifications.
   2. **Products**
      1. Electronic Access Control System General Requirements
         1. The ACS shall be an enterprise class IP access control software solution. It shall be fully embedded within a Unified Security Platform (USP). The USP shall allow the seamless unification of the ACS with an IP video management system (VMS).
         2. The ACS shall be highly scalable to support configurations consisting of thousands of doors with facilities spanning multiple geographic areas.
         3. The ACS shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
         4. The ACS shall support a variety of access control functionalities, including but not limited to:
            1. Controller (Unit) management, door management, elevator management, and area management.
            2. Cardholder and cardholder group management, credential management, and access rule management.
            3. Badge printing and template creation.
            4. Visitor Management.
            5. People counting, area presence tracking, and mustering.
            6. Offering a framework for third party hardware integration such biometric, mobile readers, or other devices over IP.
         5. Manufacturer:
            1. Genetec Security Center SaaS: *(Specifier, select one of the following)*

Synergis Enterprise

Synergis Professional

Synergis Standard

* + - 1. Certification
         1. The ACS shall be certified

UL-294

ULC-S319

EN-60839-11-1

CSPN

* + - 1. The ACS shall support changing passwords of controller units (for a list of supported units, see the Security Center Administrator Guide):
         1. The ACS shall show the strength of the current unit password.
         2. The ACS shall have the ability to change the password manually or using a string password generator for single or multiple units.
         3. The ACS shall have the ability to automatically update passwords on schedule.
         4. The ACS shall keep the history for passwords and the ability to retrieve them.
         5. The ACS shall have the ability to export passwords of units for safekeeping.
      2. The ACS shall support managing certificates of controller units used for secure command and control (HTTPS and RTSPS) (for a list of supported units, see the Security Center Administrator Guide):
         1. Push Initial Certificate
         2. Automatically switch from HTTP and RTSP to HTTPS and RTSPS
         3. Allow certificate renewal
         4. Manage certificates manually for a single device or a batch of devices
         5. Automatically update upon configured schedule for single device or batch of devices
    1. Failover and Standby Requirements
       1. The USP shall support native and off-the-shelf failover options.
       2. Failover Directory *(Specifier, Enterprise only)*
          1. The Standby Directory shall act as a replacement SSM on hot standby, ready to take over as the acting Directory in case the primary Directory fails. The failover shall occur in less than 1 minute. No action from the user shall be required.
          2. The USP shall support up to five (5) Directories on standby, lined up to take over as the acting Directory in a cascading fashion.
          3. The Standby Directory shall keep its configuration database synchronized with the primary Directory.
          4. The Standby Directory shall support disaster recovery scenarios where a server can be located in another geographic area (or building) and only take over if all other Directories become offline.
          5. The Standby Directory shall support synchronization of the configuration databases using a backup and restore mechanism. The synchronization period shall be configurable from 15 minutes to 1 week.
          6. The Standby Directory shall support real-time synchronization of the configuration databases using SQL Mirroring or SQL Always On.
       3. Off-the-shelf standby/failover options (excluding the VMS Archiver) shall include: *(Specifier, Enterprise only)*
          1. Native role failover across multiple servers
          2. Windows Clustering

Starting from Security Center 5.11, support for NEC ExpressCluster X has been discontinued.

* + 1. ACS Access Management
       1. The ACS shall be based on an open architecture able to support multiple access control hardware manufacturers. The ACS shall be able to integrate with multiple non-proprietary interface modules and controllers, access readers, and other third-party applications.
       2. The ACS shall be an IP enabled solution. All communication between the ACS and hardware controllers shall be based on standard TCP/IP protocol.
       3. Access Manager Role
          1. The Access Manager Role shall be the server that synchronizes all access control hardware units under its control, such as door controllers and I/O modules. It shall also be able to validate and log all access activities and events when the door controllers and I/O modules are online.
          2. The Access Manager Role shall maintain the communication link with the hardware controllers under its control. It shall also continuously monitor whether the controllers are online or offline.
          3. Synchronization of hardware units shall be automated and transparent to users and shall occur in the background. It shall also be possible to manually synchronize units or to synchronize units on a schedule.
          4. The Access Manager Role shall support doors and controllers located within one or more facilities. The Access Server shall support a minimum of 200 readers and up to 2000 readers per computer.
       4. The Access Server shall store all access events associated with the doors, areas, hardware zones (hardware input points), elevators, and controllers under its direct control.
    2. ACS Global Cardholder Management *(Specifier, additional license required and Enterprise only for the central site)*
       1. The ACS shall support global cardholder management and synchronization between a central independent site and remote independent sites, all of which can have their own Directory and databases.
       2. It shall be possible to synchronize the following entities and their configuration data:
          1. Cardholders (incl. custom fields)
          2. Cardholder groups
          3. Credentials
          4. Badge templates
       3. Cardholders and other synchronized entities can be added centrally and synchronized to remote sites for central cardholder management.
       4. Cardholders and other synchronized entities can be added at remote sites and synchronized to the central site and other remote sites.
       5. The ACS shall support the assignment of a single card per cardholder across all of an organization’s sites.
       6. Manual and scheduled synchronization shall be supported.
    3. ACS Hardware Compatibility List
       1. The ACS shall have an open architecture that supports the integration of third-party IP-based door controllers and I/O modules. The ACS shall simultaneously support mixed configurations of access control hardware from multiple vendors.
       2. The ACS shall support SAM onboard to hold DESfire encryption keys.
       3. The ACS shall support embedded certificate validation engine.
       4. The ACS shall support the use of TLS 1.3 and certificates.
       5. The ACS shall support OSDP Secure Channel.
       6. The ACS shall support OSDP transparent reader mode to read DESfire credentials.
       7. The ACS shall support Manufacturer OSDP command.
       8. The ACS shall support multiple types of hardware devices: single-reader controllers, 2-reader controllers, 1- to 64-reader controllers, integrated readers and door controllers, and Power-over-Ethernet (PoE) enabled door controllers.
       9. The ACS shall support most industry standard card readers that output card data using OSDP and Wiegand protocol, SSCPv2, and Clock-and-Data.
       10. The ACS shall support the following IP-enabled controllers or devices. For a description of their capabilities, refer to the specific controller or device’s A&E specifications and design:
           1. Synergis Master Controller
           2. Synergis Cloud Link
           3. Synergis Cloud Link RoadRunner
           4. Synergis IX
           5. SharpV
           6. HID VertX EVO
           7. HID Edge
           8. HID Edge EVO
           9. PW6000 controllers
           10. PW7000 controllers
           11. PRO32 controllers
           12. PRO42 controllers
           13. Mercury EP controllers
           14. Mercury LP controllers
           15. Mercury SIO module
           16. Mercury M5 Bridge
           17. Mercury MS Bridge
           18. Assa Abloy Aperio RS485 8 to 1 hub
           19. Assa Aperio AH40 (IP) hub
           20. Assa Abloy IP Locks (no DSR required)

Corbin Russwin

Sargent Passport

Sargent Profile

IN120

IN220

* + - * 1. Salto Sallis RS485 and PoE routers
        2. Salto SVN
        3. Schlage AD-300 and AD-400 electronic locks
        4. Schlage Control wireless lock
        5. Schlage NDE, LE, FE, and BE Networked wireless Mortise lock
        6. Axis A1001
        7. Axis A1601
        8. A1210 power by Genetec
        9. A1610 power by Genetec
        10. STid RS485 readers
        11. SSCP readers

STid

* + - * 1. DDS AS34/TPL4
        2. SimonsVoss Smart Intego
        3. OSDP readers

HID

STid

Cidron

Allegion

Wavelynx

Deister

PHG

* + - 1. The following USB enrollment readers shall be supported: *(Specifier, additional license required)*
         1. RF Ideas pcProx HID USB reader for enrolling proximity cards
         2. RF Ideas AIR ID Enroll iCLASS ID# USB reader for enrolling HID iCLASS cards
         3. RF Ideas AIR ID Enroll 14443/15693 CSN USB reader for enrolling a MIFARE card using the CSN (card serial number)
         4. RF Idea AIR ID Enroll pcProx Plus w/iCLASS reader for enrolling proximity and iCLASS cards
         5. STid STR-W35-E/PH5-5AA
         6. HID Omnikey 5x2x USB readers
    1. Seamless Unification with VMS
       1. Through the USP, the ACS shall support integration with an IP Video Surveillance System or MVS. Integration with an IP video surveillance system shall permit the user to view live and recorded video.
       2. Users shall be able to associate one or more video cameras to the following entity types: doors, elevator and hardware zones (input points), and more.
       3. The Monitoring UI shall present a true Unified Security Interface for access control and video surveillance. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.
       4. It shall be possible to view video associated with access control events when viewing a report.
    2. ACS Controller (Unit) Management
       1. The ACS shall support the discovery, configuration, and management of IP enabled controllers and I/O panels (hardware units). A user shall be permitted to add, delete, or modify a controller if they have the appropriate privileges.
       2. The ACS shall support unit configuration through a preconfigured door template.
       3. The ACS shall support automatic unit discovery. The user shall establish the settings for discovery ports and for the types of unit discovery and the ACS shall automatically detect all connected devices.
       4. The ACS shall support a unit swap utility for swapping out an existing controller with a new controller. The unit swap utility shall avoid the reprogramming of the system whenever a unit is replaced. All logs and events from the old unit shall be maintained.
       5. The ACS shall support pre-configuration of the system prior to the physical hardware installation.
       6. The ACS shall support Firmware upgrade in bulk from the application.
       7. The ACS shall support MIFARE DESfire configuration central management.
       8. The ACS shall centrally manage unit password policy (password strength, rotation, bulk update).
    3. ACS Cardholder and Cardholder Group Management
       1. The ACS shall support the configuration and management of cardholders and cardholder groups. A user shall be able to add, delete, or modify a cardholder or cardholder group if they have the appropriate privileges.
       2. Custom fields shall be supported for both cardholders and cardholder groups.
       3. The ACS shall permit the following activation/expiration options for a cardholder’s profile: delayed activation of a cardholder’s profile, expiration based on the date of first use of credentials, or expiration on a user-defined date.
       4. It shall be possible to set a start date and expiration date for the association of a cardholder and an access rule for temporary access.
       5. It shall be possible to associate a picture to a cardholder’s profile. The picture shall be imported from a file, captured with a digital camera, or captured from a video surveillance camera. When a cardholder event occurs, the picture of the cardholder shall be displayed in the Monitoring UI. The ACS shall support multiple standard picture formats.
       6. Cardholder groups shall enable the grouping of cardholders to facilitate mass changes to system settings. It shall be possible to assign cardholder groups to access rules, thus avoiding the assignment of one cardholder at a time.
       7. It shall be possible to search by picture association, custom fields, names, and credential codes.
       8. It shall be possible to select multiple cardholders for immediate deactivation or reactivation.
       9. The ACS shall support the synchronization of cardholders and cardholder groups through Active Directory including the credentials and pictures of the cardholders. *(Specifier, first license of Active Directory integration is included, up to 9 additional connections can be added, available in Professional and Enterprise).* It shall be possible to import cardholders from Azure AD.
       10. It shall support the ability to track unused credentials for x days.
       11. It shall support the import of cardholders, credentials, and custom fields from an external system database or CSV.
    4. ACS Credential Management
       1. The ACS shall support the configuration and management of credentials, for example access cards and keypad PIN numbers. A user shall be able to add, delete, or modify a credential if the user has the appropriate privileges.
       2. The ACS shall support reader transparent mode.
       3. Users shall be able to add Custom Fields (user-defined fields) to credentials. Creating a new credential shall be accomplished either manually or automatically.
       4. Automatic creation shall allow the user to create a credential entity by presenting a credential to a selected reader. The ACS shall read the card data and associate it to the credential entity. It shall be possible to automatically enroll any card format.
       5. The ACS shall support high assurance credentials using validation of a certificate, such as PIV, PIV-I, and CIV.
       6. The ACS shall support multiple credentials per cardholder without necessitating duplicate cardholder information. The ACS shall automatically detect and prevent attempts to register an already-registered credential.
       7. It shall be possible to natively encode DESfire credentials from the user interface using customer’s own keys and configuration.
       8. Batch enrollment of credentials shall be supported.
       9. The ACS shall provide a workflow for badge issuance and card requests.
       10. The ACS shall support the use of license plates as a credential.
       11. The ACS shall support duress pin.
       12. The ACS shall natively support the creation and management of mobile IDs in the same way as other credentials.
       13. The ACS shall support the ability to print and enroll credentials *(Requires a license)*.
       14. The ACS shall support the ability to print and encode SEOS and MIFARE credentials *(Requires a license)*.
    5. ACS Custom Card Formats
       1. A custom card format feature shall allow the administrator to add additional custom card formats using an intuitive tool within the Configuration UI. The custom card format tool shall be flexible in the following ways:
          1. Once enrolled, new custom card formats shall appear in the card format lists for manual card enrollment.
          2. An unrestricted number of additional custom card formats can be added.
          3. Shall support credential with up to 512 bits.
          4. The administrator shall be able to set the following options when defining a new format:

The order in which card fields appear in the user interface or CSA.

Whether a field is hidden from or visible to an operator.

Whether a field is read only or modifiable by an operator.

Complex parity checking schemes.

The order and location of a field’s data. Location can be defined on a bit-by-bit basis.

Application ID and keys for DESfire EV1 credentials.

* + 1. ACS Badge Designer
       1. The badge designer shall allow the creation of badge templates that define the content and presentation format of a cardholder badge to be printed.
       2. Badge production shall consist of selecting the credential, the badge template, and clicking print.
       3. Batch printing of cards shall be available.
       4. The contents of a badge template can include: cardholder’s first and last name, picture, custom fields, bitmap graphics, lines, ovals, rectangles, dynamic text labels linked to custom fields and static text labels, and barcodes (Interleaved 2 of 5, Extended Code 39).
       5. Copy and paste of badge template objects shall be available.
       6. It shall be possible to set the border thickness and color, the fill color of badge objects (content), and the color of text labels.
       7. Settings, such as object transparency, text orientation, and auto-sizing of text shall be available or transparent to the user.
       8. Supported badge formats shall be (portrait and landscape): CR70 (2.875" x 2.125"), CR80 (3.37" x 2.125"), CR90 (3.63" x 2.37"), CR100 (3.88" x 2.63"), and custom card sizes.
       9. Dual-sided badges shall be supported.
       10. A badge template import and export function shall be available to allow the sharing of badge templates between distinct or independent ACS.
       11. Chromakey shall be supported.
    2. ACS Door Management
       1. The ACS shall support the configuration and management of doors. A user shall be able to add, delete, or modify a door if they have the appropriate privileges.
       2. The ACS shall permit multiple access rules to be associated to a door.
       3. It shall be possible to unlock all doors from an area at once.
       4. The ACS shall support the following forms of authentication: Card Only, Card or Keypad (PIN), or Card and Keypad (PIN). It shall be possible to define a schedule for when Card Only or Card and Keypad authentication modes shall be required.
       5. It shall be possible to set an extended grant time on a per-door basis (in addition to the standard grant time). Cardholder properties shall include the option of using the extended grant time. When flagged cardholders are granted access, the door shall be unlocked for the duration of the extended grant time instead of the standard grant time.
       6. The ACS shall allow the configuration of the relocking mode on doors such as on door open, after a definite time, or on door close.
       7. The ACS shall support the ability to enforce the use of two valid reads from different cardholders to grant access to an area.
       8. The ACS shall support the ability to enable access rules for other cardholders once a supervisor has accessed an area.
       9. The ACS shall support the ability to enable unlocking schedule on a door once an employee has entered the facility.
       10. Readerless doors.
           1. The ACS shall support doors configured solely with a lock, a REX, and a door contact but without readers.
           2. The implementation of a readerless door shall be possible with the use of standard access hardware IO modules. External hardware, such as timers, shall not be required.
           3. Unlocking schedules shall be programmable for readerless doors.
           4. Standard door activity reports shall also be possible with readerless doors.
       11. Unlocking schedules and exceptions to unlocking schedules shall be associated with a door. An unlocking schedule shall determine when a door should be automatically unlocked. The ACS shall also support the use of a specific offline unlocking schedule. Exceptions to unlocking schedules shall be used to define time periods during which unlocking schedules shall not be applied, such as during statutory holidays.
       12. The ACS shall support one or more cameras per door. Video shall then be associated to door access events, such as access grant or access denied.
    3. ACS Elevator Management
       1. The ACS shall support the configuration and management of elevators. A user shall be able to add, delete, or modify an elevator if they have the appropriate privileges.
       2. The ACS shall be able to control access to specific floors using a reader within the elevator cab. Control shall be available through the use of a controller with an interface to a reader and to multiple output modules with relays.
       3. Elevator floor selections shall be tracked using a controller with an interface to multiple input modules. Floor tracking shall be available within an elevator activity report.
       4. The elevator control module shall continue to function in offline mode should communication between the ACS and the controller fail.
       5. The ACS shall support one or more cameras per elevator cab. Video shall then be associated to elevator access events, such as access granted or access denied.
       6. Integrating access and monitoring to elevator dispatch systems shall be supported for:

Kone

Thyssenkrupp

Otis

MCE

* + 1. ACS Visitor Management
       1. The ACS shall support the configuration and management of visitors. A user shall be able to enroll or remove a visitor if they have the appropriate privileges. The ACS shall support the check-in and check-out of visitors from the Monitoring UI.
       2. A visitor check-in wizard shall facilitate the enrollment process, allowing a user to specify the visitor’s specific information.
       3. It shall be possible to set a host leading a group of visitors and a trailing host walking behind visitors, triggering alert if a visitor is not following the delegation.
       4. The ACS shall permit the following credential options during visitor check-in:
          1. Use an existing credential.
          2. Automatically create a new credential.
          3. Manually create a new credential.
       5. The ACS shall support the creation of a pool of visitor credentials in advance. Existing visitor credentials shall be assigned to visitors during the check-in process.
       6. The ACS shall permit cardholder groups to be designated as “available for visitors”. Users shall be able to define the access privileges for the cardholder groups (visitor cardholder groups) in advance. During visitor check-in, the user shall select the appropriate visitor cardholder group to associate with a visitor. All of the visitor cardholder group access privileges shall be automatically transferred to the visitor. This feature shall permit the creation of multiple types of visitor groups and associated privileges, such as for contractors, VIPs, and day visitors. Visitors added to a visitor cardholder group in the Monitoring UI shall be automatically updated in the Configuration UI cardholder group screen.
       7. A visitor’s profile shall support the real-time modification of visitor information after a visitor has checked in.
       8. The ACS shall also provide comprehensive visitor tracking and visitor reporting. Through the real-time tracking feature, the ACS shall generate a real-time and historical visitor activity listing in the Monitoring UI. The ACS shall also generate visitor-specific reports that provide comprehensive listings of visitors as well as full details on their movement.
       9. It shall be possible to exempt a visitor from any antipassback rules in effect.
       10. The operator shall be able to print visitor badges during the check-in process. The printing of both paper badges (visitor without an assigned credential) and actual credentials shall be supported.
       11. Visitor management and reporting shall be available through the Web interface as well.
       12. It shall be possible to locate a visitor’s information or profile by swiping the visitor’s credential (card) at a USB reader.
       13. It shall be possible to tag the person visited to the visitor’s profile.
       14. It shall be possible to require that the visitor must have an escort to enter an area and that the escort must badge-in to confirm the access of the visitor.
       15. The ACS system shall support third-party visitor management solutions. It shall also be possible to delete visitor historical data after a set interval. *(Specifier, additional license required)*
    2. ACS People Counting & Area Presence Tracking (Mustering)
       1. The ACS shall support people counting (or area presence tracking). The ACS shall be able to monitor and report the number of cardholders in an area in real-time and for all areas. Monitoring shall be based on the entire access control infrastructure, for both local areas and those in remote geographic locations. People counting can also be used to perform mustering.
       2. It shall be possible to control the maximum occupancy of an area by setting a threshold and user notification when reaching the limit.
       3. The ACS shall report area presence counts in the UI. Area presence tracks shall dynamically track the total number of cardholders in an area. Displayed data shall be updated dynamically.
       4. The ACS shall support mustering through the use of mobile readers (requires additional software and hardware from third-party).
       5. The ACS shall provide a native dedicated mustering task using a USB, mobile, or wall reader.
       6. The ACS shall be able to generate an area presence report listing the cardholders located in one or more areas, accessible through the Monitoring UI. It shall be possible to filter the report by area and time period. The report shall also include activity from sub-areas (nested areas).
       7. Through people counting, the ACS shall be able to generate First Person In and Last Person Out events. The First Person In event shall detect when the first cardholder enters an empty area. The Last Person Out event shall detect when the last cardholder leaves an area. It shall be possible to trigger actions from both events such as sending a message or triggering an alarm.
       8. The ACS shall be able to determine the entry of a cardholder based on a dedicated sensor.
       9. The ACS shall provide a visual HTML dashboard to aid with the evacuation that can run on mobile devices.
       10. The ACS shall provide the ability to globally view all evacuations simultaneously or per area.
       11. On an evacuation, the ACS shall set all cardholders as unknown until they reach a mustering point.
       12. It shall be possible to mark a cardholder as safe or unsafe from the web evacuation assistant.
       13. It shall be possible to filter by cardholder groups or custom fields in the mustering dashboard.
       14. It shall be possible to use ID scanner to enroll visitors.
       15. The ACS shall support wall-mounted readers and mobile-handled devices for mustering.
       16. The ACS shall provide distinct visual indication as an area is being evacuated.
       17. The ACS shall have the ability to configure a mustering point per area.
       18. The ACS shall have the ability to reset APB at the end of an evacuation.
    3. ACS Custom Fields (User-Defined Fields)
       1. The ACS shall permit the creation of custom fields. Up to 1,000 custom fields shall be supported.
       2. Custom fields shall be supported for the following entities: cardholders, cardholder groups, credentials, and visitors.
       3. Supported custom fields shall include text, integers, decimal numbers, dates, Boolean, and images (graphics).
       4. Users shall be able to define a default value for a custom field.
       5. The creation of new custom field types shall be possible. New custom field types shall be based on the standard custom fields supported. They shall support user-defined values from which an operator must make a selection.
       6. Administrators have the ability to define which users can view and modify specific custom fields. This shall limit the access to custom field data to users with pre-defined privileges. The ACS shall support querying and report generation using custom fields.
       7. Custom fields can be grouped and ordered within these groups as defined by the user.
       8. Values for custom fields can be imported using the Import Tool.
    4. ACS Import Tool
       1. The ACS shall support an integrated Import Tool to facilitate the import of existing cardholder and credential data. The import of data shall be through the use the CSV file format. The tool shall be available from the Configuration UI.
       2. It shall be possible to connect to an external Microsoft SQL or Oracle database to import cardholders.
       3. The Import Tool shall also support the ability to manually import data that has been exported from a third-party database if it is in CSV format.
       4. The import tool shall permit the import of the following data:
          1. Cardholder name, descriptions, picture, email, and status.
          2. Cardholder group information.
          3. Credential name, status, format, and card number (including credentials with custom formats).
          4. Partition information.
          5. Custom fields.
          6. Activation date and expiration date.
          7. Update cardholder group association.
       5. Full flexibility in selecting the fields to be imported during an import session shall be available.
       6. The option to use a custom and unique cardholder key shall be specified during the import process to ensure that cardholders with duplicate names will not have their data overwritten. Cardholder key generation shall be automated. The end user shall have the option to select which fields will be used to create this unique key, for example credential number, custom fields, or cardholder name.
       7. The ACS shall also support re-importing a CSV file containing new information to update existing information in the ACS database. Re-importing shall enable bulk amendments to existing access control data.
    5. General Client Software Requirements
       1. The Client Software Applications (CSA) shall provide the user interface for USP configuration and monitoring over any network and be accessible locally or from a remote connection.
       2. The CSA shall consist of the Configuration UI for system configuration and the Monitoring UI for monitoring. The CSA shall be Windows-based and provide an easy-to-use graphical user interface (UI).
       3. The CSA for monitoring shall support running in 64-bit mode.
       4. The Server Administrator shall be used to configure the server database(s). It shall be web-based and accessible locally on the SSM or across the network.
       5. The CSA shall seamlessly merge access control, license plate recognition (ALPR), and video functionalities within the same user application.
       6. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and the .NET software framework.
       7. All applications shall provide an authentication mechanism, which verifies the validity of the user. As such, the administrator (who has all rights and privileges) can define specific access rights and privileges for each user in the system.
       8. Logging on to a CSA shall be done either through locally stored USP user accounts and passwords or using the operator’s Windows credentials when Active Directory integration is enabled. *(Specifier, Professional and up, first license of Active Directory integration included, additional licenses required for more)*
       9. When integrated with Microsoft’s Active Directory, the CSA and USP shall authenticate users using their Windows credentials. As a result, the USP will benefit from Active Directory password authentication and strong security features. *(Specifier, Professional and up, first license of Active Directory integration included, additional licenses required for more)*
       10. When integrated with an external identity provider such as Windows Active Directory, ADFS (Active Directory Federation Services) or an Open ID Connect/SAML2 identity provider (ex.: Azure AD), the CSA and USP shall authenticate using a Single-Sign On experience to the users. As a result, the USP will benefit from reusing the same credential throughout enterprise applications. *(Specifier, Professional and up).*
       11. The CSA shall support multiple languages, including but not limited to the following: 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, and Vietnamese.
       12. To enhance usability and operator efficiency, the Configuration UI and Monitoring UI shall support many of the latest UI such as:
           1. A customizable Home Page that includes favorite and recently used tasks.
           2. Task-oriented approach for administrator/operator activities where each type of activity (surveillance, visitor management, individual reports, and more) is an operator task.
           3. Consolidated and consistent workflows for video, ALPR, and access control.
           4. Single click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or track.
       13. Configuration UI and Monitoring UI Home Page and Tasks
           1. The Configuration UI and Monitoring UI shall be task oriented.
           2. A task shall be user interface design patterns whose goal is to simplify the user interface by grouping related features from different systems such as video and access, in the same display window. Features shall be grouped together in a task based on their shared ability to help the user perform a specific task.
           3. Tasks shall be accessible via the Home Page of either the Configuration or the Surveillance CSA.
           4. Newly created tasks shall be accessible via the Configuration UI or the Monitoring UI taskbar.
           5. Similar tasks shall be grouped into the following categories:

Operation: Access control management, LRP management, and more.

Investigation: access control activity reports, visitor activity reports, alarm reports, and more.

Maintenance: Access control, troubleshooters, audit trails, health-related reports, and more.

* + - * 1. An operator shall be able to launch a specific task only if they have the appropriate privileges.f
        2. The Home Page content shall be customizable through the use of privileges to hide tasks that an operator should not have access to and through a list of favorite and recently used tasks. In addition, editing a USP XML file to add new tasks on the fly shall also be possible.
        3. The configuration of the operator parameters shall be able to be imported and exported for both the Configuration and Monitoring UI.
      1. The Contractor shall provide up to XX number of simultaneous Clients, including thick client, Web, and mobile connections*. (Specifier, client connections are concurrent, the first 5 client connections are included, specify a Site License after 40 client connections (Enterprise only))*
    1. Configuration User Interface (UI)
       1. General
          1. The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration. The Configuration UI shall provide decentralized configuration and administration of the USP system from anywhere on the IP network.
          2. The configuration of all embedded ACS, VMS, and ALPR systems shall be accessible via the Configuration UI.
          3. The Configuration UI shall have a home page with single-click access to various tasks.
          4. The Configuration UI shall include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.
          5. The Configuration UI shall include a static reporting interface to:

View historical events based on entity activity. The user shall be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view.

View audit trails that show a history of user/administrator changes to an entity.

* + - * 1. Common entities such as users, schedules, alarms, and many more, can be reused by all embedded systems (ACS, VMS, and ALPR).
    1. ACS Client User Interface (UI)
       1. The Monitoring UI shall fulfill the role of a Unified Security Interface that is able to monitor video, ALPR, and access control events and alarms, as well as view live and recorded video.
       2. The Monitoring UI shall provide a graphical user interface to control and monitor the USP over any IP network. It shall allow administrators and operators with appropriate privileges to monitor their unified security platform, run reports, and manage alarms.
       3. To enhance usability and operator efficiency, the Monitoring UI shall support the following UI concepts:
          1. Dynamically adaptive interface that adjusts in real-time to what the operator is doing.
          2. Dynamic controls loaded with entity-specific widgets (for example, door and camera widgets).
          3. Use of transparent overlays that can display multiple types of data in a seamless fashion.
          4. Display tile menus and quick commands.
          5. Consolidated and consistent workflows.
          6. Tile menus and quick commands easily accessible within every display tile of the user workspace.
          7. Single-click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or to track.
       4. Monitoring UI Home Page and Tasks
          1. Similar tasks shall be grouped into the following categories:

Operation: Access control/LRP/video surveillance, visitor management, mustering, access control and video alarm monitoring, and more.

Investigation: Video bookmark/motion/archive reports, access control activity reports, visitor activity reports, alarm reports, ALPR activity reports, and more.

Maintenance: Access control and video configuration reports, troubleshooters, audit trails, and more.

* + - 1. Dynamically Adaptive UI, Controls section, and Widgets
         1. The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI Controls section.
         2. Widgets shall be mini-applications or mini-groupings in the Monitoring UI Controls section that let the operator perform common tasks and provide them with fast access to information and actions.
         3. With a single click on an entity (for example, door or camera) the specific widgets associated to that entity appear and other non-relevant widgets disappear dynamically (instantly). Widgets shall bring the operator information such as door status and camera stream information, as well as user actions, such as door unlock, PTZ controls, and more.
         4. Specific widgets include those for a door, camera, alarm, zone, display tile, video stream (statistics), PTZ camera, and more.
      2. Operator Workflows
         1. A workflow shall be a sequence of operations an operator or administrator shall execute to complete an activity. The “flow” relates to a clearly defined timeline or sequence for executing the activity.
         2. The Monitoring UI shall be equipped with consistent workflows for the ALPR, video, and access control systems that it unifies.
         3. Generating or printing a report, setting up or acknowledging an alarm, or creating an incident report shall follow the same process (workflow) whether the operator is working with video, ALPR, or access control, or with both video and access control.
      3. Each task within the Monitoring UI shall consist of one or more of the following items:
         1. Event list.
         2. Logical tree. Doors, cameras, zones, ALPR units, and elevators shall be grouped under Areas in a hierarchical fashion.
         3. Entities list of all entities being tracked.
         4. Display tiles with various patterns (1 x 1, 2 x 2, and more).
         5. Display tile menu with various commands related to cameras, doors, PTZ, and tile controls.
         6. Control section with widgets.
      4. The Monitoring UI shall support multiple event lists and display tile patterns, including:
         1. Event/alarm list layout only
         2. Display tile layout only
         3. Display tile and alarm/event list combination
         4. ALPR map and alarm/event list combination
      5. User workspace customization
         1. The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.
         2. Once customized, the user shall be able to save their workspace.
         3. The user workspace shall be accessible by a specific user from any client application on the network.
         4. Display tile patterns shall be customizable.
         5. Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.
         6. The Monitoring UI shall support multiple display tile patterns (e.g., 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).
         7. The Monitoring UI shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.
         8. Additional customization options include show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.
      6. The Monitoring UI shall provide an interface to support the following tasks and activities common to access control, ALPR, and video:
         1. Monitoring the events from a live security system (ACS and/or VMS and/or ALPR).
         2. Generating reports, including custom reports.
         3. Monitoring and acknowledging alarms.
         4. Creating and editing incidents and generating incident reports.
         5. Displaying dynamic graphical maps and floor plans, as well as executing actions from dynamic graphical maps and floor plans.
         6. Management and execution of hot actions and macros.
      7. The Monitoring UI shall be able to monitor the activity of the following entities in real-time: areas, ALPR entities, doors, elevators, cameras, cardholders, cardholder groups, zones (input points), and more. The Monitoring UI shall provide an interface to support the following access control tasks and capabilities:
         1. Monitoring and management of access events and alarms.
         2. Viewing of cardholder picture or badge IDs.
         3. Verification of cardholder picture IDs against live video.
         4. Visitor management.
         5. People counting or mustering, including resetting the people count in an area.
         6. Door control, including remotely unlocking doors, overriding a door’s unlocking schedules, and enabling door maintenance mode.
         7. Forgiving antipassback.
         8. Generation of ACS configuration and activity reports.
         9. Viewing of HTML files including alarm instructions.
      8. Entity Monitoring
         1. The USP shall permit the user to select multiple entities to monitor from the Monitoring UI by adding the entities one by one to the tracking list.
         2. The Monitoring UI shall provide the option to filter which events shall be displayed in the display tile layout, event list layout, or both.
         3. It shall be possible to lock a Monitoring UI display tile so that it only tracks the activity of a specific entity (for example, a specific door or camera).
         4. The user shall be able to drag and drop an event from an event list (or an alarm from an alarm list) onto a display tile to view a license plate read, cardholder picture ID, badge ID, or live/archived video, among other options.
         5. Event, alarm, monitoring/tracking, and report lists shall contain cardholder pictures where applicable.
         6. The user shall be permitted to start or pause the viewing of events within each display tile.
      9. Display Tile Packing and Unpacking
         1. The Monitoring UI shall support single-click unpacking and packing for areas, doors, zones, and alarms.
         2. The packing and unpacking of entities shall allow operators to quickly obtain additional information and camera views of a specific entity.
         3. The unpacking of an entity shall display associated entities. For example, unpacking a door with multiple associated cameras shall display all cameras associated with that door. Unpacking shall reconfigure the display tiles to be able to display all associated entities. For example, unpacking a door (or a zone or alarm) that is currently in a 1 x 1 tile configuration and that has 3 cameras tied to it will create a 1 x 3 display tile arrangement for viewing all associated entities.
         4. Packing will return the display to the original tile pattern.
      10. The following additional tools or utilities shall be available from the Monitoring UI: create credentials, create cardholders, and access control troubleshooter.
    1. Server Administrator User Interface Requirements
       1. The Server Administrator shall be used to configure the SSM and the Directory Role (main configuration) and its database(s), to apply the license, and more.
       2. The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.
       3. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.
       4. The Server Administrator shall allow the administrator (user) to perform the following functions:
          1. Manage the system license.
          2. Configure the database(s) and database server for the Directory Role.
          3. Activate/Deactivate the Directory Role.
          4. Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.
          5. Define the client-to-server communications security settings.
          6. Configure the network communications hardware, including connection addresses and ports.
    2. Unified Web Interface (UWI) General Requirements
       1. The USP shall support a unified web interface (UWI) for access control, video, and automatic license plate recognition (ALPR).
       2. The UWI shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.
       3. The UWI shall be platform independent and run within Microsoft Edge, MS Internet Explorer, Firefox, Safari, and Google Chrome.
       4. The UWI shall be designed as an HTML5 application.
       5. The UWI shall support display on tablet format.
       6. The UWI will support native H.264 video in the web interface.
       7. Web pages for the web interface shall be managed and pushed by the Web Interface Server. Microsoft IIS or any other web hosting service shall not be required given that all the web pages shall be hosted by the Mobile Server.
       8. The Web Interface Server shall provide the ability to define a unique URL to access the web interface, to ensure the security of the application.
       9. The UWI shall provide the ability to load a camera layout.
       10. The UWI shall provide the ability to configure, save, and reload private camera layouts.
       11. The UWI shall provide the ability to control PTZ cameras.
       12. Functionalities:
           1. Log in support shall be available using:

Username and password

Active Directory *(Specifier, Professional and up, first Active Directory integration included, addition licenses required for more)*

Azure Active Directory, ADFS, OpenID Connect or SAML2 identity provider *(Specifier, Professional and up, additional license required for OIDC & SAML2)*

* + - * 1. Ability for user to change their password.
        2. Encrypted communications for all transactions.
        3. Print reports and export to CSV file. Unified reports that can be printed, exported to CSV file, and filtered by:

Alarms

Bookmarks

Camera & door events

ALPR hits & reads

Incidents

Time period or specific dates

Specific area

* + - * 1. Access Control.

Cardholder and group (add/modify/delete)

Credential management (add/modify/delete)

Access rules management (add/modify/delete)

Visitor management (check-in/modify/check-out)

Unlock door

Override the unlocking schedule on a door

Door Activities report

* + - * 1. Alarms.

Alarm report

* + - * 1. Threat Level management.
        2. Automatic License Plate Recognition (ALPR).

Live monitoring of the ALPR cameras

ALPR reads and hits report

Addition of plate numbers to hotlists

* + - * 1. Maps.

Ability to display a geographical map with USP entities geo-located on the map.

