T33238

VIEŠOJO PIRKIMO – PARDAVIMO SUTARTIS

Pirkimo pavadinimas:

Patekimo kontrolės sistemos pirkimas

Prekių viešojo pirkimo-pardavimo sutartis Nr.

Prekių pirkimo-pardavimo sutarties Specialiosios sąlygos

1. straipsnis. Sutarties šalys

1.1. **Pirkėjas:**

1.1.1. Pavadinimas: VĮ Ignalinos atominė elektrinė
1.1.2. Juridinio asmens kodas: 255450080
1.1.3. Adresas: Elektrinės g. 4, K47, Drūkšinių k., LT-31152, Visagino sav.
1.1.4. PVM mokėtojo kodas: LT554500811
1.1.5. Atsiskaitomoji sąskaita: LT10 7300 0100 0261 4996
1.1.6. Bankas, banko kodas: AB "Swedbank", banko kodas 73000, SWIFT kodas: HABALT22XXX
1.1.7. Telefonas: +370 386 28985
1.1.8. El. paštas: iae@iae.lt
1.1.9. Šalies atstovas:
1.1.10. Atstovavimo pagrindas: Valstybės įmonės Ignalinos atominės elektrinės generalinio direktoriaus 2025-01-17 įgaliojimas Nr. ĮmIg-8(1.204E)

Toliau – pirkėjas

ir

1.2. **Tiekėjas:**

1.2.1. Pavadinimas: UAB „Spectra Baltic“
1.2.2. Juridinio asmens kodas: 304635904
1.2.3. Adresas: Baltų pr. 145, LT-47125 Kaunas
1.2.4. PVM mokėtojo kodas: LT100012460119
1.2.5. Atsiskaitomoji sąskaita:
1.2.6. Bankas, banko kodas: AB SEB Bankas
1.2.7. Telefonas: +37037331620
1.2.8. El. paštas: info@spectrabaltic.lt
1.2.9. Šalies atstovas:
1.2.10. Atstovavimo pagrindas: Įmonės įstatai.

Toliau – tiekėjas

sudarė šią prekių viešojo pirkimo-pardavimo sutartį (toliau – Sutartis).

2. straipsnis. Atsakingi asmenys

2.1. Pirkėjo kontaktiniai asmenys, atsakingi už Sutarties vykdymą, sąskaitų per sąskaitų administravimo bendrąją informacinę sistemą SABIS priėmimą:

2.2. Tiekėjo kontaktiniai asmenys, atsakingi už Sutarties vykdymą:

3. straipsnis. Sutarties dalykas

3.1. Sutarties dalykas: Tiekėjas įsipareigoja Sutartyje numatytomis sąlygomis perduoti pirkėjui Sutarties specialiųjų sąlygų 5 straipsnyje nurodytas prekes, įskaitant prekių pristatymą, montavimą, paleidimą, derinimą, personalo apmokymą (toliau vadinama – prekės). Išsamus sutarties dalyko aprašymas ir kiti reikalavimai nustatyti Sutarties priede Nr. 1 pateiktoje techninėje specifikacijoje ir jos paaiškinimuose (toliau – Techninė specifikacija) bei Sutarties priede Nr. 2 pateiktame tiekėjo pasiūlyme ir jo paaiškinimuose.

3.2. Pirkimo pavadinimas ir numeris: Patekimo kontrolės sistemos pirkimas, Nr. 1984530.

3.3. Informacija apie Europos Sąjungos lėšomis finansuojamą projektą arba kitą projektą: netaikoma.

4. straipsnis. Pristatymo terminai ir perdavimo-priėmimo tvarka

4.1. Prekių pristatymo terminas: Tiekėjas pagal atskirą užsakymą įsipareigoja pristatyti Prekes ne vėliau kaip per Techninės specifikacijos 6 p. numatytus terminus.

Prekės turi būti pristatomos šiuo adresu: Visos prekės turi būti pristatytos ir kitos susijusios paslaugos suteiktos VĮ Ignalinos atominės elektrinės pagrindinėje aikštelėje, Panaudoto branduolinio kuro saugyklos aikštelėje ir Laikinosios panaudoto branduolinio kuro saugyklos aikštelėje Drūkšinių k., 31152 Visagino sav.

4.2. Prekių (ar jų dalies) pristatymo termino pratęsimas: netaikoma.

4.3. Užsakymų teikimo tvarka: Užsakymai teikiami tiekėjo nurodytu elektroniniu paštu ir laikomi gautais po 24 (dvidešimt keturių valandų) nuo užsakymo pateikimo. Prekių pristatymas ir visų susijusių paslaugų (prekių montavimo, paleidimo, derinimo bei personalo apmokymo paslaugos) suteikimas vykdomas Techninės specifikacijos 6 p. nustatyta tvarka ir terminais.

4.4. Dėl Prekių pristatymo dalimis vertės / apimties: netaikoma.

4.5. Kartu su Prekėmis pateikiami šie dokumentai: Žr. techninę specifikaciją. Tiekėjui nepateikus nurodytų dokumentų, laikoma, kad Prekės neatitinka Sutartyje nustatytų reikalavimų.

4.6. Techninės specifikacijos 4.1.- 4.2. p., 4.5.- 4.11. p. nurodytos prekės Tiekėjo pristatomos visa Techninėje specifikacijoje nurodyta apimtimi. Dėl Techninės specifikacijos 4.3-4.4. p. nurodytų prekių Tiekėjui bus pateiktas atskiras užsakymas, kuriame bus nurodytas galutinis pristatomas šių

prekių kiekis, techninėje specifikacijoje nurodyti šių prekių maksimalūs (ir preliminarūs) perkami kiekiai.

5. straipsnis. Sutarties kaina ir atsiskaitymo tvarka

5.1. Sutarčiai taikomas kainos apskaičiavimo būdas: fiksuoto įkainio kainodara.

5.2. Pradinės Sutarties vertė ir Sutarties kaina:

							Valiuta: Eurai
Eil. Nr.	**Prekės pavadinimas**	**Prekės gamintojas**	**Prekės modelis**	**Mato vnt.**	**Vieneto įkainis be PVM**	**Preliminarus kiekis[1]**	**Preliminari suma be PVM[2]**
1	Patekimo kontrolės sistemos (toliau - PKS) programinė įranga serveriui (1 vnt.) ir darbo stotims (9 vnt.)	Inner range (Australija)	996901C; 996940-60; 995200PEEU3; 996018PCBK; 996535PCBK;	kompl.	42954,66	1	42954,66
2	PKS leidimų kortelė	Inner range (Australija)	994610	vnt.	4,80	3000	14400,00
3	PKS skaitytuvas su klaviatūra	Inner range (Australija)	994725MF + 999046	vnt.	347,10	78	27073,80
4	PKS skaitytuvas be klaviatūros	Inner range (Australija)	994720MF + 999037	vnt.	132,50	67	8877,50
5	PKS kortelių spausdintuvas	FARGO (JAV)	DTC1250e	vnt.	3982,90	2	7965,80
6	Vartų valdymo pultas	Spectra Baltic UAB (Lietuva)	Nestandartinė, pagal spec. užsakymą gaminama prekė	vnt.	2500,00	1	2500,00
7	Fotografavimo įrenginiai su tvirtinimo prie sienos laikikliais	Hewlett-Packard (JAV)	HP 95 0 4K	kompl.	200,00	2	400,00
8	Vartelių užblokavimo mechanizmai, valdomi per durų procesorius	Eff-Eff (Vokietija)	118E.13---A71 PROFIX2	vnt.	60,00	7	420,00
9	Durų užblokavimo mechanizmai, valdomi per durų procesorius	Eff-Eff (Vokietija)	E7	vnt.	28,50	2	57,00
10	Įrangos montavimo, paleidimo, derinimo ir darbuotojų	Spectra Baltic UAB (Lietuva)	Įrangos montavimo, paleidimo, derinimo	kompl.	30000,00	1	30000,00

	apmokymo paslaugos [5]		ir darbuotojų apmokymo paslaugos				
Bendra preliminari kaina be PVM:							134648,76
PVM (21 %) kaina:							28276,24
Bendra preliminari kaina su PVM:							162925,00
Bendra preliminari kaina su PVM žodžiais: **Vienas šimtas šešiasdešimt du tūkstančiai devyni šimtai dvidešimt penki eurai 00 ct**							

Jei suma skaičiais neatitinka sumos žodžiais, teisinga laikoma suma žodžiais.

[1] **- kiekvienoje pozicijoje nurodytas prekių kiekis yra maksimalus.**

Šioje Sutartyje Pradinė Sutarties vertė yra lygi Tiekėjo pasiūlymo kainai be PVM, apskaičiuotai sudauginus maksimalų Prekių kiekį iš Tiekėjo pasiūlyto įkainio be PVM. Pirkėjas perka Prekes pagal poreikį Sutartyje nurodytais įkainiais, neviršijant jame nurodyto Prekių maksimalaus kiekio. Pirkėjas neįsipareigoja išpirkti preliminaraus Prekių kiekio ar bet kokios jo dalies. Pradinė Sutarties vertė vykdymo metu, išskyrus šioje Sutartyje numatytus atvejus negali būti keičiama.

5.3. Sutarties kainos / įkainių perskaičiavimas taikant peržiūros taisykles:

Sutarties įkainiai bus perskaičiuojami:

- dėl PVM tarifo pasikeitimo;

- dėl kainų lygio pokyčio.

5.3.1. Sutarties įkainių peržiūra dėl PVM tarifo pasikeitimo:

Jeigu Sutarties vykdymo metu pasikeičia PVM mokėjimą reglamentuojantys teisės aktai, darantys tiesioginę įtaką Tiekėjo tiekiamų Prekių Sutartyje nurodytiems įkainiams, Sutarties įkainiai perskaičiuojami nekeičiant Prekių įkainio be PVM. Perskaičiuota Sutarties įkainiai įforminami Susitarimu, kuris tampa neatskiriama Sutarties dalimi, ir turi būti taikomi nuo naujo PVM įvedimo datos (nepriklausomai nuo to, kada pasirašytas Susitarimas).

5.3.2. Sutarties įkainių peržiūra dėl kitų mokesčių, lemiančių Prekių kainos pokytį, pasikeitimo: netaikoma.

5.3.3. Sutarties įkainių peržiūra dėl kainų lygio pokyčio:

5.3.3.1. Bet kuri Sutarties šalis Sutarties galiojimo metu turi teisę inicijuoti Sutarties įkainių peržiūrą (keitimą) ne anksčiau kaip po 6 (šeši) mėnesių nuo Sutarties įsigaliojimo dienos (jeigu peržiūra jau buvo atlikta – nuo Susitarimo dėl paskutinio perskaičiavimo pagal šį Specialiųjų sąlygų punktą įsigaliojimo dienos), jeigu kainų pokytis, apskaičiuotas kaip nustatyta Sutarties sąlygose, viršija 5 procentus. Sutarties įkainių peržiūra atliekama ne dažniau kaip kas 6 (šeši) mėnesiai(-ių).

5.3.3.2. Sutarties įkainiai peržiūrimi tik tai Sutarties daliai, kuri nėra išpirkta, t. y. Prekėms, kurios nėra priimtos ir apmokėtos. Vėlesnė Sutarties įkainių peržiūra negali apimti laikotarpio, už kurį jau buvo atliktas peržiūra.

5.3.3.3. Jeigu Prekių tiekimas vėluoja dėl tiekėjo kaltės, uždelstų pristatyti Prekių įkainiai nėra perskaičiuojami dėl kainų lygio kilimo (negali būti didinami).

5.3.3.4. Atlikdamos Sutarties įkainių peržiūrą Šalys vadovaujasi Valstybės duomenų agentūros viešai Oficialiosios statistikos portale paskelbtais Rodiklių duomenų bazės duomenimis. Iš kitos Šalies nereikalaujama pateikti oficialaus Valstybės duomenų agentūros ar kitos institucijos išduoto dokumento ar patvirtinimo.

5.3.3.5. Šalys privalo Susitarime nurodyti šaltinio, kuriuo vadovaujamasi atliekama peržiūrą, reikšmę laikotarpio pradžioje ir jo nustatymo datą, reikšmę laikotarpio pabaigoje ir jo nustatymo datą, kainų pokytį (k), perskaičiuotus Sutarties įkainius, perskaičiuotą Pradinės Sutarties vertę.

5.3.3.6. Nauji Sutarties įkainiai apskaičiuojami pagal žemiau pateiktą formulę:

$$a_1 = a + \left(\frac{k}{100} \times a \right)$$

a - įkainis be PVM (jei įkainis jau buvo perskaičiuotas, imamas įkainis po paskutinio perskaičiavimo);

a_1 - perskaičiuotas (pakeistas) įkainis be PVM;

k - kainos pokytis (padidėjimas arba sumažėjimas) procentais (teigiamas, kai yra kainos padidėjimas, ir neigiamas, kai yra kainos sumažėjimas), apskaičiuotas pagal indeksą: Ūkis ir finansai (makroekonomika)_Kainų indeksai, pokyčiai ir kainos_Importuotų prekių kainų indeksai (2021 m. – 100): B_TO_E Pramonė..

"k" reikšmė skaičiuojama pagal formulę:

$$k = \left(\frac{Ind_{naujausias}}{Ind_{pradžia}} \times 100 \right) - 100$$

$Ind_{naujausias}$ - kreipimosi dėl kainos perskaičiavimo išsiuntimo kitai šaliai datą naujausias paskelbtas indeksas;

$Ind_{pradžia}$ - laikotarpio pradžios datos (mėnesio) indeksas. Pirmojo perskaičiavimo atveju laikotarpio pradžia (mėnuo) yra Sutarties įsigaliojimo dienos mėnuo. Antrojo ir vėlesnių perskaičiavimų atveju laikotarpio pradžia (mėnuo) yra paskutinio perskaičiavimo metu naudotos paskelbto atitinkamo indekso reikšmės mėnuo.

5.3.3.7. Skaičiavimams indeksų reikšmės ($Ind_{naujausias}$, $Ind_{pradžia}$) imamos keturių skaitmenų po kablelio tikslumu. Apskaičiuotas kainų pokytis (k) tolimesniems skaičiavimams naudojamas, jį suapvalinus iki vieno skaitmens po kablelio, o perskaičiuoti įkainiai (a_1) suapvalinami iki tiek skaitmenų po kablelio, su kiek skaitmenų po kalbelio buvo nurodyti atitinkami įkainiai Sutartyje iki pirmo perskaičiavimo. Perskaičiavus įkainius, perskaičiuojama bendra preliminari Sutarties kaina, prie iki perskaičiavimo įvykdytų sutartinių įsipareigojimų vertės su PVM pridedant likusių sutartinių įsipareigojimų bendrą preliminarią vertę su PVM, apskaičiuotą remiantis perskaičiuotais įkainiais.

5.3.3.8. Šalis, siekianti Sutarties įkainio peržiūros, privalo raštu kreiptis į kitą Šalį ir prašyme pateikti visą reikalingą informaciją: Sutarties pavadinimą, numerį, datą, neperduotų ir neapmokėtų Prekių

sąrašą su kiekiais, Indekso reikšmes su nuorodomis į viešus šaltinius Valstybės duomenų agentūros Oficialiosios statistikos portale arba kitus oficialius šaltinių duomenis, kita svarbi informacija. Prašyme Šalis neturi teisės nurodyti kito Indekso ar prašyti perskaičiavimo pagal kitą Indeksą nei nurodytas šioje Sutartyje.

5.3.3.9. Susitarimas turi būti sudarytas per 10 darbo dienų nuo Šalies pateikto tinkamo prašymo perskaičiuoti Sutarties įkainius gavimo dienos.

5.3.3.10. Susitarimu Šalys neturi teisės keisti Sutartyje nurodytos tvarkos ar kitų Sutarties nuostatų, išskyrus, jei keitimas atliekamas pagal VPĮ nuostatas.

5.3.4. Sutarties įkainių peržiūra dėl kainų lygio pokyčio pagal Prekių grupių kainų pokyčius: netaikoma.

5.4. Sutarties įkainių apskaičiavimas taikant kiekio (apimties) keitimo taisykles: netaikoma.

5.5. Atsiskaitymo su tiekėju terminas ir tvarka:

5.5.1. Pirkėjas atsiskaito su Tiekėju ne vėliau kaip per 30 kalendorinių dienų nuo Sąskaitos gavimo dienos.

5.5.2. Apmokėjimo sąlygos: Mokėjimas atliekamas remiantis tiekėjo pateikta elektronine sąskaita-faktūra/PVM sąskaita-faktūra (toliau – elektroninė sąskaita) už faktiškai įvykdytus tiekėjo įsipareigojimus. Elektroninė sąskaita turi atitikti perdavimo-priėmimo aktą pagal turinį.

5.5.3. Tarpiniai ir galutinis mokėjimai atliekami tik po to, kai abi šalys pasirašo perdavimo - priėmimo aktą, kaip nustatyta Sutarties Bendrosiose sąlygose.

5.6. Avansas: netaikoma.

5.7. Avanso užtikrinimas: netaikoma.

6. Prekių kokybė ir garantiniai įsipareigojimai

6.1. Garantinis terminas: Prekėms nustatomas Tiekėjo pasiūlytas arba Prekių gamintojo taikomas Garantinis terminas, tačiau bet kokiu atveju ne trumpesnis kaip 24 (dvidešimt keturių) mėnesių Garantinis terminas skaičiuojamas nuo Prekių perdavimo–priėmimo akto pasirašymo dienos.

6.2. Garantinė priežiūra: Sąlygos, susijusios su garantine priežiūra yra nurodytos Sutarties priede Nr. 1 pateiktoje techninėje specifikacijoje.

7. straipsnis. Sutarties vykdymui pasitelkiami subtiekėjai

7.1. Sutarties vykdymui pasitelkiami subtiekėjai ir (ar) specialistai: Sutarties vykdymui subtiekėjai ir (ar) specialistai nepasitelkiami.

8. straipsnis. Prievolių pagal Sutartį įvykdymo užtikrinimas

8.1. Prievolių pagal Sutartį įvykdymas užtikrinamas:

- netesybomis (delspinigiais, bauda).

8.2. Sutarties įvykdymo užtikrinimo galiojimo terminas: netaikoma.

8.3. Sutarties įvykdymo užtikrinimo pateikimas: netaikoma.

9. straipsnis. Šalių atsakomybė

9.1. Pirkėjui taikomos netesybos už mokėjimų pagal Sutartį vėlavimą:

9.1.1. Jei pirkėjas, gavęs tinkamai pateiktą ir užpildytą Sąskaitą, uždelsia atsiskaityti už tinkamai tiekėjo perduotas kokybiškas Prekes per Sutartyje nurodytą terminą, tiekėjas nuo kitos nei nustatytas terminas dienos skaičiuoja pirkėjui 3 procento dydžio delspinigius nuo neapmokėtos sumos be PVM už kiekvieną vėlavimo dieną.

9.2. Tiekėjui taikomos netesybos:

9.2.1. Jeigu tiekėjas vėluoja vykdyti užsakymą, tiekti Prekes ar ištaisyti jų trūkumus, arba nevykdo kitų sutartinių įsipareigojimų, pirkėjas nuo kitos nei nustatytas terminas dienos tiekėjui skaičiuoja 3 procento dydžio delspinigius už kiekvieną uždelstą dieną nuo laiku neperduotų Prekių ar Prekių, turinčių trūkumų, kainos be PVM.

9.2.2. Tiekėjas privalo sumokėti Pirkėjui netesybas per 30 (trisdešimt) dienų nuo pirkėjo pareikalavimo, jeigu netesybų suma nėra išskaitoma iš tiekėjui mokėtinos sumos.

9.3. Tiekėjui / Pirkėjui taikoma bauda nutraukus Sutartį dėl esminio Sutarties pažeidimo:

9.3.1. Nutraukus Sutartį dėl esminio Sutarties pažeidimo, nustatyto Sutarties Specialiosiose sąlygose, mokama 10 (dešimt) procentų dydžio bauda nuo Pradinės Sutarties vertės, nurodytos Specialiųjų sąlygų 5.2 punkte.