Ability to view any entity configured on the map.

Ability to search for entities or locations on the map.

Display locations of Mobile users.

* + - * 1. Incident management.

Ability to view active incidents, sort and group them for a customized view.

Ability to trigger incidents manually.

Ability to get all details about an incident including related incidents, entities and documents.

Ability to take ownership of an incident and respond to the defined standard operating procedure geared towards incident resolution.

* + - * 1. Watchlist to monitor specific entities of interest.
    1. Smartphone and Tablet App General Requirements
       1. The USP shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the USP over any Wi-Fi or cellular network connection.
       2. Mobile apps shall communicate with the USP via a Mobile Server Role (MSR). All communication between the mobile apps and MSR shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.
       3. Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):
          1. Apple devices running iOS 13.0 or later
          2. Android devices 10.0 or later
       4. It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play).
       5. It shall be possible to push configuration to mobile devices through a Mobile Device Management solution such as VMWare Workspace One or Microsoft Intune.
       6. Functionalities
          1. Core

Ability to logon/logoff the UPS using an authorized use profile of the system.

Ability to support passive authentication from a single sign-on provider (OpenID Connect or SAML2 identity provider).

Ability to use biometric features (thumbprint, face ID, etc.) to perform connection to the system.

Ability to change the picture or the password of the user of the mobile app.

Ability to view the current Threat Level of the system.

Ability to change the current Threat Level of the system.

Ability to execute hot actions configured in the user profile.

Ability to view entities from the USP:

Cameras

Doors

ALPR cameras

Web Tile Plugins

Layouts

Camera Sequences

Macros

Maps (geographical maps only) *(Specifier, Professional and Enterprise)*

Ability to navigate the system hierarchical view of the entities and search entities in the system.

* + - * 1. Video

Ability to view live and recorded video from the cameras of the USP. A maximum of eight cameras shall be displayed.

Ability to view video in native format (H.264).

Ability to display live and recorded video side-by-side for a specific camera.

Ability to perform digital zoom on cameras.

Ability to perform actions on cameras, such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, and start/stop recording.

Ability to view camera layouts.

Ability to view camera sequences.

Ability to run a camera events report.

Ability to change the video quality on the cameras displayed on the mobile app.

Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system

* + - * 1. Access Control

Ability to view the door state and the door lock state.

Ability to perform actions on a door such as unlock the door, set the door in maintenance mode, and override the door unlocking schedule.

Ability to manage cardholders, including changing or taking their picture and managing their credentials.

* + - * 1. Automatic License Plate Recognition

Ability to view live events raised by an ALPR camera.

Ability to view the read image, context image, and all metadata captured by the ALPR camera.

Ability to run an ALPR event report.

Ability to add a license plate to a hotlist on the system.

* + - * 1. Alarm Management

Ability to receive push notifications to notify mobile operators that an alarm was received.

Ability to view all active alarms assigned to the mobile operator.

Ability to perform action on an alarm such as acknowledge, investigate, or alternate-acknowledge an active alarm.

Ability to view entities attached to the alarm.

* + - * 1. Map *(Specifier, Professional and Enterprise)*

Ability to display a geographical map with USP entities geo-located on the map.

Ability to view any entity configured on the map.

Ability to go to pre-defined map locations using preset buttons.

Ability to search for entities or locations on the map.

* + - * 1. Incident management

Ability to view active incidents, sort and group them for a customized view.

Ability to trigger incidents manually.

Ability to get all details about an incident including related incidents, entities and documents.

Ability to take ownership of an incident and respond to the defined standard operating procedure geared towards incident resolution.

* + - 1. It shall be possible to send a message from the client user interface to a mobile operator.
      2. It shall be possible to send a live or playback video sequence from the client UI to a mobile operator.
      3. It shall be possible to view mobile operators who enabled location tracking on a map in the system. The location of the mobile operator should be updated in real time. *(Specifier, Professional and Enterprise)*
    1. Health Monitor
       1. The USP shall monitor the health of the system, log health-related events, and calculate statistics.
       2. USP services, roles, agents, units, and client apps will trigger health events.
       3. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.
       4. A dedicated role, the Health Monitoring Role, shall perform the following actions:
          1. Monitor the health of the entire system and log events.
          2. Calculate statistics within a specified time frame (hours, days, months).
          3. Calculates availability for clients, servers and video/access/ALPR units.
       5. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.
       6. A Health Monitoring dashboard task shall be available in the client application user interface to provide a live display, such as pie charts and event lists, for quick visual assessment on the general health of the system.
       7. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.
       8. Detailed system care statistics will be available through a web-based dashboard providing health metrics of USP entities and roles, including Uptime and mean-time-between-failures.
       9. All health events raised in the system can be used for automating the USP event/action management.
       10. Health events shall be accessible via the SDK (can be used to create SNMP traps).
       11. The Hardware inventory report shall display levels of encryption, password strength, and recommended firmware version.
       12. It shall be able to centrally manage firmware upgrades through the hardware inventory report allowing mass unit update or schedule future update.
    2. USP General Requirements
       1. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.
       2. The USP shall support the seamless unification of IP access control system (ACS), IP video management system (VMS), and IP automatic license plate recognition system (ALPR) under a single platform. The USP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, and reporting of embedded ACS, VMS and ALPR systems, and associated edge devices.
       3. Functionalities available with the USP shall include:
          1. Configuration of embedded systems, such as ACS, ALPR, and VMS systems.
          2. Live event monitoring.
          3. Live video monitoring and playback of archived video.
          4. Alarm management.
          5. Reporting, including creating custom report templates and incident reports.
          6. The Federation™ feature for global monitoring, reporting, and alarm management of multiple remote and independent ACS, VMS, and or ALPR systems spread across multiple facilities and geographic areas*. (Specifier, Enterprise only, additional license required)*
          7. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system. *(Specifier, Enterprise Only, additional license required for each site)*
          8. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts. *(Specifier, Professional and up, first integration included, addition licenses required for more)*
          9. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming). *(Specifier, Professional and up, additional license required)*
          10. SIP Intercom device integration for bi-directional communication.
          11. Integration with third party systems and databases via plug-ins (access control, video analytics, point of sale, and more). *(Specifier, Professional and up, additional license required)*
          12. Dynamic graphical map viewing.
          13. Asset management system integration. *(Specifier, Professional and up, additional license required)*
       4. The USP shall be deployed in one or more of the following types of installations:
          1. Unified access, ALPR, video platform, and any combination thereof.
          2. Standalone access control, video, or ALPR platform.
          3. Unified access and video platform that federates multiple remote ACS, VMS, and ALPR.
          4. Standalone access control that federates multiple independent remote ACS.
       5. Licensing:
          1. A single central license shall be applied centrally on the configuration server.
          2. There shall be no requirement to apply a license at every server computer or client workstation.
          3. Based on selected options, one or more embedded systems shall be enabled or disabled.
       6. Hardware and Software Requirements:
          1. The USP and embedded systems (video, license plate recognition, and access control) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.
          2. The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.
          3. The USP database server(s) shall be built on Microsoft’s SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.
          4. The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.
          5. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and .NET software framework.
    3. USP Architecture
       1. The USP shall be based on a client/server model. The USP shall consist of a standard Server Software Module (SSM) and Client Software Applications (CSA).
       2. The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       3. The SSM shall be a Windows service that can be configured to start when the operating system is booted and run in the background. The SSM shall automatically launch at computer startup, regardless of whether or not a user is logged on the machine.
       4. Users shall be able to deploy the SSM on a single server or across several servers for a distributed architecture. The USP shall not be restricted in the number of SSM deployed.
       5. The USP shall support the concept of The Federation feature whereby multiple independent ACS, VMS, and ALPR installations can be merged into a single large virtual system for centralized monitoring, reporting, and alarm management. *(Specifier, Enterprise only, additional license required)*
       6. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
       7. The USP shall support up to one thousand instances of CSA connected at the same time. However, an unrestricted number of CSA can be installed at any time. *(Specifier, Maximum 5 with Standard; Maximum 10 with Professional; Unrestricted with Enterprise)*
       8. The USP shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
       9. Roles-Based Architecture:
          1. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.
          2. Each role shall execute a specific set of tasks related to either core system, automatic license plate recognition (ALPR), video (VMS), or access control (ACS) functionalities, among many others. Installation shall be streamlined through the ability of the USP to allow administrators to:

Deploy one or several SSM across the network prior to activating roles.

Activate and deactivate roles as needed on each and every SSM.

Centralize role configuration and management.

Support remote configuration.

Move roles over from one SSM to another.

* + - * 1. Each role, where needed, shall have its own database to store events and role-specific configuration information.
        2. Roles without databases, such as The Federation feature, Active Directory, and Global Cardholder Management, shall support near real-time standby without any third-party failover software being required.
        3. Directory Role:

The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.

The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.

The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:

Security Partitions, users, and user groups

Areas

Zones, input/output (IO) linking rules, and custom output behavior

Alarms. Schedules, and scheduled tasks

Custom events

Macros or custom scripts

The Directory Role shall support the configuration/management of the following components specific to VMS:

Video servers and their peripherals (for example audio, IOs, and serial ports)

PTZ

Camera sequences

Recording and archiving schedules

The Directory Role shall support the configuration/management of the following components specific to ACS:

Door controllers, and input and output (IO) modules

Doors, Elevators, and Access rules

Cardholders and cardholder groups, credentials, and badge templates

The Directory Role shall support the configuration/management of the following components specific to ALPR:

ALPR units and cameras

Hotlists, permit lists, and overtime rules

* + - * 1. The Video Archiver Role shall be responsible for managing cameras and encoders under its control and archiving.
        2. The Media Router Role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).
        3. The Access Manager Role shall be responsible for synchronizing access control hardware units under its control, such as door controllers and I/O modules. This role shall also be responsible for validating and logging all access activities and events when the door controllers and I/O modules are online.
        4. The Automatic License Plate Recognition (ALPR) Role shall be responsible for synchronizing fixed ALPR units (cameras) and mobile ALPR applications under its control. The ALPR Role shall also be responsible for logging all ALPR activities and events.
        5. The Zone Manager Role shall be responsible for managing all software zones (collection of inputs) and logging associated zone events. Zones shall consist of inputs from both access control and video devices.
        6. The Health Monitoring Role shall be responsible for monitoring and logging health events and warnings from the various client applications, roles, and services that are part of the USP. This role shall also be responsible for logging events within the Windows Event Log and for generating reports on health statistics and health history.
        7. The Data Ingestion Role shall be responsible for ingesting data from external sources in order to enhance the system reporting and dashboarding capabilities.
        8. Optional Roles

The Federation Role shall be responsible for creating a large virtual system consisting of hundreds or thousands of independent and remote ACS, VMS, and/or ALPR systems. *(Specifier, Enterprise only, additional license required)*

The Global Cardholder Synchronizer Role shall be responsible for synchronizing cardholder and credential data between the local site and a central site. Synchronization between remote sites shall also be supported. *(Specifier, Enterprise only, first connection included, additional licenses required for more)*

The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server. *(Specifier, Professional and up, additional license required)*

The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database.

The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports. *(Specifier, Professional and up, additional license required)*

The Plug-in Manager Role shall be responsible for the communication between the USP and third-party systems such as video analytics, access control, video, ALPR, and building management systems. *(Specifier, Professional and up, additional license required)*

The Web SDK Role shall be responsible for connecting the USP to any application or interface developed with the Web Service SDK. Applications developed with the Web Service SDK shall be platform independent and rely on the REST protocol for communications. *(Specifier, Professional and up, additional license required)*

The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

* + - 1. Server Monitoring Service (Watchdog):
         1. The USP shall include a Server Monitoring Service that continuously monitors the state of the Server Software Module (SSM) service.
         2. The Server Monitoring Service shall be a Windows service that automatically launches at system startup, regardless of whether or not a user is logged into his account.
         3. The Server Monitoring Service shall be installed on all PCs/servers running an SSM. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the PC/server should it be unable to restart the service.
    1. USP Access Control, Video, and ALPR Unification
       1. The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ACS, VMS, and ALPR. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.
       2. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.
       3. The user shall be able to associate one or more video cameras to the following entity types: areas, doors, elevators, zones, alarms, intrusion panels, ALPR cameras, and more.
       4. It shall be possible to view video associated to access control events when viewing a report.
       5. It shall be possible to view video associated to intrusion panel events when viewing a report.
       6. It shall be possible to view video associated to ALPR events when viewing a report.
    2. USP Alarm Management
       1. The USP shall support the following Alarm Management functionality:
          1. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
          2. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.
          3. Set the priority level of an alarm and its reactivation threshold.
          4. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
          5. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
          6. Provide the ability to group alarms by source and by type.
          7. Define the time period after which the alarm is automatically acknowledged.
          8. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
          9. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
          10. Define whether to display the source of the alarm, one or more entities, or an HTML page.
          11. Specify whether an incident report is mandatory during acknowledgment.
       2. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.
       3. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, and VMS systems.
       4. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.
       5. The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.
       6. Alarm unpacking and packing shall be supported where all the entities associated to an alarm can be displayed in the Monitoring UI with the single click of a button.
       7. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.
       8. The user shall be able to spontaneously trigger alarms based on something he or she sees in the system.
       9. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.
       10. The user shall be able to investigate an alarm without acknowledging it.
       11. Through reporting on alarm, it shall be possible to add a column to see the delta time between when the alarm was triggered and the time that user acknowledged it.
    3. USP Threat Levels *(Specifier, Professional and Enterprise)*
       1. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.
       2. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.
       3. Threat Levels shall be set on an area or on the entire system.
       4. Threat Levels shall affect the system behavior by executing any action available in the USP such as: trigger output, start recording, block camera, override recording quality, arm zone, set a door in maintenance mode, and more.
       5. The following specific actions shall be available with Threat Level:
          1. Set minimum security clearance to restrict or permit access to cardholders on specific areas on top of the restrictions imposed by the access rules.
          2. Set minimum user level to automatically log out user from the USP.
          3. Set reader mode to change how the doors are accessed (for example card and PIN, or card or PIN).
       6. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.
    4. USP Advanced Task Management
       1. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day-to-day activities, and reporting.
       2. Administrators shall be able to assign tasks and lock the operator’s workspace. The user management of their workspace shall be limited by their assigned privileges.
       3. Operators shall be able to save their tasks as either Public tasks or Private tasks and in a specific partition. Public tasks shall be available to all users. Private tasks shall only be available to the owner of the task.
       4. Operators shall be able to share their tasks by sending them to one or more online users. Recipients shall have the option to accept the sent task.
       5. Operators shall be able to duplicate a task.
    5. USP Reporting
       1. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.
       2. Each and every report in the system shall be a USP task, each associated with its own privilege. A user shall have access to a specific report task if they have the appropriate privilege.
       3. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.
       4. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.
       5. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.
       6. The USP shall support the following types of reports:
          1. Alarm reports
          2. Video-specific reports (archive, bookmark, motion, and more)
          3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)
          4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more)
          5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more)
          6. Health activity and health statistics reports
          7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports
       7. Generic Reports, Custom Reports and Report Templates:
          1. The user shall have the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.
          2. The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).
          3. All report templates shall be created within the Monitoring UI.
          4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
          5. An unrestricted number of custom reports and templates shall be supported.
       8. A reporting task layout shall consist of panes with settings (report length, filters, go and reset commands, etc.), the actual report data in column format, and a pane with display tiles. The user shall be able to drag and drop individual records in a report onto one or more display tiles to view a cardholder’s picture ID, playback a video sequence, or an ALPR event.
       9. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.
       10. The reporting task shall have the ability to display results through graphics such as line charts, bar charts, stacked bar charts, doughnut charts, and pie charts.
       11. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.
       12. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, export the graphics chart in JPG/PNG, and automatically email a report based on a schedule and a list of one or more recipients, including users with accounts outside the UPS.
       13. Should the user not having the right to export, a second user credential should be required, with the privilege to do the export shall be available for the export to be authorized by the first user.
       14. Shall allow the ability to insert a custom logo when generating reports.
    6. USP Dashboards
       1. The USP shall support the ability to create dashboards.
       2. Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to the dashboards should also be allowed to users granted the appropriate privilege.
       3. Dashboards in the system shall be a USP task. A user shall have access to a specific dashboard task if they have the appropriate privilege.
       4. Dashboards shall be saved either in a private folder or a public folder.
       5. A dashboard shall consist of a canvas with various widgets displayed on the canvas. All widgets should offer the ability to specify location and size to the widget, a title to the widget, a background color to the widget, and the ability to refresh periodically the content of the widget.
       6. Dashboard widget types shall be:
          1. Image: provides the ability to display an image (JPG, PNG, GIF, BMP) on a dashboard.
          2. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, color, and alignment can be specified by the user.
          3. Tile: provides the ability to display any entity of the USP inside of a tile.
          4. Web page: provides the ability to display a URL on a dashboard.
          5. Entity Count: provides the ability to display the total number of a specific entity type in the USP.
          6. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.
          7. Map: Provides the ability to display and interact with maps on a dashboard.
       7. It shall be possible to extend the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
       8. The USP shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.
    7. USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)*
       1. The USP shall support the concept of a Federation feature for access control, video, and ALPR.
       2. The Federation feature shall allow multiple independent USP systems (Federated systems) to be unified into a larger virtual system (the Federation feature). This shall facilitate the global monitoring of multiple independent USP systems.
       3. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.
       4. The Federation feature shall support the unification of multiple independent access control systems or ACS.
       5. The Federation feature shall support the unification of multiple independent license plate recognition systems or ALPR.
       6. Entities that shall federated and monitored centrally from the Federation feature shall include alarms, areas, cameras, cardholders and cardholder groups, credentials, doors, elevators, ALPR events, and zones (monitored inputs).
       7. The Federation feature shall support a cloud-based deployment, whereby the service and infrastructure will be updated automatically and provisioned by the service provider, without need for on-site hardware.
       8. The Federation feature shall support Global Alarm Management from the Monitoring UI for access control, video, and ALPR.
       9. The Federation feature shall support Global Report Generation from the Monitoring UI for access control, video, and ALPR.
       10. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (for example generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).
    8. USP Zone Management
       1. The USP shall support the configuration and management of zones for input point monitoring via the Zone Manager Role. A user shall be able to add, delete, or modify a zone if they have the appropriate privileges.
       2. A zone shall monitor the status of one or more input points. Zone monitoring or input point monitoring shall be possible through the use of a controller and one or more input modules. Inputs from video cameras or video encoders shall also be accessible via a zone.
       3. Depending on the hardware installed, supervised inputs shall be supported. Depending on the input module used, both 3-state and 4-state supervision shall be available.
       4. A schedule shall be defined for a zone, indicating when the zone will be monitored.
       5. Custom Events shall provide full flexibility in creating custom events tailored to a zone. Users shall be able to associate custom events to state changes in monitored inputs.
       6. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.
       7. Input/Output (IO) Linking
          1. Zone management shall support Input/Output (IO) Linking. I/O Linking shall allow one or more inputs to trigger one or more outputs.
          2. I/O Linking shall be available in offline mode when communication between the server and hardware is not available.
          3. Custom Output Behaviors shall provide full flexibility in creating a variety of complex output signal patterns: simple pulses, periodic pulses, variable duty-cycle pulses, and state changes.
          4. Through the “trigger an output” action, the ACS shall support the triggering of outputs with custom output behaviors.
    9. USP User and User Group Security, Partitions, and Privileges Management
       1. The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if they have the appropriate privileges.
       2. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:
          1. ADFS (Active Directory Federation Services)
          2. Azure Active Directory (through OpenID Connect)
          3. Ping Identity (through OpenID Connect)
          4. KeyCloak (through OpenID Connect)
          5. Other Open ID Connect / SAML2 authentication agents
       3. Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups. User group nesting shall be allowed.
       4. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR shall have associated privileges.
       5. Specific entities, such as cardholders, cardholder groups, and credentials shall include a more granular set of privileges, such as the right to access custom fields and change the activation or profile status of an entity.
       6. Partitions:
          1. The USP shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a system into multiple security partitions.
          2. All entities that are part of the USP can be assigned to one or more partitions.
          3. A user who is given access to a specific partition shall only be able to view entities (components) within the partition to which they have been assigned. Access is given by assigning the user as an accepted user to view the entities that are members of a particular partition.
          4. A user or user group can be assigned administrator rights over the partition.
       7. It shall be possible to specify user and user group privileges on a per partition basis.
       8. Advanced logon options shall be available such as dual logon and more.
       9. It shall be possible to specify an inactive period for the Monitoring UI after which time the application shall automatically lock, while still preserving access to currently displayed camera feeds. It shall also be possible to log the user out immediately after the inactivity period or within an amount of time from when the application was locked.
       10. It shall be possible to review used permissions and determine:
           1. For any entity in the system, which user group or user can view or modify it.
           2. For any user group or user in the system, what are its privileges.
           3. For any privilege in the system, which used group or used is allowed to perform the underlying action.
    10. USP Event/Action Management
        1. The USP shall support the configuration and management of events for video and ALPR. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.
        2. The USP shall receive all incoming events from one or more ACS, VMS, and/or ALPR. The USP shall take the appropriate actions based on user-defined event/action relationships.
        3. The USP shall receive and log the following events:
           1. System-wide events
           2. Application events (clients and servers)
           3. Area, camera, door, elevator, and ALPR events (reads and hits)
           4. Cardholder and credential events
           5. Unit events
           6. Zone events
           7. Alarm events
           8. ALPR events
           9. First Person In and Last Person Out events and antipassback events
           10. Intrusion events
           11. Asset management events
           12. Health monitoring events.
        4. The USP shall allow the creation of custom events.
        5. The USP shall have the capability to execute an action in response to an access control, video, and ALPR event.
        6. The USP shall allow a schedule to be associated with an action. The action shall be executed only if it is an appropriate action for the current time period.
    11. USP Schedules and Scheduled Tasks
        1. Schedules
           1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if they have the appropriate privileges.
           2. The USP shall provide full flexibility and granularity in creating a schedule. The user shall be able to define a schedule in 1-minute or 15-minute increments.
           3. Daily, weekly, ordinal, and specific schedules shall be supported.
        2. Scheduled Tasks
           1. The USP shall support scheduled tasks for access control, video, and ALPR.
           2. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.
           3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email, emailing a report or triggering incidents.
    12. USP Macros and Custom Scripts
        1. The USP shall enable users to automate and extend the functionalities of the system through the use of macros or custom scripts for access control, video, and ALPR.
        2. Custom macros shall be created with the USP Software Development Kit (SDK).
        3. A macro shall be executed either automatically or manually.
        4. In the Monitoring UI, a macro shall be launched through hot actions.
    13. USP Dynamic Graphical Maps (DGM)
        1. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.
        2. The USP shall provide a map centric interface with the ability to command and control all the USP capabilities from a full screen map interface.
        3. It shall be possible to span the map over all screens of the USP client station. In the scenario where the map is spanned over all the screens of the USP client station it shall be possible to navigate the map including pan and zoom, and the map’s moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same command and control capabilities as in a single screen display.
        4. The DGM shall support the following file format and protocol for importing map background:
           1. PDF
           2. JPG
           3. PNG
           4. Web Tile Map Service (WMTS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
           5. BeNomad
           6. AutoCAD (DWG & DXF)
        5. The DGM shall provide the following online map providers for use as map background and provide the ability to manage their service license if they require one:
           1. Google Map, aerial, terrain (Licensed)
           2. Bing Map, aerial, satellite, hybrid (Licensed)
           3. ESRI ArcGIS (Licensed)
           4. OpenStreet Map aerial (Licensed)
           5. OVI hybrid
        6. It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.
        7. The DGM shall provide the ability to display all native entities with associated name of the USP including:
           1. Cameras, fix, and PTZ
           2. Doors
           3. Camera sequences
           4. Areas
           5. Intrusion areas
           6. Intrusion zones
           7. License Plate Recognition cameras
           8. Digital inputs
           9. Digital outputs
           10. Intercoms
           11. Alarms
           12. Macros
           13. Police Car Patrollers
           14. Entity name
        8. The DGM shall provide the ability to draw and display information over the map in the form of:
           1. Vectoral shapes: line, rectangles, polygons, ellipse
           2. Pictures
           3. Text
        9. The DGM shall provide the ability to display any type of third-party entities integrated through an SDK.
        10. The DGM shall provide the ability to display a layer of information in Keyhole Markup Language (KML) format.
        11. The DGM shall provide the ability to the operator to manage layers of entities displayed over the map, being able to turn them on and off and changing the superposition order.
        12. The DGM shall provide the ability to import data layers from one or more ESRI ArcGIS servers.
        13. The DGM shall provide the operators with the ability to manage layers that are imported from ESRI ArcGIS. The operators shall be able to turn the layers on and off, as well as sort the layers.
        14. The DGM shall offer built-in map data backup and restore for both map backgrounds and layers of entities.
        15. The DGM shall provide the ability to import configurations from an external file such as:
            1. AutoCAD layer for objects
            2. CSV, Excel file
        16. The DGM shall provide the ability to print a map in the following file formats:
            1. PDF
            2. PNG
        17. The DGM shall offer failover capabilities.
        18. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.
        19. The DGM shall provide a means to update a map background without affecting the map object configuration.
        20. The DGM shall offer a user-friendly graphical map designer to configure the maps.
        21. The DGM shall provide user friendly and intuitive navigation that includes:
            1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
            2. The ability to define favorites for recurrent position recall.
            3. The possibility to create links between maps. The map links shall allow the link from one map to multiple maps representing the floors of a building. Navigating between floors of a building shall keep the level of the map.
            4. A common user experience regarding navigation into the map for both GIS and private maps.
        22. It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.
        23. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.
        24. The DGM shall offer a smart selection tool to access the video. By clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.
        25. It shall be possible to select a location by drawing a zone of interest on the DGM, and to display all the entities that are part of that zone of interest at once.
        26. The user shall be able to select and display the content of multiple USP entities on the map in pop-up windows.
        27. The user shall be able to move, resize, and pin the USP entity pop-up windows to the map.
        28. It shall be possible to access live and playback video from the map.
        29. It shall be possible to monitor all entity event notifications from the DGM. Users shall be able to turn notifications on and off per entity.
        30. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:
            1. Center the map on entities related to the alarm.
            2. Visualize the Alarm notifications on the map and access the related videos from the map.
            3. Trigger and receive alarms.
            4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
            5. Visualize that an alarm occurred in an underlying linked map.
        31. The DGM shall provide the following search capabilities:
            1. Search and center by entity name.
            2. From the Display of an entity in the USP, locate the entity on the map and offer the ability to select another one close-by.
            3. By street address, city, landmark, point of interest (using geocoder license from Google, ESRI, or other providers).
        32. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.
        33. The DGM shall support the use of GIS maps or private maps or a combination of both for map background.
        34. The DGM shall be compatible with any GIS compliant maps with the OGC and supporting WMTS and WMS. This includes, but is not limited to, ESRI maps. The DGM shall allow the selection of the appropriate GIS layers.
        35. The DGM shall provide an intuitive built-in map designer for entity positioning on the map using drag and drop. Any configuration shall be graphic.
        36. It shall be possible to edit and configure multiple map objects at once.
        37. All map design modifications shall be logged in an audit trail.
        38. Various actions shall be available within maps for execution through simple and intuitive double-click, right-click, or drag-and-drop functionality. Examples of actions available through maps shall include unlocking a door and acknowledging an alarm.
        39. Through the following functionality, the DGM shall allow the management of USP alarms from the map:
            1. Locate on the map entities related to the alarm.
            2. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.
            3. List, select, and locate alarms.
            4. Auto center the map on the highest priority alarm.
            5. Handle the alarm from the map, including acknowledgement, forwarding, and investigation.
            6. All map containers, such as hotspots or map links shall reflect the alarm status of the contained entities.
        40. It shall be possible to add advanced functionality to maps object using the SDK. Any functionality available through the USP SDK shall be available within maps.
        41. The DGM shall offer lasso tools for:
            1. Displaying entities at one location through a single action.
            2. Triggering an action on all entities at one location in a single click.
            3. Editing multiple entities at one location simultaneously.
        42. The DGM shall allow the display of USP entities selected from the map on a remote monitor (video wall).
        43. The DGM shall provide the ability to search within the map by entity name.
        44. The DGM shall allow the use of KML overlay map information for both GIS and private maps. Movable objects shall be supported using KML.
        45. The Contractor shall provide licenses for each entity that is required to be shown on the graphical maps.
    14. USP Audit and User Activity Trails (Logs)
        1. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.
        2. Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
        3. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
        4. The USP shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the USP such as login, camera viewed, ALPR event viewed, badge printing, video export, and more.
        5. The ACS shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file. An option to have 2 users to approve the export shall also be available and definable by user.
    15. USP Incident Reports
        1. Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.
        2. The operator shall be able to create standalone incident reports or incident reports tied to alarms.
        3. The operator shall be able to link multiple video sequences to an incident, access them in an incident report, and change the date or time of the sequences later on.
        4. It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.
        5. Incident reports shall allow the creation of a custom form on which to input information on an incident.
        6. Incident reports shall allow entities, events, and alarms to be added to support at the report’s conclusions.
        7. Incident reports shall allow the use of a custom logo, the default Mission Control logo or no logo at all.
    16. USP Data Ingestion
        1. USP shall allow the possibility to import external data from outside sources to enhance unification of data sources within the USP.
        2. Each data source shall be defined by a set of fields and field types that describe the data source. Field types shall be:
           1. String
           2. 32-bit and 64-bit integer
           3. Floating point number
           4. Boolean
           5. Timestamp
           6. Binary (in a file or base 64)
        3. The visualization of each data point from a data source shall be configurable to determine what fields from the data should be displayed. The configuration of each field should be:
           1. Which fields are displayed or hidden
           2. What order are the fields displayed
           3. A label to specify the name of the filed (to have a key:value format)
           4. An option to specify how to display the field (text value, image, clipboard value, hyperlink to a web page, hyperlink to an entity in the system, sound file)
        4. A privilege should be available for each data source to allow or deny access to specific users and user groups of the USP.
        5. Ingested data shall be available in the USP reporting system.
        6. Ingested data shall be available to display in the USP dashboards.
    17. USP Third Party Integration
        1. Microsoft Active Directory Integration: *(Specifier, Professional and up, first integration included, additional licenses required for more)*
           1. The USP shall support a direct connection to one or multiple Microsoft Active Directory server via the Active Directory Role(s). Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.
           2. Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups.
           3. The USP shall support ADFS for user login.
           4. The USP shall be able to connect to and synchronize data from multiple Active Directory servers (up to 10).
           5. The USP shall support Azure AD for cardholder synchronization.
           6. The USP shall support synchronizing Active Directory Universal Groups as well as security groups belonging to other domains within the same forest.
           7. The USP shall support Microsoft Active Directory encryption using LDAP SSL.
           8. When enabled, Active Directory shall manage user logon to the USP client applications through the user’s Windows credentials. Logging on to the USP shall utilize native Active Directory password management and authentication features.
           9. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:

Users (username, first and last names, email address, and more)

User groups (user group name, description, and group email address)

Cardholders (first and last names, description, email, picture and more)

Cardholder groups (cardholder group name, description, and group email address)

Active Directory attributes to USP custom fields

* + - * 1. When enabled, the addition, removal, or suspension of a user’s Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent user account in the USP.
        2. When enabled, the addition, removal, or suspension of a user’s Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent cardholder account in the USP.
        3. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include on first logon (users only), manual synchronization, and scheduled synchronization.
        4. The USP shall support user connections across independent organizations by connecting to an external identity provider using claims-based authentication such as ADFS (Active Directory Federation Services), Azure Active Directory, other OpenID Connect & SAML2 providers.
      1. Intrusion Detection Integration: *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
         1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
         2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):

Arm and disarm intrusion devices (manually, on schedule, or following a USP event)

Activate or trigger intrusion device outputs

View intrusion events and alarms

Monitor the status, including arming status, of the intrusion devices

Video verification of intrusion events and alarms with video panels

Create USP zones using intrusion device inputs

Alarm panel user management from the USP interface (when supported and available from the alarm panel)

* + - * 1. Currently supported intrusion panels include:

Bosch Legacy G Series panels

Bosch B & G Series panels

Bosch Map 5000

DSC Power Series panels

DMP XR Series panels

Honeywell Galaxy Dimension and Flex panels

Vanderbilt SPC

UTC Advisor Master and Advanced

Satel INTEGRA panels

Telenot Complex 400H panels

* + - * 1. Additional intrusion devices supported include:

Buytime

Alarm Panel Receiver

Southwest Microwave RPMII

* + - 1. Third Party Access Control Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third-party access control software via the SDK. Communications with access control software shall be over an IP network and should not support administrative tasks such as cardholder management.
         2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

Synchronize access control entities and receive associated events and states within the USP, including:

Cardholders

Visitors

Readers and doors

Alarms

Inputs and outputs

Monitor access control events

Monitor and acknowledge access control alarms

Trigger actions and outputs in the access control software using hot actions and event-to-actions

Lock and unlock doors in the access control software

Video verification of access control events and alarms

Configure event-to-actions using the access control events and alarms

Generate Security Center reports using the access control data

View and monitor states of door entities in the USP maps

* + - * 1. Currently supported access control manufacturers include:

Tyco Software CCURE

UTC Lenel Onguard

Amag Symmetry

Siemens Sipass

* + - 1. Third Party Destination Dispatch Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third party destination dispatch (elevator control) software via the SDK. Communications with destination dispatch software shall be over an IP network.
         2. Integrating with destination dispatch software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of destination dispatch software with the USP shall include the following (where supported by the destination dispatch solution):

Destination dispatch entity creation and reception of associated events and state within the USP, including:

Floors and landings

Elevator cars (front/rear doors) and kiosks

Cardholders and credentials (if applicable)

Monitor destination dispatch events.

Trigger manual dispatch actions.

Video verification of destination dispatch events.

Configure event-to-actions using the destination dispatch events.

Generate Security Center reports using the destination dispatch data.

Support multiple readers:

Kiosk internal readers

USP readers

Kiosk advanced modes and passenger types.

* + - * 1. Currently supported destination dispatch manufacturers include:

Otis Compass

Thyssenkrupp

MCE

KONE

* + - 1. Asset Management Integration: *(Specifier, requires an additional license, Professional and up)*
         1. The USP shall integrate with third party asset management systems via the Asset Management Role.
         2. Communications with asset management solutions shall be over an IP network (via software communications).
         3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):

Synchronize asset management system assets with USP asset entities.

Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

Synchronization of asset management alarms with Security Center alarms.

Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

Real-time tracking of asset locations on a per area basis.

Asset Management Inventory reporting task that details the current location (area) of an asset.

Asset Activity reporting task that provides a historical review of asset-related events and activity.

* + - * 1. Currently supported asset management systems include:

Deister Key management

Morsewatchmans

TRAKA

Key Systems

* + - 1. Additional Third-Party Integrations
         1. The USP shall support multiple approaches to integrating third party systems. These shall include: Software Development Kits (SDKs), REST-based Web Service SDKs, RTSP Service SDKs, and more. *(Specifier, Professional and up, SDK package and license required)*
         2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as: *(Specifier, refer to the website for how these are licensed, for an updated list of available Third-Party Integrations, please refer to the supported plugin guide)*

Third party video systems

Third party access control systems

ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors

Building management systems

Access Control ecosystem (such as IDscanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)

Transaction monitoring (POS, Barcode scanning, ATM)

Industrial IoT: Data ingestion from external devices through standard communication protocols (Modbus, BACnet, OPC, SNMP, HTTP Server, MQTT Client, TCP Server)

Industrial Protocol Interface: Data exposure from GSC to external protocol interfaces using standard communication protocols (BACnet, SNMP)

Videowall (Barco, Eizo)

Human resource management systems (HRMS)

Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))

Gunshot Detection (Shot Spotter, Guardian GunShot)

Dynamic Logbook: Customizable forms with reporting capabilities

* + 1. USP Software Development Kit (SDK) *(Specifier, Professional and up, additional license required)*
       1. A USP SDK shall be available to support custom development for the platform.
       2. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.
       3. Integration with external applications and databases shall be possible with the SDK.
       4. The SDK shall support an API to allow third party access control hardware integration.
       5. The SDK shall enable end-users to develop new functionality (user interface, standalone applications, or services) to link the USP to third party business systems and applications such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.
       6. The SDK shall be based on the .NET framework.
       7. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.
       8. The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
       9. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.
       10. The SDK shall provide an extensive list of programming functions to view and configure most ACS entities such as cardholders, cardholder groups, visitors, credentials, access rules (modify only), and custom fields.
       11. The SDK shall be able to receive real time events from the following USP entities: users and user groups, areas, zones, cameras, video units, doors, door controllers (units), elevators, cardholders, cardholder groups, and credentials.
       12. The SDK shall be able to query the history of events for areas, cameras, zones, alarms, cardholders, credentials, visitors, doors, query license plate read events, license plate hit events, generate a license plate hits report, generate a license plate reads report.
       13. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.
  1. **Execution**
     1. Warranty
        1. The product shall perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use. Software defects are covered through Service Releases and Cumulative Updates which are available for a period of 1 year from the date of the software purchase.
        2. Extended warranty, up to 5 years, shall be available through the purchase of the Genetec Advantage support service which includes the following additional services over the standard warranty:
           1. Access to phone support and online chat for technical assistance
           2. Online case management
           3. Online system availability monitor
           4. Access to Major and Minor Release Upgrades
           5. 24/7 pager support and dedicated support specialist *(Specifier, additional cost)*
     2. Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 
        1. General Requirements:
           1. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:

Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

Complex enterprise installations involving advanced functionality (for example The Federation feature, failover, plugins) and/or multiple systems (for example access control, video, ALPR) and/or third-party integrations.

Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

* + - * 1. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.
      1. Deployment Management Service:
         1. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization and who will be responsible for:

Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

Providing a project plan for the deployment of the vendor's USP.

Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

* + - 1. Solution Architect Service:
         1. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:

Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews, as well as performance reviews of the vendor’s USP.

Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.

Providing upgrade and migration strategy for the vendor’s USP where applicable.

Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

* + - 1. System Configuration and Commissioning Service:
         1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

Assisting the contractor’s or subcontractor’s onsite/remote technicians with the configuration and commissioning of the vendor’s USP at the client site.

Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.

Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

* + 1. Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)*
       1. The contractor shall engage the services of the USP vendor to assist in the end user training of the USP at the end-user site.

**End of Section**

1. **Section 28 17 00 – Physical Access Management System**
   1. **General**
      1. Related work
         1. Section 28 13 00 – Access Control Software and Database Management
      2. Definitions
         1. ACS – Access Control System
         2. CSA – Client Software Application
         3. DGM – Dynamic Graphical Maps
         4. ALPR – Automatic License Plate Recognition
         5. SDK – Software Development Kit
         6. GLM – Genetec Lifecycle Management
         7. SSM – Server Software Module
         8. UI – User Interface
         9. USP – Unified Security Platform
         10. UWI - Unified Web Interface
         11. VMS – Video Management System
         12. PAMS – Physical Access Management System
         13. SLA – Service Level Agreement
         14. API – Application Programming Interface
         15. HSM – Hardware Security Module
         16. FIPS – Federal Information Processing Standards
         17. HTTPS - Hypertext Transfer Protocol Secure
         18. TLS - Transport Layer Security
         19. AES – Advanced Encryption Standard
         20. SSO – Single Sign-On
         21. AD – Active Directory
      3. Qualifications
         1. The system programmer shall have attended manufacturer training, along with the following certifications:
            1. Security Center 5.x Synergis™ Technical Certification (SC-STC-001)
            2. Security Center 5.x Synergis™ Advanced Configuration and Troubleshooting (SC-STC-002)
            3. Security Center 5.x ClearID – Level 2 (SC-CID-002)
         2. The system programmer shall have the “Accredited” level status in the Genetec Channel Partner Program with the follow level of qualification: *(Specifier, select one of the following)*
            1. Certified Reseller or up
            2. Elite Reseller or up
            3. Unified Elite Reseller
         3. The system programmer shall submit proof of certifications.
   2. **Products**
      1. Physical Access Management System (PAMS)
         1. The system shall be an enterprise class Physical Access Management System. It shall fully integrate within a Unified Security Platform (USP). The USP shall allow the seamless integration of the PAMS with Synergis Access Control System (ACS). It is the access provisioning solution for Synergis Access Control System (ACS).
         2. The PAMS shall be highly scalable for global deployments.
            1. The PAMS to support configurations with Synergis Access Control System.
            2. The PAMS system shall support licensing up to:

1,000,000 unique identities, up to 300,000/system

500 sites

1,000 visitor kiosks

1,000,000 visits yearly

* + - * 1. Additionally, each account shall support up to:

10,000 roles, with up to 100,000 identities in one role

200,000 areas

* + - 1. The PAMS shall support a variety of identity management functionalities, including but not limited to:
         1. Programmable management of cardholders for automatic access assignment
         2. Manual management of cardholders via workflows
      2. Manufacturer:
         1. Genetec ClearID
      3. Certification:
         1. The PAMS shall be an ISO/IEC 27001:2013 certified Information Security Management System.
    1. Architecture
       1. There exists a globally distributed cloud architecture and a Europe only architecture:
          1. Microsoft Azure

Distributed global services

Policies and rules

User authentication

Area management

API

Self-service portal

Workflows engine

Email notification

Automatic provisioning

Regional Services

The cardholders, credentials, areas, cardholder groups, access rules and schedules will be stored in the data center that was selected during configuration.

Data is distributed across siloed, independent repositories.

Local sites

Security Center Synergis™

Local custom fields

Plugins

* + - * 1. High availability

99.9% SLA

Geo-redundant data storage

* + - * 1. Security Controls

Data encryption

AES 256

RSA 2048

Symmetric keys and asymmetric keys

Keys are managed using Azure Key Vault

FIPS 140-2 Level 2 validated HSMs

Data integrity

Digital signatures based on SHA 512 with RSA 2048 are used to validate data.

Communication encryption

Hypertext Transfer Protocol Secure (HTTPS) protocol TLS 1.2

Transport Layer Security (TLS) certificates

Zero-trust architecture

Customer data is segmented into microservices, which only have the minimum data access requires to perform that task.

All communication between microservices is encrypted and digitally signed.

Service monitoring

Controls are updated based on various security threat feeds and services.

System is running constant metrics analysis, including synthetic transactions to emulate user activity.

Systems are monitored by and notify development and operations teams of any issues.

User authentications

Azure Active Directory (AD) B2B by default

Option for federation of existing AD user identities through Azure AD B2B or OpenID Connect to provide Single Sign-On (SSO).

Also support:

OneLogin

Okta

Auth0

Ping

MyID

* + - 1. ClearID Plugin
         1. Installed on a Security Center server to integrate Genetec ClearID and Security Center, providing communications between Synergis™ and ClearID Cloud Services.
         2. Plugin is also installed on a Config Tool workstation, which allows that administrator to create and configure the plugin role and configure database settings and connection settings for ClearID.
         3. Plugin will update automatically if an internet connection is available when a new release is published by Genetec.
    1. Management
       1. Identity management
          1. Identity Information:

General personal information

Company information

Supervisors for this identity

System shall synchronize identity information with the following sources:

CSV file exported from and HR database

SQL Server or Oracle database

Microsoft Active Directory via LDAP

Azure Active Directory

System shall have externally available Identity REST API for synchronization of identity information from external sources

* + - * 1. Direct report management

Supervisor can view a report of their direct report.

Supervisor can manage access and role membership of their direct report.

Supervisor can setup the delegation on behalf of their direct report. This action will delegate their direct report’s tasks to someone else in the organization while their direct report is away on leave. The delegates will have the same set of permissions as the delegator and can manage the tasks on their behalf.

* + - * 1. Identity request workflow

Single request workflow or CSV import workflow to request identities that would add to system using the web portal.

Identity template can be customized with pre-defined fields.

Identity template is selected during identity request.

Identity request approval workflow can be customized.

Identity approvers can be assigned to approve an identity request.

Supervisors and identity approvers can be required to approve, edit, and deny identity requests.

Approvers can process identity requests using the ClearID web portal.

Possibility of automatic role membership for newly created identity with the required areas automatically assigned based on template used.

Identity request approvers can delegate their tasks to someone else in the organization while they are away on leave. The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

Email notifications when identity is requested.

Email notifications when identity is approved or denied.

* + - * 1. Access Control

Access period

Date of activation

Date of expiration

Provisioning attributes

Associated cardholders

* + - * 1. User Permissions

Administrator can enable or disable user access to web portal

Administrator can assign user types:

Administrator

User

* + - * 1. Visitor Management

Administrator can grant user permissions to invite visitors to specific sites

* + - 1. Area Management
         1. Area Management

Area owners and approvers can view, add, and remove roles from areas.

Site owners can assign management to one of more area owners.

Area owners and approvers can delegate their tasks to someone else in the organization while they are away on leave (Example: vacation leave, sick leave, etc.). The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

Area approvers can perform access reviews for their area to confirm that the area access provisioned is required and valid.

* + - * 1. Access Control

Area owners and approvers can view, add, and remove people from areas.

Area owners and approvers can grant temporary access to roles.

Employee supervisor can be required to approve employee access request.

Approvers can process access requests using the ClearID web portal.

Employee supervisors can delegate their tasks to someone else in the organization while they are away on leave. The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

* + - * 1. User Permissions

Approvers and supervisors can approve or deny access requests.

Permanent cardholders can request temporary access to areas.

Permanent cardholders can invite visitors.

* + - 1. Role management
         1. Role Management

Assign the management roles or cardholder group to one or more role owner.

Role managers can add or remove people from their groups.

Role owners can assign access to an area for their entire group.

Automatic provisioning and synchronization of cardholder groups for multiple sites.

Role managers and owners can manage roles using the ClearID web portal.

Role managers and owner can delegate their tasks to someone else in the organization while they are away on leave. The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

Role managers can perform access reviews for their role to confirm that the access, provisioning policy, and role membership are valid.

Administrator can view role access review reports for the details of the role access reviews.

* + - * 1. Attribute and role-based provisioning

Access can be granted or revoked based on employees’ locations.

Access can be granted or revoked based on specific roles or job titles in the organization, or who they report to.

Access can be granted or revoked based on completion of specific training or possession of required certificates.

Access can be granted or revoked based on a list of custom provisioning attributes synchronized from an external source.

A grace period can be configured to delay the revocation of access by a configurable time period following a change in attributes.

* + - 1. Site Management
         1. Site Management

Global management of cardholders for multiple Synergis™ systems.

Time zone support (built-in).

Site owners can delegate their tasks to someone else in the organization while they are away on leave. The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

Site owners can schedule area access reviews.

Email notifications will be sent to access review approvers that an access review is pending.

Site owners can view area access review reports for the details of the area access reviews.

* + - * 1. Access Control

Automatic synchronization of permanent credentials when someone travels between sites.

Synchronization of cardholders only happens when cardholders are changed, if cardholder has access on that Synergis™ system.

Synchronization of cardholder groups only happens when cardholder groups are changed, if the cardholder group has access on that Synergis™ system.

* + - 1. Visitor Management
         1. Visitor Management

Manual entry or CSV import pre-registration of visitors using the web portal.

Visitor approval workflow can be customized based on the area selected.

Visit event approval workflow options can be customized at the site level.

Visit event approvers can be assigned to approve a visit event.

Visit event approvers can delegate their tasks to someone else in the organization while they are away on leave. The delegate will have the same set of permissions as the delegator and can manage the tasks on their behalf.

Visitor watchlists can be used to screen visitors at an individual or company level.

Visitor watchlist behavior can block the visit confirmation from being sent to the visitor or can notify a watchlist manager that the visitor of interest is invited.

Automatic provisioning of visitors with the required areas automatically assigned.

Visitor check-in using Security Desk.

System shall support the configuration of self-service kiosks for visitor check-in.

Kiosk shall be based on iPad hardware.

Tabletop and floor stand kiosk options can be available.

Kiosk supports visitor pre-registration and on-the-spot registration.

Kiosk supports English, French, Spanish, Dutch, German, Italian, and Portuguese languages.

Visitors shall be able to check in with a government ID (over 200 supported IDs) or with an email address.

Refer to ClearID documentation for supported country IDs.

QR code data can be sent to visitors in a Visitor Confirmation email prior to the visit. Kiosk shall have the ability to process the QR code data for the purpose of visitor check-in.

Kiosk shall have the ability to print temporary visitor badge with QR code credentials.

An SMS alert can be sent to the host when a visitor completes their check in.

Kiosk supports Brother QL-820NWB and QL-820NWBc thermal printer.

Kiosk themes and color options can be configured per site.

Kiosk check-in and check-out options can be configured.

Visit events can be updated prior to the start of a visit.

Email notifications when visit request is created.

Email notifications when visit request is approved or denied.

Capture and report the visit reason.

Email invitation sent to visitor with a meeting invite (iCalendar format – RFC 2445), site details, and optional QR code for file attachments.

SMS notifications and email sent to visitor host when visitor checks in.

Refer to ClearID documentation for supported country codes.

* + - * 1. Access Control

Paper badges and temporary credentials for visitor management.

40-bit QR code sent to visitors can be utilized as a credential in Security Center.

Access to specific areas can be restricted on a per-credential basis.

Visitor escort can be required, with up to 10 unique visitor hosts.

Approvers can process visitor access requests using the ClearID web portal.

* + - 1. Platform Management
         1. Corporate logo for portal and email notifications
         2. Cloud platform
         3. HTML5 web interface with mobile support
         4. REST API available to automate any functions available in the web portal
      2. Security/Authentication Management
         1. Support multi-factor authentications for users using OpenID to connect
         2. Single Sign-On using Microsoft Office 365
         3. Single Sign-On using Microsoft Azure Active Directory (AD)
         4. ISO 27001:2013 certification
         5. AES-256 encryption with RSA 2048 bits
         6. System undergoes annual penetration testing by external accredited security firm
  1. **Execution**
     1. Execution
        1. Comply with all manufacturers’ written instructions unless more stringent requirements are indicated.
     2. Warranty:
        1. The product shall perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use. With the software subscription, defects are covered through continuous delivery.
        2. The software subscription will include the following support services:
           1. General phone support and online chat for technical assistance only during business hours.
           2. Online case management through GTAP.
     3. Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)*
        1. General requirements:
           1. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:

Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

Complex enterprise installations involving advanced functionality (for example, the Federation features, failover, plugins) and/or multiple systems (for example, access control, video, ALPR) and/or third-party integrations.

Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

* + - * 1. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.
      1. Deployment Management Service:
         1. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization, and who will be responsible for:

Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor’s USP.

Providing a project plan for the deployment of the vendor’s USP.

Managing the development and deployment of the custom solution components that will be integrated into the vendor’s USP (if applicable).

Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

Providing regular project status updates to the contractor regarding the development of custom solutions (in applicable) and the deployment of the vendor’s USP.

* + - 1. Solution Architect Service:
         1. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:

Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews, as well as performance reviews of the vendor’s USP.

Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.

Providing upgrade and migration strategy for the vendor’s USP where applicable.

Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

* + - 1. System Configuration and Commissioning Service:
         1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

Assisting the contractor’s or subcontractor’s onsite/remote technicians with the configuration and commissioning of the vendor’s USP at the client site.

Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.

Providing a knowledge transfer of the vendor’s USP to the contractor following the deployment of the USP at the client site.

* + 1. Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)*
       1. The contractor shall engage the services of the USP vendor to assist in the end user training of the USP at the end user site.

**END OF SECTION**

1. **Section 28 19 00 – Access Control Vehicle Identification Systems**
   1. **General**
      1. Related Work
         1. Section 28 13 00 – Electronic Access Control System
         2. Section 28 23 00 – Video Surveillance
         3. Section 28 51 00 – Information Management & Presentation
      2. Definitions
         1. ACS – Access Control System
         2. ALPR – Automatic License Plate Recognition
         3. CSA – Client Software Application
         4. DGM – Dynamic Graphical Maps
         5. SDK – Software Development Kit
         6. SSM – Server Software Module
         7. UI – User Interface
         8. USP – Unified Security Platform
         9. UWI - Unified Web Interface
         10. VMS – Video Management System
      3. Qualifications
         1. The system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - AutoVu™ Technical Certification.
         2. Optionally, the system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Enterprise Technical Certification.
         3. The system programmer shall be a Genetec certified partner with the following level of qualification: *(Specifier, select one of the following)*
            1. Certified Reseller or up
            2. Elite Reseller or up
            3. Unified Elite Reseller
         4. The system programmer shall submit proof of certifications.
   2. **Products**
      1. SharpV All in one Cameras
         1. Equipment is designed to provide License plate reading (LPR) functionality.
         2. Each unit contains 2 cameras, an illumination source, and a processor.
         3. Communication with units is via Ethernet.
         4. Support for IPv4 and IPv6.
         5. LPR engine can be localized to enhance performances.
         6. Database of international contexts available.
         7. High resolution (1920x1200 ((2.3Mpx)) progressive scan Monochrome CCD LPR camera.
         8. Motorized Variable Focal lenses (3m -45m (9’ – 148’))
         9. Pulsed-infrared illumination for high performance license plate reading (LPR).
         10. Automated exposure control based on feedback from the LPR engine.
         11. The optical character recognition software shall be embedded in the ALPR camera and be based on a deep neural network specifically designed to read license plates and other vehicle characteristics.
         12. The deep neural network shall be specifically trained with Monochrome images of licenses plates that originated from the ALPR camera.
         13. High resolution (1920x1200 ((2.3Mpx)) progressive scan color camera for video recording and overview imaging.
         14. The built-in analytic software shall be capable of detecting vehicles even if no license plate is visible by using a Virtual Loop algorithm.
         15. Integrated video capture hardware.
         16. Dual Opto-isolated Input/Outputs.
         17. Processing rates of 30 frames per second.
         18. Rugged, environmental enclosure and cabling designed for stationary applications.
         19. Onboard buffering of read data in case of network loss.
         20. Region of Interest to perform LPR on a polygon cropped inside the field of view (FOV).
         21. Video encoding capabilities: H.264 @ 30FPS, MJPEG @ 15FPS, 1920x1200 (2.3Mpx).
         22. Network interface - 1 X 10/100/1000 Base-T Ethernet port.
         23. WWAN: 4G/LTE Category 4 (Available only in certain countries. Talk to your representative)
         24. Satellite Positioning: GPS, Glonass, Beidou, Galileo, QZSS (Only available when 4G Antenna is installed)
         25. Advanced hardware image pre-processing that permits license plate recognition at full sensor frame rate.
         26. Available in Black or Security White.
         27. Processor – 1.6 GHz Intel Atom E3950 Quad core (2MB L2 cache), 4GB RAM.
         28. Operating system: Linux.
         29. Pulsed LED-based illumination Effective in 0LUX (total darkness) Environments: 940nm, 850nm, 740nm and 590nm wavelengths available.
         30. Tamper resistant with impact-proof front window.
         31. Includes Pan/Tilt Videotec mount and Pelco adaptor.
         32. Operating temperature -40°F to 150°F (-40°C to 65°C) ambient.
         33. Operating temperature -40°F to 130°F (-40°C to 55°C) ambient when using the India Context.
         34. Storage temperature -40°F to 185°F (-40°C to 85°C).
         35. Sealing: IEC 60529: IP66/67 (1 m submersion for 48 hrs).
         36. Impact Rating: IEC 62262:IK09
         37. Vibration and Shock Resistance: IEC 60068-2-64: 5~100Hz | 0.5g rms, IEC 60068-2-27: 10g | 16ms half-sine.
         38. Electromagnetic immunity & Emissions Rating: FCC | ICES-003 Issue 4 | CISPR32 / EN55032.
         39. EMC Directive (CE marking): 2014/30/EU.
         40. Power supply: PoE++ (Power-over-Ethernet) - 802.3bt Type 3 (31W typical, 43W max)).
         41. Optional Power supply: 24V DC input option: 27W typical, 37W max.
         42. Dimensions 2.5 X 7.6 X 8.5 inches (63 X 192 X 214 mm)(2.7 inches with Black Sunshield) 4.0in / 101.6mm with Antenna.
         43. Weight: 5.53 lbs (2.51kg).
      2. Client Software Application
         1. The CSA shall seamlessly merge automatic license plate recognition (ALPR) and video functionalities within the same user application. The VMS shall offer a complete and scalable video surveillance solution that shall allow cameras to be added on a unit-by-unit basis.
         2. The CSA shall support the ability to select multiple regions on a map and provide results that are common to all regions.
         3. The CSA shall allow the user to Protect a Read or Hit from deletion for a configurable period.
         4. The CSA shall allow the user to correct a Plate Read manually.
         5. The CSA shall present the user with a Simple Wizard for Hotlist creation.
         6. The CSA shall allow the user to create a Hotlist without the need for any attribute information other than license plate number.
         7. The CSA shall allow the user to search the configured hotlists for any data in any of the specified fields.
         8. The CSA shall allow the user to generate a read report specifically targeted to those reads that generated a hit.
         9. The CSA shall allow for map-based viewing of real-time read monitoring.
         10. The CSA shall allow the user to search for full or partial license plate numbers.
         11. The CSA shall allow the user to search for a license plate by using wildcards.
         12. The CSA shall allow the user to automate downloading Hotlists from an FTP/SFTP or HTTP/HTTPS server using username/password/certificate authentication.
         13. The CSA shall allow the user to customize the format of the Reports displayed on-screen.
      3. Surveillance User Interface (UI)
         1. The Surveillance UI shall provide an interface to support the following ALPR tasks and capabilities:
            1. Monitoring and management of ALPR events and alarms.
            2. Viewing of license plate picture(s) and context images.
            3. Viewing of license plate data (e.g., license plate reads)
            4. Verification of ALPR data against live and recorded video.
      4. Server Administrator User Interface Requirements
         1. The Server Administrator shall be used to configure the SSM and the Directory role (main configuration) and its database(s), to apply the license, and more.
         2. The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.
         3. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.
         4. The Server Administrator shall allow the administrator (user) to perform the following functions:
            1. Manage the system license.
            2. Configure the database(s) and database server for the Directory role,
            3. Activate/Deactivate the Directory role.
            4. Manually back up the Directory role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.
            5. Define the client-to-server communications security settings.
            6. Configure the network communications hardware, including connection addresses and ports.
            7. Configure system SMTP settings (mail server and port).
            8. Configure event and alarm history storage options.
      5. Unified Web Interface (UWI) General Requirements
         1. The USP shall support a unified web interface (UWI) for access control, video, and automatic license plate recognition.
         2. The UWI shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.
         3. The UWI shall be platform independent and run within Microsoft Internet Explorer, Firefox, Safari, and Google Chrome.
         4. The UWI shall be designed as an HTML5 application.
         5. The UWI shall support display on tablet format.
         6. The UWI shall support native H.264 video in the web interface.
         7. Web pages for the web interface shall be managed and pushed by the Web Interface Server. Microsoft IIS or any other web hosting service shall not be required given that all web pages shall be hosted by the Mobile Server.
         8. The Web Interface Server shall provide the ability to define a unique URL to access the web interface, to ensure the security of the application.
         9. The UWI shall provide the ability to load a camera layout.
         10. The UWI shall provide the ability to configure, save, and reload private camera layouts.
         11. The UWI shall provide the ability to control PTZ cameras.
         12. Functionalities:
             1. Log in support shall be available using:

Username and password

Active Directory *(Specifier, Professional and up, first integration included, additional licenses required more)*

Azure Active Directory, ADFS, OpenID Connect, or SAML2 identity provider *(Specifier, Professional and up, additional license required for OIDC & SAML2)*

* + - * 1. Ability for the user to change its password.
        2. Encrypt communications for all transactions.
        3. Print reports and export to CSV file.
        4. Access Control:

Cardholder and group (add/modify/delete)

Credential management (add/modify/delete)

Access rules management (add/modify/delete)

Visitor management (check-in/modify/check-out)

Unlock door

Override the unlocking schedule on a door

Door Activities report

* + - * 1. Alarms

Alarm report

* + - * 1. Threat Level management
        2. Automatic License Plate Recognition (ALPR)

Live monitoring of the ALPR cameras

ALPR reads and hits report

Addition of plate numbers to hotlists

* + 1. Health Monitor
       1. The USP shall monitor the health of the system, log health-related events, and calculate statistics.
       2. USP services, roles, agents, units, and client apps will trigger health events.
       3. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.
       4. A dedicated role, the Health Monitoring role, shall perform the following actions:
          1. Monitor the health of the entire system and log events.
          2. Calculate statistics within a specified time frame (hours, days, months).
          3. Calculates availability for clients, servers and ALPR/access/video units.
       5. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.
       6. A Health Monitoring dashboard task shall be available in the client application user interface to provide a live display, such as pie charts and event lists, for quick visual assessment on the general health of the system.
       7. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.
       8. Detailed system care statistics will be available through a web-based dashboard providing health metrics of USP entities and roles, including Uptime and mean-time-between-failures.
       9. All health events raised in the system can be used for automating the USP event/action management.
       10. Health events shall be accessible via the SDK (can be used to create SNMP traps).
    2. USP General Requirements
       1. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.
       2. The USP shall support the seamless unification of IP automatic license plate recognition system (ALPR), IP access control system (ACS), and IP video management system (VMS) under a single platform. The USP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, and reporting of embedded ALPR, ACS, and VMS systems and associated edge devices.
       3. Functionalities available with the USP shall include:
          1. Configuration of embedded systems, such as ALPR, ACS, and VMS systems.
          2. Live event monitoring.
          3. Live video monitoring and playback of archived video.
          4. Alarm management.
          5. Reporting, including creating custom report templates and incident reports.
          6. The Federation feature for global monitoring, reporting, and alarm management of multiple remote and independent ALPR, ACS, and/or VMS systems spread across multiple facilities and geographic areas. *(Specifier, Enterprise only, additional license required)*
          7. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system. *(Specifier, Enterprise Only, additional license required for each site)*
          8. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts. *(Specifier, Professional and up, first integration included, additional licenses required for more)*
          9. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming). *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
          10. SIP Intercom device integration for bi-directional communication.
          11. Integration with third party systems and databases via plug-ins (access control, video analytics, point of sale, and more). *(Specifier, Professional and up, additional license required)*
          12. Dynamic graphical map viewing.
          13. Asset management system integration. *(Specifier, Professional and up, additional license required)*
       4. The USP shall be deployed in one or more of the following types of installations:
          1. Unified ALPR, access, and video platform, and any combination thereof.
          2. Standalone ALPR, access control, or video platform.
          3. Unified access and video platform that federates multiple remote ALPR, ACS, and VMS.
          4. Standalone video platform that federates multiple independent remote ALPR.
          5. Standalone video platform that federates multiple independent remote VMS.
          6. Standalone access control that federates multiple independent remote ACS.
       5. Licensing:
          1. A single central license shall be applied centrally on the configuration server.
          2. There shall be no requirement to apply a license at every server computer or client workstation.
          3. Based on selected options, one or more embedded systems shall be enabled or disabled.
       6. Hardware and Software Requirements:
          1. The USP and embedded systems (automatic license plate recognition, access control, and video) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.
          2. The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.
          3. The USP database server(s) shall be built on Microsoft’s SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.
          4. The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.
          5. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and .NET software framework.
    3. USP Architecture
       1. The USP shall be based on a client/server model. The USP shall consist of a standard Server Software Module (SSM) and Client Software Applications (CSA).
       2. The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       3. The SSM shall be a Windows service that can be configured to start when the operating system is booted and run in the background. The SSM shall automatically launch at computer startup, regardless of whether or not a user is logged on the machine.
       4. Users shall be able to deploy the SSM on a single server or across several servers for a distributed architecture. The USP shall not be restricted in the number of SSM deployed.
       5. The USP shall support the concept of The Federation feature whereby multiple independent ALPR, ACS, and VMS installations can be merged into a single large virtual system for centralized monitoring, reporting, and alarm management. *(Specifier, Enterprise only, additional license required)*
       6. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
       7. The USP shall support up to one thousand instances of CSA connected at the same time. However, an unrestricted number of CSA can be installed at any time. *(Specifier, Maximum 5 with Standard; Maximum 10 with Professional; Unrestricted with Enterprise)*
       8. The USP shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
       9. The USP shall support uninterrupted video streaming. The CSA shall keep existing video connections active in the event that an SSM (except Archiver) becomes unavailable.
       10. Role-Based Architecture:
           1. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.
           2. Each role shall execute a specific set of tasks related to either core system, automatic license plate recognition (ALPR), access control (ACS), or video (VMS) functionalities, among many others. Installation shall be streamlined through the ability of the USP to allow administrators to:

Deploy one or several SSM across the network prior to activating roles.

Activate and deactivate roles as needed on each SSM.

Centralize role configuration and management.

Support remote configuration.

Move roles over from one SSM to another.

* + - * 1. Each role, where needed, shall have its own database to store events and role-specific configuration information.
        2. Roles without databases, such as The Federation feature, Active Directory, and Global Cardholder Management, shall support near real-time standby without any third-party failover software being required.
        3. Directory Role

The Directory role shall manage the central database that contains all the system information and component configuration of the USP.

The Directory role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.

The Directory role shall support the configuration/management of the following components common to the ALPR, ACS, and VMS sub-systems:

Security Partitions, users and user groups

Areas

Zones, input/output (IO) linking rules, and custom output behavior

Alarms. Schedules, and scheduled tasks

Custom events

Macros or custom scripts

The Directory role shall support the configuration/management of the following components specific to ALPR:

ALPR units and cameras

Hotlists, permit lists, and overtime rules

The Directory role shall support the configuration/management of the following components specific to ACS:

Door controllers, and input and output (IO) modules

Doors, Elevators, and Access rules

Cardholders and cardholder groups, credentials, and badge templates

The Directory role shall support the configuration/management of the following components specific to VMS:

Video servers and their peripherals (e.g., audio, IOs, and serial ports)

PTZ

Camera sequences

Recording and archiving schedules

* + - * 1. The Automatic License Plate Recognition (ALPR) role shall be responsible for synchronizing fixed ALPR units (cameras) and mobile ALPR applications under its control. The ALPR role shall also be responsible for logging all ALPR activities and events.
        2. The Video Archiver role shall be responsible for managing cameras and encoders under its control and archiving.
        3. The Media Router role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).
        4. The Access Manager role shall be responsible for synchronizing access control hardware units under its control, such as door controllers and I/O modules. This role shall also be responsible for validating and logging all access activities and events when the door controllers and I/O modules are online.
        5. The Zone Manager role shall be responsible for managing all software zones (collection of inputs) and logging associated zone events. Zones shall consist of inputs from both access control and video devices.
        6. The Health Monitoring role shall be responsible for monitoring and logging health events and warnings from the various client applications, roles, and services that are part of the USP. This role shall also be responsible for logging events within the Windows Event Log and for generating reports on health statistics and health history.
        7. Optional Roles:

The Federation role shall be responsible for creating a large virtual system consisting of hundreds or thousands of independent and remote ALPR, ACS, and/or VMS systems. *(Specifier, Enterprise only, additional license required)*

The Global Cardholder Synchronizer role shall be responsible for synchronizing cardholder and credential data between the local site and a central site. Synchronization between remote sites shall also be supported. *(Specifier, Enterprise only, additional license required)*

The Active Directory role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server. *(Specifier, Professional and up, first integration included, additional licenses required for more)*

The Intrusion Manager role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database.

The Asset Manager role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports. *(Specifier, Professional and up, additional license required)*

The Plug-in Manager role shall be responsible for the communication between the USP and third-party systems such as video analytics, ALPR, access control, video, and building management systems. *(Specifier, Professional and up, additional license required)*

The Point of Sale (POS) Manager role shall be responsible for integrating the USP with third party POS systems and for logging transactions. *(Specifier, Professional and up, additional license required)*

The Web SDK role shall be responsible for connecting the USP to any application or interface developed with the Web Service SDK. Applications developed with the Web Service SDK shall be platform independent and rely on the REST protocol for communications. *(Specifier, Professional and up, additional license required)*

The Communication Management role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

The Video Redirector role shall be responsible for connecting any video stream to a third-party system using standard RTSP protocol. This role shall provide access to live video. *(Specifier, Professional and up, requires the SDK packages, additional license required)*