9.4. Tiekėjui taikoma bauda dėl esamų subtiekėjų ar specialistų pakeitimo / naujų subtiekėjų pasitelkimo nesilaikant Bendrosiose sąlygose nurodytos subtiekėjų ir (ar) specialistų keitimo tvarkos: netaikoma.

9.5. Tiekėjui taikomos baudos dėl aplinkosauginių ir (arba) socialinių kriterijų nesilaikymo: netaikoma.

9.6. Tiekėjui / Pirkėjui taikoma bauda dėl konfidencialumo reikalavimų nesilaikymo: netaikoma.

9.7. Tiekėjui taikomos netesybos dėl pirkimo dokumentuose nustatytų kokybinių kriterijų nepasiekimo Sutarties vykdymo metu: netaikoma.

9.8. Tiekėjui taikomos netesybos dėl Sutarties įvykdymo užtikrinimo nepratęsimo: netaikoma.

9.9. Kitos netesybos: netaikoma.

10. straipsnis. Sutarties galiojimas ir keitimas

10.1. Sutarties sudarymas ir įsigaliojimas: Ši Sutartis laikoma sudaryta ir įsigalioja nuo Sutarties pasirašymo dienos (antrosios Šalies pasirašymo dieną).

Sutartis galioja iki visiško prievolių įvykdymo (kol bus išnaudota Pradinės Sutarties vertė), bet jos terminas negali būti ilgesnis kaip 12 (dvylika) mėnesių nuo sutarties įsigaliojimo dienos.

10.2. Sutarties galiojimo termino pratęsimas: netaikoma.

11. straipsnis. Sutarties nutraukimas

11.1. Sutarties nutraukimo pagrindai: Sutartis gali būti nutraukiama rašytiniu Šalių susitarimu arba vienašališkai Bendrosiose sąlygose nustatyta tvarka.

11.2. Esminiai Sutarties pažeidimai:

11.2.1. jeigu tiekėjas nevykdo prisiimtų įsipareigojimų už Sutartyje nustatytą Sutarties kainą / įkainius;

11.2.2. jeigu tiekėjas nesilaiko Sutartyje nustatytų Prekių tiekimo terminų 2 (du) kartus iš eilės arba vėluoja pristatyti Prekes daugiau nei 120 kalendorinių dienų po Sutartyje nustatyto Prekių pristatymo termino pabaigos;

11.2.3. jeigu tiekėjas pažeidžia Prekių pristatymo terminus ir priskaičiuotų netesybų už vėlavimą suma viršija 20 (dvidešimt) procentų Pradinės sutarties vertės;

11.2.4. Tiekėjas pažeidžia Prekių pristatymo terminus ir dėl Prekių pristatymo vėlavimo Prekės tampa nebereikalingos;

11.2.5. Tiekėjas daugiau kaip 2 (du) kartus pristato Prekes, kurios neatitinka Sutartyje ir (ar) Įstatymuose nustatytų reikalavimų Prekėms;

11.2.6. Tiekėjo kvalifikacija tapo nebeatitinkančia pirkimo dokumentuose nustatytų Sutarties tinkamam vykdymui būtinų reikalavimų, arba tiekėjas prarado teisę verstis veiklą jonizuojančios spinduliuotės aplinkoje, jei to buvo reikalaujama. ir šie neatitikimai nebuvo ištaisyti per 14 (keturiolika) kalendorinių dienų nuo kvalifikacijos tapimo neatitinkančia arba teisės praradimo dienos;

11.2.7.Tiekėjas pažeidžia šios Sutarties nuostatas, reglamentuojančias konkurenciją, intelektinės nuosavybės ar konfidencialios informacijos valdymą;

11.2.8. Tiekėjas pažeidžia Bendrųjų sąlygų nuostatas dėl Sutarties vykdymui pasitelkiamų naujų subtiekėjų ir (ar specialistų) / esamų subtiekėjų ir (ar) specialistų keitimo.

12. Aplinkosauginiai ir (ar) socialiniai kriterijai

12.1. Aplinkosauginių kriterijų nustatymo teisinis pagrindas: Aplinkosauginiai kriterijai Prekėms nustatomi vadovaujantis Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto 2011 m. birželio 28 d. įsakymu D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ (toliau – Tvarkos aprašas) 4.4.4.1. papunkčiu.

12.2. Su Prekių pakuotėmis susiję aplinkosauginiai kriterijai: netaikoma.

12.3. Su Prekių pristatymu susiję aplinkosauginiai kriterijai: netaikoma.

12.4. Su Prekėmis susijusių paslaugų (pavyzdžiui, montavimo, apmokymo ir kitos parengimui naudoti skirtos paslaugos) teikimu susiję aplinkosauginiai kriterijai: Maksimaliai mažinamas popieriaus sunaudojimas dokumentams, dokumentų kopijavimui ir spausdinimui, teikiant pirmenybę skaitmeninėms dokumentų kopijoms, siunčiant elektroniniu paštu, pasinaudojant elektroninio parašo funkcijos galimybėmis ar kitais būdais. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka žaliojo pirkimo reikalavimus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakyme Nr. Dl-508 „Dėl Produktų, kurių viešiesiems pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos turi taikyti pirkdamos prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“.

12.5. Su perkamomis Prekėmis susiję socialiniai kriterijai: netaikoma.

12.6. Kiti su Prekėmis susiję aplinkosauginiai ir (ar) socialiniai kriterijai: Maksimaliai mažinamas popieriaus sunaudojimas dokumentams, dokumentų kopijavimui ir spausdinimui, teikiant pirmenybę skaitmeninėms dokumentų kopijoms, siunčiant elektroniniu paštu, pasinaudojant elektroninio parašo funkcijos galimybėmis ar kitais būdais. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka žaliojo pirkimo reikalavimus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakyme Nr. Dl-508 „Dėl Produktų, kurių viešiesiems pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos turi taikyti pirkdamos prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“.

13. straipsnis. Bendrųjų sąlygų pakeitimai ir papildymai

13.1. Šalys susitaria pakeisti nurodytą Sutarties Bendrųjų sąlygų punktą ir išdėstyti jį nauja redakcija:

13.1.1. Pakeisti Sutarties bendrųjų sąlygų 3 skirsnio „Tiekėjas ir kiti sutarties vykdymui pasitelkiami asmenys“ 3.2. poskirsnio „Subtiekėjų bei specialistų pasitelkimas ir keitimas“ 3.2.3. punktą ir išdėstyti jį taip:

„3.2.3. Tiekėjas turi teisę Sutarties vykdymui pasitelkti naujus, Specialiosiose sąlygose nenurodytus subtiekėjus, kurių pajėgumais nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Pirkėjui pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Pirkėjas taip pat reikalauja, kad Tiekėjas ne vėliau nei prieš 5 (penkias) darbo dienas informuotų apie minėtos informacijos pasikeitimus bei naujų subtiekėjų pasitelkimą visu Sutarties vykdymo metu. Pirkėjas (jeigu buvo taikoma pirkimo dokumentuose) turi patikrinti, ar nėra subtiekėjo pašalinimo pagrindų ir subtiekėjo atitiktį nacionalinio saugumo interesams ir kilmės reikalavimams. Jeigu subtiekėjo padėtis neatitinka bet vieno iš nurodytų reikalavimų, Pirkėjas reikalauja pakeisti šį subtiekėją reikalavimus atitinkančiu subtiekėju. Pirkėjas per 10 (dešimt) darbo dienų raštu informuoja Tiekėją apie leidimą pasitelkti naują subtiekėją, kurio pajėgumais Tiekėjas nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.“

13.1.2. Pakeisti Sutarties bendrųjų sąlygų 3 skirsnio „Tiekėjas ir kiti sutarties vykdymui pasitelkiami asmenys“ 3.2. poskirsnio „Subtiekėjų bei specialistų pasitelkimas ir keitimas“ 3.2.5. punktą ir išdėstyti jį taip:

„3.2.5. Subtiekėjus, kurių pajėgumais Tiekėjas nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti, Tiekėjas gali keisti savo nuožiūra, apie tai raštu ne vėliau, kaip

prieš 5 (penkias) darbo dienas informuodamas Pirkėją. Pirkėjas (jeigu buvo taikoma pirkimo dokumentuose) turi patikrinti, ar nėra subtiekėjo pašalinimo pagrindų ir subtiekėjo atitiktį nacionalinio saugumo interesams ir kilmės reikalavimams. Jeigu subtiekėjo padėtis neatitinka bet vieno iš nurodytų reikalavimų, Pirkėjas reikalauja pakeisti šį subtiekėją reikalavimus atitinkančiu subtiekėju. Pirkėjas per 10 (dešimt) darbo dienų raštu informuoja Tiekėją apie leidimą pakeisti subtiekėją. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.“

13.1.3. Pakeisti Sutarties bendrųjų sąlygų 3 skirsnio „Tiekėjas ir kiti sutarties vykdymui pasitelkiami asmenys“ 3.2. poskirsnio „Subtiekėjų bei specialistų pasitelkimas ir keitimas“ 3.2.9. punktą ir išdėstyti jį taip:

„3.2.9. Pirkėjas, gavęs Tiekėjo prašymą su kitais Sutartyje nurodytais dokumentais, per 10 (dešimt) darbo dienų įvertina keitimo galimybes ir raštu informuoja Tiekėją apie leidimą pakeisti subtiekėją ar specialistą. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.“

13.1.4. Pakeisti Sutarties bendrųjų sąlygų 3 skirsnio „Tiekėjas ir kiti sutarties vykdymui pasitelkiami asmenys“ 3.3. poskirsnio „Jungtinės veiklos partnerių keitimas“ 3.3.4. punktą ir išdėstyti jį taip:

„3.3.4. Pirkėjas, gavęs Tiekėjo prašymą su kitais Sutartyje nurodytais dokumentais, per 15 (penkiolika) darbo dienų įvertina keitimo galimybes ir raštu informuoja Tiekėją apie Sutarties nutraukimą arba apie leidimą atsisakyti ar pakeisti partnerį. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.“

13.1.5. Pakeisti Sutarties bendrųjų sąlygų 6 skirsnio „Prekių tiekimo pabaiga ir prekių priėmimas“ 6.2. poskirsnio „Prekių perdavimas-priėmimas“ 6.2.3.1. punktą ir išdėstyti jį taip:

„6.2.3.1. ne vėliau kaip per 20 (dvidešimt) darbo dienų nuo faktinio Prekių perdavimo priimti Prekes, pasirašydamas Prekių perdavimo–priėmimo aktą; arba;“

13.1.6. Pakeisti Sutarties bendrųjų sąlygų 6 skirsnio „Prekių tiekimo pabaiga ir prekių priėmimas“ 6.2. poskirsnio „Prekių perdavimas-priėmimas“ 6.2.7. punktą ir išdėstyti jį taip:

„6.2.7. Jeigu Pirkėjas per 20 (dvidešimt) darbo dienų nepateikia (neišsiunčia) Tiekėjui Defektų akto, laikoma, kad Pirkėjas Prekes priėmė ir joms pretenzijų neturi;“

13.1.7. Pakeisti Sutarties bendrųjų sąlygų 7 skirsnio „Tiekėjo garantiniai įsipareigojimai“ 7.3. poskirsnio „Prekių trūkumų šalinimas“ 7.3.7. punktą ir išdėstyti jį taip:

„7.3.7. Pirkėjas per 20 (dvidešimt) darbo dienų po Tiekėjo pranešimo apie Prekių trūkumų pašalinimą gavimo privalo patikrinti trūkumus, nurodytus Defektų akte arba Pirkėjo pretenzijoje, ir raštu patvirtinti, kurie Prekių trūkumai buvo pašalinti.“

13.1.8. Pakeisti Sutarties bendrųjų sąlygų 20 skirsnio „Sutarties pakeitimai“ 20.3. punktą ir išdėstyti jį taip:

„20.3. Šalis, inicijuojanti Susitarimą, privalo pateikti kitai Šaliai pranešimą dėl Sutarties pakeitimo bei pagrindimą dėl to, jog yra faktinis ir teisinis pagrindas sudaryti Susitarimą. Kita Šalis per 15 (penkiolika) darbo dienų (arba per kitą Šalių raštu sutartą terminą) privalo išanalizuoti ir įvertinti gautą informaciją, pateikti savo pastabas ir pasiūlymus, pagrįstus Sutarties arba imperatyviomis įstatymų bei kitų teisės aktų nuostatomis.“

13.1.9. Pakeisti Sutarties bendrųjų sąlygų 21 skirsnio „Sutarties sustabdymas“ 21.5.1. punktą ir išdėstyti jį taip:

„21.5.1. Atsiradus aplinkybėms, dėl kurių Tiekėjas negali vykdyti sutartinių įsipareigojimų, Tiekėjas apie tai nedelsdamas privalo informuoti Pirkėją. Tiekėjo rašytiniame prašyme turi būti nurodyta stabdymo aplinkybė (Bendrųjų sąlygų 21.2 punktas) ir aplinkybės atsiradimą bei galimą terminą pagrindžiantys argumentai, objektyvūs faktai ir įrodymai. Pirkėjas, įvertinęs prašymą, ne vėliau kaip per 7 (septynias) darbo dienas raštu informuoja Tiekėją apie priimtą sprendimą dėl sutartinių įsipareigojimų vykdymo stabdymo. Tiekėjui nepateikus konkrečių argumentų, faktų, pagrįstų įrodymais, Pirkėjas turi teisę raštu atsisakyti patvirtinti stabdymą.“

13.1.10. Pakeisti Sutarties bendrųjų sąlygų 22 skirsnio „Sutarties nutraukimas“ 22.1. poskirsnio „Pretenzijos dėl Sutarties pažeidimų“ 22.1.2. punktą ir išdėstyti jį taip:

„22.1.2. Pretenziją gavusi Šalis privalo nedelsdama, bet ne vėliau nei per 10 (dešimt) darbo dienų, atsakyti į pretenziją ir nurodyti, kokių priemonių imsis siekdama ištaisyti pažeidimą per pretenzijoje nustatytą terminą arba motyvuotai pasiūlyti kitą pagrįstą terminą. Tiekėjo teisė siūlyti kitą terminą nelaikoma Pirkėjo pareiga tą terminą priimti. Pretenziją gavusios Šalies pasiūlytasis terminas pakeičia terminą, nurodytą pretenzijoje, tik jeigu kita Šalis jį patvirtina.“

13.2. Šalys susitaria papildyti Sutarties Bendrąsias sąlygas nurodytu punktu, tačiau kitų punktų numeracijos nekeisti:

13.2.1. Papildyti Sutarties bendrųjų sąlygų 3 skirsnio „Tiekėjas ir kiti sutarties vykdymui pasitelkiami asmenys" 3.1 poskirsnį „Kvalifikacija ir kiti Tiekėjo pasiūlymu prisiimti įsipareigojimai" 3.1.4. punktu ir išdėstyti jį taip:

„3.1.4. Pirkėjas, praėjus daugiau kaip vieneriems metams nuo šios Sutarties įsigaliojimo dienos, turi teisę tarptautinių sankcijų ir/ar Lietuvos Respublikos įstatymais nustatytų ribojamųjų priemonių įgyvendinimo tikslu prašyti Tiekėją atnaujinti viešojo pirkimo procedūrų metu dėl šios Sutarties sudarymo pateiktą šio pobūdžio informaciją.“

13.3. Šalys susitaria išbraukti nurodytą Sutarties Bendrųjų sąlygų punktą, tačiau kitų punktų numeracijos nekeisti: netaikoma.

13.4. Sutarties Bendrosiose sąlygose nurodytos alternatyvios nuostatos (su prierašu „jei taikoma“ ir pan.) taikomos tik tokiu atveju, jeigu jos konkrečiai aprašomos Sutarties Specialiosiose sąlygose.

14. straipsnis. Sutarties priedai

14.1. 1 priedas. Techninė specifikacija ir perkančiosios organizacijos iki pasiūlymų pateikimo termino išsiųsti paaiškinimai:

14.1.1. 2025 m. balandžio 16 d. „Patekimo kontrolės sistemos pirkimo techninė specifikacija“ Nr. Spc-25(13.66E);

14.1.2. VĮ Ignalinos atominės elektrinės (toliau – VĮ IAE) 2025-05-19 raštas „Dėl pirkimo dokumentų paaiškinimo“ Nr. ĮS-1969(13.66E);

14.1.2. VĮ Ignalinos atominės elektrinės 2025-05-08 raštas „Dėl pirkimo dokumentų paaiškinimo ir patikslinimo“ Nr. ĮS-1830(13.66E).

14.2. 2 priedas. Tiekėjo pasiūlymas su priedais, perkančiosios organizacijos prašymai paaiškinti pasiūlymą bei tiekėjo paaiškinimai, pateikti pirkimo procedūros metu:

14.2.1. UAB „Spectra Baltic“ 2025-05-26 pasiūlymas su priedais;

14.2.2. VĮ IAE 2025-07-09 rašto „Dėl pateikto pasiūlymo paaiškinimo (pirkimo Nr.1984530)“ Nr. ĮS-2759(13.66E) nuorašas;

14.2.3. UAB „Spectra Baltic“ 2025-07-15 pranešimo (pranešimo ID 280760), pateikto CVP IS priemonėmis, kopija.

14.3. 3 priedas. Prekių perdavimo – priėmimo aktų formos.

14.4. 4 priedas. Garantinių įsipareigojimų įvykdymo akto forma.

14.5. 5 priedas. Trišalės atsiskaitymo sutarties forma.

15. straipsnis. Šalies atstovų parašai

Pirkėjas		**Tiekėjas**	
Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:	
Parašas:		Parašas:	
Data:		Data:	

T33238

PREKIŲ PIRKIMO–PARDAVIMO SUTARTIES BENDROSIOS SĄLYGOS

1. PAGRINDINĖS SĄVOKOS IR SUTARTIES AIŠKINIMAS

1.1. Sąvokos

1.1.1. Šioje Sutartyje didžiąja raide rašomos sąvokos turi paskiau nurodytas reikšmes:
1.1.1.1. **Bendrosios sąlygos** – ši Sutarties dalis, kuri vadinasi „Prekių pirkimo–pardavimo sutarties Bendrosios sąlygos“;
1.1.1.2. **Pirkėjas** – asmuo, kuris Specialiosiose sąlygose yra įvardytas kaip Pirkėjas, įsigyjantis Specialiosiose sąlygose ir Sutarties prieduose nurodytas Prekes;
1.1.1.3. **Pradinės sutarties vertė** – Specialiosiose sąlygose nurodyta vertė (be PVM);
1.1.1.4. **Prekės** – Specialiosiose sąlygose ir Sutarties prieduose nurodytos prekės (prekių pirkimas, nuoma, finansinė nuoma (lizingas), pirkimas išsimokėtinai, numatant jas įsigyti ar to nenumatant), taip pat įsigyjamų prekių pristatymo, montavimo, diegimo ir kitos jų parengimo naudoti paslaugos (toliau – su Prekėmis susijusios paslaugos), jeigu šios paslaugos tik papildo prekių tiekimą, kurias Tiekėjas įsipareigoja tiekti Pirkėjui pagal Sutartį ir galiojančių įstatymų bei kitų teisės aktų reikalavimus;
1.1.1.5. **Prekių perdavimo–priėmimo aktas** – dokumentas, kuriuo Tiekėjas perduoda, o Pirkėjas priima Prekes ir kuriuo Šalys patvirtina, kad pristatytos Prekės atitinka nustatytus reikalavimus. Jeigu Sutartyje yra numatytas Prekių pristatymas dalimis, Prekių perdavimo–priėmimo aktas gali būti sudaromas dėl kiekvienos dalies atskirai;
1.1.1.6. **Prekių trūkumai** – Prekių perdavimo–priėmimo metu ar Prekių garantinio termino galiojimo metu Pirkėjo ar (ir) trečiųjų asmenų nustatyti Prekių kokybės neatitikimai Sutarties ar (ir) įstatymų bei kitų teisės aktų reikalavimams, Prekių gedimai, paslėpti defektai, veiklos sutrikimai ar pan., dėl kurių Prekių nebūtų galima naudoti tam tikslui, kuriam Pirkėjas (jas) ketino naudoti, arba dėl kurių Prekių naudingumas sumažėtų taip, kad Pirkėjas, apie tuos trūkumus žinodamas, arba apskritai nebūtų tų Prekių pirkęs, arba nebūtų už Prekes mokėjęs tokio dydžio kainą;
1.1.1.7. **Sąskaita** – Tiekėjo išrašoma ir Pirkėjui apmokėjimui pateikiama sąskaita faktūra, PVM sąskaita faktūra ar kitas mokėjimo dokumentas už Tiekėjo perduotas bei Pirkėjo priimtas Prekes. Jeigu Sutartyje yra numatytas Prekių pristatymas dalimis, Sąskaita gali būti pateikiama dėl kiekvienos dalies atskirai;
1.1.1.8. **Specialiosios sąlygos** – Sutarties dalis, kuri vadinasi „Prekių pirkimo-pardavimo sutarties Specialiosios sąlygos“ ir kurioje yra nurodytos konkretaus pirkimo objekto įsigijimą aptariančios sąlygos (tokios kaip Pradinės sutarties vertė, Prekių tiekimo terminai ir pan.) bei kiti konkretūs duomenys (tokie kaip Šalys, Prekės ir pan.), išvardyti priedai, taip pat nurodyti Bendrųjų sąlygų pakeitimai ir papildymai (jeigu tokie padaryti);
1.1.1.9. **Susitarimas** – tai dokumentas, kurį Šalys sudaro keisdamos Sutarties sąlygas VPĮ leidžiama apimtimi;
1.1.1.10. **Sutarties kaina** – pagal Sutartį Tiekėjui mokėtina galutinė suma, įskaitant visus privalomus mokesčius ir išlaidas;
1.1.1.11. **Sutarties sąlygos** – Bendrosios sąlygos ir Specialiosios sąlygos kartu;
1.1.1.12. **Sutartis** – Prekių pirkimo–pardavimo sutartis, kurią sudaro Sutarties sąlygos, Specialiosiose sąlygose išvardyti priedai ir Susitarimai;
1.1.1.13. **Šalis** – Pirkėjas arba Tiekėjas, kiekvienas atskirai, priklausomai nuo konteksto;
1.1.1.14. **Šalys** – Pirkėjas ir Tiekėjas kartu;
1.1.1.15. **Tiekėjas** – asmuo, kuris Specialiosiose sąlygose yra įvardytas kaip Tiekėjas, tiekiantis Specialiosiose sąlygose nurodytas Prekes;
1.1.1.16. **VPĮ** – Lietuvos Respublikos viešųjų pirkimų įstatymas.
1.1.1.17. Kitų Sutartyje didžiąja raide rašomų sąvokų reikšmės yra nurodytos Sutarties tekste.