* + - 1. Server Monitoring Service (Watchdog):
         1. The USP shall include a Server Monitoring Service that continuously monitors the state of the Server Software Module (SSM) service.
         2. The Server Monitoring Service shall be a Windows service that automatically launches at system startup, regardless of whether or not a user is logged into his account.
         3. The Server Monitoring Service shall be installed on all PCs/servers running an SSM. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the PC/server should it be unable to restart the service.
    1. USP ALPR, Video, and Access Control Unification
       1. The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ALPR, ACS, and VMS. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.
       2. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ALPR, ACS, and VMS.
       3. The user shall be able to associate one or more video cameras to the following entity types: ALPR cameras, areas, doors, elevators, zones, alarms, intrusion panels, and more.
       4. It shall be possible to view video associated to ALPR events when viewing a report.
       5. The USP shall support the following Alarm Management functionality:
          1. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
          2. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.
          3. Set the priority level of an alarm and its reactivation threshold.
          4. Provide the ability to group alarms by source and by type.
          5. Define the time period after which the alarm is automatically acknowledged.
          6. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
          7. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
          8. Define whether to display the source of the alarm, one or more entities, or an HTML page.
          9. Specify whether an incident report is mandatory during acknowledgment.
       6. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for ALPR, access control, and video alarms.
       7. Alarms shall be federated, allowing global alarm management across multiple independent ALPR, USP, ACS, and VMS systems.
       8. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.
       9. The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.
       10. Alarm unpacking and packing shall be supported where all the entities associated to an alarm can be displayed in the Monitoring UI with the single click of a button.
       11. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.
       12. The user shall be able to spontaneously trigger alarms based on something they see in the system.
       13. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.
       14. The user shall be able to investigate an alarm without acknowledging it.
    2. USP Threat Levels *(Specifier, Professional and Enterprise)*
       1. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.
       2. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.
       3. Threat Levels shall be set on an area or on the entire system.
       4. Threat Levels shall affect the system behavior by executing any action available in the USP such as: trigger output, start recording, block camera, override recording quality, arm zone, set a door in maintenance mode, and more.
       5. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.
    3. USP Remote Task
       1. The USP shall provide, through a Remote Task, capabilities to remotely monitor and control the content of other workstations running the CSA (Monitoring UI) that are part of the same system.
       2. The USP shall support video wall applications by connecting and controlling multiple workstations and monitors simultaneously.
       3. The Remote Task shall be a graphical interface showing a replication of the remote workstation running the CSA (Monitoring UI).
       4. The Remote Task shall allow the connection to other workstations using a low bandwidth mode to receive only snapshots of video viewed remotely.
       5. The Remote Task shall allow the connection to other workstations using a spy mode to remain invisible to the remotely connected workstation. The spy mode option should be available to the user with permission to access the feature.
       6. The functionality provided by the remote monitoring and control capability shall include:
          1. Remote monitoring and control of the monitoring and alarm monitoring tasks.
          2. Ability to remotely switch cameras, doors and zones into display tiles.
          3. Ability to remotely control live and playback video.
          4. Ability to remotely change the tile pattern.
          5. Ability to remotely create and delete tasks.
          6. Ability to remotely start/stop task cycling.
          7. Ability to remotely go into full screen mode.
          8. Ability to remotely save and reload the workspace.
    4. USP Advanced Task Management
       1. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day-to-day activities, and reporting.
       2. Administrators shall be able to assign tasks and lock the operator’s workspace. The user management of their workspace shall be limited by their assigned privileges.
       3. Operators shall be able save their tasks as either Public Tasks or Private Tasks and in a specific partition. Public tasks shall be available to all users. Private tasks shall only be available to the owner of the task.
       4. Operators shall be able to share their tasks by sending them to one or more online users. Recipients shall have the option to accept the sent task.
       5. Operators shall be able to duplicate a task.
    5. USP Reporting
       1. The USP shall support report generation (database reporting) for ALPR, access control, video, and intrusion.
       2. Each report in the system shall be a USP task, each associated with its own privilege. A user shall have access to a specific report task if they have the appropriate privilege.
       3. The workflows to create, modify, and run a report shall be consistent for ALPR, access control, and video reports.
       4. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ALPR, ACS, and VMS systems.
       5. ALPR shall support license plate pictures, and access control shall support cardholder pictures.
       6. The USP shall support the following types of reports:
          1. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more)
          2. Alarm reports
          3. Video-specific reports (archive, bookmark, motion, and more)
          4. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)
          5. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more)
          6. Health activity and health statistics reports
          7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports
       7. Generic Reports, Custom Reports, and Report Templates
          1. The user shall have the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.
          2. The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).
          3. All report templates shall be created within the Monitoring UI.
          4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
          5. An unrestricted number of custom reports and templates shall be supported.
       8. A reporting task layout shall consist of panes with settings (report length, filters, go and reset commands, etc.), the actual report data in column format, and a pane with display tiles. The user shall be able to drag and drop individual records in a report onto one or more display tiles to view an ALPR event, cardholder’s picture ID, or playback a video sequence.
       9. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.
       10. The reporting task shall have the ability to display results through graphics such as line charts, bar charts, stacked bar charts, doughnut charts, and pie charts.
       11. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.
       12. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, export the graphics chart in JPG/PNG, and automatically email a report based on a schedule and a list of one or more recipients.
       13. Shall allow the ability to insert a custom logo when generating reports.
    6. USP Dashboards
       1. The USP shall support the ability to create dashboards.
       2. Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to dashboards should also be allowed to users granted the appropriate privilege.
       3. Dashboards in the system shall be a USP task. A user shall have access to a specific dashboard task if they have the appropriate privilege.
       4. Dashboards shall be saved either in a private folder or a public folder.
       5. A dashboard shall consist of a canvas with various widgets displayed on the canvas. All widgets should offer the ability to specify location and size to the widget, a title to the widget, a background color to the widget, and the ability to refresh periodically the content of the widget.
       6. Dashboard widget types shall be:
          1. Image: provides the ability to display an image (JPG, PNG, GIF, BMP) on a dashboard.
          2. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, color, and alignment can be specified by the user.
          3. Tile: provides the ability to display a URL on a dashboard.
          4. Web page: provides the ability to display a URL on a dashboard.
          5. Entity Count: provides the ability to display the total number of a specific entity type in the USP.
          6. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.
          7. Map: Provides the ability to display and interact with maps on a dashboard.
       7. It shall be possible to extend the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
       8. The USP shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.
    7. USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)*
       1. The USP shall support the concept of a Federation feature for ALPR, access control, and video.
       2. The Federation feature shall allow multiple independent USP systems (Federated systems) to be unified into a larger virtual system (the Federation feature). This shall facilitate the global monitoring of multiple independent USP systems.
       3. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.
       4. Entities that shall be federated and monitored centrally from the Federation feature shall include ALPR events, alarms, areas, cameras, cardholders and cardholder groups, credentials, doors, elevators, and zones (monitored inputs).
       5. The Federation feature shall support a cloud-based deployment, whereby the service and infrastructure will be updated automatically and provisioned by the service provider, without need for on-site hardware.
       6. The Federation feature shall support Global Alarm Management from the Monitoring UI for ALPR, access control, and video.
       7. The Federation feature shall support Global Report Generation from the Monitoring UI for ALPR, access control, and video.
       8. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (for example, generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).
    8. USP User and User Group Security, Partitions, and Privileges Management
       1. The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if they have the appropriate privileges.
       2. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:
          1. ADFS (Active Directory Federation Services)
          2. Azure Active Directory (through OpenID Connect)
          3. Ping Identity (through OpenID Connect)
          4. KeyCloak (through OpenID Connect)
          5. Other Open ID Connect / SAML2 authentication agents
       3. Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups. User group nesting shall be allowed.
       4. User privileges shall be extensive in the USP. All configurable entities for the USP, including ALPR, access control, and video shall have associated privileges.
       5. Specific entities, such as cardholders, cardholder groups, and credentials, shall include a more granular set of privileges, such as the right to access custom fields and change the activation or profile status of an entity.
       6. Partitions:
          1. The USP shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a system into multiple security partitions.
          2. All entities that are part of the USP can be assigned to one or more partitions.
          3. A user who is given access to a specific partition shall only be able to view entities (components) within the partition to which they have been assigned. Access is given by assigning the user as an accepted user to view the entities that are members of a particular partition.
          4. A user or user group can be assigned administrator rights over the partition.
       7. It shall be possible to specify user and user group privileges on a per partition basis.
       8. Advanced logon options shall be available such as dual logon and more.
       9. It shall be possible to specify an inactive period for the Monitoring UI after which time the application shall automatically lock, while still preserving access to currently displayed camera feeds. It shall also be possible to log the user out immediately after the inactivity period or within an amount of time from when the application was locked.
       10. It shall be possible to review user permissions and determine:
           1. For any entity in the system, which user group or user can view or modify it.
           2. For any user group or user in the system, what are its privileges.
           3. For any privilege in the system, which user group or user is allowed to perform the underlying action.
    9. USP Event/Action Management
       1. The USP shall support the configuration and management of events for ALPR and video. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.
       2. The USP shall receive all incoming events from one or more ALPR, ACS, and/or VMS systems. The USP shall take the appropriate actions based on user-defined event/action relationships.
       3. The USP shall receive and log the following events:
          1. ALPR events
          2. System-wide events
          3. Application events (clients and servers)
          4. Area, camera, door, elevator, and ALPR events (reads and hits)
          5. Unit events
          6. Zone events
          7. Alarm events
          8. Health monitoring events
       4. The USP shall allow the creation of custom events.
       5. The USP shall have the capability to execute an action in response to an ALPR, access control, and video event. The USP shall support the following list of actions, without being limited to:
          1. Add bookmark
          2. Block and unblock video
          3. Display a camera on an analog monitor
          4. Display an entity in the CSA
          5. Email a report
          6. Email a snapshot
          7. Export report
          8. Go home
          9. Go to preset
          10. Override recording quality
          11. Play a sound
          12. Reboot unit
          13. Run a macro
          14. Run a pattern
          15. Send a message
          16. Send an email
          17. Set threat level
          18. Start/Stop applying video protection
          19. Start/Stop recording
          20. Start/Stop transfer
          21. Trigger alarm
          22. Trigger output
          23. Set maintenance mode
          24. Trigger incident
          25. Set interface background color
          26. Set minimum security clearance
       6. The USP shall allow a schedule to be associated with an action. The action shall be executed only if it is an appropriate action for the current time period.
    10. USP Schedules and Scheduled Tasks
        1. Schedules:
           1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if they have the appropriate privileges.
           2. The USP shall provide full flexibility and granularity in creating a schedule. The user shall be able to define a schedule in 1-minute or 15-minute increments.
           3. Daily, weekly, ordinal, and specific schedules shall be supported.
        2. Scheduled Tasks:
           1. The USP shall support scheduled tasks for ALPR and video.
           2. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.
           3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email, emailing a report or triggering incidents.
    11. USP Macros and Custom Scripts
        1. The USP shall enable users to automate and extend the functionalities of the system through the use of macros or custom scripts for ALPR, access control, and video.
        2. Custom macros shall be created with the USP Software Development Kit (SDK).
        3. A macro shall be executed either automatically or manually.
        4. In the Monitoring UI, a macro shall be launched through hot actions.
    12. USP Dynamic Graphical Maps (DGM)
        1. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.
        2. The USP shall provide a map centric interface with the ability to command and control all the USP capabilities from a full screen map interface.
        3. It shall be possible to span the map over all screens of the USP client station. In the scenario where the map is spanned over all the screens of the USP client station it shall be possible to navigate the map including pan and zoom, and the map’s moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same command and control capabilities than in a single screen display.
        4. The DGM shall support the following file format and protocol for importing map background:
           1. PDF
           2. JPG
           3. PNG
           4. Web Tile Map Service (WMTS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
           5. BeNomad
           6. AutoCAD (DWG & DXF)
        5. The DGM shall provide the following online map providers for use as map background and provide the ability to manage their service license if they require one:
           1. Google Map, aerial, terrain (Licensed)
           2. Bing Map, aerial, satellite, hybrid (Licensed)
           3. ESRI ArcGIS (Licensed)
           4. OpenStreet Map aerial (Licensed)
           5. OVI hybrid
        6. It shall be possible to configure a mixed set of maps made of GIS, online providers, and private imported files and link them together.
        7. The DGM shall provide the ability to display all native entities of the USP including:
           1. Cameras, fix, and PTZ
           2. Doors
           3. Camera sequences
           4. Areas
           5. Intrusion areas
           6. Intrusion zones
           7. License Plate Recognition cameras
           8. Digital inputs
           9. Digital outputs
           10. Intercoms
           11. Alarms
           12. Macros
           13. Police Car Patrollers
        8. The DGM shall provide the ability to draw and display information over the map in the form of:
           1. Vectoral shapes: lines, rectangles, polygons, ellipse
           2. Pictures
           3. Text
        9. The DGM shall provide the ability to display any type of third-party entities integrated through an SDK.
        10. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.
        11. The DGM shall provide the ability to the operator to manage layers of entities displayed over the map and select the desired layer including the entity name, being able to turn them on and off and changing the superposition order.
        12. The DGM shall provide the ability to display entity type based on zoom level.
        13. The DGM shall provide the ability to import data layers from one or more ESRI ArcGIS servers.
        14. The DGM shall provide the operators with the ability to manage layers that are imported from ESRI ArcGIS. The operators shall be able to turn the layers on and off, as well as sort the layers.
        15. The DGM shall offer built-in map data backup and restore for both map backgrounds and layers of entities.
        16. The DGM shall offer failover capabilities.
        17. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.
        18. The DGM shall provide a means to update a map background without affecting the map object configuration.
        19. The DGM shall offer a user-friendly graphical map designer to configure the maps.
        20. The DGM shall provide a user friendly and intuitive navigation that includes:
            1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
            2. The ability to define favorites for recurrent position recall.
            3. The possibility to create links between maps. The map links shall allow the link from one map to multiple maps representing the floors of a building. Navigating between floors of a building shall keep the zoom level of the map.
            4. A common user experience regarding navigation into the map for both GIS and private maps. *(Specifier, Professional or Enterprise required for GIS)*
        21. It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.
        22. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.
        23. The DGM shall offer a smart selection tool to access the video. By clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.
        24. It shall be possible to select a location by drawing a zone of interest on the DGM, and to display all the entities that are part of that zone of interest at once.
        25. The user shall be able to select and display the content of multiple USP entities on the map in pop-up windows.
        26. The user shall be able to move, resize, and pin the USP entity pop-up windows to the map.
        27. It shall be possible to access live and playback video from the map.
        28. It shall be possible to monitor all entity event notifications from the DGM. Users shall be able to turn notifications on and off per entity.
        29. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:
            1. Center the map on entities related to the alarm.
            2. Visualize the Alarm notifications on the map and access the related videos from the map.
            3. Trigger and receive alarms.
            4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
            5. Visualize that an alarm occurred in an underlying linked map.
        30. The DGM shall provide the following search capabilities:
            1. Search and center by entity name.
            2. From the Display of an entity in the USP, locate the entity on the map and offer the ability to select another one close-by.
        31. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.
        32. The DGM shall support the use of GIS maps or private maps or a combination of both for map background. *(Specifier, Professional or Enterprise required for GIS)*
        33. The DGM shall be compatible with any GIS compliant maps with the OGC and supporting WMTS and WMS. This includes, but is not limited to, ESRI maps. The DGM shall allow the selection of the appropriate GIS layers. *(Specifier, Professional or Enterprise required for GIS)*
        34. The DGM shall provide an intuitive built-in map designer for entity positioning on the map using drag and drop. Any configuration shall be graphic.
        35. It shall be possible to edit and configure multiple map objects at once.
        36. All map design modifications shall be logged in an audit trail.
        37. Various actions shall be available within maps for execution through simple and intuitive double-click, right-click, or drag-and-drop functionality. Examples of actions available through maps shall include unlocking a door and acknowledging an alarm.
        38. Through the following functionality, the DGM shall allow the management of USP alarms from the map:
            1. Locate on the map entities related to the alarm.
            2. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.
            3. List, select, and locate alarms.
            4. Auto center the map on the highest priority alarm.
            5. Handle the alarm from the map, including acknowledgement, forwarding, and investigation.
            6. All map containers, such as hotspots or map links shall reflect the alarm status of the contained entities.
        39. It shall be possible to add advanced functionality to maps object using the SDK. Any functionality available through the USP SDK shall be available within maps.
        40. The DGM shall offer lasso tools for:
            1. Displaying entities at one location through a single action.
            2. Triggering an action on all entities at one location in a single click.
            3. Editing multiple entities at one location simultaneously.
        41. The DGM shall allow the display of USP entities selected from the map on a remote monitor (video wall).
        42. The DGM shall provide the ability to search within the map by entity name.
        43. The DGM shall allow the use of KML overlay map information for both GIS and private maps. Movable objects shall be supported using KML. *(Specifier, Professional and Enterprise)*
        44. The Contractor shall provide licenses for each entity that is required to be shown on the graphical maps.
    13. USP Audit and User Activity Trails (Logs)
        1. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.
        2. Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
        3. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
        4. The USP shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the USP such as login, ALPR event viewed, hotlist edits, camera viewed, badge printing, video export, and more.
        5. The ACS shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/ CSV file.
    14. USP Incident Reports
        1. Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.
        2. The operator shall be able to create standalone incident reports or incident reports tied to alarms.
        3. The operator shall be able to link multiple video sequences to an incident, access them in an incident report, and change the date or time of the sequences later on.
        4. It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.
        5. Incident reports shall allow the creation of a custom form on which to input information on an incident.
        6. Incident reports shall allow entities, events, and alarms to be added to support at the report’s conclusions.
        7. Incident reports shall allow the use of a custom logo, the default Mission Control logo or no logo at all.
    15. USP Data Ingestion
        1. The USP shall allow the possibility to import external data from outside sources to enhance unification of data sources within the USP.
        2. Each data source shall be defined by a set of fields and field types that describe the data source. Field types shall be:
           1. String
           2. 32-bit and 64-bit integer
           3. Floating point number
           4. Boolean
           5. Timestamp
           6. Binary (in a file or base 64)
           7. Data/Time
        3. The visualization of each data point from a data source shall be configurable to determine what fields from the data should be displayed. The configuration of each field should be:
           1. Which fields are displayed or hidden
           2. What order are the fields displayed
           3. A label to specify the name of the field (to have a key:value format)
           4. An option to specify how to display the field (text value, image, clipboard value, hyperlink to a web page, hyperlink to an entity in the system, sound file)
        4. A privilege should be available for each data source to allow / deny access to specific user & user groups of the USP.
        5. Ingested data shall be available in the USP reporting system.
        6. Ingested data shall be available to display in the USP Dashboards.
    16. USP Third Party Integration
        1. Microsoft Active Directory Integration *(Specifier, Professional and up, first integration included, additional licenses required for more)*
           1. The USP shall support a direct connection to one or multiple Microsoft Active Directory server via the Active Directory role(s). Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.
           2. Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups.
           3. The USP shall be able to connect to and synchronize data from multiple Active Directory servers (up to 10).
           4. The USP shall support synchronizing Active Directory Universal Groups as well as security groups belonging to other domains within the same forest.
           5. The USP shall support Microsoft Active Directory encryption using LDAP SSL.
           6. When enabled, Active Directory shall manage user logon to the USP client applications through the user’s Windows credentials. Logging to the USP shall utilize native Active Directory password management and authentication features.
           7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:

Users (username, first and last names, email address, and more)

User groups (user group name, description, and group email address)

Active Directory attributes to USP custom fields

* + - * 1. When enabled, the addition, removal, or suspension of a user’s Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent user account in the USP.
        2. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include on first logon (users only), manual synchronization, and scheduled synchronization.
        3. The USP shall support user connections across independent organizations by connecting to an external identity provider using claims-based authentication such as ADFS (Active Directory Federation Services), Azure Active Directory, other OpenID Connect & SAML2 providers.
      1. Intrusion Detection Integration: *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
         1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
         2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):

Arm and disarm intrusion devices (manually, on schedule, or following a USP event).

Activate or trigger intrusion device outputs.

View intrusion events and alarms.

Monitor the status, including arming status, of the intrusion devices.

Video verification of intrusion events and alarms with video panels.

Create USP zones using intrusion device inputs.

* + - * 1. Currently supported intrusion panels include:

Bosch Legacy G Series panels

Bosch B & G Series panels

Bosch Map 5000

DSC Power Series panels

DMP XR Series panels

Honeywell Galaxy Dimension and Flex panels

Vanderbilt SPC

UTC Advisor Master and Advanced

Satel INTEGRA panels

Telenot Complex 400H panels

* + - * 1. Additional intrusion devices supported include:

Buytime

Alarm Panel Receiver

Southwest Microwave RPMII

* + - 1. Third Party Access Control Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network and should not support administrative tasks such as cardholder management.
         2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

Synchronize access control entities and receive associated events and states within the USP, including:

Cardholders

Visitors

Readers and doors

Alarms

Inputs and outputs

Monitor access control events.

Monitor and Acknowledge access control alarms.

Trigger actions and outputs in the access control software using hot actions and event-to-actions.

Lock and unlock doors in the access control software.

Video verification of access control events and alarms.

Configure event-to-actions using the access control events and alarms.

Generate Security Center reports using from the in the access control data.

View and monitor states of door entities in the USP maps.

* + - * 1. Currently supported access control manufacturers include:

Tyco Softwarehouse CCURE

UTC Lenel Onguard

Amag Symmetry

Siemens Sipass

AssaAbloy ARX

* + - 1. Third Party Destination Dispatch Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third party destination dispatch (elevator control) software via the SDK. Communications with destination dispatch software shall be over an IP network.
         2. Integrating with destination dispatch software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of destination dispatch software with the USP shall include the following (where supported by the destination dispatch solution):

Destination dispatch entity creation and reception of associated events and state within the USP, including:

Floors and landings

Elevator cars (front/rear doors) and kiosks

Cardholders and credentials (if applicable)

Monitor destination dispatch events.

Trigger manual dispatch actions.

Video verification of destination dispatch events.

Configure event-to-actions using the destination dispatch events.

Generate Security Center reports using the destination dispatch data.

Support multiple readers:

Kiosk internal readers

USP readers

Kiosk advanced modes and passenger types.

* + - * 1. Currently supported destination dispatch manufacturers include:

Otis Compass

Thyssenkrupp

MCE

KONE

* + - 1. Asset Management Integration: *(Specifier, requires an additional license, Professional and up)*
         1. The USP shall integrate with third party asset management systems via the Asset Management Role.
         2. Communications with asset management solutions shall be over an IP network (via software communications).
         3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):

Synchronize asset management system assets with USP asset entities.

Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

Synchronization of asset management alarms with Security Center alarms.

Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

Real-time tracking of asset locations on a per area basis.

Asset Management Inventory reporting task that details the current location (area) of an asset.

Asset Activity reporting task that provides a historical review of asset-related events and activity.

* + - * 1. Currently supported asset management systems include:

Deister Key management

Morsewatchmans

TRAKA

Key Systems

* + - 1. Additional Third-Party Integrations
         1. The USP shall support multiple approaches to integrating third party systems. These shall include: Software Development Kits (SDKs), REST-based Web Service SDKs, RTSP Service SDKs, and more. *(Specifier, Professional and up, SDK package and license required)*
         2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as: *(Specifier, refer to the website for how these are licensed, for an updated list of available Third-Party Integrations, please refer to the supported plugin guide)*

Third-party video systems

Third-party access control systems

ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors

Building management systems

Access Control ecosystem (such as IDscanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)

Transaction monitoring (POS, Barcode scanning, ATM)

Industrial IoT: Data ingestion from external devices through standard communication protocols (Modbus, BACnet, OPC, SNMP, HTTP Server, MQTT Client, TCP Server)

Industrial Protocol Interface: Data exposure from GSC to external protocol interfaces using standard communication protocols (BACnet, SNMP)

Videowall (Barco, Eizo)

Human resource management systems (HRMS)

Autonomous Drone Integration

Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))

Gunshot Detection (Shot Spotter, Guardian GunShot)

Dynamic Logbook: Customizable forms with reporting capabilities

* + 1. USP Software Development Kit (SDK)
       1. A USP SDK shall be available to support custom development for the platform.
       2. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.
       3. Integration with external applications and databases shall be possible with the SDK.
       4. The SDK shall enable end-users to develop new functionality (user interface, standalone applications or services) to link the USP to third party business systems and applications, such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.
       5. The SDK shall be based on the .NET framework.
       6. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.
       7. The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
       8. The SDK shall provide an extensive list of programming functions to view and configure ALPR, ACS, and VMS.
       9. The SDK shall provide an extensive list of programming functions to view and configure most ALPR entities.
       10. The SDK shall be able to receive real time events from the following USP entities: users and user groups, areas, zones, cameras, video units, doors, door controllers (units), elevators, cardholders, cardholder groups, and credentials.
       11. The SDK shall be able to query the history of events for areas, cameras, zones, alarms, cardholders, credentials, visitors, doors, query license plate read events, license plate hit events, generate a license plate hits report, generate a license plate reads report.
       12. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.
  1. **Execution**
     1. Warranty
        1. The product shall perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use. Software defects are covered through Service Releases and Cumulative Updates which are available for a period of 1 year from the date of the software purchase.
        2. Extended warranty, up to 5 years, shall be available through the purchase of the Genetec Advantage support service which includes the following additional services over the standard warranty:
           1. Access to phone support and online chat for technical assistance.
           2. Online case management.
           3. Online system availability monitor.
           4. Access to Major and Minor Release Upgrades.
           5. 24/7 pager support and dedicated support specialist. *(Specifier, additional cost)*
        3. Genetec AutoVu Hardware Warranty:
           1. One year Return and Repair warranty is included with all AutoVu hardware.
           2. Optional advanced replacement warranty can be purchased.
           3. Extended hardware warranty can be purchased up to 5 years from the date of purchase.
     2. Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 
        1. General Requirements:
           1. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:

Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

Complex enterprise installations involving advanced functionality (for example The Federation feature, failover, plugins) and/or multiple systems (for example access control, video, ALPR) and/or third-party integrations.

Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

* + - * 1. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.
      1. Deployment Management Service:
         1. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization and who will be responsible for:

Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

Providing a project plan for the deployment of the vendor's USP.

Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

* + - 1. Solution Architect Service:
         1. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:

Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews, as well as performance reviews of the vendor’s USP.

Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.

Providing upgrade and migration strategy for the vendor’s USP where applicable.

Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

* + - 1. System Configuration and Commissioning Service:
         1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

Assisting the contractor’s or subcontractor’s onsite/remote technicians with the configuration and commissioning of the vendor’s USP at the client site.

Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.

Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

* + 1. Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)*
       1. The contractor shall engage the services of the USP vendor to assist in the end user training of the USP at the end-user site.

Genetec, Omnicast, Synergis, Federation, Sipelia, the Genetec Logo, and the Mobius Strip Logo, are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

1. **Section 28 23 00 – Video Management System**
   1. **General**
      1. Related Work
         1. Division 14 - General Elevator Requirements
         2. Section 28 13 00 – Electronic Access Control System
      2. Definitions
         1. ACS – Access Control System
         2. CSA – Client Software Application
         3. DGM – Dynamic Graphical Maps
         4. DVS – Digital Video Server
         5. ALPR – Automatic License Plate Recognition
         6. SDK – Software Development Kit
         7. GLM – Genetec Lifecycle Management
         8. SSM – Server Software Module
         9. UI – User Interface
         10. USP – Unified Security Platform
         11. UWI - Unified Web Interface
         12. VMS – Video Management System
      3. Qualifications
         1. The system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Omnicast™ Technical Certification.
         2. Optionally, the system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Enterprise Technical Certification.
         3. The system programmer shall be a Genetec certified partner with the following level of qualification: *(Specifier, select one of the following)*
            1. Certified Reseller or up
            2. Elite Reseller or up
            3. Unified Elite Reseller
         4. The system programmer shall submit proof of certifications.
   2. **Products**
      1. VMS General Requirements
         1. The VMS shall support updating its camera drivers independent from the VMS installation. New drivers shall be released multiple times a year to extend support for new devices and features.
         2. The VMS shall be based on a true open architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure, and non-proprietary storage.
         3. The VMS shall offer a complete and scalable video surveillance solution that shall allow cameras to be added on a unit-by-unit basis.
         4. The VMS shall interface with analog-to-digital video encoders and IP cameras and with digital-to-analog video decoders, hereafter referred to as digital video servers (DVS). The VMS shall support DVS from various manufacturers.
         5. The VMS shall integrate DVS using the DVS native SDK or using the following industry standards to interface to the DVS:
            1. ONVIF
         6. All video streams supplied from analog cameras or IP cameras shall be digitally encoded in H.265, H.264, MPEG-4, MPEG-2, MJPEG, MxPEG, Wavelet, or JPEG2000 compression formats and recorded simultaneously in real time.
         7. All audio streams supplied from IP video servers shall be digitally encoded in g711 (u-law), g721, g723, or AAC compression formats and recorded simultaneously in real time.
         8. Each camera’s bit rate, frame rate, and resolution shall be set independently from other cameras in the system and altering these settings shall not affect the recording and display settings of other cameras.
         9. The VMS shall be able to use multiple CCTV keyboards to operate the entire set of cameras throughout the system, including brands of cameras from various manufacturers and including their PTZ functionalities (i.e., Pelco keyboard controls Panasonic dome or vice-versa).
         10. The VMS shall be able to retrieve and set the current position of PTZ cameras using XYZ coordinates.
         11. The VMS shall support PTZ camera protocols from multiple manufacturers, including analog and IP protocols.
         12. The VMS shall arbitrate the user conflict on PTZ usage based on user levels per camera.
         13. The VMS shall support the following list of [CCTV keyboards](https://www.genetec.com/binaries/content/assets/genetec/en-genetec-security-center-supported-hardware-list.pdf):
             1. American Dynamics 2078 ASCII, and American Dynamics 2088 ASCII
             2. Bosch Autodome, Bosch Intuikey
             3. DVTel
             4. DT (before version 3.0)
             5. GE ImpactNet
             6. Panasonic, Pelco ASCII, Pelco KBD-300, Pelco 9760, and Pelco P.
             7. Radionics
             8. Hanwha Techwin SSC-100, SPC-600, SPC-2010, SPC-6000, and SPC-7000.
             9. Video alarm
             10. Samsung SSC-1000
             11. Sony RM-NS1000
             12. Panasonic WV-CU161C
             13. Panasonic WV-CU950 Ethernet keyboard
         14. The VMS shall support the following list of joysticks:
             1. Axis 295
             2. Axis T8310, T8311, T8312, T8313 Video Surveillance Control Board
             3. Any USB joystick detected as a Windows Game Controller
         15. The VMS shall support changing passwords of video units (for a list of supported units, see the Security Center Administrator Guide):
             1. The VMS shall show the strength of the current unit password.
             2. The VMS shall have the ability to change the password manually or using a string password generator for single or multiple units.
             3. The VMS shall have the ability to automatically update passwords on schedule.
             4. The VMS shall keep the history for passwords and the ability to retrieve them.
             5. The VMS shall have the ability to export passwords of units for safekeeping.
         16. The VMS shall support managing certificates of video units used for secure command and control (HTTPS and RTSPS) (for a list of supported units, see the Security Center Administrator Guide):
             1. Push Initial Certificate
             2. Automatically switch from HTTP and RTSP to HTTPS and RTSPS
             3. Allow certificate renewal
             4. Manage certificates manually for a single device or a batch of devices
             5. Automatically update upon configured schedule for single device or batch of devices
         17. The VMS shall allow for the configuration of a time zone for each camera connected to a DVS. For playback review, users shall have the ability to search for video based on the following options:
             1. Local time of the camera
             2. Local time of the SSM
             3. Local time of user’s workstation
             4. GMT Time
             5. Other time zone
         18. Audio and Video storage configuration for the SSM shall either be:
             1. Internal or external IDE/SATA/SAS organized or not in a RAID configuration.
             2. Internal or external SCSI/iSCSI/Fiber Channel organized or not in a RAID configuration.
             3. Within the overall storage system, it shall be possible to include disks located on:

External PCs on a LAN or WAN

Network Attached Servers (NAS) on a LAN or WAN

Storage Area Networks (SAN)

* + - 1. The SSM shall not limit the actual storage capacity configured per server.
      2. Manufacturer:
         1. Genetec Security Center: *(Specifier, select one of the following)*

Enterprise

Professional

Standard

* + 1. Cyber Security Requirements
       1. The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       2. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:
          1. ADFS (Active Directory Federation Services)
          2. Azure Active Directory (through OpenID Connect)
          3. Ping Identity (through OpenID Connect)
          4. KeyCloak (through OpenID Connect)
          5. Other Open ID Connect / SAML2 authentication agents
       3. The USP shall limit the IP ports in use and shall provide the Administrator with the ability to configure these ports.
       4. The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.
       5. The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate-based AES 128-bits encryption. The VMS shall:
          1. Allow encryption to be set on a per camera basis for all or some of the cameras.
          2. Provide up to 20 different certificates for different groups of CSA or users who have been granted access to decrypted streams.
          3. Not decrease the recording performance by more than 50% when encryption is enabled.
          4. Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.
          5. Use a random encryption key and change periodically.
          6. Allow encrypted streams to be exported.
       6. The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.
       7. The USP shall support encryption for all communications with its databases.
       8. The USP shall provide in its main user interface a visual list showing the state of all configuration items relating to the cyber security hardening of the features of the system.
       9. The USP shall provide recommendations relating to the passwords used to access the hardware units in the system. The recommendation should display if the passwords used on the units are weak, average, strong, or very strong.
       10. The USP shall provide the ability to manually or automatically change the video unit passwords with manufacturer’s native API, standard Genetec Protocol or ONVIF. The VMS shall support password change for video units as follows:
           1. In batch or per unit
           2. On schedule
           3. From an event
           4. Based on manufacturer’s policies
           5. The USP shall allow backup of last 5 passwords.
           6. The USP shall allow copying password to clipboard to be used in the device webpage if the user has the appropriate privileges.
           7. The USP shall provide the ability to export the video unit passwords if the user has the appropriate privileges.
       11. The USP shall provide recommendations relating to the firmware of the hardware units enrolled in the system. Recommendations should display if the firmware is up to date, out of date, or if it has known security vulnerabilities.
    2. Failover and Standby Requirements
       1. The USP shall support native and off-the-shelf failover options.
       2. Failover Directory:
          1. The Standby Directory shall act as a replacement SSM on hot standby, ready to take over as the acting Directory in case the primary Directory fails. The failover shall occur in less than one minute. No action from the user shall be required.
          2. The USP shall support up to five (5) Directories on standby, lined up to take over as the acting Directory in a cascading fashion.
          3. The Standby Directory shall keep its configuration database synchronized with the primary Directory.
          4. The Standby Directory shall support disaster recovery scenarios where a server can be located in another geographic area (or building) and only take over if all other Directories become offline.
          5. The Standby Directory shall support synchronization of the configuration databases using a backup and restore mechanism. The synchronization period shall be configurable from 15 minutes to 1 week.
          6. The Standby Directory shall support real-time synchronization of the configuration databases using SQL Mirroring or SQL Always On.
       3. Standby Archiver. Refer to section 2.05 Standby Archiver for more information.
       4. Off-the-shelf standby/failover options (excluding the VMS Archiver) shall include: *(Specifier, additional license required per server that will failover, Enterprise only)*
          1. Windows Clustering
    3. Archiving
       1. The Archiver (role) shall use an event and timestamp database for the advanced search of audio/video archives. This database shall use Microsoft SQL.
       2. The Archiver shall protect archived audio/video files and the system database against network access and non-administrative user access.
       3. The Archiver shall digitally sign recorded video using an EdDSA signature algorithm based on a public/private key cryptography.
       4. The Archiver shall offer a plug and play type hardware discovery service with the following functionalities:
          1. Automatically discover DVS units as they are attached to the network.
          2. Discover DVS units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.
       5. The Archiver shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.
       6. The Archiver shall provide a pre-alarm and post-alarm recording option that can be set between one second and 5 minutes on a per camera basis.
       7. The Archiver shall provide the functionality of storing of video and audio streams based on triggering events, such as:
          1. Digital motion detection
          2. Digital input activation
          3. Macros
          4. Through SDK application recording
       8. The Archiver shall perform video motion detection on each individual camera based on a grid of 1320 motion detection blocks. All of the video motion detection settings are configurable on schedule. A global sensitivity threshold is available to reduce motion detection sensitivity when the video signal is noisy or when a lot of false hits are incurred. Video motion detection itself can be set into four different modes:
          1. Full Screen: All 1320 blocks on screen are activated, and a general threshold for the overall motion in the entire image can be set, and when it is reached, it can trigger recording and a motion event or a custom event.
          2. Full Screen Unit: This is the same as the Full Screen, but the motion detection takes place in the DVS.
          3. Detection Zone: Six overlapping zones can be defined in the 1320 blocks on screen with each of these zones having its own threshold, and, when that threshold is reached, each one of them can trigger recording and a motion event or a custom event. Each zone triggering its own event allows for the configuration of directional motion detection events and other complex motion detection logic.
          4. Detection Zone Unit: This is the same as the Detection Zone, but the motion detection takes place in the DVS and only one zone is supported.
          5. Disabled: No motion detection is performed on this camera.
       9. The Archiver shall be able to detect motion in video within 200 milliseconds and not only on key frames.
       10. The Archiver shall allow for multiple recording schedules to be assigned to a single camera. Each schedule shall be created with the following parameters:
           1. Recording mode:

Continuous

On Motion/Manual

Manual

Disabled

* + - * 1. Recurrence pattern:

Once on specific days

Specific days on a yearly basis

Specific days on a monthly basis

Specific days on a weekly basis

Daily

* + - 1. Time coverage:

All day.

Specific time range(s).

Daytime or nighttime based on the times of sunrise and sunset that are automatically calculated from the time of year and a geographical location. Provision shall be given to offset the calculated sunrise or sunset time by plus or minus 3 hours.

* + - 1. The Archiver shall allow each camera (video source) to be encoded multiple times in the same or different video formats (H.265, H.264, MPEG-4, MPEG-2, MJPEG, MxPEG, Wavelet, or JPEG2000), limited only by the capabilities of each DVS.
      2. Whenever multiple video streams are available from the same camera, users shall be free to use any one of them based on their assigned usage. The standard video stream usages are:
         1. Live
         2. Recording
         3. Remote
         4. Low resolution
         5. High resolution
      3. The Archiver shall allow the video quality to vary according to predefined schedules. Such schedules shall have the same configuration flexibility as the recording schedules mentioned earlier. The video quality shall be based on, but not limited to, the following parameters:
         1. Maximum bit rate
         2. Maximum frame rate
         3. Image quality
         4. Key frame interval
      4. The Archiver shall have the ability to dynamically boost the quality of the "recording stream" (see previous bullet) based on specific events:
         1. When recording is started manually by a user.
         2. When recording is triggered by a macro, an alarm or detected motion.
      5. The Archiver shall have the capacity to communicate with the DVS using 128 bits SSL encryption.
      6. The Archiver shall have the capacity to communicate with the DVS using HTTPS secure protocol.
      7. The Archiver shall have the capacity to receive multicast UDP streams directly from the DVS.
      8. For network topologies that restrict the DVS from sending multicast UDP streams, the Archiver shall redirect audio/video streams to active viewing clients on the network using multicast UDP.
      9. The Archiver shall have the capacity to redirect audio/video streams to active viewing clients on the network using unicast UDP or TCP.
      10. The Archiver shall empower the administrator with a full range of disk management options:
          1. The Archiver shall allow the administrator to choose which disks to use for archiving and to set a maximum quota for each.
          2. The Archiver shall allow the administrator to spread the archiving of different cameras on different disk groups (groups of disks controlled by the same controller) so that archiving could be carried out in parallel on multiple disks.
          3. The Archiver shall have the capacity to move video archives to the Azure Cloud. The archives will be moved after a preset number of days.
      11. The Archiver shall empower the administrator with a full range of archive management options:
          1. The Archiver shall provide a graphical representation of video sequences and recording gaps.
          2. The Archiver shall provide the percentage of available video displayed over the queried time range.
          3. The Archiver shall provide a way to identify the location of the video sequences.
      12. The Archiver shall offer the following options to clean up old archives, on a camera-by-camera basis:
          1. After a preset number of days.
          2. Deleting oldest archives first when disks run out of space.
          3. Stop archiving when disks are full.
      13. The Archiver shall allow important video sequences to be protected against normal disk cleanup routines.
      14. Users shall have the following options when protecting a video sequence:
          1. Until a specified date
          2. For a specified number of days
          3. Indefinitely (until the protection is explicitly removed)
      15. The Archiver shall allow the administrator to put a cap on the percentage of storage space occupied by protected video.
      16. The Archiver shall keep a log and compile statistics on disk space usage.
          1. The statistics shall be available by disk group or for the whole Archiver.
          2. The statistics shall show the percentage of protected video over the total used disk space.
      17. The Archiver shall have the capacity to down-sample video streams for storage saving purposes. The down-sampling options available are the following:
          1. For H.264, MPEG-4, and H.265, streams the down-sampling options are: all key frames, 1 fps, 2 sec./frame, 5 sec./frame, 10 sec./frame, 15 sec./frame, 30 sec./frame, 60 sec./frame, 120 sec./frame.
          2. For MJPEG streams the down-sampling options are: 15 fps, 10 fps, 5 fps, 2 fps, 1 fps, 2 sec./frame, 5 sec./frame, 10 sec./frame, 15 sec./frame, 30 sec./frame, 60 sec./frame, 120 sec./frame.
      18. The Archiver shall support DVS with edge recording capabilities and offer the following capacity:
          1. The ability to playback the video recorded on the DVS at different speeds.
          2. The ability to offload (video trickling) the video recorded on the DVS on schedule, on event, or manually to store it on the Archiver.
          3. It shall be possible to filter the video that is being offloaded using one or multiple of the following filters:

Time interval

Playback request

Video analytic events

Motion events

Bookmarks

Alarms

Input pin events

Unit offline events

* + - 1. The Archiver shall be provided with proven performance and scalability figures:
         1. The Archiver’s performance shall be guaranteed during the rebuild of a disk from a raid 5 disk group. The rebuild process shall not affect the recording and playback capabilities.
         2. The recommended server specification from the Genetec Security Center Hardware Requirement shall allow Archiver to perform up to 300 cameras or 300Mbs throughput first limit reached.
         3. The high-performance archiver specification from the Genetec Security Center Hardware Requirement shall allow Archiver to perform: *(Specifier, for prequalified machines)*

Up to 500 cameras or 500Mbs throughput first limit reached with a 1Gbps NIC.

Up to 700 cameras or 1300Mbs throughput first limit reached with a 10Gbps NIC.

* + - 1. The Archiver shall provide the ability to encrypt the media stream coming from the DVS including the video, audio and metadata: *(Specifier, Enterprise only, additional license required)*
         1. Media encryption shall be optional and can be activated on a per DVS basis.
         2. Media encryption shall be performed with AES 128-bits.
         3. Media encryption shall encrypt all video, audio and metadata at rest and in transit. Once media encryption is turned on for a DVS, all media stored or redirected by the Archiver shall be encrypted and shall require the private key to be decoded.
         4. It shall be possible to export the encrypted media into a non-encrypted ASF file.
    1. Auxiliary Archiver *(Specifier, Enterprise only)*
       1. The Auxiliary Archiver shall be used to produce redundant archives (video, events, or bookmarks) for any camera in the system, on a case-by-case basis.
       2. The Auxiliary Archiver shall have the ability to record a camera on a different schedule than the Archiver.
       3. The Auxiliary Archiver shall have the ability to archive any of the standard video streams for archiving. The standard video stream usages are: Live, Recording, Remote, Low Resolution, and High Resolution.
    2. Standby Archiver *(Specifier, Enterprise only)*
       1. The Standby Archiver shall act as a replacement Archiver role on hot standby, ready to take over the functions of the primary Archiver role. The failover will occur in less than 1 minute. No action from the user will be required.
       2. The Standby Archiver assigned to an Archiver role entity shall automatically provide protection for all DVS connected to that Archiver role.
       3. The Standby Archiver shall protect the primary Archiver role against the following failures:
          1. Server failure (hardware or software).
          2. Storage failure, such as Archiver Role detects that it cannot read or write to any of its allocated disks.
       4. It shall be possible for a single USP server to act as the standby server of multiple Archiver roles.
          1. Each Archiver role shall have priority value if multiple Archiver Roles fail at the same time on the same standby server.
       5. It shall be possible for any Archiver role in the system to be designated as another's standby and vice-versa.
       6. For each Archiver role it shall be possible to set up to 2 standby Archiver so that if the first failover Archiver fails the failover will automatically occur to a third server.
       7. The Standby Archiver shall have the ability to act as a Redundant Archiver.
       8. It shall be possible to set a different retention period for the Archiver and the Redundant Archiver.
       9. The Redundant Archiver shall have the ability to maintain an exact copy of everything recorded by the default Archiver and/or to configure different recording qualities, i.e., audio/video archives, events, and bookmarks.
       10. Redundancy shall be configured on a camera-by-camera basis.
       11. The Redundant Archiver shall have the ability to use a multicast video stream from the DVS and shall not require an additional connection to any DVS.
       12. A Standby Archiver shall be used only for live.
       13. Redundant or Standby Archivers can have different retention day configurations.
       14. You can have a Redundant Archiver and a Standby Archiver at the same time. One shall be set to record redundant and the other set to only record on failover.
    3. Cloud Archiving
       1. The VMS shall support the automatic transfer of video recorded on the Archiver to the cloud, based on the age of the video.
       2. The Archiver shall encrypt recordings using AES-256 prior to transferring video to the cloud.
       3. The Archiver shall rotate the encryption key at every file. The encryption key shall be encrypted with a certificate kept in Azure Key Vault.
       4. The VMS shall support TLS encryption between the on-premises Archiver and the cloud.
       5. The VMS shall allow users to search video stored in the cloud through the same functionality used when querying video that is stored locally.
       6. The VMS will maintain a local cache of video downloaded from the cloud to playback recordings without requiring an additional transfer.
       7. The VMS shall support different tiers to support the video sequences.
          1. The VSM shall allow users to differentiate the video sequences available for real-time and delayed retrieval.
          2. The VMS shall automatically move video sequences from the real-time access to delayed retrieval after a configurable delay.
    4. VMS Media Streaming
       1. The Media Router Role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).
       2. The Media Router Role shall support multiple transport protocols, such as unicast TCP, unicast UDP, and multicast UDP.
       3. The Media Router shall support IGMP (Internet Group Management Protocol) to establish multicast group memberships:
          1. IGMP v3, including SSM (Source-Specific Multicast) shall be supported.
       4. The Media Router Role using Redirector Agents shall be responsible for redirecting a stream from a source IP endpoint to a destination IP endpoint.
       5. The Redirector Agents shall be capable of converting a stream from and to any supported transport protocols:
          1. Multicast UDP to Unicast TCP
          2. Multicast UDP to Unicast UDP
          3. Unicast TCP to Multicast UDP
          4. Unicast UDP to Multicast UDP
       6. It shall be possible to limit the number of concurrent live and playback video redirections for each Redirector Agent in order to better control the bandwidth across multiple sites.
       7. It shall be possible to limit the bandwidth consumed by live and playback video from the CSA to better control the bandwidth across multiple sites. The SSM shall be able to prioritize video streaming to the CSA based on user level.
       8. It shall be possible to protect the Media Router Role against hardware or software unavailability by configuring another Media Router Role to act as a hot standby server.
       9. Multiple Redirector Agents shall be used on a large VMS installation to increase the service availability and to provide automatic load balancing.
    5. VMS Video Archives Transfer capabilities
       1. Archive transfer shall provide the ability to:
          1. Transfer video from a server to another server in the same system.
          2. Transfer video from a federated server to another server.
          3. Transfer video from camera storage to a server.
       2. It shall be possible to program video transfers either on a recurrent schedule, or to trigger them manually or upon connection.
       3. It shall be possible to filter the video of interest for a transfer. The video of interest shall be defined with the following filters:
          1. All archives when the camera was offline.
          2. Alarms.
          3. Playback request from the edge.
          4. Video analytics events.
          5. Motion events.
          6. Bookmarks.
          7. Input triggers.
          8. Time range.
       4. It shall be possible to define the length of video before and after the event used as a filter to determine the video of interest.
       5. The USP shall offer an interface for displaying all video archive transfer requests. This interface shall display all the current, requested and scheduled video transfer requests. It shall be possible to edit, trigger, and cancel video archive transfers from this interface.
       6. The USP shall offer an interface for querying past video transfers and their outcome.
    6. Wearable Camera Manager
       1. A body-worn camera, also known as a wearable camera, is a video recording system that is typically used by law enforcement with the purpose of gathering video evidence and public interaction.
       2. A body-worn camera station is a physical device or software used to automatically upload media from a body-worn camera into the VMS system.
       3. The Wearable Camera Manager shall be used to configure and manage body-worn camera devices, configure camera stations, add officers (wearable camera users), upload content to an Archiver, and set the retention period for uploaded evidence.
       4. The Wearable Camera Manager shall allow for automatic officer creation and hardware serial number association.
       5. The Wearable Camera Manager shall support that activation and deactivation of officers.
       6. The Wearable Camera Manager shall support the uploading od the following types of data:
          1. Video
          2. Audio
          3. Metadata
       7. The system shall assign multiple archivers to the Wearable Camera Manager for performance and load balance purposes.
       8. The Wearable Camera Manager shall automatically upload data when the body-worn camera is connected to the body-worn camera docking station.
       9. The Wearable Camera Evidence report shall log the user, the evidence name, the capture time, the upload time, and the conversion status and progress.
       10. The Wearable Camera Evidence report shall support queries based on the following filters:
           1. Time range
           2. During the last year, month, weeks, days, hours, minutes, seconds
           3. Specific range
           4. Date and time options
           5. Capture time
           6. Upload time
           7. Conversion status
           8. Error
           9. Pending
           10. In progress
           11. Completed
       11. The system shall generate an evidence ready event when the uploaded video and conversion is completed.
       12. The monitoring UI investigation task shall support the possibility to search and investigate body wearable camera archives.
       13. The Wearable Camera Manager shall be provided with the following proven performance and scalability figures:
           1. A Wearable Camera Manager can support up to 1000 body-worn camera entities
           2. Upon officer incident recording
           3. Dedicated Archiver for when more than 20 concurrent officers are uploading video at the same time

Maximum of 100 current officers uploading at the same time

Maximum of 300 officers per Archiver

* + - * 1. Upon officer continuous recording
        2. Dedicated Archiver if more than 5 concurrent officers are uploading video at the same time

Maximum of 30 concurrent officers uploading at the same time

Maximum of 100 officers per Archiver

* + 1. Security Video Analytics
       1. The analytics shall be completely unified with the Video Management System.
       2. Configuration shall natively be performed in the configuration interface of the Video Management System.
       3. The analytics shall feature dedicated configuration possibilities for the following scenarios:
          1. Perimeter protection
          2. Positional tracking
          3. Area protection
          4. Direction control
          5. Object detection
          6. Stopped vehicle detection
          7. Tailgating Detection
       4. Each of the scenarios shall trigger events in the Video Management System, which correspond to their functionality.
       5. Additional to these scenarios, the analytics shall allow to configure custom intrusion detection and object detection scenarios as well as allow to import settings to allow maximum flexibility.
       6. The analytics license shall allow to configure any one of these scenarios per camera.
       7. The analytics shall allow at least two different detection variants:

Trigger an alarm if a motion pattern moves from zone A (source) through zone B into zone C (sink).

Trigger an alarm if a motion pattern moves anywhere inside a specified zone.

* + - 1. The analytics shall support an unlimited number of detection areas.
      2. The analytics feature rain-filters to filter out disturbances.
      3. The analytics shall feature live configuration to immediately see the effects of parameter changes in the configuration interface without prior saving new configurations.
      4. The configuration of the analytics shall be possible on recorded video streams.
      5. The analytics shall offer the possibility to configure object movement paths.
      6. The analytics shall not employ tripwires or crosslines.
      7. Areas and the scenes perspective (near & far object size) shall be configured on-screen using a point-and-click interface.
      8. The analytics shall feature filters for movement speed, distance, and direction to detect events.
      9. The analytics shall feature options to separately show or hide areas, area names, and detection overlays.
      10. The analytics shall be fully server-based, with no calculation on cameras necessary.
      11. The analytics shall operate with color, thermal, and infrared cameras.
      12. The accuracy of KiwiVision Intrusion Detector has been evaluated and approved by the National Protective Security Authority (NPSA) Video Analytics Program of the United Kingdom, and has been included in the Catalogue of Security Equipment (CSE).
    1. Camera Integrity Monitor
       1. Description:
          1. Automatically checks camera feeds to detect if cameras have been tampered with.
          2. Can be used for near-real-time alerting of tampering events or as a maintenance tool.
          3. Reports can be run on detected tampering events.
       2. Details:
          1. It shall be completely unified with the Video Management System.
          2. It shall be possible to set the detection sensitivity per camera stream between low, medium, and high.
          3. It shall be possible to choose on which servers the analytics shall run.
          4. The camera stream used for analytics shall be configurable.
          5. It shall be possible to define how many cameras are being analyzed at the same time.
          6. To utilize minimum hardware resources, it shall be definable how often camera streams are analyzed.
          7. There shall be an overview over which cameras are configured to be analyzed.
    2. Privacy Protector
       1. Description:
          1. Automatically obscures all movement in surveillance videos in real-time.
          2. Live privacy masking of moving objects (such as people and vehicles).
          3. Completely unified with the video management system.
          4. Native configuration in the configuration interface of the video management system.
       2. Details:
          1. Privacy masking can be removed either per camera or for all cameras currently viewed. Masking for all cameras viewed can be removed and added either manually with a button or automatically with an action.
          2. Indoor / outdoor modes using flexible background modeling:

Indoor: Learning model with up to 10 different illumination states – this allows to adapt to fast lighting changes such as lights switching on and off.

Outdoor: Foreground detection based on edge detection rather than color – this allows to adapt to heavily changing lighting conditions such as clouds temporarily blocking sunlight.

* + - * 1. Detects movements using an absolute difference image, calculated by subtracting the current frame from a calculated background model.
        2. Masks movements using blocks, thus obscuring the outline of an object or person.
        3. Three different scrambling methods: Pixelation, Colorize, and Transparency.
        4. Masking grids can be configured in a point-and-click interface.
        5. Past preview mode to see configuration changes in the configuration interface without necessity to save the configuration.
        6. Zones can be freely definable polygons with a point-and-click interface.
        7. Option to set analysis resolution to optimize performance.
        8. No calculation on the camera necessary, completely server based.
        9. Option to define zones, which should always or never be pixelated.
        10. Option to choose input stream and output stream parameters, including resolutions, frame rate, and encoding.
        11. Utilizes server-side hardware acceleration to maximize the amount of cameras analyzed per server.
    1. People Counter
       1. The analytics shall feature dedicated configuration possibilities for the following scenarios:
          1. People counting
          2. Crowd estimation
       2. Description:
          1. Automatically counts people in a camera's field of view.
          2. Provides live dashboard widgets dedicated for people counting and crowd estimation.
          3. Completely unified in the video management system.
          4. Native configuration in the configuration interface of the video management system.
       3. Details:
          1. Based on deep-learning models trained on crowd size estimation to exclude non-human objects.
          2. Dedicated dashboard widgets for crowd estimation with the following features:

Charts: Displays the number of people inside the selected regions during a specific time on a bar or line chart.

Throughput: Show number of persons in given time frame.

Occupancy: Displays the number of people currently in the selected regions.

* + - * 1. Counts adults and children.
        2. Counts crowds of 5 up to more than 500 people in a single frame
        3. Counts persons in wheelchairs.
        4. Triggers events in regular intervals containing the estimated size of the crowd for the configured area. One event per area.
        5. Triggers events if more than a defined amount of people is counted in a defined area.
        6. Supports top-down camera views.
        7. Supports bi-directional counting.
        8. Supports tilted camera views.
        9. Option to show/hide overlays with detected persons and counting line with dedicated people, crowds, counting lines, and areas.
        10. No GPU required to run.
        11. The occupancy widget support resetting the count at a defined time option to define zones, which should always or never be pixelated.
        12. Supports organizing cameras into areas and show these areas in widgets.
        13. Utilizes server-side hardware acceleration to maximize the amount of cameras analyzed per server.
        14. Counts can be integrated to external systems using CSV exports and a .NET SDK.
    1. General Client Software Requirements
       1. The Client Software Applications (CSA) shall provide the user interface for USP configuration and monitoring over any network and be accessible locally or from a remote connection.
       2. The CSA shall consist of the Configuration UI for system configuration and the Monitoring UI for monitoring. The CSA shall be Windows-based and provide an easy-to-use graphical user interface (UI).
       3. The CSA for monitoring shall support running in 64-bit mode.
       4. The Server Administrator shall be used to configure the server database(s). It shall be web-based and accessible locally on the SSM or across the network.
       5. The CSA shall seamlessly merge access control, license plate recognition (ALPR), and video functionalities within the same user application.
       6. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and the .NET software framework.
       7. All applications shall provide an authentication mechanism, which verifies the validity of the user. As such, the administrator (who has all rights and privileges) can define specific access rights and privileges for each user in the system.
       8. Logging on to a CSA shall be done either through locally stored USP user accounts and passwords or using the operator’s Windows credentials when Active Directory integration is enabled. *(Specifier, Professional and up, first integration included, additional licenses required for more)*
       9. When integrated with Microsoft’s Active Directory, the CSA and USP shall authenticate users using their Windows credentials. As a result, the USP will benefit from Active Directory password authentication and strong security features. *(Specifier, Professional and up, first integration included, additional licenses required for more)*
       10. When integrated with an external identity provider such as Windows Active Directory, ADFS (Active Directory Federation Services) or an Open ID Connect/SAML2 identity provider (ex.: Azure AD), the CSA and USP shall authenticate using a Single-Sign On experience to the users. As a result, the USP will benefit from reusing the same credential throughout enterprise applications. *(Specifier, Professional and up, additional license required)*
       11. The CSA shall support multiple languages, including but not limited to the following: English, French, Arabic, Croatian, Czech, Dutch, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Persian (Farsi), Polish, Portuguese (Brazilian), Simplified and Traditional Chinese, Romanian, Russian, Spanish, Swedish, Thai, Turkish, and Vietnamese.
       12. To enhance usability and operator efficiency, the Configuration UI and Monitoring UI shall support many of the latest UI such as:
           1. A customizable Home Page that includes favorite and recently used tasks.
           2. Task-oriented approach for administrator/operator activities where each type of activity (surveillance, visitor management, individual reports, and more) is an operator task.
           3. Consolidated and consistent workflows for video, ALPR, and access control.
           4. Single click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or track.
       13. Configuration UI and Monitoring UI Home Page and Tasks
           1. The Configuration UI and Monitoring UI shall be task oriented.
           2. A task shall be user interface design patterns whose goal is to simplify the user interface by grouping related features from different systems, such as video and access, in the same display window. Features shall be grouped together in a task based on their shared ability to help the user perform a specific task.
           3. Tasks shall be accessible via the Home Page of either the Configuration or the Surveillance CSA.
           4. Newly created tasks shall be accessible via the Configuration UI or the Monitoring UI taskbar.
           5. Similar tasks shall be grouped into the following categories:

Operation: Access control management, LRP management, and more.

Investigation: Video bookmark/motion/archive reports, access control activity reports, visitor activity reports, alarm reports, ALPR activity reports, and more.

Maintenance: Access control and video configuration reports, troubleshooters, audit trails, health-related reports, and more.

* + - * 1. An operator shall be able to launch a specific task only if they have the appropriate privileges.
        2. The Home Page content shall be customizable through the use of privileges to hide tasks that an operator should not have access to and through a list of favorite and recently used tasks. In addition, editing a USP XML file to add new tasks on the fly shall also be possible.
      1. The Contractor shall provide up to XX number of simultaneous Clients*. (Specifier, client connections are concurrent, the first 5 client connections are included, specify a Site License after 40 client connections (Enterprise only))*
    1. Configuration User Interface (UI)
       1. General:
          1. The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration. The Configuration UI shall provide decentralized configuration and administration of the USP system from anywhere on the IP network.
          2. The configuration of all embedded ACS, VMS, and ALPR systems shall be accessible via the Configuration UI.
          3. The Configuration UI shall have a home page with single-click access to various tasks.
          4. The Configuration UI shall include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.
          5. The Configuration UI shall include a static reporting interface to:

View historical events based on entity activity. The user shall be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view.

View audit trails that show a history of user/administrator changes to an entity.

* + - * 1. Common entities such as users, schedules, alarms and many more, can be reused by all embedded systems (ACS, VMS, and ALPR).
      1. Video management system:
         1. The Configuration UI shall allow the administrator or users with appropriate privileges to change video configuration.
         2. The Configuration UI shall provide the ability to change video quality, bandwidth, and frame rate parameters on a per camera (stream) basis for both live and recorded video.
         3. The Configuration UI shall provide the ability to change video quality by a selection of predefined video quality template.
         4. The Configuration UI shall provide the ability to configure brightness, contrast, and hue settings for each camera on the same DVS.
         5. The Configuration UI shall provide the capability to enable audio recording on DVS units that support audio.
         6. The Configuration UI shall provide the ability to change the audio parameters, serial port and I/O configuration of individual DVS units.
         7. The Configuration UI shall provide the capability to rename all DVS units based on system topology and to add descriptive information to each DVS.
         8. The Configuration UI shall provide the ability to set recording schedules and modes for each individual camera. The recording mode can be:

Continuous

On motion and Manual

Manual only

Disabled

* + - * 1. The Configuration UI shall support the creation of schedules to which any of the following functional aspects can be attached:

Video quality (for each video stream per camera)

Recording (for each camera)

Motion detection (for each detection zone per camera)

Brightness, Contrast, and Hue (for each camera)

Camera sequence execution

* + - * 1. The Configuration UI shall support the creation of unlimited recording schedules and the assigning of any camera to any schedule.
        2. The Configuration UI shall detect and warn user of any conflict within assigned schedules.
        3. The Configuration UI shall provide the capability to set a PTZ protocol to a specific DVS serial port and shall allow mixing domes of various manufacturers within a system.
        4. User shall have the ability to configure a return to home function after a predefined time of inactivity for PTZ cameras. This period of inactivity time shall be configurable from 1 to 7200 seconds.
    1. VMS Client User Interface (UI)
       1. The Monitoring UI shall fulfill the role of a Unified Security Interface that is able to monitor video, ALPR, and access control events and alarms, as well as view live and recorded video.
       2. The Monitoring UI shall provide a graphical user interface to control and monitor the USP over any IP network. It shall allow administrators and operators with appropriate privileges to monitor their unified security platform, run reports, and manage alarms.
       3. To enhance usability and operator efficiency, the Monitoring UI shall support the following UI concepts:
          1. Dynamically adaptive interface that adjusts in real-time to what the operator is doing.
          2. A dynamic controls section loaded with entity-specific widgets (e.g., door and camera widgets).
          3. Use of transparent overlays that can display multiple types of data in a seamless fashion.
          4. Display tile menus and quick commands.
          5. Consolidated and consistent workflows.
          6. Tile menus and quick commands easily accessible within every display tile of the user workspace.
          7. Single click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or to track.
       4. Monitoring UI Home Page and Tasks:
          1. Similar tasks shall be grouped into the following categories:

Operation: Access control/LRP/video surveillance, visitor management, mustering, access control and video alarm monitoring, and more.

Investigation: Video bookmark/motion/archive reports, access control activity reports, visitor activity reports, alarm reports, ALPR activity reports, and more.

Maintenance: Access control and video configuration reports, troubleshooters, audit trails, and more.

* + - 1. Dynamically Adaptive UI, Controls section, and Widgets:
         1. The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI Controls section.
         2. Widgets shall be mini-applications or mini-groupings in the Monitoring UI Controls section that let the operator perform common tasks and provide them with fast access to information and actions.
         3. With a single click on an entity (for example door or camera) the specific widgets associated to that entity appear and other non-relevant widgets disappear dynamically (instantly). Widgets shall bring the operator information such as door status and camera stream information, as well as user actions, such as door unlock, PTZ controls, and more.
         4. Specific widgets include those for a door, camera, alarm, zone, display tile, video stream (statistics), PTZ camera, and more.
      2. Operator Workflows:
         1. A workflow shall be a sequence of operations an operator or administrator shall execute to complete an activity. The “flow” relates to a clearly defined timeline or sequence for executing the activity.
         2. The Monitoring UI shall be equipped with consistent workflows for the ALPR, video, and access control systems that it unifies.
         3. Generating or printing a report, setting up or acknowledging an alarm, or creating an incident report shall follow the same process (workflow) whether the operator is working with video, ALPR, or access control, or with both video and access control.
      3. Each task within the Monitoring UI shall consist of one or more of the following items:
         1. Event list.
         2. Logical tree: Doors, cameras, zones, ALPR units, and elevators shall be grouped under Areas in a hierarchical fashion.
         3. Entities list of all entities being tracked.
         4. Display tiles with various patterns (1 x 1, 2 x 2, and more).
         5. Display tile menu with various commands related to cameras, doors, PTZ, and tile controls.
         6. Controls section with widgets.
      4. The Monitoring UI shall support multiple event lists and display tile patterns, including:
         1. Event/alarm list layout only
         2. Display tile layout only
         3. Display tile and alarm/event list combination
         4. ALPR map and alarm/event list combination
      5. User workspace customization
         1. The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.
         2. Once customized, the user shall be able to save his or her workspace.
         3. The user workspace shall be accessible by a specific user from any client application on the network.
         4. Display tile patterns shall be customizable.
         5. Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.
         6. The Monitoring UI shall support multiple display tile patterns (for example one display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).
         7. The Monitoring UI shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.
         8. Additional customization options include show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.
      6. The Monitoring UI shall provide an interface to support the following tasks and activities common to access control, ALPR, and video:
         1. Monitoring the events from a live security system (ACS and/or VMS and/or ALPR).
         2. Generating reports, including custom reports.
         3. Monitoring and acknowledging alarms.
         4. Creating and editing incidents and generating incident reports.
         5. Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans.
         6. Management and execution of hot actions and macros.
      7. The Monitoring UI shall be able to monitor the activity of the following entities in real-time: areas, ALPR entities, doors, elevators, cameras, cardholders, cardholder groups, zones (input points), and more.
      8. The Monitoring UI shall include advanced video capabilities, including:
         1. Advanced live video viewing functionality.
         2. Advanced archive playing and video playback functionality.
         3. Monitoring and management of video system events and alarms.
         4. Intercom or duplex audio.
         5. Generation of video reports.
         6. Control of PTZ cameras.
         7. Creating and monitoring archive transfer requests.
         8. Display metadata overlaid on live or playback video.
      9. The Monitoring UI shall leverage the Graphical Processing Unit (GPU) for video decoding.
         1. The following GPU technologies shall be supported:

NVidia CUDA

Intel Quick Sync

* + - * 1. The Monitoring UI shall have the ability to decode video through the optimal simultaneous use of the GPU and Computer Processing Units (CPU).
      1. The live video viewing capabilities of the Monitoring UI shall include:
         1. The ability to display all cameras attached to the USP and all cameras attached to federated systems.
         2. Support for live video monitoring on each and every display tile within a task in the user’s workspace.
         3. The USP shall support uninterrupted video streaming. The CSA shall keep existing video connections active in the event that an SSM (except Archiver) becomes unavailable.
         4. The ability to drag and drop a camera into a display tile for live viewing.
         5. The ability to drag and drop a camera into a display tile for live viewing on an analog monitor connected to an IP hardware decoder (converting an IP encoded stream into an analog video signal).
         6. The ability to drag and drop a camera from a map into a display tile for live viewing.
         7. Support for digital zoom on live camera video streams.
         8. The ability for audio communication with video units with audio input and output.
         9. The ability to control pan-tilt-zoom, iris, focus, and presets.
         10. The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.
         11. The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.
         12. The ability to activate or de-activate viewing of all system events as they occur.
         13. The ability to switch to instant replay of the video for any archiving camera with the simple click of button.
         14. The ability to take snapshots of live video and be able to save or print the snapshots.
         15. The ability to view the same camera multiple times in different tiles.
      2. The video playback (archive playing) capabilities of the Monitoring UI shall include:
         1. Support for audio and video playback for any time span.
         2. Support for video playback on each and every display tile.
         3. The ability to instantly replay the video for any archiving camera with the simple click of a button.
         4. The ability to select between instant synch of all video streams in playback mode, allowing operators to view events from multiple angles or across several camera fields, or non-synchronous playback.
         5. The ability to simultaneously view the same camera in multiple tiles at different time intervals.
         6. The ability to control playback with:

Pause

Lock Speed

Forward and Reverse Playback at: 1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x

Forward and Reverse Playback frame by frame

Slow Forward and Reverse Playback at: 1/8x, 1/4x, 1/3x, 1/2x

Loop playback between two time markers

* + - * 1. The ability to display a single timeline or one timeline for each selected video stream, which would allow the operator to navigate through the video sequence by simply clicking on any point in the timeline.
        2. The ability to display the level of motion at any point on a timeline.
        3. The ability to clearly display bookmarked events on the timeline(s).
        4. The ability to query archived video using various search criteria, including, but not limited to, time, date, camera, and area.
        5. The tool necessary for searching video and associated audio based on user-defined events or motion parameters.
        6. The ability to define an area of the video field in which to search for motion as well as define the amount of motion that will trigger search results. The Monitoring UI shall then retrieve all archived video streams that contain motion that meets the search parameters. There shall be a graphical timeline on which the time of each search hit shall be indicated.
        7. The ability to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing.
        8. The ability to add bookmarks to previously archived video for easier searching and retrieval.
        9. Support for digital zoom on playback video streams.
        10. Still image export to PNG, JPEG, GIF, and BMP format with Date and Time stamp, and Camera Name on the image (snapshot).
        11. Tools for exporting video and a self-contained video player on various media such as USB keys or CD/DVD-ROM. This video player shall be easy to use without training and shall still support reviewing video metadata, such as bookmark, or navigating the video with functions like panoramic camera view dewarping.
        12. Tools for exporting video sequences in standard video formats, such as ASF or MP4.
        13. The ability to encrypt exported video files.
        14. The ability for an operator to load previously exported video files from their computer or network.
        15. The ability for queries to be saved upon closing the CSA and reappear when the application is reopened.
        16. The ability to dynamically block, on demand, video stream dynamically to lower-level users to prevent access, for a specific time, to live and recorded video.
        17. A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.
        18. The ability to store the video export and still image export at a pre-defined storage location.
        19. An interface with the ability to list, search, and manipulate previously generated video exports.
        20. The ability to export sequences of video in open standards including ASF and MP4.
      1. The Monitoring UI shall provide an interface to support the following ALPR tasks and capabilities:
         1. Monitoring and management of ALPR events and alarms.
         2. Viewing of license plate picture(s) and context images.
         3. Viewing of license plate data (e.g., license plate reads)
         4. Verification of ALPR data against live and recorded video.
      2. Entity Monitoring:
         1. The USP shall permit the user to select multiple entities to monitor from the Monitoring UI by adding the entities one by one to the tracking list.
         2. The Monitoring UI shall provide the option to filter which events shall be displayed in the display tile layout and/or event list layout.
         3. It shall be possible to lock a Monitoring UI display tile so that it only tracks the activity of a specific entity (e.g., specific door or camera).
         4. The user shall be able to drag and drop an event from an event list (or an alarm from an alarm list) onto a display tile to view a license plate read, cardholder picture ID, badge ID, or live/archived video, among other options.
         5. Event, alarm, monitoring/tracking, and report lists shall contain cardholder pictures where applicable.
         6. The user shall be permitted to start or pause the viewing of events within each display tile.
      3. Display Tile Packing and Unpacking:
         1. The Monitoring UI shall support single-click unpacking and packing for ALPR hits, ALPR reads, areas, doors, zones, camera sequences, and alarms.
         2. The packing and unpacking of entities shall allow operators to quickly obtain additional information and camera views of a specific entity.
         3. The unpacking of an entity shall display associated entities. For example, unpacking a door with multiple associated cameras shall display all cameras associated with that door. Unpacking shall reconfigure the display tiles to be able to display all associated entities. For example, unpacking a door (or a zone or alarm) that is currently in a 1 x 1 tile configuration and that has 3 cameras tied to it will create a 1 x 3 display tile arrangement for viewing all associated entities.
         4. Packing will return the display to the original tile pattern.
      4. Visual Tracking:
         1. The Monitoring UI shall support the ability to manually track a moving target with the single click of a button.
         2. The ability to switch from one camera view to an adjacent camera shall be done within a single display tile.
         3. Switching between camera streams shall be accomplished by simply clicking on a semi-transparent shape or overlay.
         4. Visual tracking shall be available with both live and recorded video.
    1. Server Administrator User Interface Requirements
       1. The Server Administrator shall be used to configure the SSM and the Directory Role (main configuration) and its database(s), to apply the license, and more.
       2. The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.
       3. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.
       4. The Server Administrator shall allow the administrator (user) to perform the following functions:
          1. Manage the system license.
          2. Configure the database(s) and database server for the Directory Role,
          3. Activate/Deactivate the Directory Role.
          4. Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.
          5. Define the client-to-server communications security settings.
          6. Configure the network communications hardware, including connection addresses and ports.
          7. Configure system SMTP settings (mail server and port).
          8. Configure event and alarm history storage options.
    2. Unified Web Interface (UWI) General Requirements
       1. The USP shall support a unified web interface (UWI) for access control and video.
       2. The UWI shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.
       3. The UWI shall be platform independent and run within Microsoft Edge, Internet Explorer, Firefox, Safari, and Google Chrome.
       4. Web pages for the web interface shall be managed and pushed by the Web Server Role. Microsoft IIS or any other web hosting service shall not be required given that all the web pages shall be hosted by the Web Server Role.
       5. The UWI shall support display on tablet format.
       6. The UWI shall support native H.264 video in the web interface.
       7. Web pages for the web interface shall be managed and pushed by the Web Interface Server. Microsoft IIS or any other web hosting service shall not be required given that all the web pages shall be hosted by the Mobile Server.
       8. The Contractor shall provide up to XX number of simultaneous Web interfaces. *(Specifier, web interface connections are concurrent, the first 5 web interface connections are included, specify a Site License after 40 web interface connections (Enterprise only))*
       9. The Web Interface Server shall provide the ability to define a unique URL to access the web interface, to ensure the security of the application.
       10. The UWI shall provide the ability to load a camera layout.
       11. The UWI shall provide the ability to configure, save, and reload private camera layouts.
       12. The UWI shall provide the ability to control PTZ cameras.
       13. Functionalities:
           1. Log in support shall be available using:

Username and password

Active Directory. *(Specifier, Professional and up, first integration included, additional licenses required for more)*

Azure Active Directory, ADFS, OpenID Connect or SAML2 identity provider. *(Specifier, Professional and up, additional license required for OIDC & SAML2)*

Ability for user to change their password.

* + - * 1. Encrypted communications for all transactions.
        2. Print reports and export to CSV file.
        3. Customer logo customization shall be available for multi-tenant and hosted services applications.
        4. Video:

Live and playback video at 320 x 240, 640 x 480 or 1280 x 1024 @ 15 fps

Video export

1, 4, 6 or 9 tiles

Basic PTZ Controls (Pan/Tilt, Zoom, go to presets, start pattern)

Start / Stop recording

Sample web page for customers to see how to view video for their own development

Add bookmarks

* + - * 1. Alarms:

Alarm report

* + - * 1. Threat Level.
        2. Communication

Ability to make/receive calls from the client user interface or intercom.

Ability to see the list of contacts.

Ability to unlock a door during a call.

* + 1. Smartphone and Tablet App General Requirements
       1. The USP shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the Mobile Server of the USP over any Wi-Fi or cellular network connection.
       2. Mobile apps shall communicate with the USP via a Mobile Server Role (MSR). All communication between the mobile apps and MSR shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.
       3. Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):
          1. Apple devices running iOS 13.0 or later
          2. Android devices 10.0 or later
       4. It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play).
       5. It shall be possible to push configuration to the mobile devices through a Mobile Device Management solution such as VMWare Workspace One or Microsoft Intune.
       6. Functionalities:
          1. Core

Ability to logon/logoff to the USP using an authorized user profile of the system.

Ability to support passive authentication from a single sign-on provider (OpenID Connect or SAML2 identity provider).

Ability to use biometric features (thumbprint, face ID, etc.) to perform connection to the system.

Ability to change the picture or the password of the user of the mobile app.

Ability to view the current Threat Level of the system.

Ability to change the current Threat Level of the system.

Ability to execute hot actions configured in the user profile.

Ability to view entities from the USP:

Cameras

Doors

ALPR cameras

Web Tile Plugins

Layouts

Camera Sequences

Macros

Maps (geographical maps only*) (Specifier, Professional and Enterprise)*

Intercoms

Ability to navigate the system hierarchical view of the entities and search entities in the system.

* + - * 1. Video

Ability to view live and recorded video from the cameras of the USP. A maximum of four cameras shall be displayed.

Ability to view video in native format (H.264).

Ability to display live and recorded video side-by-side for a specific camera.

Ability to perform digital zoom on cameras.

Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording.

Ability to view camera layouts.

Ability to view camera sequences.

Ability to run a camera events report.

Ability to change the video quality on the cameras displayed on the mobile app.

Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system.

* + - * 1. Access Control

Ability to view the door state and door lock state.

Ability to perform actions on a door such as unlock the door, set the door in maintenance mode, override the door unlocking schedule.