1.1.1.18. Sutartyje neapibrėžtos sąvokos suprantamos ir aiškinamos taip, kaip jas apibrėžia VPĮ ir kiti įstatymai bei teisės aktai, galiojantys Sutarties sudarymo ir vykdymo metu.
1.1.1.19. Kitos Sutartyje vartojamos sąvokos ir terminai turi bendrinę reikšmę arba artimiausią Sutarties pobūdžiui specialiąją reikšmę, jei Sutartyje nėra nustatyta ir paaiškinta kitokia jų reikšmė.

1.2. Sutarties aiškinimas

1.2.1. Sutartis yra sudaryta ir turi būti aiškinama pagal Lietuvos Respublikos teisės aktus.
1.2.2. Jei Bendrosios sąlygos ir (ar) Specialiosios sąlygos prieštarauja VPĮ ir kitų teisės aktų reikalavimams, taikomos VPĮ ir kitų teisės aktų nuostatos.
1.2.3. Diena Sutartyje reiškia kalendorinę dieną.
1.2.4. Darbo diena Sutartyje reiškia bet kurią dieną, išskyrus šeštadienį, sekmadienį ir švenčių dienas Lietuvoje, nurodytas Lietuvos Respublikos darbo kodekse.
1.2.5. Terminai pagal Sutartį yra skaičiuojami metais, mėnesiais, savaitėmis, darbo dienomis, kalendorinėmis dienomis ir valandomis.
1.2.6. Kvalifikacija, rėmimasis kitų ūkio subjektų pajėgumais, Prekių apimtis, peržiūra suprantami taip, kaip nustatyta VPĮ bei jį įgyvendinančiuose teisės aktuose.
1.2.7. Jeigu Prekių perdavimo–priėmimo akto, kaip atskiro dokumento, reikalauti neprivaloma, Šalys susitaria, ir tai aiškiai nurodo Specialiosiose sąlygose, Prekių perdavimo–priėmimo aktu laikoma Sąskaita. Tais atvejais, kai išrašoma Sąskaita ir Prekių perdavimo–priėmimo aktas nepasirašomas, Sutarties nuostatos dėl Prekių perdavimo–priėmimo akto išrašymo taikomos ir Sąskaitos išrašymui.
1.2.8. Informuoti, pranešti, įspėti arba atsakyti reiškia pateikti informaciją, pranešimą, įspėjimą arba atsakymą Bendrosiose ir (ar) Specialiosiose sąlygose nustatyta tvarka.
1.2.9. Patvirtinti reiškia pateikti patvirtinimą raštu arba pasirašyti dokumentą be išlygų ar su išlygomis, išskyrus atvejus, kai asmuo, pasirašydamas dokumentą, nurodo, jog atsisako jį patvirtinti.
1.2.10. Jeigu Sutartyje nenurodyta kitaip, žodžiai, vartojami vienaskaitos forma taip pat reiškia ir daugiskaitą ir atvirkščiai, vienos giminės žodžiai apima ir kitos giminės atitinkamus žodžius, žodis asmuo reiškia tiek fizinius, tiek ir juridinius asmenis.
1.2.11. Jeigu Sutartyje nurodyta reikšmė skaičiais ir žodžiais skiriasi, vadovaujamasi žodžiais nurodyta reikšme.
1.2.12. Jei pateikiamos nuorodos į teisės aktus, turi būti taikomos aktualios teisės aktų redakcijos, jeigu nenurodyta kitaip.

1.3. Dokumentų viršenybė

1.3.1. Sutartį sudarantys dokumentai turi būti suprantami kaip papildantys vienas kitą. Bet kokio Sutarties dokumentų sąlygų neatitikimo ar neaiškumo atveju, toks neatitikimas ar neaiškumas pašalinamas dokumentus aiškinant tokia eilės tvarka:
1.3.1.1. Techninė specifikacija;
1.3.1.2. Specialiosios sąlygos;
1.3.1.3. Bendrosios sąlygos;
1.3.1.4. Pirkimo dokumentai (išskyrus techninę specifikaciją);
1.3.1.5. Pasiūlymas;
1.3.1.6. Kiti Specialiosiose sąlygose išvardinti priedai.
1.3.2. Tuo atveju, kai Šalių Susitarimu yra keičiamos Sutarties sąlygos, naujai sutartos Sutarties sąlygos turi viršenybę prieš pakeistąsias.
1.3.3. Jeigu Šalys susitaria dėl Sutarties sąlygų arba priedo papildymo nauja sąlyga, neatitikimo ar neaiškumo atveju tokia sąlyga turi viršenybę atitinkamai kitų Sutarties sąlygų arba kitų to priedo sąlygų atžvilgiu.
1.3.4. Jeigu Šalys susitaria dėl naujo priedo, Šalys turi sutarti dėl naujojo priedo įtraukimo į priedų sąrašą vietos ir jo reikšmės aiškinant Sutartį. Jeigu naujas priedas yra įterpiamas į priedų sąrašą, jam

turi būti suteikiamas eilės numeris su viršutiniu indeksu, atsižvelgiant į priedų eiliškumą ir svarbą (pavyzdžiui, priedas Nr. 41).

2. SUTARTIES DALYKAS

2.1. Tiekėjas įsipareigoja Sutartyje nustatytomis sąlygomis ir tvarka perduoti Pirkėjui Prekes, atitinkančias Sutartyje nustatytus reikalavimus, o Pirkėjas įsipareigoja priimti Sutarties sąlygas atitinkančias ir tinkamai patiektas Prekes bei sumokėti Tiekėjui Sutartyje nurodytą kainą Sutartyje nustatytomis sąlygomis ir tvarka.
2.2. Šalys, vykdydamos Sutartį, įsipareigoja laikytis visų Sutarties vykdymui taikytinų įstatymų bei kitų teisės aktų reikalavimų. Šalis turi teisę reikalauti, kad kita Šalis įvykdytų visus įstatymų bei kitų teisės aktų reikalavimus, taikomus Sutarties vykdymui. Nė viena iš Sutarties sąlygų nereiškia ir negali būti aiškinama kaip Pirkėjo atsisakymas įstatymuose bei kituose teisės aktuose numatytų ir Sutartimi neaptartų Pirkėjo kitų teisių ir garantijų, susijusių su netinkamu Prekių tiekimu ar jų kokybe, arba kaip Tiekėjo atsisakymas įstatymuose bei kituose teisės aktuose numatytų ir Sutartimi neaptartų Tiekėjo kitų teisių ir garantijų dėl atlyginimo už Prekes gavimo.
2.3. Tiekėjas privalo užtikrinti, kad Prekės atitiktų techninės specifikacijos reikalavimus ir Tiekėjo pasiūlymo sąlygas, būtų kokybiškos, tiekiamos tinkamai ir laiku, laikantis Sutarties sąlygų taip, kad tai labiausiai atitiktų Pirkėjo interesus, pagal geriausius visuotinai pripažįstamus profesinius, techninius standartus ir praktiką, panaudodamas visus reikiamus įgūdžius ir žinias.

3. TIEKĖJAS IR KITI SUTARTIES VYKDYMUI PASITELKIAMI ASMENYS

3.1. Kvalifikacija ir kiti Tiekėjo pasiūlymu prisiimti įsipareigojimai

3.1.1. Tiekėjas atsako už tai, kad visą Sutarties vykdymo laikotarpį Tiekėjas būtų kompetentingas, patikimas ir pajėgus (įskaitant ūkio subjektų, kurių pajėgumais remiasi Tiekėjas, pajėgumus) įvykdyti Sutarties reikalavimus:
3.1.1.1. turėtų teisę verstis ta veikla, kuri yra reikalinga Sutarčiai įvykdyti;
3.1.1.2. atitiktų tiekėjų kvalifikacijai pirkimo dokumentuose nustatytus Sutarties tinkamam vykdymui būtinus reikalavimus bei neturėtų pirkimo dokumentuose nustatytų pašalinimo pagrindų;
3.1.1.3. laikytųsi Tiekėjo pasiūlyme nurodytų įsipareigojimų, įskaitant, bet neapsiribojant – atitiktų pirkimo dokumentuose nustatytus kokybinių kriterijų reikšmes ir parametrus;
3.1.1.4. užtikrintų nustatytų kokybės vadybos sistemos ir (arba) aplinkos apsaugos vadybos sistemos standartų taikymą, jeigu to reikalaujama pirkimo dokumentuose, ir turėtų tą patvirtinančius dokumentus;
3.1.1.5. atitiktų nacionalinio saugumo interesus bei kilmės reikalavimus, jei tokie reikalavimai buvo numatyti pirkimo dokumentuose.
3.1.2. Tuo atveju, kai Tiekėjas yra jungtinės veiklos partneriai, jie Pirkėjui už Sutarties vykdymą atsako solidariai. Jeigu Tiekėjas remiasi ūkio subjektų pajėgumais, siekdamas atitikti finansinio ir ekonominio pajėgumo reikalavimus, Tiekėjas su tokiais ūkio subjektais už Sutarties vykdymą atsako solidariai (jeigu to buvo reikalaujama pirkimo dokumentuose).
3.1.3. Tiekėjas taip pat atsako už tai, kad Tiekėjas, Sutartį tiesiogiai vykdantys subtiekėjai ir specialistai atitiktų jiems įstatymų bei kitų teisės aktų ir (arba) pirkimo dokumentų nustatytus profesinės kvalifikacijos ir kitus reikalavimus bei turėtų teisę verstis ta veikla, kuriai jie pasitelkiami.

3.2. Subtiekėjų bei specialistų pasitelkimas ir keitimas

3.2.1. Tiekėjas įsipareigoja užtikrinti, kad Sutartį vykdys pirkime pasiūlyti ir kvalifikacijos bei kitus pirkimo dokumentuose nustatytus reikalavimus atitinkantys subtiekėjai ir (ar) specialistai. Šių

asmenų veiksmai vykdant Sutartį Tiekėjui sukelia tokias pačias pasekmes ir atsakomybę, kaip jo paties veiksmai. Tiekėjas atsako už savo subtiekėjų ir specialistų veiksmus ar neveikimą.
3.2.2. Sutarties vykdymui pasitelkiami subtiekėjai ir (ar) specialistai (jeigu tokie pasitelkiami) nurodomi Specialiosiose sąlygose.
3.2.3. Tiekėjas turi teisę Sutarties vykdymui pasitelkti naujus, Specialiosiose sąlygose nenurodytus subtiekėjus, kurių pajėgumais nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti. Sudarius Sutartį, tačiau ne vėliau negu Sutartis pradedama vykdyti, Tiekėjas įsipareigoja Pirkėjui pranešti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Pirkėjas taip pat reikalauja, kad Tiekėjas ne vėliau nei prieš 5 (penkias) darbo dienas informuotų apie minėtos informacijos pasikeitimus bei naujų subtiekėjų pasitelkimą visu Sutarties vykdymo metu. Pirkėjas (jeigu buvo taikoma pirkimo dokumentuose) turi patikrinti, ar nėra subtiekėjo pašalinimo pagrindų ir subtiekėjo atitiktį nacionalinio saugumo interesams ir kilmės reikalavimams. Jeigu subtiekėjo padėtis neatitinka bet vieno iš nurodytų reikalavimų, Pirkėjas reikalauja pakeisti šį subtiekėją reikalavimus atitinkančiu subtiekėju. Pirkėjas per 5 (penkias) darbo dienas raštu informuoja Tiekėją apie leidimą pasitelkti naują subtiekėją, kurio pajėgumais Tiekėjas nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.
3.2.4. Tiekėjas gali keisti Sutartyje nurodytus subtiekėjus ir (ar) specialistus šiame Sutarties poskyryje nustatytais atvejais ir tvarka gavęs Pirkėjo rašytinį sutikimą.
3.2.5. Subtiekėjus, kurių pajėgumais Tiekėjas nesirėmė pirkimo dokumentuose numatytiems kvalifikacijos reikalavimams pagrįsti, Tiekėjas gali keisti savo nuožiūra, apie tai raštu ne vėliau, kaip prieš 5 (penkias) darbo dienas informuodamas Pirkėją. Pirkėjas (jeigu buvo taikoma pirkimo dokumentuose) turi patikrinti, ar nėra subtiekėjo pašalinimo pagrindų ir subtiekėjo atitiktį nacionalinio saugumo interesams ir kilmės reikalavimams. Jeigu subtiekėjo padėtis neatitinka bet vieno iš nurodytų reikalavimų, Pirkėjas reikalauja pakeisti šį subtiekėją reikalavimus atitinkančiu subtiekėju. Pirkėjas per 5 (penkias) darbo dienas raštu informuoja Tiekėją apie leidimą pakeisti subtiekėją. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.
3.2.6. Subtiekėjas, kurio pajėgumais Tiekėjas rėmėsi, kad atitiktų pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus, gali būti keičiamas tik šiais atvejais:
3.2.6.1. kai subtiekėjui iškelta bankroto byla, pradėtas bankroto procesas ne teismo tvarka, jis tampa nemokus arba yra nemokumo tikimybė, sustabdo ūkinę veiklą ar kai įstatymuose ir kituose teisės aktuose nustatyta tvarka susidaro analogiška situacija;
3.2.6.2. kai subtiekėjas dėl objektyvių priežasčių (pavyzdžiui, subtiekėjui atsisakius dalyvauti Sutarties vykdyme, nutrūkus teisiniams santykiams su Tiekėju ir pan.) nebegali vykdyti visų ar dalies Sutartyje numatytų įsipareigojimų.
3.2.6.3. Naujas subtiekėjas, kuris keičiamas vietoje subtiekėjo, kurio pajėgumais Tiekėjas rėmėsi, kad atitiktų pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus (toliau – naujas subtiekėjas), turi atitikti pirkimo dokumentuose nustatytus reikalavimus dėl pašalinimo pagrindų nebuvimo, keliamus kvalifikacijos reikalavimus, Tiekėjo pasiūlyme nurodytą keičiamo subtiekėjo kvalifikaciją pirkimo dokumentuose nustatytiems kokybiniams kriterijams pagrįsti ir nacionalinio saugumo interesus bei kilmės reikalavimus (jei taikoma).
3.2.7. Tiekėjo (ar subtiekėjų) specialistas, vykdysiantis Sutartį, gali būti pakeisti šiais atvejais:
3.2.7.1. Tiekėjo iniciatyva dėl objektyvių priežasčių (pavyzdžiui, atostogų, ligos, nutrūkus darbo santykiams ir pan.), pateikus duomenis apie numatomą naujai skirti specialistą bei jo kvalifikaciją ir atitiktį kitiems pirkimo dokumentuose keliamiems reikalavimams patvirtinančius dokumentus;
3.2.7.2. Pirkėjo iniciatyva, jei Pirkėjas turi pagrįstų įtarimų, kad Tiekėjo Sutarties vykdymui paskirtas specialistas nekompetentingas vykdyti nustatytas pareigas.
3.2.7.3. Naujas specialistas turi turėti ne žemesnę nei pirkimo dokumentuose specialistui keliamą kvalifikaciją, Tiekėjo pasiūlyme nurodytą keičiamo specialisto kvalifikaciją pirkimo dokumentuose nustatytiems kokybiniams kriterijams pagrįsti ir nacionalinio saugumo interesus bei kilmės reikalavimus, nurodytus pirkimo dokumentuose (jei taikoma).

3.2.8. Tiekėjas privalo ne vėliau nei prieš 5 (penkias) darbo dienas iki numatomo subtiekėjo, kurio pajėgumais Tiekėjas rėmėsi, kad atitiktų pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus, ar specialisto keitimo pateikti Pirkėjui argumentuotą rašytinį prašymą ir šiuos dokumentus:
3.2.8.1. prašymą pakeisti subtiekėją ar specialistą, paaiškinant keitimo aplinkybę. Pirkėjas pasilieka teisę paprašyti įrodymų, pagrindžiančių keitimo aplinkybę;
3.2.8.2. naujo subtiekėjo ar specialisto kvalifikaciją, pašalinimo pagrindų nebuvimą ir atitiktį nacionalinio saugumo interesams bei kilmės reikalavimams įrodančius dokumentus pagal Sutarties reikalavimus.
3.2.9. Pirkėjas, gavęs Tiekėjo prašymą su kitais Sutartyje nurodytais dokumentais, per 5 (penkias) darbo dienas įvertina keitimo galimybes ir raštu informuoja Tiekėją apie leidimą pakeisti subtiekėją ar specialistą. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.
3.2.10. Naujas subtiekėjas ar specialistas gali pradėti vykdyti jiems Tiekėjo pavestus įsipareigojimus pagal Sutartį ne anksčiau, nei bus pasirašytas Susitarimas.
3.2.11. Tiekėjas privalo pakeisti subtiekėją ar specialistą, jei paaiškėja, kad jis neatitinka jam pirkimo dokumentuose keliamų reikalavimų.
3.2.12. Jei Tiekėjas pakeičia esamą arba pasitelkia naują subtiekėją ar specialistą, negavęs Pirkėjo raštiško sutikimo, arba sutartinius įsipareigojimus pagal Sutartį vykdo subtiekėjai ar specialistai, neatitinkantys pirkimo dokumentuose nustatytų kvalifikacijos reikalavimų, reikalavimų dėl pašalinimo pagrindų nebuvimo, atitikties nacionalinio saugumo interesams bei kilmės reikalavimams (jei taikoma) ir Tiekėjo pasiūlyme nurodytų sąlygų pirkimo dokumentuose nustatytiems kokybiniams kriterijams pagrįsti (jei taikoma), Tiekėjui taikoma Specialiosiose sąlygose nustatyto dydžio bauda.

3.3. Jungtinės veiklos partnerių keitimas

3.3.1. Tiekėjas, vykdantis Sutartį jungtinės veiklos pagrindu, turi teisę atsisakyti jungtinės veiklos partnerio (toliau – partneris), jei dėl objektyvių ir pagrįstų aplinkybių partneris nebegali vykdyti Sutarties, įskaitant, bet neapsiribojant atvejais, kai partneris neatitinka VPĮ ar kitų teisės aktų nuostatų, kelia grėsmę nacionaliniam saugumui, partneriui pritaikytos tarptautinės sankcijos kaip jos suprantamos Lietuvos Respublikos tarptautinių sankcijų įstatyme (toliau – Sankcijų įstatymas), partnerio sunki finansinė būklė, lemianti Sutarties nevykdymą ir (ar) atsisakymą ją vykdyti ar atsirado kitos nenumatytos objektyvios priežastys, lemiančios partnerio pasitraukimą iš jungtinės veiklos sutarties.
3.3.2. Tiekėjas, vykdantis Sutartį jungtinės veiklos pagrindu, turi teisę pakeisti partnerį, jei dėl reorganizavimo, restruktūrizavimo ar bankroto procedūrų, pradinio partnerio teises ir pareigas visiškai arba iš dalies perima kitas partneris. Toks Tiekėjo pakeitimas negali lemti kitų esminių Sutarties pakeitimų ir taip negali būti siekiama išvengti VPĮ ir kitų teisės aktų taikymo.
3.3.3. Tiekėjas privalo ne vėliau nei prieš 10 (dešimt) darbo dienų iki numatomo partnerio keitimo arba atsisakymo pateikti Pirkėjui argumentuotą rašytinį prašymą ir šiuos dokumentus:
3.3.3.1. prašymą pakeisti Tiekėjo sudėtį ir įrodymus, pagrindžiančius bent vieną partnerio atsisakymo ar keitimo aplinkybę, nurodytą Sutartyje;
3.3.3.2. naujos jungtinės veiklos sutarties ar esamos jungtinės veiklos sutarties pakeitimo kopiją, kurioje, jeigu partneris pasitraukia, turi būti nurodyta, kad pasitraukiančiojo partnerio įsipareigojimus visa apimtimi perima pasiliekantis jungtinės veiklos partneris (toliau – pasiliekantysis partneris);
3.3.3.3. pasiliekančiojo ar naujai pasitelkiamo partnerio kvalifikaciją patvirtinančius dokumentus. Visais atvejais pasiliekančiojo partnerio ar naujai pasitelkto partnerio kvalifikacija turi būti ne žemesnė nei pasitraukiančiojo partnerio (atitinkanti pirkimo dokumentuose nustatytus kvalifikacijos reikalavimus, kuriuos atitiko pasitraukiantysis partneris, ir atitinkanti pasitraukiančiojo partnerio pasiūlyme nurodytą specialistų kvalifikaciją ir kitas sąlygas pirkimo dokumentuose nustatytiems kokybiniams kriterijams pagrįsti (jei taikoma). Jei pasitelkiamas naujas partneris, taip pat, vadovaujantis pirkimo dokumentuose nurodytais reikalavimais, pateikiami dokumentai,

pagrindžiantys pasitelkiamo partnerio pašalinimo pagrindų nebuvimą ir atitiktį nacionalinio saugumo interesams bei kilmės reikalavimams (jei taikoma).
3.3.4. Pirkėjas, gavęs Tiekėjo prašymą su kitais Sutartyje nurodytais dokumentais, per 10 (dešimt) darbo dienų įvertina keitimo galimybes ir raštu informuoja Tiekėją apie Sutarties nutraukimą arba apie leidimą atsisakyti ar pakeisti partnerį. Pirkėjui sutikus, Šalys pasirašo Susitarimą, kuris laikomas neatsiejama Sutarties dalimi.

3.4. Susitarimai dėl tiesioginio atsiskaitymo su subtiekėjais

3.4.1. Subtiekėjams pageidaujant, Pirkėjas su jais atsiskaitys tiesiogiai. Pirkėjas numato tiesioginio atsiskaitymo galimybę su Sutartyje nurodytais subtiekėjais tokiomis sąlygomis ir tvarka:
3.4.1.1. sudarius Sutartį, Tiekėjas ne vėliau negu Sutartis pradedama vykdyti, įsipareigoja Pirkėjui raštu pateikti tuo metu žinomų subtiekėjų pavadinimus, kontaktinius duomenis ir jų atstovus. Pirkėjas taip pat reikalauja, kad Tiekėjas informuotų apie minėtos informacijos pasikeitimus bei naujų subtiekėjų pasitelkimą visu Sutarties vykdymo metu;
3.4.1.2. Pirkėjas ne vėliau kaip per 3 (tris) darbo dienas nuo Bendrųjų sąlygų 3.4.1.1 punkte nurodytos informacijos gavimo dienos raštu informuoja subtiekėjus apie tiesioginio atsiskaitymo galimybę;
3.4.1.3. subtiekėjas, norėdamas pasinaudoti tokia galimybe, raštu pateikia prašymą Pirkėjui. Kai subtiekėjas išreiškia norą pasinaudoti tiesioginio atsiskaitymo galimybe, sudaroma trišalė sutartis tarp Pirkėjo, Tiekėjo ir šio subtiekėjo, kurioje aprašoma tiesioginio atsiskaitymo su subtiekėju tvarka, atsižvelgiant į Sutartyje ir subtiekimo sutartyje nustatytus reikalavimus;
3.4.1.4. tiesioginio atsiskaitymo su subtiekėjais galimybė nekeičia Tiekėjo atsakomybės dėl Sutarties įvykdymo.

4. ŠALIŲ BENDRADARBIAVIMAS

4.1. Šalių bendradarbiavimo pareiga

4.1.1. Vykdydamos Sutartį, Šalys privalo maksimaliai bendradarbiauti ir operatyviai keistis informacija, taip pat pateikti viena kitai rašytinius pranešimus nedelsiant apie tai, kad atsirado ar egzistuoja bet koks įvykis, sąlyga ar aplinkybė, kuri gali paveikti Sutarties vykdymą ar sąlygoti jos pažeidimą.
4.1.2. Šalys įsipareigoja užtikrinti, kad viena kitai teiks dokumentus ir (ar) kitą informaciją, kurie yra būtini Šalių tinkamam įsipareigojimų įvykdymui pagal Sutartį.
4.1.3. Jeigu Šalis susiduria su Sutarties vykdymo kliūtimi, ji turi nedelsdama, bet ne vėliau kaip per 5 (penkias) darbo dienas, įspėti kitą Šalį apie tokias kliūtis ir imtis visų nuo jos priklausančių protingų priemonių toms kliūtims pašalinti.

4.2. Kontaktiniai asmenys

4.2.1. Kiekviena iš Šalių Sutarties sudarymo metu privalo paskirti kontaktinį asmenį, atsakingą už Sutarties vykdymą (pavyzdžiui, Prekių priėmimą, užsakymų teikimą ir gavimą ir kt.), ir nurodyti jų kontaktinius duomenis Specialiosiose sąlygose.
4.2.2. Tuo atveju, kai Šalis nori atšaukti paskirtąjį kontaktinį asmenį ir paskirti kitą asmenį arba nori paskirti kitą asmenį laikinai vykdyti kontaktinio asmens funkcijas kontaktinio asmens laikino negalėjimo vykdyti savo funkcijas laikotarpiu, Šalis privalo iš anksto apie tai informuoti kitą Šalį ir pateikti kitai Šaliai tokio asmens kontaktinius duomenis: vardą, pavardę, el. paštą ir telefono numerį.
4.2.3. Tuo atveju, kai paaiškėja, kad Šalies kontaktinis asmuo laikinai negali vykdyti savo pareigų (dėl ligos, traumos ar kitų nenumatytų priežasčių), Šalis privalo nedelsdama, bet ne vėliau nei kitą darbo dieną, paskirti kitą kontaktinį asmenį laikinai vykdyti kontaktinio asmens funkcijas ir pranešti

apie tai kitai Šaliai. Keičiant kontaktinių asmenų funkcijas atliekančius asmenis Susitarimas, vadovaujantis Bendrųjų sąlygų 20.5 punktu, nesudaromas.

5. SUTARTIES VYKDYMO METU PATEIKIAMI DOKUMENTAI

5.1. Jeigu Tiekėjas turi parengti ir (ar) pateikti Pirkėjui Prekių naudojimo instrukcijas, jos turi būti aiškios ir detalios, kad Pirkėjas, vadovaudamasis jomis, galėtų tinkamai naudoti patiektas Prekes.
5.2. Tuo atveju, kai pagal Sutartį turi būti vykdomi mokymai ir (arba) atliekami bandymai, Tiekėjas privalo perduoti Pirkėjui naudojimo instrukcijas prieš tokius mokymus ir (arba) bandymus, o po mokymų ir (arba) bandymų patikslinti ir papildyti naudojimo instrukcijas, atsižvelgdamas į mokymų ir (arba) bandymų eigą ir rezultatus.
5.3. Jei Prekių naudojimui būtiniems dokumentams reikalingas vertimas, su tuo susijusios išlaidos tenka Tiekėjui. Jei Tiekėjas Prekių naudojimui būtinus dokumentus verčia savarankiškai, jis atsako už šių dokumentų vertimo tikslumą.

6. PREKIŲ TIEKIMO PABAIGA IR PREKIŲ PRIĖMIMAS

6.1. Prekių tiekimo pabaiga

6.1.1. Prekių tiekimas laikomas užbaigtu, kai yra įvykdytos visos šios sąlygos:
6.1.1.1. Tiekėjas pristatė visas Prekes pagal Sutarties ir įstatymų bei kitų teisės aktų reikalavimus (ir kai suteiktos visos su Prekėmis susijusios paslaugos, jei to reikalaujama),
6.1.1.2. Tiekėjas perdavė Pirkėjui visą reikalingą dokumentaciją, įskaitant naudojimo instrukcijas ir garantijas (jei to reikalaujama),
6.1.1.3. Tiekėjas apmokė Pirkėjo personalą, kaip naudoti Prekes (jeigu to reikalaujama),
6.1.1.4. buvo įformintas Prekių perdavimo-priėmimo aktas ar Prekių perdavimo–priėmimo aktai, jei numatytas Prekių pristatymas dalimis, ar kitas Sutartyje numatytas dokumentas, nuo kurio pasirašymo laikoma, kad Prekės buvo priimtos,
6.1.1.5. Tiekėjas įvykdė kitas sąlygas, numatytas įstatymuose bei kituose teisės aktuose, Sutartyje ir pasiūlyme, kurios turi būti įvykdytos tam, kad būtų laikoma, jog Prekių tiekimas yra užbaigtas, ir pateikė Pirkėjui tai įrodančius dokumentus.

6.2. Prekių perdavimas–priėmimas

6.2.1. Tiekėjas privalo pristatyti ir perduoti Prekes Pirkėjui, o Pirkėjas privalo kokybiškas ir Sutarties bei įstatymų ir kitų teisės aktų reikalavimus atitinkančias Prekes priimti. Prekės pristatomos Specialiosiose sąlygose nurodytais terminais ir adresu, pristatymą iš anksto suderinus su Pirkėju.
6.2.2. Prekės perduodamos Šalims pasirašant Prekių perdavimo–priėmimo aktą, kuris pasirašomas 2 (dviem) vienodą teisinę galią turinčiais egzemplioriais (išskyrus atvejus, kai Prekių perdavimo–priėmimo aktas pasirašomas saugiu elektroniniu parašu), po vieną kiekvienai Šaliai. Jeigu Prekių perdavimo–priėmimo akto, kaip atskiro dokumento, reikalauti neprivaloma, Šalys susitaria, ir tai aiškiai nurodo Specialiosiose sąlygose, Prekių perdavimo–priėmimo aktu laikoma Sąskaita.
6.2.3. Tiekėjui pristačius Prekes, Pirkėjas atlieka jų patikrinimą ir privalo:
6.2.3.1. ne vėliau kaip per 5 (penkias) darbo dienas nuo faktinio Prekių perdavimo priimti Prekes, pasirašydamas Prekių perdavimo–priėmimo aktą; arba
6.2.3.2. priimti Prekes su išlygomis, pasirašydamas Prekių perdavimo–priėmimo aktą ir Prekių patikrinimo metu sudarytą defektų aktą, kuriame Pirkėjas privalo nurodyti per Prekių priėmimą pastebėtus Prekių ar pateikiamų Tiekėjo dokumentų trūkumus ir tų trūkumų pašalinimo tvarką (toliau – Defektų aktas); arba
6.2.3.3. atsisakyti priimti Prekes ar jų dalį ir įteikti (arba išsiųsti) Defektų aktą Tiekėjui dėl netinkamų Prekių ar jų dalies.

6.2.4. Prekių perdavimo–priėmimo akte turi būti nurodoma data, kada Tiekėjas pristatė visas Prekes (ar atitinkamą jų dalį, kai Sutartyje numatytas pristatymas dalimis) ir pateikė visus reikiamus dokumentus.
6.2.5. Prekes, neatitinkančias Sutarties, įstatymų bei kitų teisės aktų (jei taikoma) reikalavimų, Tiekėjas privalo atsiimti savo sąskaita per Pirkėjo Defektų akte nustatytą terminą, taip pat Pirkėjo reikalavimu atlyginti tokių Prekių saugojimo išlaidas.
6.2.6. Jeigu nustatoma Prekių trūkumų, kurie nereiškia neatitikimo Sutartyje nustatytiems reikalavimams, ir jų pašalinimas netrukdo Pirkėjui naudotis Prekėmis pagal paskirtį, Pirkėjas gali priimti Prekes su išlygomis, sudaryti Defektų aktą ir nustatyti protingus terminus Tiekėjui pašalinti Prekių trūkumus. Tiekėjas privalo pašalinti Prekių trūkumus per Pirkėjo nurodytus protingus terminus, vadovaudamasis Bendrųjų sąlygų 7.3 poskyriu „Prekių trūkumų šalinimas“. Jeigu Tiekėjas praleidžia Prekių trūkumų pašalinimo terminus, taikomos Bendrųjų sąlygų 7.4 poskyrio „Pirkėjo teisės, Tiekėjui nepašalinus Prekių trūkumų“ nuostatos.
6.2.7. Jeigu Pirkėjas per 5 (penkias) darbo dienas nepateikia (neišsiunčia) Tiekėjui Defektų akto, laikoma, kad Pirkėjas Prekes priėmė ir joms pretenzijų neturi.
6.2.8. Prekių praradimo ar sugadinimo ar atsitiktinio žuvimo rizika Pirkėjui iš Tiekėjo pereina nuo faktinio Prekių priėmimo momento.
6.2.9. Pirkėjas turi teisę naudotis Prekėmis tik po Prekių perdavimo-priėmimo akto pasirašymo.
6.2.10. Jeigu Tiekėjas Prekes pristatė per Specialiosiose sąlygose nustatytą Prekių pristatymo terminą, tačiau jos turi trūkumų ir Tiekėjas šių trūkumų neištaiso iki Specialiosiose sąlygose nurodyto Prekių pristatymo termino pabaigos, Tiekėjui iki tinkamų Prekių pristatymo dienos taikomos Specialiosiose sąlygose nurodyto dydžio netesybos.

7. TIEKĖJO GARANTINIAI ĮSIPAREIGOJIMAI

7.1. Garantiniai terminai (jei taikoma)

7.1.1. Prekėms taikomas teisės aktuose nustatytas ir (ar) gamintojo taikomas garantinis terminas, jeigu Techninėje specifikacijoje ar Specialiosiose sąlygose nėra nurodytas kitas garantinis terminas. Jeigu garantinis terminas nėra niekur nustatytas, Prekėms taikomas 24 (dvidešimt keturių) mėnesių garantinis terminas. Garantinis terminas pradedamas skaičiuoti nuo pristatytų Prekių perdavimo–priėmimo akto pasirašymo dienos.
7.1.2. Garantiniai terminai sustabdomi tiek laiko, kiek Pirkėjas negali tinkamai naudoti Prekių dėl nustatytų Prekių trūkumų, už kuriuos atsako Tiekėjas. Jeigu Pirkėjas dėl Prekių trūkumų negali naudoti tik apibrėžtos Prekių dalies, garantiniai terminai sustabdomi tik tokios dalies atžvilgiu.
7.1.3. Tiekėjas neatsako už Prekių trūkumus, kurie atsirado dėl Prekių normalaus susidėvėjimo, jų netinkamo naudojimo ar priežiūros arba Pirkėjo, jo personalo arba trečiųjų asmenų kaltės, su sąlyga, kad nėra Tiekėjo kaltės dėl tokių Prekių trūkumų, Prekių netinkamo naudojimo ar priežiūros.

7.2. Pretenzijos dėl Prekių trūkumų

7.2.1. Pirkėjas, per garantinius terminus nustatęs Prekių trūkumų, turi nedelsdamas, bet ne vėliau nei per 30 (trisdešimt) dienų ir ne vėliau nei iki garantinio termino pabaigos, pareikšti rašytinę pretenziją Tiekėjui ir nustatyti protingus terminus, jeigu jų nėra nustatyta Specialiosiose sąlygose, Prekių trūkumams pašalinti.
7.2.2. Tiekėjas privalo neatlygintinai pašalinti visus Prekių trūkumus, už kuriuos atsako Tiekėjas, per Pirkėjo pretenzijoje nustatytus protingus terminus, jeigu konkretūs terminai nėra nustatyti Specialiosiose sąlygose, kurie skaičiuojami nuo pretenzijos gavimo dienos.
7.2.3. Jei Tiekėjas nepripažįsta Prekių trūkumų, kiekviena iš Šalių gali kreiptis dėl nepriklausomos ekspertizės atlikimo. Jei Tiekėjas ilgiau nei 10 (dešimt) dienų nuo Pirkėjo kreipimosi neatsako / nepasitelkia nepriklausomo su Pirkėju suderinto (Pirkėjas negali nepagrįstai neduoti pritarimo

Tiekėjui pasitelkti siūlomą ekspertą eksperto ginčui spręsti ar (ir) jei ginčas užtruko ilgiau nei 30 (trisdešimt) dienų nuo Pirkėjo pirmojo kreipimosi), tai Pirkėjas turi teisę savarankiškai kreiptis dėl ekspertizės atlikimo prieš tai suderinęs su Tiekėju nepriklausomo eksperto kandidatūrą. Tokiu atveju ekspertizės išlaidas padengia:
7.2.3.1. jei Prekės atitinka Sutartyje nurodytus reikalavimus – Pirkėjas;
7.2.3.2. jei Prekės neatitinka Sutartyje nurodytų reikalavimų – Tiekėjas.

7.3. Prekių trūkumų šalinimas

7.3.1. Tiekėjas privalo pašalinti Prekių trūkumus, sutaisydamas Prekes ar jų dalį arba pakeisdamas Prekę nauja Preke ar jos dalimi.
7.3.2. Pirkėjas privalo suteikti prieigą Tiekėjui atlikti Prekių trūkumų pašalinimą, kad Tiekėjas galėtų atlikti tai per nustatytus terminus. Jei Prekių trūkumai šalinami Prekių naudojimo vietoje, Pirkėjas ir Tiekėjas privalo susitarti dėl Prekių trūkumų šalinimo laiko.
7.3.3. Sutaisytoje Prekių dalyje pakartotinai nustačius Prekių trūkumų, Tiekėjas privalo pakeisti Prekes naujomis kokybiškomis Prekėmis, nebent Pirkėjas raštu sutiktų Prekes dar kartą taisyti.
7.3.4. Pašalinus Prekių trūkumus, garantinis terminas sutaisytajai Prekių daliai ar naujoms Prekėms vėl pradedamas skaičiuoti nuo tinkamai sutaisytų ar pakeistų Prekių (ar jų dalių) perdavimo Pirkėjui dienos.
7.3.5. Jeigu Prekių trūkumų šalinimas gali turėti įtakos Prekių funkcionalumui, Pirkėjas gali pareikalauti Tiekėjo pakartotinai atlikti bandymus, atliktus pagal Sutartį (jei tokie buvo numatyti). Pirkėjas privalo raštu pateikti Tiekėjui tokį reikalavimą per 30 (trisdešimt) dienų po Prekių trūkumų pašalinimo. Tokie bandymai atliekami pagal anksčiau atliktų bandymų sąlygas, išskyrus tai, kad jie visais atvejais turi būti atliekami Tiekėjo rizika ir sąskaita.
7.3.6. Tiekėjas, pašalinęs visus Prekių trūkumus, privalo apie tai informuoti Pirkėją.
7.3.7. Pirkėjas per 5 (penkias) darbo dienas po Tiekėjo pranešimo apie Prekių trūkumų pašalinimą gavimo privalo patikrinti trūkumus, nurodytus Defektų akte arba Pirkėjo pretenzijoje, ir raštu patvirtinti, kurie Prekių trūkumai buvo pašalinti.