Ability to monitor live cardholder activities per door, such as cardholder name, pictures, access denied and reason for access denied.

* + - * 1. Automatic License Plate Recognition

Ability to view live events raised by an ALPR camera.

Ability to view the read image, context image, and all metadata captured by the ALPR camera.

Ability to run an ALPR event report.

Ability to add a license plate to a hotlist on the system.

* + - * 1. Alarm Management

Ability to receive push notifications to notify mobile operators that an alarm was received.

Ability to view all active alarms assigned to the mobile operator.

Ability to perform action on an alarm such as acknowledge, investigate, or alternate-acknowledge an active alarm.

Ability to view entities attached to the alarm.

* + - * 1. Map *(Specifier, Professional and Enterprise)*

Ability to display a geographic map with USP entities geo-located on the map.

Ability to view any entity configured on the map.

Ability to search entities or location on the map.

* + - * 1. Communication

Abillity to make/receive calls from the client user interface or intercom.

Ability to see the list of contacts.

Ability to unlock a door during a call.

* + - 1. It shall be possible to send a message from the client user interface to a mobile operator.
      2. It shall be possible to send a live or playback video sequence from the client UI to a mobile operator.
      3. It shall be possible to view mobile operators who enabled location tracking on a map in the system. The location of the mobile operator should be updated in real time. *(Specifier, Professional and Enterprise)*
    1. Health Monitor
       1. The USP shall monitor the health of the system, log health-related events, and calculate statistics.
       2. USP services, roles, agents, units, and client apps will trigger health events.
       3. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.
       4. A dedicated role, the Health Monitoring Role, shall perform the following actions:
          1. Monitor the health of the entire system and log events.
          2. Calculate statistics within a specified time frame (hours, days, months).
          3. Calculates availability for clients, servers and video/access/ALPR units.
       5. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.
       6. A Health Monitoring dashboard task shall be available in the client application user interface to provide a live display, such as pie charts and event lists, for quick visual assessment on the general health of the system.
       7. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.
       8. Detailed system care statistics will be available through a web-based dashboard providing health metrics of USP entities and roles, including Uptime and mean-time-between-failures.
       9. All health events raised in the system can be used for automating the USP event/action management.
       10. Health events shall be accessible via the SDK (can be used to create SNMP traps).
    2. Session Initiation Protocol (SIP) Communication Management (CM)
       1. An operator of the USP shall be able to, within the USP Monitoring UI, initiate calls to and answer calls from other operator and edge voice devices such as intercoms, emergency call stations, information desks, softphones, or phone devices.
       2. The USP shall support CM between the USP client User Interface and SIP endpoint devices.
       3. SIP endpoints shall be able to register to the USP using a standard SIP protocol.
       4. The USP shall support CM between two SIP endpoint devices.
       5. The USP shall allow the configuration of SIP trunk connections to multiple SIP Servers supporting SIP Trunks.
       6. The CM shall support the management of calls to and from other SIP Servers connected though SIP Trunks.
       7. The USP shall support the configuration of paging zones for pre-recorded and live message announcements.
       8. The CM is a service of the USP and shall not require the addition of any third-party software.
       9. The CM shall support the following video codecs:
          1. H.264
          2. H.263
          3. H.263+ (1998)
       10. The CM shall support the following audio codecs:
           1. PCMA (G.711 aLaw)
           2. PCMU (G.711 uLaw)
           3. G.722
           4. G.729
           5. iLBC
           6. GSM
           7. telephone event
           8. Speex (Narrowband)
           9. Speex (Wideband)
           10. Speex (Ultrawideband)
           11. L.16
           12. L.16-44-1
           13. G.728
           14. G.726-16
           15. G.726-24
           16. G.726-32
           17. G.723
           18. G.726-40
       11. The CM shall certify SIP devices from the following manufacturers:
           1. 2N Telekomunikace
           2. Algo
           3. Axis
           4. Baudisch
           5. Castel
           6. Cisco
           7. Code Blue
           8. Commend
           9. EMCOM
           10. Grandstream networks
           11. Jacques
           12. Mobotix
           13. Siedle
           14. TalkaPhone
           15. TOA Corporation
           16. Valcom
           17. Vingtor-Stentofon
           18. Zenitel
           19. Intelbras
       12. The CM shall allow bidirectional audio and video recording of call sessions. The USP shall offer the following recording capabilities:
           1. Automatic cleanup of call session files after a programmable number of days.
           2. Deactivation of call recording between operators.
           3. Deactivation of call recording with specific operators.
           4. Deactivation of call recording with specific voice devices.
           5. Selection of the storage path for call session recordings.
       13. The CM shall provide the capability to reach a physical location identified by its own extension number regardless of the user connected to the USP.
       14. The CM shall provide the flexibility for the administrator to define the network ports used to communicate between the USP servers and the following:
           1. USP Operator Client User Interfaces
           2. SIP devices
           3. SIP servers
       15. The CM shall provide the capability to create Ring Groups. A Ring Group is a group of call numbers grouped under a single call number. It shall be possible to set a Ring Group to simultaneously or sequentially call the members of the group. Dwell time for sequence mode shall be configurable.
       16. The CM shall allow the automatic routing of calls through the configuration of a collection of rules (Dial Plan). Dial Plans shall support the following capabilities:
           1. Match a phone number with regular expression.
           2. Route calls based on matching the phone numbers from which calls are made.
           3. Route calls based on matching the destination phone numbers to which calls are made.
           4. Change the phone extension from which calls are received.
           5. Change the phone extensions to which calls are sent.
           6. A combination of any of the above capabilities in a configured priority and based on a schedule.
       17. Dial Plans shall be applicable to calls between SIP entities registered to the USP as well as to and from external SIP servers.
       18. The USP shall unify, within a simple user interface, the workflow between the associated security entities of a call session, including the call box, cameras, doors, intrusion zones and outputs.
       19. The USP shall support video and audio calls:
           1. Between USP Client User Interfaces
           2. To and from USP Client User Interfaces and SIP devices
           3. Between SIP devices
       20. The USP shall provide an advanced and friendly call management user interface that allows operators to:
           1. Connect standard USB headsets and webcams to USP Client User Interface workstations so that USP users can make voice and video calls through the USP Client User Interface.
           2. Display the video associated with the call and switch between multiple video sources.
           3. Receive incoming call notifications directly through a notification tray.
           4. Initiate, answer, forward, place on hold, or cancel calls from a dedicated call dialog box.
           5. Control cameras, doors, zones, and device outputs during a call.
           6. Create a customizable list of contacts, so that users can quickly call their contacts. Contact lists shall include other USP users, as well as SIP devices.
           7. Dial a phone number to make a call.
           8. Dial a DTMF sequence during a call.
           9. Monitor the availability status of a user and set its own availability status.
           10. Access a history log of calls that the operator both initiated and received. This log shall show the time of the call, duration, direction and the reason for its ending. It shall be possible to redial one of the entries in the log.
       21. The USP shall allow an operator to manage up to 10 calls simultaneously. The call queue shall show the status of each call: incoming, in call, or on hold. It shall be possible to hold and resume a call directly from the call queue.
       22. The USP shall offer a call window. It shall be possible within the call windows to:
           1. Switch between cameras associated with the call participant.
           2. Open and lock doors associated with the call participant.
           3. Arm and Disarm zones associated with the call participant.
           4. Trigger outputs associated with the call participant.
           5. Put on hold, resume, forward, and end a call.
           6. Mute the microphone.
           7. Hide the webcam video feed.
       23. The USP shall have a built-in address book. The address book shall be available in the call dialog box, in which users can view and manage their list of contacts. From the address book, users shall be able to do the following:
           1. Call a contact by simply double-clicking the contact name.
           2. See the availability status of their contacts (users and SIP Devices).
           3. Quickly display a contact's information, such as photo, name, and number.
           4. Filter their contacts by type (SIP Device or User).
           5. Create a list of favorites by adding and removing contacts.
           6. Search for and call numbers that appear in the contact list.
       24. The USP shall provide a graphical dial pad to allow the operator to make calls and dial DTMF tones during a call.
       25. The USP shall provide the ability to send public announcements via a microphone or uploaded pre-recorded messages. The users shall be able to do the following:
           1. Create paging zones.
           2. Associate any SIP callable entity with a paging zone.
           3. Upload pre-recorded messages.
           4. Trigger a live or pre-recorded message.
       26. The USP shall provide call reporting capabilities to allow for the investigation of the activities during specific call sessions. The report shall provide the capability to replay audio recordings and watch call sessions that have associated video. The Call report shall provide filters to query the call records by:
           1. Date and time
           2. Call session duration
           3. Involved users and call stations
           4. Call events and actions
           5. Actions taken by a user on doors, intrusion zones, and outputs during the call session
       27. The USP shall give the capability to export a call session, including bidirectional audio, associated video, and log journal of the call session.
       28. It shall be possible to place the voice devices as icons on a map that shall display the call status of the voice device with a color code. A right click on the voice device map icon shall allow the user to:
           1. Answer or reject an incoming call.
           2. Initiate a call to the device.
           3. Put on hold and resume a call with the device.
       29. It shall be possible for an operator to select and broadcast his or her availability status, with the possible statuses being Available, Away and Busy. This status will appear with a color code in the call dialog box of other operators.
       30. The Contractor shall provide up to XX number of SIP connections. *(Specifier, SIP stations are a per connection license)*
       31. It shall be possible to do a failover and bidirectional audio and video recording for each SIP device.
       32. It shall be possible to do SIP public address.
       33. The CM shall provide the ability to broadcast public addressing messages to a collection of SIP devices included in a paging zone. The PA (Public address) feature shall support the following capability:
           1. Define paging zones and assign SIP entities for each of them
           2. Broadcast live and pre-recorded messages
    3. USP General Requirements
       1. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.
       2. The USP shall support the seamless unification of IP access control system (ACS), IP video management system (VMS), and IP automatic license plate recognition system (ALPR) under a single platform. The USP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, and reporting of embedded ACS, VMS, and ALPR systems and associated edge devices.
       3. Functionalities available with the USP shall include:
          1. Configuration of embedded systems, such as ACS, ALPR, and VMS systems.
          2. Live event monitoring.
          3. Live video monitoring and playback of archived video.
          4. Alarm management.
          5. Reporting, including creating custom report templates and incident reports.
          6. The Federation feature for global monitoring, reporting, and alarm management of multiple remote and independent ACS, VMS, and/or ALPR systems spread across multiple facilities and geographic areas*. (Specifier, Enterprise only, additional license required)*
          7. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system. *(Specifier, Enterprise Only, additional license required for each site)*
          8. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts. *(Specifier, Professional and up, first integration included, additional licenses required for more)*
          9. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming). *(Specifier, Standard, Professional and up, additional license required)*
          10. SIP Intercom device integration for bi-directional communication.
          11. Integration with third party systems and databases via plug-ins (access control, video analytics, point of sale, and more). *(Specifier, Professional and up, additional license required)*
          12. Dynamic graphical map viewing.
          13. Asset management system integration. *(Specifier, Professional and up, additional license required)*
       4. The USP shall be deployed in one or more of the following types of installations:
          1. Unified access, ALPR, video platform, and any combination thereof.
          2. Standalone access control, ALPR, or video platform.
          3. Unified access and video platform that federates multiple remote ACS, VMS, ALPR.
          4. Standalone video platform that federates multiple independent remote VMS.
          5. Standalone access control that federates multiple independent remote ACS.
          6. Standalone access control that federates multiple independent remote ALPR.
       5. Licensing:
          1. A single central license shall be applied centrally on the configuration server.
          2. There shall be no requirement to apply a license at every server computer or client workstation.
          3. Based on selected options, one or more embedded systems shall be enabled or disabled.
       6. Hardware and Software Requirements:
          1. The USP and embedded systems (video, license plate recognition, and access control) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.
          2. The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.
          3. The USP database server(s) shall be built on Microsoft’s SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.
          4. The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.
          5. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and .NET software framework.
    4. USP Architecture
       1. The USP shall be based on a client/server model. The USP shall consist of a standard Server Software Module (SSM) and Client Software Applications (CSA).
       2. The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       3. The SSM shall be a Windows service that can be configured to start when the operating system is booted and run in the background. The SSM shall automatically launch at computer startup, regardless of whether or not a user is logged on the machine.
       4. Users shall be able to deploy the SSM on a single server or across several servers for a distributed architecture. The USP shall not be restricted in the number of SSM deployed.
       5. The USP shall support the concept of The Federation feature whereby multiple independent ACS, VMS, and ALPR installations can be merged into a single large virtual system for centralized monitoring, reporting, and alarm management. *(Specifier, Enterprise only, additional license required)*
       6. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
       7. The USP shall support up to one thousand instances of CSA connected at the same time. However, an unrestricted number of CSA can be installed at any time. *(Specifier, Maximum 5 with Standard; Maximum 10 with Professional; Unrestricted with Enterprise)*
       8. The USP shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
       9. The USP shall support uninterrupted video streaming. The CSA shall keep existing video connections active in the event that an SSM (except Archiver) becomes unavailable.
       10. Roles-Based Architecture:
           1. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.
           2. Each role shall execute a specific set of tasks related to either core system, automatic license plate recognition (ALPR), video (VMS), or access control (ACS) functionalities, among many others. Installation shall be streamlined through the ability of the USP to allow administrators to:

Deploy one or several SSM across the network prior to activating roles.

Activate and deactivate roles as needed on each and every SSM.

Centralize role configuration and management.

Support remote configuration.

Move roles over from one SSM to another.

* + - * 1. Each role, where needed, shall have its own database to store events and role-specific configuration information.
        2. Roles without databases, such as The Federation feature, Active Directory, and Global Cardholder Management, shall support near real-time standby without any third-party failover software being required.
        3. Directory Role:

The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.

The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.

The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:

Security Partitions, users and user groups

Areas

Zones, input/output (IO) linking rules, and custom output behavior

Alarms. Schedules, and scheduled tasks

Custom events

Macros or custom scripts

The Directory Role shall support the configuration/management of the following components specific to VMS:

Video servers and their peripherals (e.g., audio, IOs, and serial ports)

PTZ

Camera sequences

Recording and archiving schedules

The Directory Role shall support the configuration/management of the following components specific to ACS:

Door controllers, and input and output (IO) modules

Doors, Elevators, and Access rules

Cardholders and cardholder groups, credentials, and badge templates

The Directory Role shall support the configuration/management of the following components specific to ALPR:

ALPR units and cameras

Hotlists, permit lists, and overtime rules

* + - * 1. The Video Archiver Role shall be responsible for managing cameras and encoders under its control and archiving.
        2. The Media Router Role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).
        3. The Access Manager Role shall be responsible for synchronizing access control hardware units under its control, such as door controllers and I/O modules. This role shall also be responsible for validating and logging all access activities and events when the door controllers and I/O modules are online.
        4. The Automatic License Plate Recognition (ALPR) Role shall be responsible for synchronizing fixed ALPR units (cameras) and mobile ALPR applications under its control. The ALPR Role shall also be responsible for logging all ALPR activities and events.
        5. The Zone Manager Role shall be responsible for managing all software zones (collection of inputs) and logging associated zone events. Zones shall consist of inputs from both access control and video devices.
        6. The Health Monitoring Role shall be responsible for monitoring and logging health events and warnings from the various client applications, roles, and services that are part of the USP. This role shall also be responsible for logging events within the Windows Event Log and for generating reports on health statistics and health history.
        7. Optional Roles:

The Federation Role shall be responsible for creating a large virtual system consisting of hundreds or thousands of independent and remote ACS, VMS, and/or ALPR systems. *(Specifier, Enterprise only, additional license required)*

The Global Cardholder Synchronizer Role shall be responsible for synchronizing cardholder and credential data between the local site and a central site. Synchronization between remote sites shall also be supported. *(Specifier, Enterprise only, additional license required)*

The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server. *(Specifier, Professional and up, first integration included, additional licenses required for more)*

The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database.

The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports. *(Specifier, Professional and up, additional license required)*

The Plug-in Manager Role shall be responsible for the communication between the USP and third-party systems such as video analytics, access control, ALPR, video, and building management systems. *(Specifier, Professional and up, additional license required)*

The Point of Sale (POS) Manager Role shall be responsible for integrating the USP with third party POS systems and for logging transactions. *(Specifier, Professional and up, additional license required)*

The Web SDK Role shall be responsible for connecting the USP to any application or interface developed with the Web Service SDK. Applications developed with the Web Service SDK shall be platform independent and rely on the REST protocol for communications. *(Specifier, Professional and up, additional license required)*

The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

The Web Server Role shall be responsible for managing incoming Web interface connection and hosting the web pages for the Web interface. The Web Server Role acts as a proxy for the client connections and can be installed in a DMZ for additional security.

The Media Gateway Role shall be responsible for connecting any video stream to a third-party system using standard RTSP/RTSPS protocol. This role shall provide access to live and playback video. *(Specifier, Professional and up, requires the SDK packages, additional license required)*

* + - 1. Server Monitoring Service (Watchdog):
         1. The USP shall include a Server Monitoring Service that continuously monitors the state of the Server Software Module (SSM) service.
         2. The Server Monitoring Service shall be a Windows service that automatically launches at system startup, regardless of whether or not a user is logged into his account.
         3. The Server Monitoring Service shall be installed on all PCs/servers running an SSM. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the PC/server should it be unable to restart the service.
    1. USP Access Control, Video, and ALPR Unification
       1. The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ACS, VMS, and ALPR. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.
       2. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.
       3. The user shall be able to associate one or more video cameras to the following entity types: areas, doors, elevators, zones, alarms, intrusion panels, ALPR cameras, and more.
       4. It shall be possible to view video associated to access control events when viewing a report.
       5. It shall be possible to view video associated to intrusion panel events when viewing a report.
       6. It shall be possible to view video associated to ALPR events when viewing a report.
       7. The USP shall support the following Alarm Management functionality:
          1. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
          2. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.
          3. Set the priority level of an alarm and its reactivation threshold.
          4. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
          5. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
          6. Provide the ability to group alarms by source and by type.
          7. Define the time period after which the alarm is automatically acknowledged.
          8. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
          9. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
          10. Define whether to display the source of the alarm, one or more entities, or an HTML page.
          11. Specify whether an incident report is mandatory during acknowledgment.
       8. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.
       9. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, VMS, and ALPR systems.
       10. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.
       11. The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.
       12. Alarm unpacking and packing shall be supported where all the entities associated to an alarm can be displayed in the Monitoring UI with the single click of a button.
       13. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.
       14. The user shall be able to spontaneously trigger alarms based on something they see in the system.
       15. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.
       16. The user shall be able to investigate an alarm without acknowledging it.
    2. USP Threat Levels *(Specifier, Professional and Enterprise)*
       1. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.
       2. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.
       3. Threat Levels shall be set on an area or on the entire system.
       4. Threat Levels shall affect the system behavior by executing any action available in the USP such as: trigger output, start recording, block camera, override recording quality, arm zone, set a door in maintenance mode, and more.
       5. The following specific actions shall be available with Threat Level:
          1. Set minimum security clearance to restrict or permit access to cardholders on specific areas on top of the restrictions imposed by the access rules.
          2. Set minimum user level to automatically log out user from the USP.
          3. Set reader mode to change how the doors are accessed (for example card and PIN, or card or PIN).
       6. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.
    3. USP Remote Task
       1. The USP shall provide, through a Remote Task, capabilities to remotely monitor and control the content of other workstations running the CSA (Monitoring UI) that are part of the same system.
       2. The USP shall support video wall applications by connecting and controlling multiple workstations and monitors simultaneously.
       3. The Remote Task shall be a graphical interface showing a replication of the remote workstation running the CSA (Monitoring UI).
       4. The Remote Task shall allow the connection to other workstations using a low bandwidth mode to receive only snapshots of video viewed remotely.
       5. The Remote Task shall allow the connection to other workstations using a spy mode to remain invisible to the remotely connected workstation. The spy mode option should be available to the user with permission to access the feature.
       6. The functionality provided by the remote monitoring and control capability shall include:
          1. Remote monitoring and control of the monitoring and alarm monitoring tasks.
          2. Ability to remotely switch cameras, doors and zones into display tiles.
          3. Ability to remotely control live and playback video.
          4. Ability to remotely change the tile pattern.
          5. Ability to remotely create and delete tasks.
          6. Ability to remotely start/stop task cycling.
          7. Ability to remotely go into full screen mode.
          8. Ability to remotely save and reload the workspace.
    4. USP Advanced Task Management
       1. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day to day activities, and reporting.
       2. Administrators shall be able to assign tasks and lock the operator’s workspace. The user management of their workspace shall be limited by their assigned privileges.
       3. Operators shall be able to save their tasks as either Public tasks or Private tasks and in a specific partition. Public tasks shall be available to all users. Private tasks shall only be available to the owner of the task.
       4. Operators shall be able to share their tasks by sending them to one or more online users. Recipients shall have the option to accept the sent task.
       5. Operators shall be able to duplicate a task.
    5. USP Reporting
       1. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.
       2. Each and every report in the system shall be a USP task, each associated with its own privilege. A user shall have access to a specific report task if they have the appropriate privilege.
       3. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.
       4. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.
       5. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.
       6. The USP shall support the following types of reports:
          1. Alarm reports
          2. Video-specific reports (archive, bookmark, motion, and more)
          3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)
          4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more)
          5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more)
          6. Health activity and health statistics reports
          7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports
       7. Generic Reports, Custom Reports, and Report Templates:
          1. The user shall have the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.
          2. The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).
          3. All report templates shall be created within the Monitoring UI.
          4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
          5. An unrestricted number of custom reports and templates shall be supported.
       8. A reporting task layout shall consist of panes with settings (report length, filters, go and reset commands, etc.), the actual report data in column format, and a pane with display tiles. The user shall be able to drag and drop individual records in a report onto one or more display tiles to view a cardholder’s picture ID, playback a video sequence, or an ALPR event.
       9. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.
       10. The reporting task shall have the ability to display results through graphics such as line charts, bar charts, stacked bar charts, doughnut charts, and pie charts.
       11. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.
       12. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, export the graphics chart in JPG/PNG, and automatically email a report based on a schedule and a list of one or more recipients.
       13. Shall allow the ability to insert a custom logo when generating reports.
    6. USP Dashboards
       1. The USP shall support the ability to create dashboards.
       2. Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to dashboards should also be allowed to users granted the appropriate privilege.
       3. Dashboards in the system shall be a USP task. A user shall have access to a specific dashboard task if they have the appropriate privilege.
       4. Dashboards shall be saved either in a private folder or a public folder.
       5. A dashboard shall consist of a canvas with carious widgets displayed on the canvas. All widgets should offer the ability to specify location and size to the widget, a title to the widget, a background color to the widget, and the ability to refresh periodically the content of the widget.
       6. Dashboard widget types shall be:
          1. Image: provides the ability to display an image (JPG, PNG, GIF, BMP) on a dashboard.
          2. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, color, and alignment can be specified by the user.
          3. Tile: provides the ability to display any entity of the USP inside of a tile.
          4. Web page: provides the ability to display a URL on a dashboard.
          5. Entity Count: provides the ability to display the total number of a specific entity type in the USP.
          6. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.
          7. State: based on zones, intrusion areas, reader or input including color coded state and text.
          8. Map: Provides the ability to display and interact with maps on a dashboard.
       7. It shall be possible to extend to the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
       8. The USP shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.
    7. USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)*
       1. The USP shall support the concept of a Federation feature for access control, video, and ALPR.
       2. The Federation feature shall allow multiple independent USP systems (Federated systems) to be unified into a larger virtual system (the Federation feature). This shall facilitate the global monitoring of multiple independent USP systems.
       3. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.
       4. Entities that shall be federated and monitored centrally from the Federation feature shall include alarms, areas, cameras, cardholders and cardholder groups, credentials, doors, elevators, ALPR events, and zones (monitored inputs).
       5. The Federation feature shall support a cloud-based deployment, whereby the service and infrastructure will be updated automatically and provisioned by the service provider, without need for on-site hardware.
       6. The Federation feature shall support Global Alarm Management from the Monitoring UI for access control, video, and ALPR.
       7. The Federation feature shall support Global Report Generation from the Monitoring UI for access control, video, and ALPR.
       8. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (for example, generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).
    8. USP Zone Management
       1. The USP shall support the configuration and management of zones for input point monitoring via the Zone Manager Role. A user shall be able to add, delete, or modify a zone if they have the appropriate privileges.
       2. A zone shall monitor the status of one or more inputs points. Zone monitoring or input point monitoring shall be possible through the use of a controller and one or more input modules. Inputs from video cameras or video encoders shall also be accessible via a zone.
       3. Depending on the hardware installed, supervised inputs shall be supported. Depending on the input module used, both 3-state and 4-state supervision shall be available.
       4. A schedule shall be defined for a zone, indicating when the zone will be monitored.
       5. Custom Events shall provide full flexibility in creating custom events tailored to a zone. Users shall be able to associate custom events to state changes in monitored inputs.
       6. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.
       7. Input/Output (IO) Linking:
          1. Zone management shall support Input/Output (IO) Linking. I/O Linking shall allow one or more inputs to trigger one or more outputs.
          2. IO Linking shall be available in offline mode when communication between the server and hardware is not available.
          3. Custom Output Behaviors shall provide full flexibility in creating a variety of complex output signal patterns: simple pulses, periodic pulses, variable duty-cycle pulses, and state changes.
          4. Through the “trigger an output” action, the ACS shall support the triggering of outputs with custom output behaviors.
    9. USP User and User Group Security, Partitions, and Privileges Management
       1. The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if they have the appropriate privileges.
       2. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:
          1. ADFS (Active Directory Federation Services)
          2. Azure Active Directory (through OpenID Connect)
          3. Ping Identity (through OpenID Connect)
          4. KeyCloak (through OpenID Connect)
          5. Other Open ID Connect / SAML2 authentication agents
       3. Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups. User group nesting shall be allowed.
       4. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR shall have associated privileges.
       5. Specific entities, such as cardholders, cardholder groups, and credentials shall include a more granular set of privileges, such as the right to access custom fields and change the activation or profile status of an entity.
       6. Partitions:
          1. The USP shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a system into multiple security partitions.
          2. All entities that are part of the USP can be assigned to one or more partitions.
          3. A user who is given access to a specific partition shall only be able to view entities (components) within the partition to which they have been assigned. Access is given by assigning the user as an accepted user to view the entities that are members of a particular partition.
          4. A user or user group can be assigned administrator rights over the partition.
       7. It shall be possible to specify user and user group privileges on a per partition basis.
       8. Advanced logon options shall be available such as dual logon and more.
       9. It shall be possible to specify an inactive period for the Monitoring UI after which time the application shall automatically lock, while still preserving access to currently displayed camera feeds.
       10. It shall be possible to review user permissions and determine:
           1. For any entity in the system, which user group or user can view or modify it.
           2. For any user group or user in the system, what are its privileges.
           3. For any privilege in the system, which user group or user is allowed to perform the underlying action.
    10. USP Event/Action Management
        1. The USP shall support the configuration and management of events for video and ALPR. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.
        2. The USP shall receive all incoming events from one or more ACS, VMS, and/or ALPR. The USP shall take the appropriate actions based on user-define event/action relationships.
        3. The USP shall receive and log the following events:
           1. System-wide events
           2. Application events (clients and servers)
           3. Area, camera, door, elevator, and ALPR events (reads and hits)
           4. Unit events
           5. Zone events
           6. Alarm events
           7. ALPR events
           8. Health Monitoring events
        4. The USP shall allow the creation of custom events.
        5. The USP shall have the capability to execute an action in response to an access control, video, and ALPR event. The USP shall support the following list of actions, without being limited to:
           1. Add bookmark
           2. Arm intrusion detection area
           3. Arm zone
           4. Block and unblock video
           5. Bypass input
           6. Cancel postpone intrusion detection area arming
           7. Clear input bypass
           8. Clear task
           9. Display a camera on an analog monitor
           10. Display an entity in the CSA
           11. Email a report
           12. Email a snapshot
           13. Export report
           14. Forgives antipassback violation
           15. Go home
           16. Go to preset
           17. Import from file
           18. Override recording quality
           19. Override with event recording quality
           20. Override with manual recording quality
           21. Play a sound
           22. Postpone intrusion detection area arming
           23. Reboot unit
           24. Recording quality as standard configuration
           25. Rest area people count
           26. Reset parking zone inventory
           27. Run a macro
           28. Run a pattern
           29. Send a message
           30. Send a task
           31. Send an email
           32. Set parking zone occupancy
           33. Set reader mode
           34. Set the door maintenance mode
           35. Set threat level
           36. Start/Stop applying video protection
           37. Start/Stop recording
           38. Start/Stop transfer
           39. Synchronize role
           40. Temporary override elevator schedules
           41. Trigger intrusion alarm
           42. Trigger alarm
           43. Trigger output
           44. Trigger read
           45. Unlock door explicitly
           46. Set the entity maintenance mode
           47. Trigger incident
           48. Set interface background color
           49. Set minimum security clearance
        6. The USP shall allow a schedule to be associated with an action. The action shall be executed only if it is an appropriate action for the current time period.
    11. USP Schedules and Scheduled Tasks
        1. Schedules
           1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if they have the appropriate privileges.
           2. The USP shall provide full flexibility and granularity in creating a schedule. The user shall be able to define a schedule in 1-minute or 15-minute increments.
           3. Daily, weekly, ordinal, and specific schedules shall be supported.
        2. Scheduled Tasks
           1. The USP shall support scheduled tasks for video, and ALPR.
           2. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.
           3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email or emailing a report.
    12. USP Macros and Custom Scripts
        1. The USP shall enable users to automate and extend the functionalities of the system through the use of macros or custom scripts for access control, video, and ALPR.
        2. Custom macros shall be created with the USP Software Development Kit (SDK).
        3. A macro shall be executed either automatically or manually.
        4. In the Monitoring UI, a macro shall be launched through hot actions.
    13. USP Dynamic Graphical Maps (DGM)
        1. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.
        2. The USP shall provide a map centric interface with the ability to command and control all the USP capabilities from a full screen map interface.
        3. It shall be possible to span the map over all screens of the USP client station. In the scenario where the map is spanned over all the screens of the USP client station it shall be possible to navigate the map including pan and zoom, and the map’s moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same command and control capabilities than in a single screen display.
        4. The DGM shall support the following file format and protocol for importing map background:
           1. PDF
           2. JPG
           3. PNG
           4. Web Tile Map Service (WTMS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
           5. BeNomad
           6. AutoCAD (DWG & DXF)
        5. The DGM shall provide the following online map providers for use as map background and provide the ability to manage their service license if they require one:
           1. Google Map, aerial, terrain (Licensed)
           2. Bing Map, aerial, satellite, hybrid (Licensed)
           3. ESRI ArcGIS (Licensed)
           4. OpenStreet Map aerial (Licensed)
           5. OVI hybrid
        6. It shall be possible to configure a mixed set of maps made of GIS, online providers, and private imported files and link them together.
        7. The DGM shall provide the ability to display all native entities of the USP including:
           1. Cameras, fix, and PTZ
           2. Doors
           3. Camera sequences
           4. Areas
           5. Intrusion areas
           6. Intrusion zones
           7. License Plate Recognition cameras
           8. Digital inputs
           9. Digital outputs
           10. Intercoms
           11. Alarms
           12. Macros
           13. Police Car Patrollers
        8. The DGM shall provide the ability to draw and display information over the map in the form of:
           1. Vectoral shapes: lines, rectangles, polygons, ellipse
           2. Pictures
           3. Text
        9. The DGM shall provide the ability to display any type of third-party entities integrated through an SDK.
        10. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.
        11. The DGM shall provide the ability to the operator to manage layers of entities displayed over the map, being able to turn them on and off and changing the superposition order.
        12. The DGM shall provide the ability to show or hide camera icons and their field of view based on the zoom level of the map. The icon size can be optionally set to a fixed size regardless of zoom level.
        13. The DGM shall provide the ability to import data layers from one or more ESRI ArcGIS servers.
        14. The DGM shall provide the operators with the ability to manage layers that are imported from ESRI ArcGIS. The operators shall be able to turn the layers on and off, as well as sort the layers.
        15. The DGM shall offer built-in map data backup and restore for both map background and layers of entities.
        16. The DGM shall provide the ability to import configuration from an eternal file such as:
            1. AutoCAD layer for objects
            2. CSV, Excel file
        17. The DGM shall provide the ability to print a map in the following file formats:
            1. PDF
            2. PNG
        18. The DGM shall offer failover capabilities.
        19. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.
        20. The DGM shall provide a means to update a map background without affecting the map object configuration.
        21. The DGM shall offer a user-friendly graphical map designer to configure the maps.
        22. The DGM shall provide a user friendly and intuitive navigation that includes:
            1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
            2. The ability to define favorites for recurrent position recall.
            3. The possibility to create links between maps. The map links shall allow the link from one map to multiple maps representing the floors of a building. Navigating between floors of a building shall keep the zoom level of the map.
            4. A common user experience regarding navigation into the map for both GIS and private maps. *(Specifier, Professional or Enterprise required for GIS)*
        23. It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.
        24. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.
        25. The DGM shall offer a smart selection too to access the video. By clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection too shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.
        26. It shall be possible to select a location by drawing a zone of interest on the DGM, and to display all the entities that are part of that zone or interest at once.
        27. The user shall be able to select and display the content of multiple USP entities on the map in pop-up windows.
        28. The user shall be able to move, resize, and pain the USP entity pop-up windows to the map.
        29. It shall be possible to access live and playback video from the map.
        30. It shall be possible to monitor all entity event notifications from the DGM. Users shall be able to turn notifications on and off per entity.
        31. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:
            1. Center the map on entities related to the alarm.
            2. Visualize the Alarm notifications on the map and access the related videos from the map.
            3. Trigger and receive alarms.
            4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
            5. Visualize that an alarm occurred in an underlying linked map.
        32. The DGM shall provide the following search capabilities:
            1. Search and center by entity name.
            2. From the Display of an entity in the USP, locate the entity on the map and offer the ability to select another one close-by.
            3. By street address, city, landmark, point of interest (using geocoder license from Google, ESRI, or other provider)
        33. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.
        34. The DGM shall support the use of GIS maps, private maps, or a combination of both for the map background. *(Specifier, Professional or Enterprise required for GIS).*
        35. The DGM shall be compatible with any GIS compliant maps with the OGC and supporting WMTS and WMS. This includes, but is not limited to, ESRI maps. The DGM shall allow the selection of the appropriate GIS layers. *(Specifier, Professional or Enterprise required for GIS).*
        36. The DGM shall provide an intuitive built-in map designer for entity positioning on the map using drag and drop. Any configuration shall be graphic.
        37. It shall be possible to edit and configure multiple map objects at once.
        38. All map design modifications shall be logged in an audit trail.
        39. Various actions shall be available within maps for execution through simple and intuitive double-click, right-click, or drag-and-drop functionality. Examples of actions available through maps shall include unlocking a door and acknowledging an alarm.
        40. Through the following functionalities, the DGM shall allow the management of USP alarms from the map:
            1. Locate on the map entities related to the alarm.
            2. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.
            3. List, select, and locate alarms.
            4. Auto center the map on the highest priority alarm.
            5. Handle the alarm from the map, including acknowledgement, forwarding, and investigation.
            6. All map containers, such as hotspots or map links, shall reflect the alarm status of the contained entities.
        41. It shall be possible to add advanced functionality to map objects using the SDK. Any functionality available through the USP SDK shall be available within maps.
        42. The DGM shall offer lasso tools for:
            1. Displaying entities at one location through a single action.
            2. Triggering an action on all entities at one location in a single click.
            3. Editing multiple entities at one location simultaneously.
        43. The DGM shall allow the display of USP entities selected from the map on a remote monitor (video wall).
        44. The DGM shall provide the ability to search within the map by entity name.
        45. The DGM shall allow the use of KML overlay map information for both GIS and private maps. Moveable objects shall be supported using the KML. *(Specifier, Professional and Enterprise)*
        46. The Contractor shall provide licenses for each entity that is required to be shown on the graphical maps.
    14. USP Digital Evidence Management System (DEMS) *(Specifier, Genetec Clearance, separate subscription required)*
        1. The USP shall support the ability to electronically share video exports with third parties.
        2. The USP shall allow recipients to natively review exported video from a web browser, without the need to install software or browser plugins.
        3. Video exported from the USP will include the original file and timestamp information, as well as the system, workstation, and camera source metadata that can be viewed from the DEMS.
        4. The USP shall support the ability to create a case within the DEMS, and assign associated incident details, when exporting video.
        5. The USP shall support the ability to publish a list of cameras in a DEMS camera registry.
        6. The USP shall allow for participants in the DEMS camera registry to be displayed on the map of the USP.
        7. The USP shall process video requests originating from the DEMS without requiring operator intervention.
        8. Video requests sent from the DEMS to the USP shall be processed from the following sources:
           1. Cameras connected to the USP.
           2. Federated cameras connected to the USP.
           3. Vehicle and onboard systems connected to the USP.
        9. Video from vehicle and onboard systems sent to the DEMS shall include the following features:
           1. Ability to request and playback video from onboard cameras through the web interface of the DEMS.
           2. Display of metadata from vehicle sensors such as:

GPS coordinates

Vehicle triggers

Vehicle speed

* + - * 1. Display of vehicle route on a map through the web interface of the DEMS.
      1. The USP shall support the automatic upload of video exports and snapshots to the DEMS.
         1. It shall be possible to trigger automatic upload of exports to the DEMS based on USP events:

System

Video analytic

Motion detection

Door activity

Zone activity

Alarm

Manual action

Scheduled task

The USP shall allow for configuration of the length of video export to automatically export to the DEMS for each event type:

Up to 24 hours before the event

Up to 24 hours after the event

* + 1. USP Audit and User Activity Trails (Logs)
       1. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.
       2. Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
       3. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
       4. The USP shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the USP such as login, camera viewed, ALPR event viewed, badge printing, video export, and more.
       5. The ACS shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.
    2. USP Incident Reports
       1. Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.
       2. The operator shall be able to create standalone incident reports or incident reports tied to alarms.
       3. The operator shall be able to link multiple video sequences to an incident, access them in an incident report, and change the date or time of the sequences later on.
       4. It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.
       5. Incident reports shall allow the creation of a custom form on which to input information on an incident.
       6. Incident reports shall allow entities, events, and alarms to be added to support at the report’s conclusions.
    3. USP Data Ingestion
       1. The USP Shall allow the possibility to import external data from outside sources to enhance unification of data sources within the USP.
       2. Each data source shall be defined by a set of fields and field types that describe the data source. Field types shall be:
          1. String
          2. 32 bit & 64 bit integer
          3. Floating point number
          4. Boolean
          5. Timestamp
          6. Binary (in a file or base 64)
       3. The visualization of each data point from a data source shall be configurable to determine what fields from the data should be displayed. The configuration of each field shall be:
          1. Which fields are displayed or hidden
          2. What order are the fields displayed
          3. A label to specify the name of the field (to have a key:value format)
          4. An option to specify how to display the field (text value, Image, clipboard value, hyperlink to a web page, hyperlink to an entity in the system, sound file)
       4. A privilege should be available for each data source to allow / deny access to specific user & user groups of the USP.
       5. Ingested data shall be available in the USP reporting system.
       6. Ingested data shall be available to display in the USP Dashboards.
    4. USP Third Party Integration
       1. Microsoft Active Directory Integration *(Specifier, Professional and up, first integration included, additional licenses required for more)*
          1. The USP shall support a direct connection to one or multiple Microsoft Active Directory server via the Active Directory Role(s). Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.
          2. Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups.
          3. The USP shall be able to connect to and synchronize data from multiple Active Directory servers (up to 10).
          4. The USP shall support synchronizing Active Directory Universal Groups as well as security groups belonging to other domains within the same forest.
          5. The USP shall support Microsoft Active Directory encryption using LDAP SSL.
          6. When enabled, Active Directory shall manage user logon to the USP client applications through the user’s Windows credentials. Logging on to the USP shall utilize native Active Directory password management and authentication features.
          7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:

Users (username, first and last names, email address, and more)

User groups (user group name, description, and group email address)

Active Directory attributes to USP custom fields

* + - * 1. When enabled, the addition, removal, or suspension of a user’s Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent user account in the USP.
        2. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include on first logon (users only), manual synchronization, and scheduled synchronization.
        3. The USP shall support user connections across independent organizations by connecting to an identity provider using claims-based authentication such as ADFS (Active Directory Federation Services), Azure Active Directory, other OpenID Connect & SAML2 providers.
      1. Intrusion Detection Integration: *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
         1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
         2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):

Arm and disarm intrusion devices (manually, on schedule, or following a USP event).