7.4. Pirkėjo teisės, Tiekėjui nepašalinus Prekių trūkumų

7.4.1. Jeigu Tiekėjas atsisako pašalinti arba nepašalina Prekių trūkumų per Pirkėjo nustatytus protingus terminus, Pirkėjas turi teisę:
7.4.1.1. pašalinti Prekių trūkumus pats arba pasamdydamas trečiuosius asmenis, iš anksto apie tai informuodamas Tiekėją, ir pareikalauti Tiekėjo atlyginti Prekių ekspertizės bei Prekių trūkumų šalinimo išlaidas ir padengti patirtus nuostolius; arba
7.4.1.2. reikalauti sumažinti Tiekėjui mokėtiną sumą ir grąžinti dėl šios sumos sumažinimo susidariusią permoką per 30 (trisdešimt) dienų nuo Tiekėjui nustatyto termino pašalinti Prekių trūkumus pabaigos; arba
7.4.1.3. grąžinti Prekes Tiekėjui ir nemokėti už tokias Prekes ar reikalauti grąžinti už Prekes sumokėtą sumą bei nutraukti Sutartį.
7.4.2. Tiekėjui pagal Sutartį mokėtina suma sumažinama tiek, kiek sumažėja Prekių vertė Pirkėjui dėl Prekių trūkumų. Į Prekių vertės sumažėjimą, be kita ko, įskaičiuojamos Pirkėjo išlaidos Prekių trūkumų įvertinimui ir šalinimui, Prekių vertės sumažėjimas, Pirkėjo esamų ar būsimų išlaidų Prekių eksploatavimui padidėjimas (jeigu tokios išlaidos buvo vertinamos pirkimo metu).
7.4.3. Tiekėjas privalo patenkinti Pirkėjo pagal Bendrųjų sąlygų 7.4.4 punktą pareikštą piniginį reikalavimą per 30 (trisdešimt) dienų arba per ilgesnį Pirkėjo reikalavime nurodytą protingą terminą.
7.4.4. Už vėlavimą pašalinti Prekių trūkumus Pirkėjas privalo reikalauti Tiekėjo sumokėti Specialiosiose sąlygose nustatyto dydžio netesybas.

8. PRISTATYMO TERMINAI

8.1. Pristatymo terminai ir Prekių tiekimo grafikas

8.1.1. Tiekėjas privalo pristatyti Prekes laikydamasis terminų, nurodytų Specialiosiose sąlygose.

8.1.2. Jei taikytina, Pirkėjas privalo ne vėliau kaip per 14 (keturiolika) darbo dienų nuo Sutarties įsigaliojimo arba per kitą pirkimo dokumentuose nurodytą terminą parengti ir pateikti Tiekėjui suderinimui Prekių tiekimo grafiką (toliau – Grafikas).

8.1.3. Jei aktualu, Grafike turi būti pažymėta, kurios Prekės gali būti pristatomos lygiagrečiai, o kurios gali būti pristatomos tik numatytu eiliškumu.

8.2. Netesybos už Prekių pristatymo vėlavimą

8.2.1. Jeigu Tiekėjas praleidžia Prekių pristatymo terminus, nustatytus Specialiosiose sąlygose, Tiekėjui iki Prekių pristatymo datos taikomos Specialiosiose sąlygose nurodyto dydžio netesybos.

8.2.2. Tiekėjui praleidus Prekių dalies pristatymo terminą, netesybos skaičiuojamos nuo Prekių dalies pristatymo termino pabaigos (neįskaitytinai) iki Prekių dalies pristatymo datos (įskaitytinai), nustatytos pagal Prekių perdavimo–priėmimo aktus.

8.2.3. Jei Tiekėjui pagal šią Sutartį yra priskaičiuotos netesybos, Pirkėjo už Prekes mokėtina suma mažinama priskaičiuotų netesybų suma. Taip pat Pirkėjas turi teisę priskaičiuotas netesybas vienašališkai išskaičiuoti iš bet kokių Tiekėjui atliekamų mokėjimų teisės aktų nustatyta tvarka, pranešant Tiekėjui raštu apie tokių netesybų įskaitymą.

9. PRIEVOLIŲ PAGAL SUTARTĮ ĮVYKDYMO UŽTIKRINIMO BŪDAI

9.1. Šalių prievolių pagal Sutartį įvykdymas yra užtikrinamas Specialiųjų sąlygų 8 skyriuje nurodytais prievolių pagal Sutartį įvykdymo užtikrinimo būdais, Bendrųjų sąlygų 10 skyriuje nustatyta sutartinių įsipareigojimų įvykdymo užtikrinimo tvarka, Bendrųjų sąlygų 12.1.3 punkte nurodytu avanso užtikrinimu (jeigu Specialiosiose sąlygose yra nurodytas avanso dydis ir yra reikalaujama avanso užtikrinimo), Specialiųjų sąlygų 9 skyriuje nurodytomis netesybomis.

10. SUTARTIES ĮVYKDYMO UŽTIKRINIMAS (JEI TAIKOMA)

10.1. Šio skyriaus nuostatos taikomos tuomet, jei Specialiosiose sąlygose numatyta, kad tinkamam Sutarties įvykdymui užtikrinti Tiekėjas turi pateikti banko garantiją arba draudimo bendrovės laidavimo draudimo raštą arba kitą Specialiosiose sąlygose nurodytą sutartinių įsipareigojimų įvykdymo užtikrinimą.
Pastaba. Kai Specialiosiose sąlygose nurodoma, kad Pirkėjas reikalauja pateikti kredito unijos išduotą Sutarties įvykdymo užtikrinimą, šio skyriaus nuostatos taikomos pagal poreikį ir Pirkėjas gali nusimatyti papildomus reikalavimus Specialiosiose sąlygose tokio Sutarties įvykdymo užtikrinimo pateikimui, atitinkančius įstatymų bei kitų teisės aktų nuostatas.
10.2. Tiekėjas privalo pateikti Pirkėjui Specialiosiose sąlygose nurodytos rūšies ir dydžio Sutarties įvykdymo užtikrinimą – pirmo pareikalavimo banko garantiją arba draudimo bendrovės laidavimo draudimo raštą (kartu su draudimo bendrovės laidavimo draudimo raštu turi būti pateiktas ir pasirašytas draudimo liudijimas (polisas) bei dokumentas, įrodantis, kad draudimo įmoka už išduotą laidavimo draudimo raštą yra sumokėta), atitinkantį Bendrųjų sąlygų 10 skyriuje nurodytas sąlygas, per Specialiosiose sąlygose nustatytą terminą (toliau – Sutarties įvykdymo užtikrinimas).

10.3. Jei Tiekėjas nepateikia Pirkėjui Sutartyje nustatytos vertės Sutarties įvykdymo užtikrinimo per Sutartyje nustatytą terminą, laikoma, kad Tiekėjas atsisakė sudaryti Sutartį ir Pirkėjas turi teisę VPĮ nustatyta tvarka pasiūlyti sudaryti Sutartį kitam tiekėjui.
10.4. Prieš pateikdamas Sutarties įvykdymo užtikrinimą, Tiekėjas gali prašyti Pirkėjo patvirtinti, kad Pirkėjas sutinka priimti Tiekėjo siūlomą Sutarties įvykdymo užtikrinimą. Tokiu atveju, Pirkėjas privalo atsakyti Tiekėjui ne vėliau kaip per 3 (tris) darbo dienas nuo Tiekėjo prašymo gavimo dienos.
10.5. Sutarties įvykdymo užtikrinime bankas (draudimo bendrovė) privalo neatšaukiamai ir besąlygiškai įsipareigoti ne vėliau kaip per 15 (penkiolika) dienų nuo Pirkėjo raštiško pranešimo apie Tiekėjo Sutartyje nustatytų prievolių pažeidimą, dalinį ar visišką jų nevykdymą arba netinkamą vykdymą gavimo dienos, sumokėti Pirkėjui Sutarties įvykdymo užtikrinime nurodytą sumą, pinigus pervedant į Pirkėjo sąskaitą.
10.6. Sutarties įvykdymo užtikrinime negali būti nurodyta, kad bankas (draudimo bendrovė) atsako tik už tiesioginių nuostolių atlyginimą. Bankas (draudimo bendrovė) neturi teisės reikalauti, kad Pirkėjas pagrįstų savo reikalavimą. Pirkėjas pranešime bankui (draudimo bendrovei) nurodo, kad Sutarties įvykdymo užtikrinimo suma jam priklauso dėl to, kad Tiekėjas iš dalies ar visiškai neįvykdė Sutarties ir (arba) ji buvo nutraukta dėl Tiekėjo kaltės. Pirkėjas neįsipareigoja įrodyti realiai patirtų nuostolių ir Tiekėjas, pasirašydamas Sutartį ir pateikdamas Sutarties įvykdymo užtikrinimą, patvirtina, kad Sutarties įvykdymo užtikrinimo suma laikytina minimaliais neįrodinėjamais Pirkėjo nuostoliais.
10.7. Sutarties įvykdymo užtikrinimas turi įsigalioti ne vėliau negu jo pateikimo Pirkėjui dieną.
10.8. Sutarties įvykdymo užtikrinimo suma turi būti nurodoma ir išmokama eurais.
10.9. Sutarties įvykdymo užtikrinimas turi būti surašytas lietuvių arba kita kalba (esant Pirkėjo prašymui, turi būti pateiktas vertimas į lietuvių kalbą).
10.10. Sutarties įvykdymo užtikrinime nurodytas jo galiojimo terminas turi būti ne trumpesnis nei Sutarties galiojimo terminas.
10.11. Jeigu Sutarties trukmė yra ilgesnė nei 1 (vieneri) metai, Tiekėjas turi teisę pateikti 1 (vienerius) metus galiojantį Sutarties įvykdymo užtikrinimą, tačiau privalo pratęsti Sutarties įvykdymo užtikrinimo terminą arba pateikti naują Sutarties įvykdymo užtikrinimą ne vėliau kaip prieš 10 (dešimt) darbo dienų iki Sutarties įvykdymo užtikrinimo galiojimo termino pabaigos.
10.12. Jeigu Sutartyje nustatytomis sąlygomis Prekių pristatymo terminas yra pratęsiamas arba nukeliamas dėl Sutarties sustabdymo arba pristatyti Prekes arba taisyti Prekių trūkumus yra vėluojama, Tiekėjas privalo užtikrinti Sutarties įvykdymo užtikrinimo galiojimą visą Sutarties galiojimo laikotarpį ir ne vėliau kaip iki Sutarties įvykdymo užtikrinimo galiojimo termino pabaigos privalo Pirkėjui pateikti naują arba pratęstą Sutarties įvykdymo užtikrinimą.
10.13. Tiekėjui laiku nepratęsus Sutarties įvykdymo užtikrinimo galiojimo termino arba nepateikus naujo Sutarties įvykdymo užtikrinimo, Pirkėjas turi teisę reikalauti Specialiosiose sąlygose nustatyto dydžio netesybų už kiekvieną pradelstą dieną.
10.14. Pirkėjas nepriima Sutarties įvykdymo užtikrinimo ir (ar) laiko jį negaliojančiu, ir (ar) kreipiasi į Tiekėją dėl naujo Sutarties įvykdymo užtikrinimo pateikimo Pirkėjui, o Tiekėjas privalo Sutarties įvykdymo užtikrinimą pateikti per trumpiausiai įmanomą terminą, jei Sutarties įvykdymo užtikrinimas neatitinka Sutartyje keliamų reikalavimų arba Pirkėjas turi informacijos, susijusios su Sutarties įvykdymo užtikrinimą išdavusio banko (draudimo bendrovės) veiklos sustabdymu arba galimu veiklos sustabdymu (įskaitant nemokumą, likvidavimą ar teisinės apsaugos taikymo procedūras).
10.15. Jei Tiekėjas pažeidžia Sutartimi nustatytus įsipareigojimus, dalinai ar visiškai įsipareigojimų nevykdo (ar juos vykdo ne pagal Sutarties sąlygas), Pirkėjas gali pasinaudoti Sutarties įvykdymo užtikrinimu. Tiekėjas, siekdamas toliau vykdyti Sutarties įsipareigojimus, privalo per 10 (dešimt) darbo dienų nuo pranešimo apie Sutarties įvykdymo užtikrinimo sumokėjimą Pirkėjui pranešimo gavimo dienos pateikti Pirkėjui naują Specialiosiose sąlygose nurodyto dydžio Sutarties įvykdymo užtikrinimą.

10.16. Pirkėjas gali pasinaudoti Sutarties įvykdymo užtikrinimu, esant bet kuriai iš žemiau nurodytų aplinkybių:
10.16.1. Tiekėjas neįvykdė, nevykdo arba netinkamai vykdo savo įsipareigojimus pagal Sutartį;
10.16.2. Tiekėjas per protingai nustatytą laikotarpį neįvykdo Pirkėjo nurodymo ištaisyti Prekių trūkumus;
10.16.3. jei dėl bet kokių Tiekėjo veiksmų (veikimo ar neveikimo) Pirkėjas patyrė nuostolius (įskaitant, bet neapribojant, papildomas išlaidas, negautas pajamas ar kitus tiesioginius ir netiesioginius nuostolius, delspinigius ir (arba) baudas (jei tai yra numatyta Specialiosiose sutarties sąlygose);
10.16.4. Tiekėjas be pateisinamos priežasties (ne Sutartyje nustatytais atvejais) vienašališkai nutraukia Sutartį.

11. SUTARTIES KAINA IR JOS PERSKAIČIAVIMAS

11.1. Sutarties kaina, kurią Pirkėjas privalo sumokėti Tiekėjui už faktiškai pristatytas Prekes pagal Sutarties sąlygas, įskaitant visus Susitarimus, yra apskaičiuojama, taikant kainos apskaičiavimo būdą ar būdus, nurodytus Specialiosiose sąlygose.
11.2. Pradinės sutarties vertė yra nurodyta Specialiosiose sąlygose.
11.3. Laikoma, kad į Sutarties kainą yra įtrauktos visos Tiekėjo išlaidos, susijusios su visų Prekių pristatymu, taip pat su tinkamu šioje Sutartyje numatytų kitų Tiekėjo įsipareigojimų įvykdymu, įskaitant draudimus, muitus ir kitokias išlaidas, Tiekėjo patirtas vykdant Sutartyje numatytus įsipareigojimus.
11.4. Sutarties kainos peržiūra atliekama Specialiosiose sąlygose nustatyta tvarka.

12. ATSISKAITYMO TVARKA

12.1. Išankstinis mokėjimas (avansas) (jei taikoma)

12.1.1. Bendrųjų sąlygų 12.1 poskyrio sąlygos taikomos tuo atveju, jei Specialiosiose sąlygose yra nurodyta, kad Tiekėjui mokamas išankstinis mokėjimas (avansas) (toliau – avansas).
12.1.2. Pirkėjas sumoka Tiekėjui avansą – ne daugiau kaip Specialiosiose sąlygose nurodytas avanso dydis.
12.1.3. Jei Specialiosiose sąlygose to reikalaujama, Tiekėjas, norėdamas gauti avansą, kreipdamasis dėl avanso išmokėjimo, ne vėliau kaip per 10 (dešimt) darbo dienų nuo Sutarties įsigaliojimo dienos kartu su išankstinio mokėjimo sąskaita Pirkėjui turi pateikti avanso užtikrinimą – banko garantiją arba draudimo bendrovės laidavimo draudimo raštą arba kitą sutartinių įsipareigojimų įvykdymo užtikrinimą ne mažesnei kaip Specialiosiose sąlygose prašomo avanso dydžio sumai (toliau – Avanso užtikrinimas).
Pastaba. Kai Specialiosiose sąlygose nurodoma, kad Pirkėjas reikalauja pateikti kredito unijos išduotą Avanso užtikrinimą, šio poskyrio nuostatos taikomos pagal poreikį ir Pirkėjas gali nusimatyti papildomus reikalavimus Specialiosiose sąlygose tokio Avanso užtikrinimo pateikimui, atitinkančius įstatymų bei kitų teisės aktų nuostatas.
12.1.4. Prieš pateikdamas Avanso užtikrinimą, Tiekėjas gali prašyti Pirkėjo patvirtinti, kad Pirkėjas sutinka priimti Tiekėjo siūlomą Avanso užtikrinimą. Tokiu atveju, Pirkėjas privalo atsakyti Tiekėjui ne vėliau kaip per 5 (penkias) darbo dienas nuo Tiekėjo prašymo gavimo dienos.
12.1.5. Avanso užtikrinimu bankas (draudimo bendrovė) privalo neatšaukiamai ir besąlygiškai įsipareigoti ne vėliau kaip per 15 (penkiolika) dienų nuo Pirkėjo raštiško pranešimo apie Sutarties neįvykdymą ar Sutarties nutraukimą dėl Tiekėjo kaltės, sumokėti Pirkėjui sumą, neviršijančią išmokėto avanso sumos ir užtikrinimo sumos, pinigus pervedant į Pirkėjo sąskaitą.
12.1.6. Bankas (draudimo bendrovė) neturi teisės reikalauti, kad Pirkėjas pagrįstų savo reikalavimą. Pirkėjas pranešime bankui (draudimo bendrovei) nurodys, kad Avanso užtikrinimo suma jam

priklauso dėl to, kad Tiekėjas iš dalies ar visiškai neįvykdė Sutarties sąlygų ir (arba) ji buvo nutraukta dėl Tiekėjo kaltės ir Tiekėjas negrąžino avanso.
12.1.7. Avanso užtikrinimo suma turi būti nurodoma ir išmokama eurais.
12.1.8. Avanso užtikrinimas turi būti surašytas lietuvių arba kita kalba (esant Pirkėjo prašymui, turi būti pateiktas vertimas į lietuvių kalbą).
12.1.9. Avanso užtikrinimas, neatitinkantis šiame Sutarties poskyryje nustatytų reikalavimų, nebus priimamas.
12.1.10. Jei Sutarties vykdymo metu Avanso užtikrinimą išdavęs bankas (draudimo bendrovė) negali įvykdyti savo įsipareigojimų, Pirkėjas gali raštu pareikalauti Tiekėjo per 10 (dešimt) darbo dienų pateikti naują Avanso užtikrinimą, tokiomis pačiomis sąlygomis kaip ir ankstesnysis.
12.1.11. Pirkėjas sumoka Tiekėjui avansą per Specialiosiose sąlygose numatytą terminą nuo išankstinio mokėjimo sąskaitos ir Avanso užtikrinimo (jei taikoma) gavimo dienos. Sumokėto avanso suma išskaitoma iš mokėtinos sumos.
12.1.12. Nutraukus Sutartį, Tiekėjas privalo grąžinti Pirkėjui gautą avansą per 5 (penkias) darbo dienas (jeigu dalis Prekių pristatyta, Pirkėjas jas yra priėmęs ir jomis gali naudotis pagal paskirtį – grąžinama ta avanso dalis, kuri viršija Pirkėjo priimtų Prekių kainą). Jei Tiekėjas negrąžina gauto avanso, Pirkėjas pasinaudoja Avanso užtikrinimu (jei taikoma). Tais atvejais, jei nebuvo taikytas Bendrųjų sąlygų 12.1.3 punktas, Tiekėjas turi sumokėti Specialiosiose sąlygose nurodyto dydžio netesybas, skaičiuojamas nuo grąžintinos avanso sumos už laikotarpį nuo avanso išmokėjimo iki jo grąžinimo.

12.2. Mokėjimų tvarka

12.2.1. Tiekėjas išrašo Sąskaitą tik Šalims pasirašius Prekių perdavimo–priėmimo aktą, jeigu kitaip nenumatyta Specialiosiose sąlygose:
12.2.1.1. elektroninę sąskaitą faktūrą, atitinkančią Europos elektroninių sąskaitų faktūrų standartą, kurio nuoroda paskelbta 2017 m. spalio 16 d. Komisijos įgyvendinimo sprendime (ES) 2017/1870 dėl nuorodos į Europos elektroninių sąskaitų faktūrų standartą ir sintaksių sąrašo paskelbimo pagal Europos Parlamento ir Tarybos direktyvą 2014/55/ES (toliau – Europos elektroninių sąskaitų faktūrų standartas), Tiekėjas gali pateikti per sąskaitų administravimo bendrąją informacinę sistemą SABIS (https://sabis.nbfc.lt/) arba per kitą savo pasirinktą informacinę sistemą;
12.2.1.2. Europos elektroninių sąskaitų faktūrų standarto neatitinkančią elektroninę sąskaitą faktūrą Tiekėjas privalo pateikti, naudodamasis SABIS priemonėmis (https://sabis.nbfc.lt/).
12.2.2. Pirkėjas elektronines sąskaitas faktūras priima ir apdoroja naudodamasis SABIS priemonėmis, išskyrus VPĮ nustatytus išimtinius atvejus.
12.2.3. Išankstinio mokėjimo sąskaitas (jeigu Specialiosiose sąlygose yra numatytas avanso mokėjimas) Tiekėjas privalo pateikti šiame Sutarties poskyryje nustatyta tvarka.
12.2.4. Pirkėjas atlieka mokėjimus už Prekes Specialiosiose sąlygose nustatytais terminais.
12.2.5. Už mokėjimų pagal Sutartį vėlavimus, Pirkėjui taikomos netesybos Specialiosiose sąlygose nustatyta tvarka.
12.2.6. Jei Prekės pristatomos dalimis, aukščiau nurodyta atsiskaitymo tvarka galioja kiekvienai tokiai daliai, jei Specialiosiose sąlygose nenustatyta kitaip.
12.2.7. Jeigu Šalys sudaro trišalį susitarimą su subtiekėju, Pirkėjas privalo pervesti subtiekėjui mokėtiną sumą į subtiekėjo banko sąskaitą, nurodytą trišaliame susitarime, o likutį pervesti į Tiekėjo banko sąskaitą po to, kai pagal Sutarties ir trišalio susitarimo reikalavimus sudaromas pristatytų Prekių perdavimo–priėmimo aktas ir Tiekėjas pateikia Sąskaitą už Prekes Pirkėjui.

12.3. Kiti atsiskaitymo klausimai

12.3.1. Pirkėjas privalo pervesti mokėjimus Tiekėjui į Tiekėjo banko sąskaitą, nurodytą Specialiosiose sąlygose.

12.3.2. Pirkėjas turi teisę sumas, gautinas iš Tiekėjo, išskaityti iš mokėjimų Tiekėjui pagal Sutartį (vienašališkai daryti įskaitymus). Dėl šios priežasties Tiekėjas neturi teisės perleisti arba įkeisti reikalavimo teisių į gautinas pagal Sutartį sumas tretiesiems asmenims arba kitaip jomis disponuoti be Pirkėjo sutikimo.
12.3.3. Visi mokėjimai pagal Sutartį atliekami eurais.
12.3.4. Už pavėluotus mokėjimus pagal Sutartį mokančioji Šalis privalo sumokėti kitai Šaliai Specialiosiose sąlygose nurodyto dydžio netesybas.

13. KONFIDENCIALI INFORMACIJA

13.1. Šalys įsipareigoja laikytis konfidencialumo ir be kitos Šalies rašytinio sutikimo neatskleisti tos Šalies informacijos, nurodytos kaip konfidencialios, jokiems Šalies darbuotojams, su Šalimi susijusiems ar kitiems tretiesiems asmenims, kuriems nėra būtina šią informaciją naudoti jų darbo tikslais, išskyrus žemiau nurodytus atvejus.
13.2. Šalis turi teisę atskleisti kitos Šalies konfidencialią informaciją šiais atvejais:
13.2.1. konfidencialios informacijos atskleidimas yra būtinas tinkamam Šalies teisių ar pareigų pagal Sutartį įgyvendinimui – tačiau tokiu atveju informaciją galima atskleisti tik ta apimtimi, kiek tai yra reikalinga sutartinių teisių ar pareigų įgyvendinimui, ir tik tokiems tretiesiems asmenims, kuriems būtina, su sąlyga, kad konfidencialią informaciją gaunantys tretieji asmenys prisiima tokius pačius konfidencialumo įsipareigojimus, kokie yra nustatyti šioje Sutartyje. Jeigu tretieji asmenys atskleidžia konfidencialią informaciją, Šalis atsako už jų veiksmus kaip už savo;
13.2.2. konfidencialią informaciją yra būtina atskleisti pagal įstatymų bei kitų teisės aktų reikalavimus, įskaitant atvejus, kai to reikalauja viešojo administravimo subjektai, taip, kai jie apibrėžti Lietuvos Respublikos viešojo administravimo įstatyme.
13.3. Prieš atskleisdama konfidencialią informaciją, Šalis privalo informuoti kitą Šalį (tiek, kiek tai nedraudžiama pagal įstatymus bei kitus teisės aktus) apie būtinybę arba gautą viešojo administravimo subjekto reikalavimą atskleisti konfidencialią informaciją ir imtis protingų priemonių, siekdama užtikrinti atskleistos informacijos konfidencialumą.
13.4. Šalis atsako:
13.4.1. už bet kokį neteisėtą, įskaitant atsitiktinį, kitos Šalies konfidencialios informacijos ar bet kurios jos dalies atskleidimą ar perdavimą arba konfidencialios informacijos neteisėtą naudojimą;
13.4.2. už tai, kad nesiėmė visų protingų veiksmų, kad išsaugotų ir apsaugotų kitos Šalies konfidencialią informaciją ar bet kurią jos dalį, užkirstų kelią tolesniam jos neteisėtam atskleidimui, perdavimui ar naudojimui.
13.5. Šalis nepagrįstai atskleidusi kitos Šalies konfidencialią informaciją privalo sumokėti kitai Šaliai Specialiosiose sąlygose nurodyto dydžio baudą.

14. ASMENS DUOMENŲ APSAUGA

14.1. Šalys įsipareigoja užtikrinti asmens duomenų saugumą bei asmens duomenų tvarkymą vykdyti teisėtai, vadovaujantis 2016 m. balandžio 27 d. priimto Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą, nuostatomis.
14.2. Šalys patvirtina, kad jeigu siekiant užtikrinti tinkamą Sutarties vykdymą bus tvarkomi asmens duomenys, Šalys įsipareigoja sudaryti atskirą susitarimą dėl duomenų tvarkymo, kuriuo nustato duomenų tvarkymo dalyką ir trukmę, duomenų tvarkymo pobūdį ir tikslą, asmens duomenų rūšis ir duomenų subjektų kategorijas bei duomenų valdytojo prievoles ir teises.

15. INTELEKTINĖ NUOSAVYBĖ

15.1. Visi rezultatai ir su jais susijusios teisės, įgytos vykdant Sutartį, įskaitant intelektinės nuosavybės teises, išskyrus asmenines neturtines teises į intelektinės veiklos rezultatus, yra Pirkėjo nuosavybė, pereinanti Pirkėjui nuo Prekių perdavimo–priėmimo momento be jokių apribojimų, kurią Pirkėjas gali naudoti, publikuoti, perleisti ar perduoti be atskiro Tiekėjo sutikimo tretiesiems asmenims, jei Specialiosiose sąlygose nenumatyta kitaip ar intelektinės nuosavybės teisės negali būti perduodamos nuosavybės teise dėl Prekių pobūdžio ar (ir) Prekių gamintojo išimtinių teisių, patentų ir kt.
15.2. Tiekėjas įsipareigoja atlyginti nuostolius Pirkėjui dėl bet kokių reikalavimų, kylančių dėl intelektinės nuosavybės teisių, įskaitant, bet neapsiribojant, dėl patento, prekių ženklo, pramoninio dizaino savininko (naudotojo) teisės (registruojamos arba ne), teisės, kylančios iš paraiškų bet kurioms minėtoms teisėms įregistruoti, autoriaus teisės, duomenų bazių gamintojų (sui generis) teisės, firmų, įmonių, organizacijų, verslo pavadinimų ar vardų savininkų ir kitos panašios teisės ar įsipareigojimai, nepriklausomai nuo to, ar jie registruoti Lietuvos Respublikoje, ar kitose šalyse, ar neregistruotini, kaip numatyta Sutartyje, išskyrus atvejus, kai toks pažeidimas atsiranda dėl Pirkėjo kaltės.
15.3. Tiekėjas neturi teisės be išankstinio rašytinio Pirkėjo sutikimo naudoti Pirkėjo simbolių, pavadinimo ir ženklo reklamoje, rinkodaroje, taip pat naudotis Pirkėjo sukurtais intelektiniais veiklos rezultatais. Pažeidus reikalavimą, Tiekėjui taikoma 1 (vieno) procento bauda nuo Sutarties kainos be PVM.

16. PAREIŠKIMAI IR GARANTIJOS

16.1. Kiekviena iš Šalių pareiškia ir garantuoja kitai Šaliai, kad:
16.1.1. yra teisėtai priimti ir galioja visi būtini sprendimai, gauti leidimai bei sutikimai, taip pat teisėtai atlikti ir galioja kiti teisiniai veiksmai, reikalingi Sutarties sudarymui, galiojimui ir vykdymui;
16.1.2. sudarydama Sutartį, Šalis neviršija savo kompetencijos ir nepažeidžia jai taikomų įstatymų bei kitų teisės aktų, teismo ar arbitražo teismo sprendimų, administracinių aktų, sutarčių ar kitų prievolių pagal taikomą privatinę teisę, viešąją teisę, Europos Sąjungos teisę arba tarptautinę teisę;
16.1.3. Šalies atstovas turi visus reikiamus įgaliojimus sudaryti ir įvykdyti Sutartį; Šalies atstovas, sudarydamas ir pasirašydamas Sutartį, nepažeidžia Šalies įstatų, nuostatų ir kitų vidaus dokumentų, Šalies valdymo ir kitų organų ir (ar) kreditorių teisių ir teisėtų interesų, sudarydamas Sutartį jis Šalies ir Šalies organų narių, kreditorių atžvilgiu veikia sąžiningai ir protingai;
16.1.4. Šalis įvertino visas aplinkybes, turinčias esminės reikšmės Sutarties sudarymui ir jos vykdymui; nė viena iš Sutartyje nurodytų sąlygų ir aplinkybių neturi neigiamos įtakos Šalies valiai sudaryti Sutartį tokiomis sąlygomis, kurios nurodytos Sutartyje, ir vykdyti iš Sutarties kylančius įsipareigojimus;
16.1.5. Sutartis sudaroma vadovaujantis sąžiningumo, protingumo, teisingumo ir Šalių lygiateisiškumo principais, nenaudojant apgaulės ar spaudimo. Šalys atskleidė viena kitai visą joms žinomą informaciją, turinčią esminės reikšmės Sutarties sudarymui ir jos vykdymui;
16.1.6. visi Šalies pareiškimai ir garantijos yra išsamūs ir nepalieka nutylėtų jokių aplinkybių, kurios darytų šiuos pareiškimus ar garantijas neteisingais.
16.2. Tiekėjas papildomai pareiškia ir garantuoja Pirkėjui, kad Tiekėjas, subtiekėjai, jungtinės veiklos partneriai ir specialistai turi galiojančius ir teisėtus visus įstatymuose bei kituose teisės aktuose numatytus leidimus, licencijas, atestatus, teisės pripažinimo dokumentus, reikalingus vykdant Sutartį.
16.3. Tiekėjas pareiškia, kad parduodamų Prekių disponavimo, valdymo ir naudojimosi teisės nėra apribotos ir jokie tretieji asmenys neturi pretenzijų į Sutartimi perduodamas Prekes (įkeitimai, areštai ar pan.).

17. BENDRIEJI ATSAKOMYBĖS KLAUSIMAI

17.1. Netesybų už vėlavimą ar pareigų pagal Sutartį pažeidimą sumokėjimas neatleidžia Šalies nuo Sutartyje numatytų jos pareigų vykdymo.
17.2. Netesybų sumokėjimas ir (ar) Sutarties įvykdymo užtikrinimo gavimas nepanaikina Šalies teisės reikalauti, kad kita Šalis kompensuotų jos patirtus nuostolius. Šioje Sutartyje nustatytos netesybos yra laikomos minimaliais, neįrodinėtinais Šalių nuostoliais. Kiekviena iš Šalių turi teisę gauti iš kitos Šalies nuostolių, atsiradusių dėl kitos Šalies netinkamo įsipareigojimų pagal Sutartį vykdymo ar nevykdymo, neviršijant Pradinės sutarties vertės be PVM, jei teisės aktai nenumato, kad privalo būti kompensuota didesnė suma. Šiame punkte numatytas atsakomybės ribojimas netaikomas, jei žala atsirado dėl konfidencialumo įsipareigojimų, asmens duomenų apsaugą reglamentuojančių teisės aktų ar intelektinės nuosavybės teisių pažeidimo.
17.3. Tuo atveju, jei paaiškėja, kad kuris nors iš šioje Sutartyje pateiktų pareiškimų ar garantijų buvo iš esmės neteisingas, melagingas ar klaidinantis, Šalis pažeidėja nukentėjusiai Šaliai privalo atlyginti visus nuostolius, kuriuos nukentėjusioji Šalis patyrė dėl tokio neteisingo, melagingo ar klaidinančio pareiškimo ar garantijos.
17.4. Šioje Sutartyje numatytos teisių gynybos priemonės neapriboja Šalių teisės pasinaudoti kitomis teisėtomis teisių gynybos priemonėmis.
17.5. Atsakomybės apribojimai pagal Sutartį netaikomi, kai žala padaroma tyčia arba dėl didelio neatsargumo, padaroma neturtinė žala, sužalojama sveikata ar atimama gyvybė, taip pat kai padaroma žala (nuostoliai) tretiesiems asmenims, įskaitant atvejus, jeigu vienos Šalies padarytą žalą tretiesiems asmenims atlygina kita Šalis.
17.6. Pasibaigus Sutarties galiojimui, Šalys neatleidžiamos nuo atsakomybės už Sutarties pažeidimą. Pasibaigus Sutarties galiojimui, Šalys nepraranda teisės reikalauti atlyginti dėl Sutarties nevykdymo patirtus nuostolius bei sumokėti netesybas.

18. NENUGALIMA JĖGA (FORCE MAJEURE)

18.1. Atsakomybė pagal Sutartį netaikoma, taip pat Šalys gali būti visiškai ar iš dalies atleistos nuo civilinės atsakomybės šiais pagrindais:
18.1.1. dėl nenugalimos jėgos (force majeure) – taikomos Lietuvos Respublikos civilinio kodekso 6.212 straipsnio ir Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo" patvirtintų taisyklių nuostatos;
18.1.2. dėl Europos Sąjungos valstybių veiksmų – kai prievolę pagal Sutartį įvykdyti neįmanoma dėl privalomų ir nenumatytų Europos Sąjungos valstybės institucijų veiksmų (aktų), kurių Šalys neturėjo teisės ginčyti ir šie veiksmai negalėjo būti iš anksto numatyti.
18.2. Šalis, prašanti ją atleisti nuo atsakomybės, privalo pranešti kitai Šaliai apie nenugalimos jėgos aplinkybes nedelsiant, bet ne vėliau kaip per 5 (penkias) dienas nuo tokių aplinkybių atsiradimo ar paaiškėjimo, pateikdama įrodymus, kad ji ėmėsi visų pagrįstų atsargumo priemonių ir dėjo visas pastangas, kad sumažintų išlaidas ar neigiamas pasekmes, taip pat pranešti galimą įsipareigojimų įvykdymo terminą. Šalis taip pat turi pateikti kitai Šaliai atitinkamą pranešimą, kai išnyksta įsipareigojimų nevykdymo pagrindas.
18.3. Pagrindas atleisti Šalį nuo atsakomybės atsiranda nuo nenugalimos jėgos aplinkybių atsiradimo momento arba, jeigu laiku nebuvo pateiktas pranešimas, nuo pranešimo pateikimo momento. Jeigu Šalis laiku neišsiunčia pranešimo arba neinformuoja, ji privalo kompensuoti kitai Šaliai žalą, kurią ši patyrė dėl laiku nepateikto pranešimo arba dėl to, kad nebuvo jokio pranešimo.
18.4. Jeigu nenugalimos jėgos (force majeure) aplinkybės tęsiasi ilgiau negu 1 (vieną) mėnesį nuo pranešimo apie jas gavimo dienos, bet kuri Šalis gali nutraukti Sutartį apie tai pranešusi kitai šaliai prieš 5 (penkias) darbo dienas. Nenugalima jėga nelaikoma tai, kad Šalis neturi reikiamų finansinių išteklių arba skolininko kontrahentai pažeidžia savo prievoles, arba skolininkas pažeidžia savo prievoles kontrahentams.

19. SUTARTIES NUOSTATŲ NEGALIOJIMAS

19.1. Jeigu kuri nors Sutarties nuostata yra arba tampa dalinai ar pilnai negaliojanti, Šalys privalo kuo skubiau sudaryti Susitarimą, ir juo pakeisti negaliojančią nuostatą kita nuostata, kuri, kiek tai yra įmanoma, turėtų tokį patį ekonominį ir teisinį efektą, kokio buvo siekta susitariant dėl negaliojančios Sutarties nuostatos. Tokia negaliojanti nuostata nedaro negaliojančiomis kitų Sutarties nuostatų, jeigu tai nepažeidžia įstatymų bei kitų teisės aktų ir galima daryti prielaidą, kad Sutartis būtų buvusi teisėtai sudaryta ir neįtraukus nuostatos, kuri yra negaliojanti.
19.2. Jeigu Specialiosiose sąlygose numatytas Bendrųjų sąlygų nuostatos pakeitimas yra arba tampa dalinai ar pilnai negaliojantis, negali būti taikoma tos Bendrųjų sąlygų nuostatos redakcija, buvusi iki pakeitimo. Tokiu atveju Šalys privalo veikti pagal Bendrųjų sąlygų 19.1 punktą.

20. SUTARTIES PAKEITIMAI

20.1. Sutarties sąlygos Sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias Sutarties sąlygas, kurių keitimas numatytas Sutartyje ir (ar) galimas vadovaujantis VPĮ nuostatomis.
20.2. Sutarties pakeitimai įforminami Šalims sudarant Susitarimą.
20.3. Šalis, inicijuojanti Susitarimą, privalo pateikti kitai Šaliai pranešimą dėl Sutarties pakeitimo bei pagrindimą dėl to, jog yra faktinis ir teisinis pagrindas sudaryti Susitarimą. Kita Šalis per 5 (penkias) darbo dienas (arba per kitą Šalių raštu sutartą terminą) privalo išanalizuoti ir įvertinti gautą informaciją, pateikti savo pastabas ir pasiūlymus, pagrįstus Sutarties arba imperatyviomis įstatymų bei kitų teisės aktų nuostatomis.
20.4. Susitarimai įsigalioja nuo jų sudarymo, jei Susitarime nenurodyta kitaip. Susitarimą Pirkėjas privalo paviešinti VPĮ 33 ir 86 straipsniuose nustatyta tvarka.
20.5. Specialiosiose sąlygose nurodytų duomenų apie kontaktinius asmenis bei rekvizitų pasikeitimas nelaikomas Sutarties pakeitimu (išskyrus Tiekėjo, jungtinės veiklos partnerio, subtiekėjo ar specialisto pakeitimą kitu asmeniu) ir Šalis turi pakeisti tuos duomenis vienašališkai, informuodama apie tai kitą Šalį. Bet kuriuo atveju Sutarties pakeitimu negali būti iš esmės keičiama Sutartis.