Activate or trigger intrusion device outputs.

View intrusion events and alarms.

Monitor the status, including arming status, of the intrusion devices.

Video verification of intrusion events and alarms with video panels.

Create USP zones using intrusion device inputs.

* + - * 1. Currently supported intrusion panels include:

Bosch Legacy G Series panels

Bosch B & G Series panels

Bosch Map 5000

DSC Power Series panels

DMP XR Series panels

Honeywell Galaxy Dimension and Flex panels

Vanderbilt SPC

UTC Advisor Master and Advanced

Satel INTEGRA panels

Telenot Complex 400H panels

* + - * 1. Additional intrusion devices supported:

Buytime

Alarm Panel Receiver

Southwest Microwave RPMII

* + - 1. Third Party Access Control Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network and should not support administrative tasks such as cardholder management.
         2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

Synchronize access control entities and receive associated events and states within the USP, including:

Cardholders

Visitors

Readers and doors

Alarms

Inputs and outputs

Monitor access control events.

Monitor and Acknowledge access control alarms.

Trigger actions and outputs in the access control software using hot actions and event-to-actions.

Lock and unlock doors in the access control software.

Video verification of access control events and alarms.

Configure event-to-actions using the access control events and alarms.

Generate Security Center reports using from the in the access control data.

View and monitor states of door entities in the USP maps.

* + - * 1. Currently supported access control manufacturers include:

Tyco Softwarehouse CCURE

UTC Lenel Onguard

Amag Symmetry

Siemens Sipass

AssaAbloy ARX

* + - 1. Third Party Destination Dispatch Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third part destination dispatch (elevator control0 software via the SDK. Communications with the destination dispatch software shall be over an IP network.
         2. Integration with destination dispatch software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of destination dispatch software with the USP shall include the following (where supported by the destination dispatch solution):

Destination dispatch entity creation and reception of associated events and states within the USP, including:

Floors and landings

Elevator cars (front/rear doors) and kiosks

Cardholders and credentials (if applicable)

Monitor destination dispatch events.

Trigger manual dispatch actions.

Video verification of destination dispatch events.

Configure event-to-actions using the destination dispatch events.

Generate Security Center reports using the destination dispatch data.

Support multiple readers

Kiosk internal readers

USP readers

Kiosk advanced modes and passenger types.

* + - * 1. Currently supported destination dispatch manufacturers include:

Otis Compass

Thyssenkrupp

MCE

KONE

* + - 1. Asset Management Integration: *(Specifier, Professional and up, additional license required)*
         1. The USP shall integrate with third party asset management systems via the Asset Management Role.
         2. Communications with asset management solutions shall be over an IP network (via software communications).
         3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):

Synchronize asset management system assets with USP asset entities.

Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

Synchronization of asset management alarms with Security Center alarms.

Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

Real-time tracking of asset locations on a per area basis.

Asset Management Inventory reporting task that details the current location (area) of an asset.

Asset Activity reporting task that provides a historical review of asset-related events and activity.

* + - * 1. Currently supported asset management systems include:

Deister Key management

Morsewatchmans

TRAKA

Key Systems

* + - 1. Additional Third-Party Integrations:
         1. The USP shall support multiple approaches to integrating third-party systems. These shall include: Software Development Kits (SDKs), REST-based Web Service SDKs, RTSP Service SDKs, and more. *(Specifier, Professional and up, SDK package and license required)*
         2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as: *(Specifier, refer to the website for how these are licensed, for an updated list of available third-party integration, please refer to the supported plugin guide)*

Video analytics

Third-party video systems

Third-party access control systems

ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors

Building management systems

Access Control ecosystem (such as ID scanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)

Transaction monitoring (POS, Barcode scanning, ATM)

Industrial IoT: Data ingestion from external devices through standard communication protocols (Modbus, BACnet, OPC, SNMP, HTTP Server, MQTT Client, TCP Server)

Industrial Protocol Interface: Data exposure from GSC to external protocol interfaces using standard communication protocols (BACnet, SNMP)

Videowall (Barco, Eizo)

Human resource management systems (HRMS)

Autonomous Drone Integration

Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))

Gunshot Detection (Shot Spotter, Guardian GunShot)

Dynamic Logbook: Customizable forms with reporting capabilities

* + 1. USP Software Development Kit (SDK)
       1. A USP SDK shall be available to support custom development for the platform.
       2. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.
       3. Integration with external applications and databases shall be possible with the SDK.
       4. The SDK shall enable end-users to develop new functionality (user interface, standalone applications or services) to link the USP to third party business systems and applications, such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.
       5. The SDK shall be based on the .NET framework.
       6. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.
       7. The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
       8. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.
       9. The SDK shall provide an extensive list of programming functions to view and configure most ACS entities such as: cardholders, cardholder groups, visitors, credentials, access rules (modify only), and custom fields.
       10. The SDK shall be able to receive real time events from the following USP entities: users and user groups, areas, zones, cameras, video units, doors, door controllers (units), elevators, cardholders, cardholder groups, and credentials.
       11. The SDK shall be able to query the history of events for areas, cameras, zones, alarms, cardholders, credentials, visitors, doors, query license plate read events, license plate hit events, generate a license plate hits report, generate a license plate reads report.
       12. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.
  1. **Execution**
     1. Warranty
        1. The product shall perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use. Software defects are covered through Service Releases and Cumulative Updates which are available for a period of 1 year from the date of the software purchase.
        2. Extended warranty, up to 5 years, shall be available through the purchase of the Genetec Advantage support service which includes the following additional services over the standard warranty:
           1. Access to phone support and online chat for technical assistance
           2. Online case management
           3. Online system availability monitor
           4. Access to Major and Minor Release Upgrades
           5. 24/7 pager support and dedicated support specialist *(Specifier, additional cost)*
     2. Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 
        1. General Requirements:
           1. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:

Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

Complex enterprise installations involving advanced functionality (for example The Federation feature, failover, plugins) and/or multiple systems (for example access control, video, ALPR) and/or third-party integrations.

Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

* + - * 1. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.
      1. Deployment Management Service:
         1. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization and who will be responsible for:

Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

Providing a project plan for the deployment of the vendor's USP.

Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

* + - 1. Solution Architect Service:
         1. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:

Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews as well as performance reviews of the vendor’s USP.

Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.

Providing upgrade and migration strategy for the vendor’s USP where applicable.

Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

* + - 1. System Configuration and Commissioning Service:
         1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

Assisting the contractor’s or subcontractor’s onsite/remote technicians with the configuration and commissioning of the vendor’s USP at the client site.

Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.

Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

* + 1. Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)*
       1. The contractor shall engage the services of the USP vendor to assist in the end user training of the USP at the end-user site.

**End of Section**

1. **Section 28 51 00 – Information Management & Presentation**
   1. **General**
      1. Related Work
         1. Division 14 – General Elevator Requirements
         2. Section 28 13 00 – Electronic Access Control System
         3. Section 28 23 00 – Video Surveillance
      2. Definitions
         1. ACS – Access Control System
         2. CSA – Client Software Application
         3. DGM – Dynamic Graphical Maps
         4. DVS – Digital Video Server
         5. CDMS – Collaborative Decision Management System
         6. ALPR – Automatic License Plate Recognition
         7. SDK – Software Development Kit
         8. SMA – Software Maintenance Agreement
         9. SSM – Server Software Module
         10. UI – User Interface
         11. USP – Unified Security Platform
         12. UWI – Unified Web Interface
         13. VMS – Video Management System
      3. Qualifications
         1. The system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Omnicast™ Technical Certification.
         2. Optionally, the system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Enterprise Technical Certification.
         3. The system programmer shall be a Genetec certified partner with the following level of qualification: *(Specifier, select one of the following)*
            1. Certified Reseller or up
            2. Elite Reseller or up
            3. Unified Elite Reseller
         4. The system programmer shall submit proof of certifications.
   2. **Products**
      1. General Requirements
         1. The CDMS shall be seamlessly embedded in the Unified Security Platform (USP).
         2. The CDMS shall be based on a true open architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure, and non-proprietary storage.
         3. The CDMS shall offer a complete and scalable operational toolset that allows real-time monitoring and situation management, as well as post-event analysis capabilities.
         4. The CDMS shall be provided by the same manufacturer as the core of the USP and shall interface natively with all components of the USP including, but not limited to, VMS, ACS, communication, intrusion, plugins, and add-ons.
         5. The USP and CDMS shall be forward compatible so upgrade of one does not prevent from using the other.
         6. The CDMS shall be seamlessly compatible with the USP and any of its components.
         7. The CDMS shall offer the following operational tools:
            1. Incident management
            2. Document management
            3. Rules Engine
            4. Automation workflows
            5. Standard operating procedures
            6. Incident monitoring operator interface
            7. Incident reports
         8. The CDMS shall provide situational intelligence to the operator with a map-centric approach and detailed overview of incident data, combining incident history, operator comments, workflow and operator action logs, standard operating procedures, relevant live and playback video, and an aggregated events sequence of the incident. Aggregation of events shall have the option to be based on the entities themselves or on designated areas on a per category basis.
         9. The CDMS shall be scalable to support an average continuous flow of up to 600 events per second, with temporary bursts of 5,000 events per second. It shall be capable of dispatching a minimum of 20 incidents per second and executing associated automation workflows.
         10. The CDMS architecture shall be highly reliable with zero single points of failure. The CDMS servers shall have the capacity to fail over with less than 1 minute of downtime and a guarantee of zero loss of events and incidents. No action from the user shall be required in the event of a server failure.
         11. The communication between components of the CDMS shall be encrypted, robust and reliable.
         12. The CDMS shall offer an SDK to customize the incident triggering, the incident closing conditions, the automation workflow activities, the incident data, and the incident details view. It shall also be possible to design custom widgets within the CDMS user interface.
         13. The CDMS shall offer a standard API to trigger and dispatch incidents, get incident configurations, get incident details including content of the dynamic standard operating procedures, change incident states, change incident priorities, change incident descriptions, link incidents, change incident locations, change incident types, set incident external id, query history of an incident.
         14. The standard API shall provide a notification mechanism to subscribe to incident updates
         15. Any of the devices or features that are already licensed in the USP shall not require additional licenses to work within the CDMS.
         16. The CDMS shall allow operator-based configuration of the CDMS users. The role-based privileges are inherited from the USP privileges.
         17. The CDMS shall log all configuration changes in an audit trail with before and after configurations.
         18. The CDMS shall log all the user activities that are executed during the time that an incident is active.
         19. The CDMS shall provide the capability to copy an incident configuration in part or in full to one or multiple incident types.
         20. The CDMS shall provide the ability to configure incidents in a test mode that would allow user with the appropriate privilege to validate different parameters before activating the incident configuration.
      2. CDMS Graphical User Interface
         1. The CDMS shall provide the flexibility to add custom fields within incidents to get updated by user’s data or input and available for reporting.
         2. The CDMS shall offer a simple and user-friendly GUI within the USP GUI. The CDMS tools shall be a series of additional tasks. The custom fields shall be available for reporting and users with privilege shall be able to edit them in the Custom fields widget.
         3. The CDMS shall provide tasks to the USP for:
            1. Incident monitoring
            2. Incident detail view
            3. Incident reporting
            4. Incident management
         4. Incident monitoring shall provide:
            1. A list of current incidents. The list of current incidents shall be adaptable to the operator’s role and needs, with tools such as multi-level grouping of incidents, and advanced filtering and searching.
            2. A Dynamic Graphical Map displaying incident locations and providing full situational awareness of the security in a geographical area.
            3. An Incident Detail Pane with all related information for the selected incident:

Overview

Latest activities

Related incidents

Related entities

Related documents

Custom views (SDK)

Additional fields

* + - * 1. Access to all controls available in the USP.
        2. Incident details pane shall be customizable with options to display only selected information.
        3. A user status field that can be set to Available or Not available.
      1. CDMS shall be designed for optimal use with multiscreen workstations, allowing a combination of the incident list, the dynamic graphical map, and the incident details to be displayed on each screen. The CDMS GUI shall be capable of synchronizing all screens so that the selection of an incident will automatically focus all other screens to this incident data. The screens shall have the capability of being synchronized by one or any combination of incident selection, view filter or column view settings.
      2. The Dynamic Graphical Map shall provide a tooltip with incident summary when selecting an incident on the map. Multiple incidents at the same location will cluster into one object on the map. The cluster shall display the incident with the highest priority level and the number of incidents in the cluster. It shall also be possible to display a list of all the incidents within the cluster.
      3. It shall be possible to configure a map to display all incidents from all maps in a single view based on their relative GPS coordinates.
      4. The Incident Monitoring task can be configured to display the list of incidents, the incident map, the incident details, or any combination of these elements.
      5. The incident list shall allow the operator to group the incident by:
         1. Incident category
         2. Incident type
         3. Incident priority
         4. Incident state
         5. Incident location
         6. Incident owner
         7. Any custom incident attributes
         8. Area
         9. Events triggered
         10. Source entities
      6. It shall be possible to save the operator interface, and the configuration of the GUI shall remain the same after an operator logon or logoff.
      7. The CDMS GUI shall provide advanced tools to assist operators when focusing on a mission. The filter can be applied to the current task or simultaneously on all tasks.
      8. The CDMS GUI shall provide an expandable display area for editing the diagram associated with a dynamic Standard Operating Procedure.
    1. CDMS Incident Management
       1. The CDMS shall be the interface that displays all situations as incidents.
       2. The CDMS Incident management shall provide the ability to trigger incidents manually or automatically, based on a correlation of events.
       3. An incident shall be the holistic description of the situation and support the following attributes:
          1. Visual:

Color.

Icon. Incident management shall provide the ability to customize incident types using a set of imported icons.

* + - * 1. Sound.
        2. Incident category. Incident category shall allow an operator to organize incident types in a logical tree.
        3. A location. The location can be an entity (camera, door, zone, area) or a geographical coordinate.
        4. A priority level.
        5. A description.
        6. States.
        7. Standard operating procedures.
        8. History of activities.
        9. Attach Entities. Entities related to the source of events triggering the incident shall be automatically associated to the incident.
        10. Attached documents. Documents and URLs providing more information or guidance on the incident and its management.
        11. A schedule during which automatic trigger of an incident by the system will be valid.
      1. The CDMS shall provide a configurable state machine that will define the transition of states. For example, you can configure state E to be available only if the incident is in state C or D. Therefore, if the incident is in state A or B, state E is not available.
      2. Incident states shall be configurable so that only specific users have the privilege to change the incident state to a particular state.
      3. The Incident management shall provide management of incident ownership. It shall be possible to explicitly request or release the ownership of an incident. Ownership of an incident shall be provided immediately to an operator who starts working on an incident.
      4. A supervisor shall be able to view all incidents that are under his supervision and see the ownership of each incident. In the same view, the supervisor shall also be provided with real-time information about who is currently monitoring an incident.
      5. The CDMS shall notify the supervisor when an operator skips a step in the standard operating procedure (SOP).
      6. The CDMS shall provide the capability to request the current owner’s consent before taking ownership of an incident.
      7. The CDMS shall provide a way to define collaborative incidents to allow multiple operators to work on the same incident.
      8. It shall be possible to configure different SOP and automation workflows for different recipients of a collaborative incident.
      9. It shall be possible to change the incident type, manually or automatically.
      10. The CDMS shall provide the capability to add custom fields that are shareable in collaborative incidents and can be modified by the operators working within them.
      11. The CDMS shall allow the export of the incident type and category configuration with custom icons. The CDMS shall allow the exported configuration to be imported.
      12. The CDMS shall allow the export of all sub-incidents attached to a collaborative incident or all incidents created from a master incident, from the automation workflow by changing the incident type manually.
      13. For each incident, it shall be possible to open the incident details or configure the incident to automatically open incident details. The incident details will open on a configurable screen and provide, based on the incident type configuration, the following information:
          1. A layout of all live and playback video related to the incident, including the camera associated to the source and location of the incident, as well as the local map centered on the incident location.
          2. History of the incident including:

All events related to the incident

System automation workflow activities

Operator actions for the incident

Comments about the incident

* + - 1. Operators shall be able to perform the following actions:
         1. Change the incident state.
         2. Change the incident type.
         3. Change the incident location.
         4. Forward the incident.
         5. Transfer the incident.
         6. Edit the incident:

Change the description

Change the priority level

Release the ownership

* + - * 1. Attach additional entities to the incident.
        2. Link related incidents.
        3. Attach a document to the incident.
      1. Incident Dispatch:
         1. The CDMS shall provide the ability to dispatch an incident to a user or group of users. Dispatching an incident to a restricted number of users will secure the access to information.

Incident dispatch shall have the capability to get dispatched to selected user group based on order of logon (round robin). If all users are logged off, incident dispatch follows the format of ordinary incident dispatch and gets dispatched to everyone in the selected user group.

* + - * 1. The CDMS shall allow the distribution of specific tasks (managed as sub-incidents) that are associated to a unique incident, to different teams. Procedures can be performed in parallel.
        2. Incident supervisors shall be able to see all sub-incidents associated with a main incident.
        3. The CDMS shall manage the dispatch of incidents by:

Incident type

Schedule

Location. Where it shall be possible to define the location by:

Entity

Area (group of entities)

User availability

* + - * 1. It shall be possible to trigger a new dispatch during the course of an incident:

By an operator action in the GUI. The user shall have the choice of:

Transferring the incident, meaning that the incident will no longer be in the user’s incident list. The user has the option to request acknowledgement of the transfer.

Forwarding the incident, meaning that the incident will continue to be in the user’s incident list and the user remains a recipient of this incident.

Requesting to take ownership of the incident.

Escalating an incident.

* + - * 1. It shall be possible to define profiles to ensure the adequate distribution of the active incidents among the operators who are currently logged on to the system and filter incidents by type and by occurrence location.

The system shall have the capability to automatically assign incident management profiles to users when they log on.

Profiles shall only be assigned to users that are logged on to the system.

Profiles shall be assigned by the system or by users with the required privileges.

It shall be possible to assign a profile to specific users or user groups.

It shall be possible to specify incident types and locations associated with a profile.

When a profile is assigned to an operator, the system shall hide all incidents not specified by the profile from the operator's view.

It shall be possible to assign multiple profiles to an operator. When multiple profiles are assigned, the operator shall see the incidents specified by all assigned profiles.

It shall be possible to activate or deactivate an existing profile.

Modifications to the profile configuration shall be traceable in a report, and the report shall be exportable.

The load shall be balanced based on availability of the operators and their privileges.

Incidents shall be automatically transferred to authorized recipients if no operator is online for a specific profile.

* + - 1. Ability to define reminders:

Reminders for the operator shall be set on a schedule.

The reminders shall display specific text messages for the operator. Reminders shall also have to ability to be added automatically through the incident automation workflow.

A warning message shall be displayed when an incident is resolved with an active reminder.

* + 1. CDMS Incident Report
       1. The CDMS shall offer a task to manage and generate reports. The ability to run a report is a user privilege.
       2. It shall be possible to query the incident history filtering by:
          1. Incident type
          2. Incident state
          3. Location
          4. Priority
          5. Trigger time range
          6. Incident owner
          7. Description
          8. Incident additional field
       3. The result of a report query shall provide a list of incidents as well as a visual of these incident locations on the map. When more than one incident is reported at the location, the GUI will cluster these incidents on the map.
       4. Selecting an incident from the list or on the map will display the incident details that contain the same information available in the Incident Monitoring task.
       5. For closed incidents, the incident shall be in read-only mode with the exception of adding links to related incidents.
       6. The Report task shall also report the user activity log of the USP for the time in which the operator was owner of the incident and was monitoring it, in order to provide a view of all actions taken towards the resolution of this incident.
       7. It shall be possible to export all the data included in the details of the incident. The incident export shall at minimum include:
          1. The incident overview: state, owner, description, ID, priority, location, and GPS.
          2. The activity log, including comments, events, and all actions taken by the system or the operator during the resolution of this incident.
          3. Related entities and documents.
          4. Map snapshot. It shall be an option for the operator when exporting.
          5. Camera snapshot at the time of the aggregated events. It shall be an option for the operator when exporting.
          6. Video sequences of the event trigger.
       8. The CDMS shall offer all reports in a visual presentation format (such as pie charts, lines, columns, and rows).
       9. The CDMS shall support the following report formats:
          1. HTML
          2. PDF
          3. XML
       10. Specific privileges shall be required to modify incidents from the report interface.
       11. It shall be possible to generate a report based on the profiles defined for the CDMS.
       12. Incident report retention period capability shall be customizable (from one to 9999 days or indefinitely).
           1. The profile report shall be exportable and printable.
           2. Profile reports shall allow filtering on profile identifier, initiators, recipient, and modification time.
           3. Columns for the profile reports shall be configurable.
       13. The CDMS shall support an option within incident properties to export reports automatically when incidents are closed.
    2. CDMS Dynamic Document Management
       1. The CDMS platform shall provide the ability to dynamically index documents to an incident in order to improve the efficiency of access to information for an operator.
       2. A document shall be automatically attached to an incident if the document properties match the incident properties. The following properties shall be available:
          1. Incident type
          2. Schedule
          3. Location. Location can be an entity or an area.
          4. User or user group of the operator monitoring the incident.
       3. The CDMS shall offer the ability to automatically link a document to a step in a standard operating procedure.
       4. Document Management shall provide a file system to store all documents as well as the document URLs for the use of third-party file systems.
       5. The CDMS shall offer the ability to attach documents during an incident occurrence.
    3. CDMS Rules Engine
       1. The CDMS shall offer an advanced Rules Engine to correlate events and trigger incidents using Boolean rules.
       2. Configuring the Rules Engine shall be graphical without need for a script.
       3. The Rules Engine shall provide the ability to configure a sequence of conditions with AND and OR so that when the sequence is matched, an incident is triggered.
       4. The condition of the Rules Engine shall allow the user to configure:
          1. A list of events from different locations or the same location with an OR operand between them.
          2. Advanced payload filtering shall be possible for selected events.
          3. The number of occurrences of any selected events.
          4. A max lapse of time during which the condition must be validated.
          5. A filter for other events in the system.
       5. It shall be possible to configure a complex sequence of rules by applying the occurrence, the interval, and event filtering.
       6. It shall also be possible to script the rules in advance and import them into the system later.
    4. CDMS Automation Workflow Engine
       1. The CDMS shall provide an Automation Workflow Engine to automate the response to an incident type.
       2. The automation workflow shall be highly scalable and enterprise class, allowing complex business rules to be implemented.
       3. The CDMS shall provide a graphical automation workflow designer. No scripting competence shall be required to implement a workflow.
       4. It shall be possible to define an automation workflow for each incident type. The automation workflow shall be a series of activities that are sequentially executed.
       5. It shall be possible to copy and paste a portion or the entire automation workflow within another automation workflow.
       6. The automation workflow shall support the execution of parallel branches.
       7. The automation workflow shall support conditional activities using IF/ELSE scenarios.
       8. It shall be possible to look at door state (locked, unlocked, secured, unsecured or opened) to enable or disable additional actions.
       9. It shall be possible to reference custom fields of the involved entities to define specific conditional rules.
       10. The Automation Workflow Engine shall provide the following activities:
           1. Acknowledge alarm
           2. Add reminders
           3. Aggregate events
           4. Arm zones
           5. Change display colors
           6. Change incident descriptions
           7. Change incident states
           8. Change incident types
           9. Change priorities
           10. Close incidents
           11. Delay
           12. Forward incidents
           13. Transfer incidents
           14. Disarm zones
           15. Display entities
           16. Dispatch to
           17. Export incidents
           18. Play sounds
           19. PTZ commands
           20. Reset area people count
           21. Run a macro
           22. Send an email
           23. Attach a report to an email
           24. Email incident snapshots taken by video entities at incident location
           25. Set threat level
           26. Trigger alarms
           27. Trigger incidents
           28. Unlock door explicitly
           29. Wait for events
           30. Wait for incident states
           31. Custom activities: build your own activities leveraging the SDK to interact with Security Center and/or external systems
           32. Play an MP3 or WAV file to a Sipelia™ public addressing system.
           33. Triggers output
           34. Enable/Disable state transition
           35. Wait for incident priority
           36. Reboot video or access control unit
           37. Enable/Disable cardholder
           38. Enable/Disable credential
           39. Change additional field value
           40. Set Maintenance mode ON or OFF for specific or incident-related entities
           41. Shunt a reader
           42. Shunt inputs on a door
           43. Shunt inputs
       11. The Automation Workflow Engine shall provide a framework to create custom activities that allow integration into a global business process.
       12. The Automation Workflow shall provide a way to access contextual information for Mail and Macro activities.
    5. CDMS Standard Operating Procedure
       1. The CDMS shall provide guidance for operators in the form of a standard operating procedure (SOP) for the response to an incident type.
       2. The SOP shall be interactive and offer an operator-acknowledgement-audit for each SOP step.
       3. The SOP shall be dynamic and provide the ability to adapt the next steps in a procedure based on the responses to previous steps in the procedure.
       4. The configuration of the dynamic sequence for the SOP shall be visually represented by a flowchart.
       5. The CDMS GUI shall provide the ability to skip a step of the SOP and request a justification for skipping the step.
       6. It shall be possible to configure an SOP to be either sequential, requiring the validation of each step in order to access the next one, or to be left at the discretion of the operator to execute the steps as a check list in a free order.
       7. The SOP shall be configurable so that the validation of all steps in the SOP is required in order to close the incident.
       8. It shall be possible for the SOP steps to be automatically answered by the system when pre-defined validation rules are configured. Validation data could be information from the incident itself, door states or custom fields of the entities that are involved in the incident. When auto validation data is not available, user will get prompted to select appropriate answer.
       9. Each step shall be optionally associated to a document in the form of a URL, or a document in a supported format (such as Word, PDF, or HTML).
       10. The CDMS shall track the elapsed time for each step of the SOP, as well as the total elapsed time from the initial response to resolution.
       11. The CDMS shall provide the capability to import and export the SOP individually as CSV files.
       12. The CDMS shall provide the ability to configure standard options when defining dynamic steps of the SOP.
       13. The CDMS shall provide the ability to configure Dynamic SOP (DSOP) with a decision tree view.
       14. The CDMS shall provide the ability to execute specific actions based on DSOP answers. Answers shall be provided via predefined or custom selections. Selections can be made using a mouse or keyboard shortcuts.
       15. The CDMS shall provide a GUI to configure the DSOP and connect the different steps based on the operator answer. The CDMS shall provide the ability to call a Sipelia™ device when using Sipelia™ integration from the dynamic SOP step.
       16. The CDMS shall provide a GUI to configure how the DSOP will update custom or additional data within the incident. It shall be possible to change a string, update numerical value, or change Boolean information from the user’s response.
       17. A maximum delay shall be allowed for a user to initiate the procedure. Automated actions associated with this time to response threshold shall be configurable.
       18. A maximum delay shall be allowed for a user to complete the procedure. Automated actions associated with this time to resolution threshold shall be configurable.
       19. A minimum time shall be allocated for a user to complete the procedure. Closing the incident before passing this time to resolution threshold shall trigger automated actions.
       20. A visual indicator shall be displayed when maximum time to response or the maximum time to resolution for the incident is exceeded.
       21. The DSOP shall provide flexibility to dynamically change the text and guidance based on the entities that triggered the incidents. This would be accomplished via custom fields that can be updated by the customer.
    6. Electronic Access Control System *(Specifier, select one of the following)*
       1. The Information Management & Presentation shall be unified seamlessly with the Access Control System specified in section 28 13 00 within the USP. All the access control features available in the USP shall be available to the Information Management & Presentation software.
       2. The Information Management & Presentation shall be unified seamlessly with the Access Control System plugins of the USP. All the access control features available in the USP shall be available to the Information Management & Presentation software.
    7. Video Management System *(Specifier, select one of the following)*
       1. The Information Management & Presentation shall be unified seamlessly with the Video Management System specified in section 28 23 00 within the USP. All video management features available in the USP shall be available to the Information Management & Presentation software.
       2. The Information Management & Presentation shall be unified seamlessly with the Video Management System plugins of the USP. All the video management features available in the USP shall be available to the Information Management & Presentation software.
    8. Server Administrator User Interface Requirements
       1. The Server Administrator shall be used to configure the SSM and the Directory Role (main configuration) and its database(s), to apply the license, and more.
       2. The Server Administrator shall be a web-based application. Through the Server Administrator, it shall be possible to access the SSM across the network or locally on the server.
       3. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.
       4. The Server Administrator shall allow the administrator (user) to perform the following functions:
          1. Manage the system license.
          2. Configure the database(s) and database server for the Directory Role.
          3. Activate/Deactivate the Directory Role.
          4. Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.
          5. Define the client-to-server communications security settings.
          6. Configure the network communications hardware, including connection addresses and ports.
    9. Smartphone and Tablet App General Requirements
       1. The USP shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the USP over any Wi-Fi or mobile network connection.
       2. Mobile apps shall communicate with the USP via a Mobile Server Role (MSR). All communication between the mobile apps and the MSR shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       3. Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):
          1. Apple devices running iOS 11 or later
          2. Android devices 6.0 or later
       4. It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play).
       5. It shall be possible to push configuration to the mobile devices through a Mobile Device Management solution such as VMWare Workspace One or Microsoft Intune.
       6. Functionalities
          1. Core

Ability to logon/logoff to the USP using an authorized user profile of the system.

Ability to support passive authentication from a single sign-on provider (Open ID Connect or SAML2 identity provider)

Ability to use biometric features (thumbprint, face ID, etc.) to perform connection to the system.

Ability to change the picture or the password of the user of the mobile app.

Ability to view the current Threat Level of the system.

Ability to change the current Threat Level of the system.

Ability to execute hot actions configured in the user profile.

Ability to view entities from the USP:

Cameras

Doors

ALPR cameras

Web Tile Plugins

Layouts

Camera Sequences

Macros

Maps (geographical maps only) *(Specifier, Professional and Enterprise)*

Intrusion entities integrated with platform

Ability to navigate the system hierarchical view of the entities and search entities in the system.

Ability to access CDMS from CDS and perform the following activities:

View active incidents.

Assign, take, and release incident ownership.

Access incident details.

View assigned incident icons and color-code incident listing.

Trigger manual incidents based on mobile locations or entity’s location.

Launch onscreen guidance during incident response.

Update incident state manually or automatically.

* + - * 1. Video

Ability to view live and recorded video from the cameras of the USP. A maximum of four cameras shall be displayed.

Ability to view video in native format (H.264).

Ability to display live and recorded video side-by-side for a specific camera.

Ability to perform digital zoom on cameras.

Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording.

Ability to view camera layouts.

Ability to view camera sequences.

Ability to run a camera events report.

Ability to change the video quality on the cameras displayed on the mobile app.

Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system.

* + - * 1. Access Control

Ability to view the door state and the door lock state.

Ability to perform actions on a door, such as unlock the door, set the door in maintenance mode, override the door unlocking schedule.

* + - * 1. Automatic License Plate Recognition

Ability to view live events raised by an ALPR camera.

Ability to view the read image, context image, and all metadata captured by the ALPR camera

Ability to run an ALPR event report.

Ability to add a license plate to a hotlist on the system.

* + - * 1. Alarm Management

Ability to receive push notifications to notify mobile operators that an alarm was received.

Ability to view all active alarms assigned to the mobile operator.

Ability to perform action on an alarm such as acknowledge, forward, or alternate-acknowledge an active alarm.

Ability to view entities attached to the alarm.

* + - * 1. Map *(Specifier, Professional and Enterprise)*

Ability to display a geographic map with USP entities geo-located on the map.

Ability to view any entity configured on the map.

Ability to search for entities or locations on the map.

* + - * 1. Incident management

Ability to view active incidents, sort and group them for a customized view.

Ability to trigger incidents manually.

Ability to get all details about an incident including related incidents, entities and documents.

Ability to take ownership of an incident and respond to the defined standard operating procedure geared towards incident resolution.

* + - * 1. Intrusion

Ability to see the list of intrusions defined in the platform.

Ability to see the state of integrated intrusions.

Ability to do the available manual operations of the integrated intrusion system.