21. SUTARTIES SUSTABDYMAS

21.1. Nesant Tiekėjo kaltės ir esant aplinkybėms, kurių Tiekėjas negalėjo numatyti, dėl kurių Tiekėjas negali vykdyti savo sutartinių įsipareigojimų ir (arba) esant kitoms nenumatytoms aplinkybėms, Sutarties šalys turi teisę inicijuoti Prekių (jų dalies) tiekimo sustabdymą iki atitinkamų aplinkybių pasibaigimo.
21.2. Prekių (jų dalies) tiekimas gali būti stabdomas esant bent vienai iš šių aplinkybių:
21.2.1. esant Bendrųjų sąlygų 18 skyriuje numatytoms nenugalimos jėgos aplinkybėms, sutartinių įsipareigojimų vykdymo terminai stabdomi nuo kliūties atsiradimo momento arba jeigu apie ją nėra laiku pranešta, nuo pranešimo momento ir atnaujinami, kai minėtos aplinkybės nebetrukdo vykdyti Sutarties;
21.2.2. Pirkėjas Sutartyje nurodyta tvarka negali priimti Prekių (pavyzdžiui, nebaigta įrengti patalpa, kurioje turi būti įmontuojamos Prekės), o Tiekėjas dėl to negali vykdyti Sutarties;
21.2.3. dėl nenumatytų prekių, paslaugų ir (ar) darbų, susijusių su perkamu objektu, kurių poreikis paaiškėjo tik vykdant Sutartį;
21.2.4. ne dėl Pirkėjo kaltės vėluoja kitos Pirkėjo pirkimo sutarties, turinčios tiesioginės įtakos šiai Sutarčiai, vykdymas;
21.2.5. esant įrodymais pagrįstoms kliūtims ar trukdymams, sukeltiems Tiekėjui kitų trečiųjų asmenų ne dėl Tiekėjo ne laiku ar netinkamai pagal Sutarties sąlygas ir tvarką įvykdytų sutartinių įsipareigojimų;
21.2.6. pasikeitus galiojančiam teisės aktui ar įsigaliojus naujam teisės aktui, kuris turi įtakos šios Sutarties vykdymui;

21.2.7. sutartinių įsipareigojimų stabdymo būtinybė atsirado dėl sustabdyto / perskirstyto / negauto ir panašiai Pirkėjo Prekių pirkimui skirto finansavimo arba finansavimo trūkumo;
21.2.8. dėl teisminių (arbitražinių) ginčų su Pirkėju ar trečiaisiais asmenimis, kurių dalykas yra tiesiogiai susijęs su Sutarties vykdymu.
21.3. Jei Prekių (jų dalies) tiekimo stabdymas atliekamas dėl Bendrųjų sąlygų 21.2 punkte nurodytų aplinkybių ir tęsiasi ne ilgiau kaip 3 (tris) mėnesius, toks stabdymas laikomas Sutarties keitimu joje numatytomis sąlygomis.
21.4. Jei Prekių (jų dalies) stabdymas vykdomas dėl kitų aplinkybių, nenurodytų Bendrųjų sąlygų 21.2 punkte ar (ir) Bendrųjų sąlygų 21.2 punkte nurodytos aplinkybės tęsiasi ilgiau nei 3 (tris) mėnesius ir (ar) nesilaikant šiame skyriuje nustatytos tvarkos, tai laikoma Sutarties keitimu, kuris turi būti atliekamas, vadovaujantis VPĮ nuostatomis.
21.5. Sutartinių įsipareigojimų vykdymas gali būti stabdomas tik Sutarties galiojimo laikotarpiu tokia tvarka:
21.5.1. Atsiradus aplinkybėms, dėl kurių Tiekėjas negali vykdyti sutartinių įsipareigojimų, Tiekėjas apie tai nedelsdamas privalo informuoti Pirkėją. Tiekėjo rašytiniame prašyme turi būti nurodyta stabdymo aplinkybė (Bendrųjų sąlygų 21.2 punktas) ir aplinkybės atsiradimą bei galimą terminą pagrindžiantys argumentai, objektyvūs faktai ir įrodymai. Pirkėjas, įvertinęs prašymą, ne vėliau kaip per 3 (tris) darbo dienas raštu informuoja Tiekėją apie priimtą sprendimą dėl sutartinių įsipareigojimų vykdymo stabdymo. Tiekėjui nepateikus konkrečių argumentų, faktų, pagrįstų įrodymais, Pirkėjas turi teisę raštu atsisakyti patvirtinti stabdymą.
21.5.2. Pirkėjui raštu informavus Tiekėją ir pateikus jam argumentuotą paaiškinimą, dėl kokių aplinkybių ir kuriam terminui yra būtina stabdyti sutartinių įsipareigojimų vykdymo terminą, Tiekėjas ne vėliau kaip per 3 (tris) darbo dienas raštu informuoja Pirkėją ir patvirtina, kad sutinka su stabdymu. Tiekėjas turi teisę prieštarauti sutartinių įsipareigojimų vykdymo stabdymui tik tuo atveju, jei Tiekėjas savo sąskaita ir jėgomis gali pašalinti atsiradusias aplinkybes, dėl kurių kilo būtinybė stabdyti sutartinių įsipareigojimų vykdymą.
21.5.3. Tiekėjas, gavęs Pirkėjo raštišką pranešimą apie stabdymą, privalo nedelsiant, bet ne vėliau kaip per 3 (tris) darbo dienas po patvirtinimo išsiuntimo Pirkėjui dienos, sustabdyti sutartinių įsipareigojimų vykdymą. Jei Sutartis sustabdyta, Šalys negali vykdyti jokių jiems pagal Sutartį priskirtų įsipareigojimų.
21.6. Šalys sutartinių įsipareigojimų vykdymo stabdymą įformina rašytiniu susitarimu, nurodant priežastis ir sustabdymo terminą, bei pridedant dokumentus, patvirtinančius sustabdymo pagrindą, ir patvirtina Šalių įgaliotų atstovų parašais. Tokie susitarimai yra neatskiriama Sutarties dalis.
21.7. Sutartinių įsipareigojimų vykdymas stabdomas ne ilgesniam kaip konkrečios, pagrįstos aplinkybės egzistavimo laikotarpiui.
21.8. Šalys susitaria, kad sutartinių įsipareigojimų vykdymo sustabdymo terminas į Sutarties vykdymo terminą nėra įskaičiuojamas, jo metu sutartiniai įsipareigojimai nevykdomi ir už šį periodą Pirkėjas Tiekėjui nemoka jokių mokėjimų, baudų ar prastovų.
21.9. Jeigu Sutartyje numatytų prievolių įvykdymo terminai buvo sustabdyti Sutartyje nustatytais pagrindais, jie atnaujinami pasibaigus sustabdymą lėmusioms aplinkybėms arba Šalių susitarime nurodytam terminui, priklausomai nuo to, kuris įvyksta anksčiau.
21.10. Atnaujinus Sutarties vykdymą, neįvykdytų prievolių (jų dalies) įvykdymo terminai ir Sutarties galiojimas nukeliami tokiam terminui, kiek buvo likę laiko jų įvykdymui (Sutarties galiojimui) jų sustabdymo metu.
21.11. Jei sutartinių įsipareigojimų vykdymas buvo sustabdytas ilgesniam nei 3 (trijų) mėnesių laikotarpiui, praėjus šiam terminui, viena Šalis gali rašytiniu pranešimu kitos Šalies pareikalauti atnaujinti Sutarties vykdymą. Šaliai be pagrįstų aplinkybių neatnaujinus Sutarties vykdymo per 10 (dešimt) dienų nuo atitinkamo kreipimosi, kita Šalis gali nutraukti Sutartį, apie tai įspėjusi kitą Šalį prieš 10 (dešimt) dienų.

22. SUTARTIES NUTRAUKIMAS

Sutartis gali būti nutraukiama VPĮ 90 straipsnyje ir Sutartyje numatytais atvejais, įskaitant galimybę nutraukti Sutartį Šalių susitarimu.

22.1. Pretenzijos dėl Sutarties pažeidimų

22.1.1. Jeigu Šalis pažeidžia Sutartį arba įstatymus bei kitus teisės aktus, kita Šalis turi teisę pareikšti jai rašytinę pretenziją, nurodyti, kokią Sutarties ar įstatymų bei kitų teisės aktų nuostatą ir kokiu būdu priešinga Šalis pažeidė bei nustatyti protingą terminą ištaisyti pažeidimą.
22.1.2. Pretenziją gavusi Šalis privalo nedelsdama, bet ne vėliau nei per 5 (penkias) darbo dienas, atsakyti į pretenziją ir nurodyti, kokių priemonių imsis siekdama ištaisyti pažeidimą per pretenzijoje nustatytą terminą arba motyvuotai pasiūlyti kitą pagrįstą terminą. Tiekėjo teisė siūlyti kitą terminą nelaikoma Pirkėjo pareiga tą terminą priimti. Pretenziją gavusios Šalies pasiūlytasis terminas pakeičia terminą, nurodytą pretenzijoje, tik jeigu kita Šalis jį patvirtina.

22.2. Sutarties nutraukimas Pirkėjo iniciatyva

22.2.1. Pirkėjas vienašališkai nutraukia Sutartį, įspėjęs Tiekėją raštu prieš ne trumpesnį nei 5 (penkių) dienų terminą, jeigu Tiekėjas padaro esminį Sutarties pažeidimą, nurodytą Specialiosiose sąlygose. Pirkėjas taip pat turi teisę nutraukti Sutartį, jeigu Tiekėjas padaro Sutarties pažeidimą, kuris atitinka esminio Sutarties pažeidimo požymius, nurodytus Lietuvos Respublikos civiliniame kodekse, ir, gavęs Pirkėjo pretenziją, per pretenzijoje nurodytą terminą neištaiso pažeidimo.
22.2.2. Pirkėjas turi teisę vienašališkai nutraukti Sutartį ar jos dalį raštu įspėjęs Tiekėją prieš ne trumpesnį nei 10 (dešimties) dienų terminą, jeigu:
22.2.2.1. Tiekėjui yra iškelta bankroto byla, pradėtas bankroto procesas ne teismo tvarka, jis tampa nemokus arba yra nemokumo tikimybė, sustabdo ūkinę veiklą ar susidaro įstatymuose ir kituose teisės aktuose nustatyta tvarka analogiška situacija;
22.2.2.2. Tiekėjo padėtis pasikeičia ir jis atitinka pirkimo dokumentuose nustatytą pašalinimo pagrindą, kuris taikomas ir Sutarties galiojimo metu;
22.2.2.3. pasikeičia teisės aktai, susiję su Sutarties objektu, Sutarties vykdymu, ar su Pirkėjo vykdoma veikla, kuriai buvo sudaryta Sutartis, ir dėl tokių pakeitimų Pirkėjas nusprendžia nutraukti Sutartį;
22.2.2.4. Pirkėjas nusprendžia nebevykdyti veiklos, kurios vykdymui Sutartimi įsigyjamos Prekės ir Sutarties poreikis išnyksta;
22.2.2.5. Pirkėjo valdymo organas priima sprendimą, dėl kurio Sutarties poreikis išnyksta;
22.2.2.6. pasikeičia (pablogėja) Pirkėjo finansinė padėtis ar Pirkėjas negauna / netenka finansavimo ir dėl šios priežasties nusprendžia nutraukti Sutartį;
22.2.2.7. keičiasi Pirkėjo organizacinė struktūra – juridinis statusas, pobūdis ar valdymo struktūra ir tai gali turėti įtakos tinkamam Sutarties įvykdymui arba Sutarties poreikiui;
22.2.2.8. nebelieka perkamų Prekių poreikio;
22.2.2.9. Pirkėjas iš pirkimų priežiūrą atliekančių institucijų gauna nurodymą / rekomendaciją nutraukti Sutartį;
22.2.2.10. Tiekėjas vėluoja pateikti Sutarties įvykdymo užtikrinimo pratęsimą ilgiau kaip 10 (dešimt) darbo dienų nuo paskutinio Sutarties įvykdymo užtikrinimo galiojimo termino pabaigos arba atsisako jį pateikti;
22.2.2.11. Tiekėjas atsisako pašalinti arba nepašalina Prekių trūkumų per Pirkėjo nustatytus protingus terminus;
22.2.2.12. Tiekėjas pažeidžia Sutartį arba įstatymus bei kitus teisės aktus ir per Pirkėjo rašytinėje pretenzijoje nurodytą terminą neištaiso pažeidimo.
22.2.3. Sutartis laikoma niekine ir negaliojančia, jei nustatoma, kad Sutarties vykdymas prieštarauja Lietuvos Respublikoje įgyvendinamoms privalomoms tarptautinėms sankcijoms, kaip tai apibrėžta Sankcijų įstatyme ir kituose tarptautiniuose, Europos Sąjungos ir Lietuvos Respublikos teisės aktuose

(bent vienai iš taikomų sankcijų). Sutarties negaliojimo momentas nustatomas vadovaujantis minėtu įstatymu.
22.2.4. Pirkėjas nedelsiant, bet ne vėliau kaip per 5 (penkias) dienas, vienašališkai nutraukia Sutartį arba sustabdo jos vykdymą privalomų tarptautinių sankcijų, kaip tai apibrėžta Sankcijų įstatyme ir kituose tarptautiniuose, Europos Sąjungos ir Lietuvos Respublikos teisės aktuose, įgyvendinimo laikotarpiui, apie tai įspėjęs Tiekėją raštu, jei Sutartis įsigaliojo iki šių tarptautinių sankcijų Lietuvos Respublikoje įgyvendinimo nustatymo. Draudžiama prisiimti naujas prievoles pagal Sutartį, kurių vykdymas prieštarautų Lietuvos Respublikoje įgyvendinamoms tarptautinėms sankcijoms.
22.2.5. Jei Sutartis nutraukiama Tiekėjui iš esmės pažeidus Sutartį ar Tiekėjui nepagrįstai nutraukus Sutarties vykdymą ne Sutartyje nustatyta tvarka, ir jeigu Specialiosiose sąlygose nėra numatyta, kad tinkamas Sutarties įvykdymas yra užtikrinamas Sutarties įvykdymo užtikrinimu, Tiekėjas įsipareigoja sumokėti Pirkėjui Specialiosiose sąlygose nurodyto dydžio baudą ir atlyginti nuostolius, susijusius su Sutarties nutraukimu. Jeigu Specialiosiose sąlygose yra numatyta, kad tinkamas Sutarties įvykdymas yra užtikrinamas Sutarties įvykdymo užtikrinimu, Tiekėjas įsipareigoja Pirkėjui sumokėti likusią dalį Specialiosiose sąlygose nurodyto dydžio baudos ir atlyginti nuostolius, susijusius su Sutarties nutraukimu, kiek jų nepadengia Sutarties įvykdymo užtikrinimas. Pirkėjui pareiškus reikalavimą atlyginti patirtus nuostolius, baudos suma įskaitoma į nuostolių atlyginimą.
22.2.6. Pirkėjas turi teisę vienašališkai nutraukti Sutartį ir kitais Specialiosiose sąlygose (jei taikoma) ir įstatymuose bei kituose teisės aktuose įtvirtintais atvejais.
22.2.7. Sutartis laikoma nutraukta kitą dieną po to, kai pasibaigia įspėjimo apie Sutarties nutraukimą terminas.
22.2.8. Tais atvejais, kai Tiekėjas pašalina pažeidimą ar išnyksta aplinkybės, dėl kurių buvo inicijuota Sutarties nutraukimo procedūra, Sutartis negali būti nutraukiama ir įspėjimas apie Sutarties nutraukimą netenka galios, jei Tiekėjas informuoja Pirkėją apie pašalintą pažeidimą ar išnykusias aplinkybes, dėl kurių buvo inicijuota Sutarties nutraukimo procedūra.

22.3. Sutarties nutraukimas Tiekėjo iniciatyva

22.3.1. Tiekėjas turi teisę vienašališkai nutraukti Sutartį, įspėjęs Pirkėją raštu prieš ne trumpesnį nei 30 (trisdešimties) dienų terminą, jeigu Pirkėjas pažeidžia atsiskaitymo su Tiekėju terminus (išskyrus atvejus, kai Pirkėjas naudojasi savo teise sulaikyti mokėjimus), ir Pirkėjo skola Tiekėjui viršija 20 (dvidešimt) proc. Pradinės sutarties vertės be PVM ir Pirkėjas, gavęs Tiekėjo pretenziją, per 30 (trisdešimt) dienų nesumoka Tiekėjui mokėtinų sumų.
22.3.2. Tiekėjas turi teisę vienašališkai nutraukti Sutartį, įspėjęs Pirkėją raštu prieš ne trumpesnį nei 10 (dešimties) dienų terminą, jeigu:
22.3.2.1. Pirkėjui yra iškelta bankroto byla, pradėtas procesas dėl bankroto ne teismo tvarka, jis tampa nemokus arba yra nemokumo tikimybė, Pirkėjas sustabdo veiklą, arba įstatymuose ir kituose teisės aktuose numatyta tvarka susidaro analogiška situacija;
22.3.2.2. Pirkėjas pažeidžia Sutartį arba įstatymus bei kitus teisės aktus ir per Tiekėjo rašytinėje pretenzijoje nurodytą terminą neištaiso pažeidimo, išskyrus Bendrųjų sąlygų 22.3.1 punkte nustatytą atvejį.
22.3.3. Jeigu Bendrųjų sąlygų 22.3.1 punkte nurodytos aplinkybės yra susijusios tik su atskira dalimi arba atskiru Susitarimu, Tiekėjas turi teisę nutraukti Sutartį tik tos dalies atžvilgiu arba nutraukti tik tokį Susitarimą.
22.3.4. Tiekėjas turi teisę vienašališkai nutraukti Sutartį ir kitais įstatymuose bei kituose teisės aktuose įtvirtintais atvejais.
22.3.5. Jei Sutartis nutraukiama Pirkėjui iš esmės pažeidus Sutartį ar Pirkėjui nepagrįstai nutraukus Sutarties vykdymą ne Sutartyje nustatyta tvarka, Pirkėjas įsipareigoja sumokėti Tiekėjui Specialiosiose sąlygose nurodyto dydžio baudą ir atlyginti nuostolius, susijusius su Sutarties nutraukimu.

22.3.6. Sutartis laikoma nutraukta kitą dieną po to, kai pasibaigia įspėjimo apie Sutarties nutraukimą terminas.
22.3.7. Tais atvejais, kai per įspėjimo apie Sutarties nutraukimą terminą Pirkėjas pašalina pažeidimą arba išnyksta aplinkybės, dėl kurių buvo inicijuota Sutarties nutraukimo procedūra, Sutartis negali būti nutraukiama ir įspėjimas apie Sutarties nutraukimą netenka galios, jei Pirkėjas informuoja apie pašalintą pažeidimą arba išnykusias aplinkybes, dėl kurių buvo inicijuota Sutarties nutraukimo procedūra, Tiekėją.

22.4. Šalių teisės ir pareigos Sutarties nutraukimo atveju

22.4.1. Sutarties nutraukimas neturi įtakos ginčų nagrinėjimo tvarką nustatančių Sutarties sąlygų ir kitų Sutarties sąlygų, kurios pagal savo esmę lieka galioti ir po Sutarties nutraukimo, galiojimui.
22.4.2. Nutraukus Sutartį, Šalys privalo:
22.4.2.1. įsitikinti, jog iki Sutarties nutraukimo dienos pristatytos Prekės ir kiti atlikti veiksmai atitinka Sutarties reikalavimus ir Šalys dėl to viena kitai nebereikš pretenzijų;
22.4.2.2. atsiskaityti už iki Sutarties nutraukimo pristatytas Prekes, atitinkančias Sutarties reikalavimus;
22.4.2.3. per 10 (dešimt) dienų nuo pranešimo apie Sutarties nutraukimą gavimo dienos ar Susitarimo dėl Sutarties nutraukimo sudarymo dienos perduoti viena kitai visus dokumentus, kuriuos buvo būtina perduoti pagal Sutarties nuostatas.