Ability to see map images configured in the platform,

* + - 1. It shall be possible to send a message from the client user interface to a mobile operator.
      2. It shall be possible to send a live or playback video sequence from the client UI to a mobile operator.
      3. It shall be possible to view mobile operators who enabled location tracking on a map in the system. The location of the mobile operator should update in real time. *(Specifier, Professional and Enterprise)*
    1. Health Monitor
       1. The USP shall monitor the health of the system, log health-related events, and calculate statistics.
       2. USP services, roles, agents, units, and client apps will trigger health events.
       3. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.
       4. A dedicated role, the Health Monitoring Role, shall perform the following actions:
          1. Monitor the health of the entire system and log events.
          2. Calculate statistics within a specified time frame (hours, days, months).
          3. Calculate availability for clients, servers, and video/access/ALPR units.
       5. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.
       6. A Health Monitoring dashboard task shall be available in the client application user interface to provide a live display, such as pie charts and event lists, for quick visual assessment on the general health of the system.
       7. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.
       8. Detailed system care statistics will be available through a web-based dashboard providing health metrics of USP entities and roles, including Uptime and mean-time-between-failures.
       9. All events raised in the system can be used for automating the UPS event/action management.
       10. Health events shall be accessible via the SDK (can be used to create SNMP traps).
    2. USP General Requirements
       1. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.
       2. The USP shall support the seamless unification of IP access control system (ACS), IP video management system (VMS), and IP automatic license plate recognition system (ALPR) under a single platform. The USP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, and reporting of embedded ACS, VMS, and ALPR systems and associated edge devices.
       3. Functionalities available with the USP shall include:
          1. Configuration of embedded systems, such as ACS, ALPR, and VMS systems.
          2. Live event monitoring.
          3. Live video monitoring and playback of archived video.
          4. Alarm management.
          5. Reporting, including creating custom report templates and incident reports.
          6. The Federation feature for global monitoring, reporting, and alarm management of multiple remote and independent ACS, VMS, and/or ALPR systems spread across multiple facilities and geographic areas*. (Specifier, Enterprise only, additional license required)*
          7. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system. *(Specifier, Enterprise Only, additional license required for each site)*
          8. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts. *(Specifier, Professional and up, first integration included, additional licenses required for more)*
          9. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming). *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
          10. SIP Intercom device integration for bi-directional communication.
          11. Integration with third-party systems and databases via plug-ins (access control, video analytics, point of sale, and more). *(Specifier, Professional and up, additional license required)*
          12. Dynamic graphical map viewing.
          13. Asset management system integration. *(Specifier, Professional and up, additional license required)*
       4. The USP shall be deployed in one or more of the following types of installations:
          1. Unified access, ALPR, video platform, and any combination thereof.
          2. Standalone access control, ALPR, or video platform.
          3. Unified access and video platform that federates multiple remote ACS, VMS, and ALPR.
          4. Standalone video platform that federates multiple independent remote VMS.
          5. Standalone access control that federates multiple independent remote ACS.
          6. Standalone access control that federates multiple independent remote ALPR.
       5. Licensing:
          1. A single central license shall be applied centrally on the configuration server.
          2. There shall be no requirement to apply a license at every server computer or client workstation.
          3. Based on selected options, one or more embedded systems shall be enabled or disabled.
       6. Hardware and Software Requirements:
          1. The USP and embedded systems (video, license plate recognition, and access control) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.
          2. The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.
          3. The USP database server(s) shall be built on Microsoft’s SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.
          4. The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.
          5. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and .NET software framework.
    3. USP Architecture
       1. The USP shall be based on a client/server model. The USP shall consist of a standard Server Software Module (SSM) and Client Software Applications (CSA).
       2. The USP shall be an IP enabled solution. All communication between the SSM and CSA shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.
       3. The SSM shall be a Windows service that can be configured to start when the operating system is booted and run in the background. The SSM shall automatically launch at computer startup, regardless of whether or not a user is logged on the machine.
       4. Users shall be able to deploy the SSM on a single server or across several servers for a distributed architecture. The USP shall not be restricted in the number of SSM deployed.
       5. The USP shall support the concept of The Federation feature whereby multiple independent ACS, VMS, ALPR installations can be merged into a single large virtual system for centralized monitoring, reporting, and alarm management. *(Specifier, Enterprise only, additional license required)*
       6. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.
       7. The USP shall support up to one thousand instances of CSA connected at the same time. However, an unrestricted number of CSA can be installed at any time. *(Specifier, Maximum 5 with Standard; Maximum 10 with Professional; Unrestricted with Enterprise)*
       8. The USP shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.
       9. The USP shall support uninterrupted video streaming. The CSA shall keep existing video connections active in the event that an SSM (except Archiver) becomes unavailable.
       10. Roles-Based Architecture:
           1. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.
           2. Each role shall execute a specific set of tasks related to either core system, automatic license plate recognition (ALPR), video (VMS), or access control (ACS) functionalities, among many others. Installation shall be streamlined through the ability of the USP to allow administrators to:

Deploy one or several SSM across the network prior to activating roles.

Activate and deactivate roles as needed on each and every SSM.

Centralize role configuration and management.

Support remote configuration.

Move roles over from one SSM to another.

* + - * 1. Each role, where needed, shall have its own database to store events and role-specific configuration information.
        2. Roles without databases, such as The Federation feature, Active Directory, and Global Cardholder Management, shall support near real-time standby without any third-party failover software being required.
        3. Directory Role:

The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.

The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.

The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:

Security Partitions, users and user groups

Areas

Zones, input/output (IO) linking rules, and custom output behavior

Alarms. Schedules, and scheduled tasks

Custom events

Macros or custom scripts

The Directory Role shall support the configuration/management of the following components specific to VMS:

Video servers and their peripherals (for example audio, IOs, and serial ports)

PTZ

Camera sequences

Recording and archiving schedules

The Directory Role shall support the configuration/management of the following components specific to ACS:

Door controllers, and input and output (IO) modules

Doors, Elevators, and Access rules

Cardholders and cardholder groups, credentials, and badge templates

The Directory Role shall support the configuration/management of the following components specific to ALPR:

ALPR units and cameras

Hotlists, permit lists, and overtime rules

* + - * 1. The Video Archiver Role shall be responsible for managing cameras and encoders under its control and archiving.
        2. The Media Router Role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).
        3. The Access Manager Role shall be responsible for synchronizing access control hardware units under its control, such as door controllers and I/O modules. This role shall also be responsible for validating and logging all access activities and events when the door controllers and I/O modules are online.
        4. The Automatic License Plate Recognition (ALPR) Role shall be responsible for synchronizing fixed ALPR units (cameras) and mobile ALPR applications under its control. The ALPR Role shall also be responsible for logging all ALPR activities and events.
        5. The Zone Manager Role shall be responsible for managing all software zones (collection of inputs) and logging associated zone events. Zones shall consist of inputs from both access control and video devices.
        6. The Health Monitoring Role shall be responsible for monitoring and logging health events and warnings from the various client applications, roles, and services that are part of the USP. This role shall also be responsible for logging events within the Windows Event Log and for generating reports on health statistics and health history.
        7. Optional Roles

The Federation Role shall be responsible for creating a large virtual system consisting of hundreds or thousands of independent and remote ACS, VMS, and/or ALPR systems. *(Specifier, Enterprise only, additional license required)*

The Global Cardholder Synchronizer Role shall be responsible for synchronizing cardholder and credential data between the local site and a central site. Synchronization between remote sites shall also be supported. *(Specifier, Enterprise only, additional license required)*

The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server. *(Specifier, Professional and up, additional license required)*

The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database. *(Specifier, first connection included, additional licenses required for more)*

The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports. *(Specifier, Professional and up, additional license required)*

The Plug-in Manager Role shall be responsible for the communication between the USP and third-party systems such as video analytics, ALPR, access control, video, and building management systems. *(Specifier, Professional and up, additional license required)*

The Point of Sale (POS) Manager Role shall be responsible for integrating the USP with third party POS systems and for logging transactions. *(Specifier, Professional and up, additional license required)*

The Web SDK Role shall be responsible for connecting the USP to any application or interface developed with the Web Service SDK. Applications developed with the Web Service SDK shall be platform independent and rely on the REST protocol for communications. *(Specifier, Professional and up, additional license required)*

The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

The Video Redirector Role shall be responsible for connecting any video stream to a third-party system using standard RTSP protocol. This role shall provide access to live video. *(Specifier, Professional and up, requires the SDK packages, additional license required)*

* + - 1. Server Monitoring Service (Watchdog):
         1. The USP shall include a Server Monitoring Service that continuously monitors the state of the Server Software Module (SSM) service.
         2. The Server Monitoring Service shall be a Windows service that automatically launches at system startup, regardless of whether or not a user is logged into his account.
         3. The Server Monitoring Service shall be installed on all PCs/servers running an SSM. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the PC/server should it be unable to restart the service.
    1. USP Access Control, Video, and ALPR Unification
       1. The Monitoring UI shall present a true Unified Security Interface for live monitoring and reporting of the ACS, VMS, and ALPR. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.
       2. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.
       3. The user shall be able to associate one or more video cameras to the following entity types: areas, doors, elevators, zones, alarms, intrusion panels, ALPR cameras, and more.
       4. It shall be possible to view video associated to access control events when viewing a report.
       5. It shall be possible to view video associated to intrusion panel events when viewing a report.
       6. It shall be possible to view video associated to ALPR events when viewing a report.
       7. The USP shall support the following Alarm Management functionality:
          1. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.
          2. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.
          3. Set the priority level of an alarm and its reactivation threshold.
          4. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
          5. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
          6. Provide the ability to group alarms by source and by type.
          7. Define the time period after which the alarm is automatically acknowledged.
          8. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.
          9. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
          10. Define whether to display the source of the alarm, one or more entities, or an HTML page.
          11. Specify whether an incident report is mandatory during acknowledgment.
       8. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.
       9. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, VMS, and ALPR systems.
       10. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.
       11. The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.
       12. Alarm unpacking and packing shall be supported where all the entities associated to an alarm can be display in the Monitoring UI with the single click of a button.
       13. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.
       14. The user shall be able to spontaneously trigger alarms based on something he or she sees in the system.
       15. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.
       16. The user shall be able to investigate an alarm without acknowledging it.
    2. USP Threat Levels *(Specifier, Professional and Enterprise)*
       1. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.
       2. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.
       3. Threat Levels shall be set on an area or on the entire system.
       4. Threat Levels shall affect the system behavior by executing any action available in the USP such as: trigger output, start recording, block camera, override recording quality, arm zone, set a door in maintenance mode, and more.
       5. The following specific actions shall be available with Threat Level:
          1. Set minimum security clearance to restrict or permit access to cardholders on specific areas on top of the restrictions imposed by the access rules.
          2. Set minimum user level to automatically log out user from the USP.
          3. Set reader mode to change how the doors are accessed (for example card and PIN, or card or PIN).
       6. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.
    3. USP Remote Task
       1. The USP shall provide, through a Remote Task, capabilities to remotely monitor and control the content of other workstations running the CSA (Monitoring UI) that are part of the same system.
       2. The USP shall support video wall applications by connecting and controlling multiple workstations and monitors simultaneously.
       3. The Remote Task shall be a graphical interface showing a replication of the remote workstation running the CSA (Monitoring UI).
       4. The Remote Task shall allow the connection to other workstations using a low bandwidth mode to receive only snapshots of video viewed remotely.
       5. The Remote Task shall allow the connection to other workstations using a spy mode to remain invisible to the remotely connected workstation. The spy mode option should be available to users with permission to access the feature.
       6. The functionality provided by the remote monitoring and control capability shall include:
          1. Remote monitoring and control of the monitoring and alarm monitoring tasks.
          2. Ability to remotely switch cameras, doors and zones into display tiles.
          3. Ability to remotely control live and playback video.
          4. Ability to remotely change the tile pattern.
          5. Ability to remotely create and delete tasks.
          6. Ability to remotely start/stop task cycling.
          7. Ability to remotely go into full screen mode.
          8. Ability to remotely save and reload the workspace.
    4. USP Advanced Task Management
       1. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day to day activities, and reporting.
       2. Administrators shall be able to assign tasks and lock the operator`s workspace. The user management of their workspace shall be limited by their assigned privileges.
       3. Operators shall be able save their tasks as either Public Tasks or Private Tasks and in a specific partition. Public tasks shall be available to all users. Private tasks shall only be available to the owner of the task.
       4. Operators shall be able to share their tasks by sending them to one or more online users. Recipients shall have the option to accept the sent task.
       5. Operators shall be able to duplicate a task.
    5. USP Reporting
       1. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.
       2. Each and every report in the system shall be a USP task, each associated with its own privilege. A user shall have access to a specific report task if they have the appropriate privilege.
       3. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.
       4. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.
       5. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.
       6. The USP shall support the following types of reports:
          1. Alarm reports
          2. Video-specific reports (archive, bookmark, motion, and more)
          3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)
          4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more)
          5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more)
          6. Health activity and health statistics reports
          7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports
       7. Generic Reports, Custom Reports, and Report Templates
          1. The user shall have the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.
          2. The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).
          3. All report templates shall be created within the Monitoring UI.
          4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
          5. An unrestricted number of custom reports and templates shall be supported.
       8. A reporting task layout shall consist of panes with settings (report length, filters, go and reset commands, etc.), the actual report data in column format, and a pane with display tiles. The user shall be able to drag and drop individual records in a report onto one or more display tiles to view a cardholder’s picture ID, playback a video sequence, or an ALPR event.
       9. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.
       10. The reporting task shall have the ability to display results through graphics such as line charts, bar charts, stacked bar charts, doughnut charts, and pie charts.
       11. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.
       12. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, export the graphics chart in JPG/PNG, and automatically email a report based on a schedule and a list of one or more recipients.
       13. Shall allow the ability to insert a custom logo when generating reports.
    6. USP Dashboards
       1. The USP shall support the ability to create dashboards.
       2. Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modifications to dashboards should also be allowed to users granted the appropriate privilege.
       3. Dashboards in the system shall be a USP task. A user shall have access to a specific dashboard task if they have the appropriate privilege.
       4. Dashboards shall be saved either in a private folder or a public folder.
       5. A dashboard shall consist of a canvas with various widgets displayed on the canvas. All widgets should offer the ability to specify location and size to the widget, a title to the widget, a background color to the widget, and the ability to refresh periodically the content of the widget.
       6. Dashboard widget types shall be:
          1. Image: provides the ability to display an image (JPG, PNG, GIF, BMP) on a dashboard.
          2. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, color, and alignment can be specified by the user.
          3. Tile: provides the ability to display any entity of the USP inside of a tile.
          4. Web page: provides the ability to display a URL on a dashboard.
          5. Entity Count: provides the ability to display the total number of a specific entity type in the USP.
          6. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.
          7. Map: provides the ability to display and interact with maps on a dashboard.
       7. It shall be possible to extend the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.
       8. The USP shall support the following actions on a dashboard: print dashboard; export dashboard to PNG file; automatically email a report based on a schedule and a list of one or more recipients.
    7. USP Federation feature: Monitoring of Remote Systems *(Specifier, Enterprise only, additional license required for each federated sites and entities)*
       1. The USP shall support the concept of a Federation feature for access control, video, and ALPR.
       2. The Federation feature shall allow multiple independent USP systems (Federated systems) to be unified into a larger virtual system (the Federation feature). This shall facilitate the global monitoring of multiple independent USP systems.
       3. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.
       4. Entities that shall be federated and monitored centrally from the Federation feature shall include alarms, areas, cameras, cardholders and cardholder groups, credentials, doors, elevators, ALPR events, and zones (monitored inputs).
       5. The Federation feature shall support a cloud-based deployment, whereby the service and infrastructure will be updated automatically and provisioned by the service provider, without need for on-site hardware.
       6. The Federation feature shall support Global Alarm Management from the Monitoring UI for access control, video, and ALPR.
       7. The Federation feature shall support Global Report Generation from the Monitoring UI for access control, video, and ALPR.
       8. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (for example, generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).
    8. USP Zone Management
       1. The USP shall support the configuration and management of zones for input point monitoring via the Zone Manager Role. A user shall be able to add, delete, or modify a zone if they have the appropriate privileges.
       2. A zone shall monitor the status of one or more inputs points. Zone monitoring or input point monitoring shall be possible through the use of a controller and one or more input modules. Inputs from video cameras or video encoders shall also be accessible via a zone.
       3. Depending on the hardware installed, supervised inputs shall be supported. Depending on the input module used, both 3-state and 4-state supervision shall be available.
       4. A schedule shall be defined for a zone, indicating when the zone will be monitored.
       5. Custom Events shall provide full flexibility in creating custom events tailored to a zone. Users shall be able to associate custom events to state changes in monitored inputs.
       6. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.
       7. Input/Output (IO) Linking:
          1. Zone management shall support Input/Output (IO) Linking. I/O Linking shall allow one or more inputs to trigger one or more outputs.
          2. IO Linking shall be available in offline mode when communication between the server and hardware is not available.
          3. Custom Output Behaviors shall provide full flexibility in creating a variety of complex output signal patterns: simple pulses, periodic pulses, variable duty-cycle pulses, and state changes.
          4. Through the “trigger an output” action, the ACS shall support the triggering of outputs with custom output behaviors.
    9. USP User and User Group Security, Partitions, and Privileges Management
       1. The USP shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if they have the appropriate privileges.
       2. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:
          1. ADFS (Active Directory Federation Services)
          2. Azure Active Directory (through OpenID Connect)
          3. Ping Identity (through OpenID Connect)
          4. KeyCloak (through OpenID Connect)
          5. Other Open ID Connect / SAML2 authentication agents
       3. Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups. User group nesting shall be allowed.
       4. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR shall have associated privileges.
       5. Specific entities, such as cardholders, cardholder groups, and credentials shall include a more granular set of privileges, such as the right to access custom fields and change the activation or profile status of an entity.
       6. Partitions:
          1. The USP shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a system into multiple security partitions.
          2. All entities that are part of the USP can be assigned to one or more partitions.
          3. A user who is given access to a specific partition shall only be able to view entities (components) within the partition to which they have been assigned. Access is given by assigning the user as an accepted user to view the entities that are members of a particular partition.
          4. A user or user group can be assigned administrator rights over the partition.
       7. It shall be possible to specify user and user group privileges on a per partition basis.
       8. Advanced logon options shall be available such as dual logon and more.
       9. It shall be possible to specify an inactive period for the Monitoring UI after which time the application shall automatically lock, while still preserving access to currently displayed camera feeds. It shall also be possible to log the user out immediately after the inactivity period or within an amount of time from when the application was locked.
       10. It shall be possible to review user permissions and determine:
           1. For any entity in the system, which user group or user can view or modify it.
           2. For any user group or user in the system, what are its privileges.
           3. For any privilege in the system, which user group or user is allowed to perform the underlying action.
    10. USP Event/Action Management
        1. The USP shall support the configuration and management of events for video and ALPR. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.
        2. The USP shall receive all incoming events from one or more ACS, VMS, and ALPR. The USP shall take the appropriate actions based on user-defined event/action relationships.
        3. The USP shall receive and log the following events:
           1. System-wide events
           2. Application events (clients and servers)
           3. Area, camera, door, elevator, and ALPR events (reads and hits)
           4. Unit events
           5. Zone events
           6. Alarm events
           7. ALPR events
           8. Health Monitoring events
        4. The USP shall allow the creation of custom events.
        5. The USP shall have the capability to execute an action in response to an access control, video, and ALPR event. The USP shall support the following list of actions, without being limited to:
           1. Add bookmark
           2. Block and unblock video
           3. Display a camera on an analog monitor
           4. Display an entity in the CSA
           5. Email a report
           6. Email a snapshot
           7. Export report
           8. Go home
           9. Go to preset
           10. Override recording quality
           11. Play a sound
           12. Reboot unit
           13. Run a macro
           14. Run a pattern
           15. Send a message
           16. Send an email
           17. Set threat level
           18. Start/Stop applying video protection
           19. Start/Stop recording
           20. Start/Stop transfer
           21. Trigger alarm
           22. Trigger output
           23. Set maintenance mode
           24. Trigger incident
           25. Set interface background color
           26. Set minimum security clearance
        6. The USP shall allow a schedule to be associated with an action. The action shall be executed only if it is an appropriate action for the current time period.
    11. USP Schedules and Scheduled Tasks
        1. Schedules
           1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if they have the appropriate privileges.
           2. The USP shall provide full flexibility and granularity in creating a schedule. The user shall be able to define a schedule in 1-minute or 15-minute increments.
           3. Daily, weekly, ordinal, and specific schedules shall be supported.
        2. Scheduled Tasks
           1. The USP shall support scheduled tasks for video, and ALPR.
           2. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.
           3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email or emailing a report.
    12. USP Macros and Custom Scripts
        1. The USP shall enable users to automate and extend the functionalities of the system through the use of macros or custom scripts for access control, video, and ALPR.
        2. Custom macros shall be created with the USP Software Development Kit (SDK).
        3. A macro shall be executed either automatically or manually.
        4. In the Monitoring UI, a macro shall be launched through hot actions.
    13. USP Dynamic Graphical Maps (DGM)
        1. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.
        2. The USP shall provide a map centric interface with the ability to command and control all the USP capabilities from a full screen map interface.
        3. It shall be possible to span the map over all screens of the USP client station. In the scenario where the map is spanned over all the screens of the USP client station it shall be possible to navigate the map including pan and zoom, and the map’s moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same command and control capabilities than in a single screen display.
        4. The DGM shall support the following file format and protocol for importing map background:
           1. PDF
           2. JPG
           3. PNG
           4. Web Map Tile Service (WMTS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
           5. BeNomad
           6. AutoCAD (DWG & DXF)
        5. The DGM shall provide the following online map providers for use as map background and provide the ability to manage their service license if they require one:
           1. Google Map, aerial, terrain (Licensed)
           2. Bing Map, aerial, satellite, hybrid (Licensed)
           3. ESRI ArcGIS (Licensed)
           4. OpenStreet Map aerial (Licensed)
           5. OVI hybrid
        6. It shall be possible to configure a mixed set of maps made of GIS, online providers, and private imported files and link them together.
        7. The DGM shall provide the ability to display all native entities of the USP including:
           1. Cameras, fix, and PTZ
           2. Doors
           3. Camera sequences
           4. Areas
           5. Intrusion areas
           6. Intrusion zones
           7. License Plate Recognition cameras
           8. Digital inputs
           9. Digital outputs
           10. Intercoms
           11. Alarms
           12. Macros
           13. Police Car Patrollers
        8. The DGM shall provide the ability to draw and display information over the map in the form of:
           1. Vectoral shapes: line, rectangles, polygons, ellipse
           2. Pictures
           3. Text
        9. The DGM shall provide the ability to display any type of third-party entities integrated through an SDK.
        10. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.
        11. The DGM shall provide the ability to the operator to manage layers of entities displayed over the map, being able to turn them on and off and changing the superposition order.
        12. The DGM shall provide the ability to import data layers from one or more ESRI ArcGIS servers.
        13. The DGM shall provide the operators with the ability to manage layers that are imported from ESRI ArcGIS. The operators shall be able to turn the layers on and off, as well as sort the layer.
        14. The DGM shall offer built-in map data backup and restore for both map background and layers of entities.
        15. The DGM shall provide the ability to import configurations from an external file such as:
            1. AutoCAD layer for objects
            2. CSV, Excel file
        16. The DGM shall provide the ability to print a map in the following file formats:
            1. PDF
            2. PNG
        17. The DGM shall offer failover capabilities.
        18. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.
        19. The DGM shall provide a means to update a map background without affecting the map object configuration.
        20. The DGM shall offer a user-friendly graphical map designer to configure the maps.
        21. The DGM shall provide a user friendly and intuitive navigation that includes:
            1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
            2. The ability to define favorites for recurrent position recall.
            3. The possibility to create links between maps. The map links shall allow the link from one map to multiple maps representing the floors of a building. Navigating between floor of a building shall keep the zoom level of the map.
            4. A common user experience regarding navigation into the map for both GIS and private maps. *(Specifier, Professional or Enterprise required for GIS)*
        22. It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.
        23. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.
        24. The DGM shall offer a smart selection tool to access the video. By clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take into consideration the obstacle and not display cameras that cannot see the location because of a wall.
        25. It shall be possible to select a location by drawing a zone of interest on the DGM and display all the entities that are part of that zone of interest at once.
        26. The user shall be able to select and display the content of multiple USP entities on the map in popup windows.
        27. The user shall be able to move, resize, and pin the USP entity pop-up windows to the map.
        28. It shall be possible to access live and playback video from the map.
        29. It shall be possible to monitor from the DGM all entities event notification. User shall be able to turn on and off the notification per entity.
        30. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:
            1. Center the map on entities related to the alarm.
            2. Visualize the Alarms notification on the map and access the related video from the map.
            3. Trigger and receive alarms.
            4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
            5. Visualize that an alarm occurred in an underlying linked map.
        31. The DGM shall provide the following search capabilities:
            1. Search and center by entity name.
            2. From the Display of an entity in the USP, locate the entity on the map and offer the ability to select another one close-by.
            3. By street address, city, landmark, point of interest (using geocoder license from Google, ESRI, or other provider).
        32. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.
        33. The DGM shall support the use of GIS maps, private maps, or a combination of both or map background. *(Specifier, Professional or Enterprise required for GIS)*
        34. The DGM shall be compatible with any GIS compliant maps with the OGC and supporting WMTS and WMS. This includes, but is not limited to, ESRI maps. The DGM shall allow the selection of the appropriate GIS layers. *(Specifier, Professional or Enterprise required for GIS)*
        35. The DGM shall provide an intuitive build-in map designer for entity positioning on the map using drag and drop. Any configuration shall be graphic.
        36. It shall be possible to edit and configure multiple map objects at once.
        37. All map design modifications shall be logged in an audit trail.
        38. Various actions shall be available within maps for execution through simple and intuitive double-click, right-click, or drag-and-drop functionality. Examples of actions available through maps shall include unlocking a door and acknowledging an alarm.
        39. Through the following functionalities, the DGM shall allow the management of USP alarms for the map:
            1. Locate on the map entities related to the alarm.
            2. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.
            3. List, select, and locate alarms.
            4. Auto center the map on the highest priority alarm.
            5. Handle the alarm from the map, including acknowledgement, forwarding, and investigation.
            6. All map containers, such as hotspots or map links, shall reflect the alarm status of the contained entities.
        40. It shall be possible to add advanced functionality to map objects using the SDK. Any functionality available through the USP SDK shall be available within maps.
        41. The DGM shall offer lasso tools for:
            1. Displaying entities at one location through a single action.
            2. Triggering an action on all entities at one location in a single click.
            3. Editing multiple entities at one location simultaneously.
        42. The DGM shall allow the display of USP entities selected from the map on a remote monitor (video wall).
        43. The DGM shall provide the ability to search within the map by entity name.
        44. The DGM shall allow the use of KML overlay map information for both GIS and private maps. Moveable objects shall be supported using KML.   
            *(Specifier, Professional and Enterprise)*
        45. The Contractor shall provide licenses for each entity that is required to be shown on the graphical maps.
    14. USP Audit and User Activity Trails (Logs)
        1. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.
        2. Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.
        3. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.
        4. The USP shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the USP such as login, camera viewed, ALPR event viewed, badge printing, video export, and more.
        5. The ACS shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.
    15. USP Incident Reports
        1. Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and access control-related incident reports shall be supported.
        2. The operator shall be able to create standalone incident reports or incident reports tied to alarms.
        3. The operator shall be able to link multiple video sequences to an incident, access them in an incident report, and change the date or time of the sequences later on.
        4. It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.
        5. Incident reports shall allow the creation of a custom form on which to input information on an incident.
        6. Incident reports shall allow entities, events, and alarms to be added to support at the report’s conclusions.
    16. USP Data Ingestion
        1. The USP shall allow the possibility to import external data from outside sources to enhance unification of data sources within the USP.
        2. Each data source shall be defined by a set of fields and field types that describe the data source. Field types shall be:
           1. String
           2. 32-bit & 64-bit integer
           3. Floating point number
           4. Boolean
           5. Timestamp
           6. Binary (in a file or base 64)
        3. The visualization of each data point from a data source shall be configurable to determine what fields from the data should be displayed. The configuration of each field should be:
           1. Which fields are displayed or hidden
           2. What order are the fields displayed
           3. A label to specify the name of the field (to have a key:value format)
           4. An option to specify how to display the field (text value, image, clipboard value, hyperlink to a web page, hyperlink to an entity in the system, sound file)
        4. A privilege should be available for each data source to allow / deny access to specific users and user groups of the USP.
        5. Ingested data shall be available in the USP reporting system.
        6. Ingested data shall be available to display in the USP Dashboards.
    17. USP Third Party Integration
        1. Microsoft Active Directory Integration *(Specifier, first integration included, additional licenses required for more)*
           1. The USP shall support a direct connection to one or multiple Microsoft Active Directory server via the Active Directory Role(s). Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.
           2. Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups.
           3. The USP shall be able to connect to and synchronize data from multiple Active Directory servers (up to 10).
           4. The USP shall support synchronizing Active Directory Universal Groups as well as security groups belonging to other domains within the same forest.
           5. The USP shall support Microsoft Active Directory encryption using LDAP SSL.
           6. When enabled, Active Directory shall manage user logon to the USP client applications through the user’s Windows credentials. Logging to the USP shall utilize native Active Directory password management and authentication features.
           7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:

Users (username, first and last names, email address, and more).

User groups (user group name, description, and group email address).

Active Directory attributes to USP custom fields.

* + - * 1. When enabled, the addition, removal, or suspension of a user’s Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent user account in the USP.
        2. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include on first logon (users only), manual synchronization, and scheduled synchronization.
        3. The USP shall support user connections across independent organizations by connecting to an external identity provider using claims-based authentication such as ADFS (Active Directory Federation Services), Azure Active Directory, other OpenID Connect & SAML2 providers.
      1. Intrusion Detection Integration *(Specifier, Standard, Professional and up, additional license required - for an extended list, refer to the Supported Plugins in Security Center document)*
         1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
         2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):

Arm and disarm intrusion devices (manually, on schedule, or following a USP event).

Activate or trigger intrusion device outputs.

View intrusion events and alarms.

Monitor the status, including arming status, of the intrusion devices.

Video verification of intrusion events and alarms with video panels.

Create USP zones using intrusion device inputs.

* + - * 1. Currently supported intrusion panels include:

Bosch Legacy G Series panels

Bosch B & G Series panels

Bosch Map 5000

DSC Power Series panels

DMP XR Series panels

Honeywell Galaxy Dimension and Flex panels

Vanderbilt SPC

UTC Advisor Master and Advanced

Satel INTEGRA panels

Telenot Complex 400H panels

* + - * 1. Additional Intrusion devices supported include:

Buytime

Alarm Panel Receiver

Southwest Microwave RPMII

* + - 1. Third Party Access Control Systems *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network and should not support administrative tasks such as cardholder management.
         2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

Synchronize access control entities and receive associated events and states within the USP, including:

Cardholders

Visitors

Readers and doors

Alarms

Inputs and outputs

Monitor access control events.

Monitor and Acknowledge access control alarms.

Trigger actions and outputs in the access control software using hot actions and event-to-actions.

Lock and unlock doors in the access control software.

Video verification of access control events and alarms.

Configure event-to-actions using the access control events and alarms.

Generate Security Center reports using from the in the access control data.

View and monitor states of door entities in the USP maps.

* + - * 1. Currently supported access control manufacturers include:

Tyco Softwarehouse CCURE

UTC Lenel Onguard

Amag Symmetry

Siemens Sipass

AssaAbloy ARX

* + - 1. Third Party Destination Dispatch Systems: *(Specifier, Professional and up, additional license required, for extended list please refer to the Security Center supported Plugins guide)*
         1. The USP shall integrate with third-party destination dispatch (elevator control) software via the SDK. Communications with the destination dispatch software shall be over an IP network.
         2. Integration with destination dispatch software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
         3. Functionality available via the integration of destination dispatch software with the USP shall include the following (where supported by the destination dispatch solution):

Destination dispatch entity creation and reception of associated events and states within the USP, including:

Floors and landings

Elevator cars (front/rear doors) and kiosks

Cardholders and credentials (if applicable)

Monitor destination dispatch events.

Trigger manual dispatch actions.

Video verification of destination dispatch events.

Configure event-to-actions using the destination dispatch events.

Generate Security Center reports using the destination dispatch data.

Support multiple readers:

Kiosk internal readers

USP readers

Kiosk advanced modes and passenger types.

* + - * 1. Currently supported destination dispatch manufacturers include:

Otis Compass

Thyssenkrupp

MCE

KONE

* + - 1. Asset Management Integration *(Specifier, Professional and up, additional license required)*
         1. The USP shall integrate with third party asset management systems via the Asset Management Role.
         2. Communications with asset management solutions shall be over an IP network (via software communications).
         3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):

Synchronize asset management system assets with USP asset entities.

Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

Synchronization of asset management alarms with Security Center alarms.

Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

Real-time tracking of asset locations on a per area basis.

Asset Management Inventory reporting task that details the current location (area) of an asset.

Asset Activity reporting task that provides a historical review of asset-related events and activity.

* + - * 1. Currently supported asset management systems include:

Deister Key management

Morsewatchmans

TRAKA

Key Systems

* + - 1. Additional Third-Party Integrations
         1. The USP shall support multiple approaches to integrating third party systems. These shall include: Software Development Kits (SDKs), REST-based Web Service SDKs, RTSP Service SDKs, and more. *(Specifier, Professional and up, SDK package and license required)*
         2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as: *(Specifier, refer to the website for how these are licensed, for an updated list of available third-party integration, please refer to the supported plugin guide)*

Video analytics

Third party video systems

Third party access control systems

ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors

Building management systems

Access Control ecosystem (such as ID scanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)

Transaction monitoring (POS, Barcode scanning, ATM)

Industrial IoT: Data ingestion from external devices through standard communication protocols (Modbus, BACnet, OPC, SNMP, HTTP Server, MQTT Client, TCP Server)

Industrial Protocol Interface: Data exposure from GSC to external protocol interfaces using standard communication protocols (BACnet, SNMP)

Videowall (Barco, Eizo)

Human resource management systems (HRMS)

Autonomous Drone Integration

Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))

Gunshot Detection (Shot Spotter, Guardian GunShot)

Dynamic Logbook: Customizable forms with reporting capabilities

* + 1. USP Software Development Kit (SDK)
       1. A USP SDK shall be available to support custom development for the platform.
       2. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.
       3. Integration with external applications and databases shall be possible with the SDK.
       4. The SDK shall enable end-users to develop new functionality (user interface, standalone applications or services) to link the USP to third party business systems and applications, such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.
       5. The SDK shall be based on the .NET framework.
       6. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.
       7. The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
       8. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.
       9. The SDK shall provide an extensive list of programming functions to view and configure most ACS entities such as: cardholders, cardholder groups, visitors, credentials, access rules (modify only), and custom fields.
       10. The SDK shall be able to receive real time events from the following USP entities: users and user groups, areas, zones, cameras, video units, doors, door controllers (units), elevators, cardholders, cardholder groups, and credentials.
       11. The SDK shall be able to query the history of events for areas, cameras, zones, alarms, cardholders, credentials, visitors, doors, query license plate read events, license plate hit events, generate a license plate hits report, generate a license plate reads report.
       12. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.
  1. **Execution**
     1. Warranty
        1. The product shall perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use. Software defects are covered through Service Releases and Cumulative Updates which are available for a period of 1 year from the date of the software purchase.
        2. Extended warranty, up to 5 years, shall be available through the purchase of a software maintenance agreement (SMA) which includes the following additional services over the standard warranty:
           1. Access to phone support and online chat for technical assistance.
           2. Online case management.
           3. Online system availability monitor.
           4. Access to Major and Minor Release Upgrades.
           5. 24/7 pager support and dedicated support specialist. *(Specifier, additional cost)*
     2. Deployment Services and System Commissioning *(Specifier, this is a per day charge plus travel, consult Genetec Inc. on number of recommended days to specify)* 
        1. General Requirements
           1. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:

Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

Complex enterprise installations involving advanced functionality (for example The Federation feature, failover, plugins) and/or multiple systems (for example access control, video, ALPR) and/or third-party integrations.

Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

* + - * 1. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.
      1. Deployment Management Service
         1. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization and who will be responsible for:

Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

Providing a project plan for the deployment of the vendor's USP.

Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

* + - 1. Solution Architect Service
         1. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:

Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews as well as performance reviews of the vendor’s USP.

Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.

Providing upgrade and migration strategy for the vendor’s USP where applicable.

Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

* + - 1. System Configuration and Commissioning Service
         1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

Assisting the contractor’s or subcontractor’s onsite/remote technicians with the configuration and commissioning of the vendor’s USP at the client site.

Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.

Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

* + 1. Manufacturer End User Operator Training *(Specifier, this is a per half-day charge plus expenses)*
       1. The contractor shall engage the services of the USP vendor to assist in the end user training of the USP at the end-user site.

**End of Section**