23. PREKIŲ MODELIO AR GAMINTOJO KEITIMAS

23.1. Tiekėjas turi teisę keisti Prekių modelį ar gamintoją, jei yra visos toliau nurodytos sąlygos:
23.1.1. jei Tiekėjo pasiūlyme nurodytos Prekės nebegaminamos ar iš esmės sutriko jų tiekimas ir gautas gamintojo patvirtinimas ir (ar) Prekės, jų gamintojas kelia grėsmę nacionaliniam saugumui ir (ar) Prekių tiekimas prieštarauja Lietuvos Respublikoje įgyvendinamoms privalomoms tarptautinėms sankcijoms, kaip tai apibrėžta Sankcijų įstatyme ir (ar) Prekės, jų sudedamosios dalys ar (ir) gamintojas neatitinka VPĮ 45 straipsnio 21 dalies nuostatų;
23.1.2. jei keičiamos Prekės visiškai atitinka visus pirkimo dokumentų reikalavimus, yra ne prastesnės, o lygiavertės ar geresnės kokybės nei Tiekėjo pasiūlyme nurodytos Prekės ir Tiekėjas pateikia tai patvirtinančius dokumentus. Jeigu pirkimo procedūrų metu Tiekėjas buvo pateikęs Prekių pavyzdžius, pristatomos Prekės turi būti ne prastesnės kokybės nei pateikti pavyzdžiai;
23.1.3. jei Tiekėjas, ne vėliau kaip prieš 10 (dešimt) dienų iki numatomo Prekių keitimo, pateikė Pirkėjui rašytinį prašymą su keitimą pagrindžiančiais dokumentais bei gavo Pirkėjo rašytinį sutikimą. Pirkėjas turi teisę nesutikti su Prekės keitimu ir turi teisę nutraukti Sutartį, jei Tiekėjas nepateikė įrodymų ar jų pateikimas nepagrindžia keičiamos Prekės atitikimo pirkimo dokumentams ir lygiavertiškumo ar geresnės kokybės nei šiuo metu tiekiamos Prekės;
23.1.4. Šalys sudarė rašytinį susitarimą prie Sutarties dėl Prekių keitimo.
23.2. Šiame Bendrųjų sąlygų skyriuje nurodytu atveju Prekės turi būti pristatytos už ne didesnę nei pasiūlyme nurodytą kainą.

24. BENDRAVIMO TVARKA IR KALBA

24.1. Sutartis sudaroma lietuvių kalba. Jeigu Sutartis ar kuris nors ją sudarantis dokumentas sudaromas kita kalba arba išverčiamas į kitą kalbą, visais atvejais autentišku laikomas tik lietuvių kalba parengtas Sutarties tekstas (jei yra neatitikimų, pirmenybė teikiama lietuvių kalba parengtam tekstui).
24.2. Jeigu Šalis praneša kitai Šaliai apie savo naujus kontaktinius duomenis, tai po to, kai kita Šalis gauna tokį pranešimą, ji visus remiantis Sutartimi siunčiamus pranešimus ir informaciją turi siųsti pagal naujuosius kontaktinius duomenis. Jei Šalis nepraneša apie kontaktinių duomenų pasikeitimą

arba kol kita Šalis negauna tokio pranešimo, pranešimo išsiuntimas pagal paskutinius Šaliai žinomus kontaktinius duomenis laikomas tinkamu.
24.3. Jeigu pranešimas yra įteikiamas asmeniškai arba siunčiamas paštu ar per kurjerį, jis turi būti įteikiamas pasirašytinai ir laikomas gautu gavimo patvirtinime nurodytą dieną.
24.4. Jeigu pranešimas siunčiamas el. paštu, laikoma, kad Šalis jį gavo kitą darbo dieną.
24.5. Jeigu pranešimas siunčiamas keliais skirtingais būdais, laikoma, kad gavėjas jį gavo tada, kai jis gavo pirmesnįjį pranešimą.

25. PRETENZIJOS IR GINČŲ SPRENDIMAS

25.1. Bet kokie ginčai, nesutarimai ar reikalavimai, kylantys iš Sutarties arba susiję su Sutartimi, jos pažeidimu, nutraukimu ar galiojimu, visų pirma privalo būti sprendžiami derybomis tarp Šalių vadovų arba jų įgaliotų asmenų.
25.2. Jeigu Šalys neišsprendžia ginčo derybų būdu tuomet toks ginčas, nesutarimas ar reikalavimas, kylantis iš šios Sutarties arba susijęs su ja ar jos pažeidimu, nutraukimu arba negaliojimu, yra galutinai sprendžiamas Lietuvos Respublikos teismuose Lietuvos Respublikos įstatymuose nustatyta tvarka.
25.3. Kilę ginčai nesudaro pagrindo Šalims atsisakyti vykdyti savo prievoles pagal Sutartį.

Nuorašas

1 priedas

VALSTYBĖS ĮMONĖS
IGNALINOS ATOMINĖS ELEKTRINĖS
FIZINĖS SAUGOS SKYRIUS

TVIRTINU

PATEKIMO KONTROLĖS SISTEMOS PIRKIMO TECHNINĖ SPECIFIKACIJA

2025 m. balandžio 16 d. Nr. Spc-25(13.66E)
Visaginas

I. PIRKIMO TIPAS

1. Prekių pirkimas.

II. TIKSLAS

2. Siekiant efektyvinti VĮ Ignalinos atominės elektrinės (toliau – IAE) objektų fizinę saugą bei atnaujinti nusidėvėjusias fizinės saugos sistemas būtina įsigyti techninėje specifikacijoje nurodytą įrangą su montavimo paslaugomis.

3. Perkamos saugai svarbios prekės.

III. PREKIŲ APRAŠYMAS IR TIEKIMO APIMTIS

4. Perkama sistema (su montavimo paslaugomis), sudaryta iš:

4.1. Patekimo kontrolės sistemos (toliau - PKS) programinės įrangos (toliau - PĮ) serveriui (1 vnt.) ir darbo stotims (9 vnt.), techniniai reikalavimai nurodyti 1 lentelėje;

4.2. PKS leidimų kortelių (3000 vnt.), techniniai reikalavimai nurodyti 3 lentelėje;

4.3. PKS skaitytuvų su klaviatūra (maksimalus kiekis 78 vnt., preliminariai planuojama įsigyti ne mažiau kaip 70 vnt.), techniniai reikalavimai nurodyti 4 lentelėje;

4.4. PKS skaitytuvų be klaviatūros (maksimalus kiekis 67 vnt., preliminariai planuojama įsigyti ne mažiau kaip 60 vnt.), techniniai reikalavimai nurodyti 5 lentelėje;

4.5. PKS kortelių spausdintuvų (2 vnt.), techniniai reikalavimai nurodyti 6 lentelėje;

4.6. Durų procesoriai (kiekis priklauso nuo siūlomos įrangos tipo);

4.7. Kompiuterių tinklo komutatoriai (kiekis priklauso nuo siūlomos įrangos tipo);

4.8. Vartų valdymo pultas (1 vnt.);

4.9. Fotografavimo įrenginiai su tvirtinimo prie sienos laikikliais (2 vnt.) , techniniai reikalavimai nurodyti 7 lentelėje;

4.10. Vartelių užblokavimo mechanizmai (7 vnt.), valdomi per durų procesorius;

4.11. Durų užblokavimo mechanizmai (2 vnt.), valdomi per durų procesorius.

5. Esamos PKS (skirtingos) branduolinės energetikos objektuose, kurias būtina pakeisti ir sujungti į vieną sistemą:

a. Sistema Nr. 1

Eil. Nr.	Patalpos (pastato) Nr. su PKS įranga	Prijungtų skaitytuvų skaičius
1.	LPBKS 01 past. R026 pat.	20 (1 turniketas, 8 durys, 2 valdymo pultai (toliau - VP))
2.	LPBKS 21 past. R114 pat.	10 (2 turniketai, 3 durys)
3.	LPBKS 02 past. R008 pat.	4 (1 turniketas, 1 durys)
4.	LMRAA (B19/2) 02 past. 105 pat.	9 (1 turniketas, 3 durys, 1 VP)

Visos patalpos sujungtos optinio tinklo komunikacijomis, visi skaitytuvai prijungti UTP 5-tos kategorijos kabeliu.

b. Sistema Nr. 2

Eil. Nr.	Patalpos (pastato) Nr. su PKS įranga	Prijungtų skaitytuvų skaičius
1.	IAE 185 past. 113 pat.	28 (8 turniketai, 6 durys)
2.	IAE 140/2 past. 105 pat.	6 (2 turniketai, 1 durys)
3.	IAE 140/1 past.	6 (2 turniketai, 1 durys)
4.	IAE 187/2	2 (1 durys)
5.	IAE 185A past.	6 (3 durys)
6.	IAE 101/1 past. D0 blokas 301 pat.	10 (3 turniketai, 2 durys)
7.	IAE 101/1 past. D1 blokas	4 (1 turniketas, 1 durys)
8.	IAE 101/1 past. D2 blokas	4 (1 turniketas, 1 durys)
9.	PBKS 194 past. 107 pat.	5 (2 durys, 1 VP)
10.	PBKS 196 past.	8 (1 turniketas, 2 durys, 1 VP, 1 durys su vienu skaitytuvu)
11.	PBKS 196A past.	3 (2 durys su vienu skaitytuvu, 1 VP)
12.	IAE 187/1A past.	7 (3 durys, 1 VP)
13.	IAE 187/3 past.	5 (2 durys, 1 VP)
14.	IAE KAIK 05 past.	8 (1 turniketas, 3 durys)

Visos patalpos sujungtos optinio tinklo komunikacijomis, visi skaitytuvai prijungti FKAR-PG-2x2x0,5 (naujesnė kabelio versija yra FQAR-PG-2x2x0,5) vytos poros kabeliu. Atstumai nuo durų procesorių iki skaitytuvų – iki 300 m.

6. Prekės, kartu su montavimo paslaugomis tiekiamos etapais:

6.1. ne vėliau nei per 90 kalendorinių dienų nuo sutarties pasirašymo dienos privalo pristatyti, suinstaliuoti ir suderinti/sukonfigūruoti PĮ (atitinkančias 1 lentelės reikalavimus, konfigūravimas atliekamas pasinaudojant siūlomos programinės įrangos funkcionalumu pagal Užsakovo pateiktas pastabas dėl bendro sistemos veikimo) į Užsakovo pateiktą dedikuotą serverį su techniniais parametrais, nurodytais 2 lentelėje (jei pateikto serverio techniniai parametrai neatitinka reikalingų PĮ įdiegimui, šio pirkimo apimtyje būtina numatyti serverio techninės įrangos išplėtimą iki programinės įrangos gamintojo numatytų parametrų arba naujo serverio pateikimą), pristatyti leidimų korteles (atitinkančias 3 lentelės reikalavimus), pristatyti, prijungti ir sukonfigūruoti kortelių spausdintuvus (2 vnt.) su eksploatacinėmis medžiagomis (3000 kortelių atspausdinti) bei

kitą įrangą, kurią sujungus į vientisą sistemą būtų galima pradėti leidimų kortelių programavimą, spausdinimą bei patekimo zonų priskyrimą. Įgyvendinus šį etapą užsakovas planuoja atlikti kortelių programavimo ir spausdinimo darbus, kurie preliminariai užtruks iki 90 kalendorių dienų. Tik užbaigus šiuos darbus bus Tiekėjas galės pradėti vykdyti antrą etapą;

6.2. Ne vėliau kaip per 90 kalendorinių dienų nuo užsakovo rašto apie montavimo paslaugų pradžią Tiekėjas privalo:

6.2.1. atlikti skaitytuvų (minimalūs techniniai reikalavimai skaitytuvams nurodyti 4 ir 5 lentelėse) bei visos kitos įrangos (durų procesorių, tinklo komutatorių ir t.t.), reikalingos sistemos normaliai eksploatacijai, sumontavimo darbus (esamos įrangos demontavimą vykdys Užsakovo darbuotojai), taip pat įvertinant, kad esamų skaitytuvų tvirtinimo prie sienos, ar turniketo konstrukcijos laikikliai gali netikti naujiems skaitytuvams, todėl laikikliai turi būti įtraukti į šio tiekimo apimtį;

6.2.2. pateikti ir sumontuoti vartų valdymo pultą 187/1A pastate (4 vartų ir 2 antitaraninių įrenginių valdymui, kiekvieno įrenginio valdymui skiriant ne mažiau kaip 3 valdymo mygtukus (atidaryti/stop/uždaryti) ir su vienu bendru stop mygtuku bei 2 šviesoforų valdymui, kiekvieno šviesoforo valdymui skiriant 2 mygtukus (raudona/žalia)) su autorizacija (skaitytuvas su klaviatūra įtrauktas į šios techninės specifikacijos apimtį);

6.2.3. atlikti vietoje šiuo metu naudojamų išėjimo mygtukų (12 durų) skaitytuvų be klaviatūros (į šios techninės specifikacijos apimtį įtraukti) sumontavimo bei komunikacinių linijų (vienoms durims iki 20 m. atstumu, bendrai – iki 480 m.) pratiesimo ir sujungimo darbus (čia ir žemiau esančiuose punktuose: komunikacinių linijų tiesimui reikalavimai nekeliami, montavimas turi būti atliktas užtikrinant gaisrinės ir elektrosaugos reikalavimus);

6.2.4. atlikti 7 vartelių skaitytuvų (į šios techninės specifikacijos apimtį įtraukti) sumontavimo ir komunikacijų pratiesimo darbus, įtraukiant į tiekimo apimtį vartelių užrakinimo mechanizmus, valdomus per durų procesorius;

6.2.5. pateikti ir atlikti fotografavimo įrangos (vaizdo kameros ar fotoaparato, sumontuoto ant sienos ir prijungto prie darbo stoties ne ilgesniu nei 10 m. USB ar Ethernet kabeliu), skirtos darbuotojų nuotraukų fotografavimui leidimų kortelėms, sumontavimo darbus (2 vnt.);

6.2.6. atlikti 2 durų į patalpas (bus nurodytos sistemos įdiegimo metu) skaitytuvų sumontavimo ir komunikacijų pratiesimo darbus, įtraukiant į tiekimo apimtį durų užrakinimo mechanizmus, valdomus per skaitytuvus;

6.2.7. užbaigus sistemos įdiegimo darbus turi būti parengtas su Užsakovu suderintas techninis darbo projektas.

1 lentelė. Programinės įrangos techniniai reikalavimai

Eil. Nr.	Reikalavimas	Reikšmė	Kiekis, vnt.
1.	Vartotojų valdymo modulis.	Turi būti	1

2.	Prieigos kontrolės modulis.	Turi būti	
3.	Prieigų planavimo modulis.	Turi būti	
4.	Modulis, leidžiantis rengti leidimų “panaudojimo” ataskaitas, pagal duomenis esančius PKS	Turi būti	
5.	Modulis, generuojantis aliarminius pranešimus: bandymas patekti neturint leidimo ir pan.	Turi būti	
6.	Modulis, leidžiantis atlikti įrenginių, konfigūravimą.	Turi būti	
7.	Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams.	Turi būti	
8.	„Anti-passback“ funkcija	Turi būti	
9.	Duomenų bazės tipas SQL	Turi būti	
10.	Programinė įranga ne mažiau kaip 9 darbo stotims	Turi būti	
11.	Licencija (jei reikalinga) prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 10 durų su skaitytuvais papildomai	Turi būti	

2 lentelė. Serverio techniniai reikalavimai

Eil. Nr.	**Reikalavimas**	**Reikšmė**
1.	Modelis	PowerEdge R360 Server
2.	Procesorius	Intel® Xeon® E-2456 3.3G, 6C/12T, 18M Cache, Turbo, HT (80W) DDR5
3.	Operatyvinė atmintis	32GB UDIMM, 4800MT/s ECC
4.	Operacinė sistema	Windows Server 2022 Standard,16CORE,FI,No Med,No CAL, Multi Language
5.	Kietasis diskas	2TB Hard Drive SATA 6Gbps 7.2K 512n 3.5in Hot-Plug
6.	Pagrindinė plokštė su tinklo plokšte	PowerEdge R360 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM

3 lentelė. Leidimų kortelių minimalūs techniniai reikalavimai

Eil. Nr.	**Reikalavimas**	**Reikšmė**	**Kiekis, vnt.**
1.	Veikimo dažnis 13,56MHz	Turi būti	3000
2.	DESFire® EV3 lustas	Turi būti	
3.	Palaikomas standartas	ISO14443A arba lygiavertis	
4.	Spalva	Balta	
5.	Galimybė veikti -25° iki +40° temperatūros intervale	Turi būti	

4 lentelė. Minimalūs skaitytuvo su klaviatūra techniniai reikalavimai

Eil. Nr.	Reikalavimas	Reikšmė	Maksimalus kiekis, vnt.
1.	Klaviatūra	Turi būti	78
2.	Šviesos indikatoriai	Turi būti	
3.	Garsinis signalas	Turi būti	
4.	13,56MHz perdavimo dažnis,	Turi būti	
5.	Darbinė įtampa	12V DC	
6.	Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas	Turi būti	
7.	OSDP duomenų perdavimo protokolas,	Turi būti	
8.	Atsparumo aplinkos poveikiui klasė, ne žemesnė	IP65	
9.	Galimybė veikti -20° iki +60° temperatūros intervale	Turi būti	

5 lentelė. Minimalūs skaitytuvo be klaviatūros techniniai reikalavimai

Eil. Nr.	Reikalavimas	Reikšmė	Maksimalus kiekis, vnt.
1.	Šviesos indikatoriai	Turi būti	67
2.	Garsinis signalas	Turi būti	
3.	13,56MHz perdavimo dažnis,	Turi būti	
4.	Darbinė įtampa	12V DC	
5.	Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas	Turi būti	
6.	OSDP duomenų perdavimo protokolas,	Turi būti	
7.	Atsparumo aplinkos poveikiui klasė, ne žemesnė	IP65	
8.	Galimybė veikti -20° iki +60° temperatūros intervale	Turi būti	

6 lentelė. Kortelių spausdintuvo minimalūs techniniai reikalavimai

Eil. Nr.	Reikalavimas	Reikšmė	Kiekis, vnt.
1.	USB, Ethernet jungtys	Turi būti	2
2.	Galimybė spausdinti spalvotai	Turi būti	
3.	Spalvoto spausdinimo rezoliucija, ne mažiau	300x300 dpi	
4.	Specializuota spausdintuvo programinė įranga	Turi būti	

5.	Eksploatacinės medžiagos 3000 spalvotų kortelių spausdinimui	Turi būti	
6.	Galimybė spausdinti ant leidimų kortelių su šios techninės specifikacijos 3 lentelėje nurodytais parametrais	Turi būti	

7 lentelė. Fotografavimo įrenginių minimalūs techniniai reikalavimai

Eil. Nr.	Reikalavimas	Reikšmė	Kiekis, vnt.
1.	Maksimali vaizdo raiška, ne mažesnė	4K Ultra HD (3840 x 2160)	2
2.	Matymo kampas (Field of View - FOV)	Reguliuojamas	
3.	Jungties tipas USB	Turi būti	

IV. REIKALAVIMAI SAUGAI SVARBIŲ PRODUKTŲ BRANDUOLINĖS ENERGETIKOS OBJEKTO AIKŠTELĖJE PIRKIMUI

7. Tiekėjas privalo vadovautis šiais dokumentais (aktualiomis redakcijomis):

7.1. Branduolinės saugos reikalavimai BSR-1.6.1-2019 „Branduolinės energetikos objektų, branduolinės energetikos objektų aikštelių, branduolinių ir branduolinio kuro ciklo medžiagų fizinė sauga“;

7.2. VĮ IAE saugai svarbių produktų tiekėjų ir subtiekėjų vertinimo bei jų veiklos kontrolės tvarkos aprašas, DVSta-1708-4 (https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103);

7.3. Valstybės įmonės Ignalinos atominės elektrinės branduolinės energetikos objektų fizinės saugos užtikrinimo tvarkos aprašas, DVSta-2108-6 (https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103);

8. Tiekėjas privalo užtikrinti galimybes įgaliotiems VĮ IAE darbuotojams ir/arba įgaliotiems VATESI darbuotojams dalyvauti produktų bandymuose ir priėmimuose, atlikti nepriklausomus Tiekėjo (visų lygių subtiekėjų) veiklos patikrinimus (auditus, inspekcijas ir pan.). Neatitiktys, nustatytos šių tikrinimų metu, privalo būti šalinamos laiku, bet ne vėliau kaip iki sutarties pabaigos. Tiekėjas turi suteikti galimybes įgaliotiems IAE darbuotojams ir / arba įgaliotiems VATESI darbuotojams įsitikinti, ar vykdomi pirkimo dokumentų, sutarties, kokybės užtikrinimo plano, vadybos sistemos dokumentų reikalavimai, t.y. pagal užklausą privalo pateikti susijusius dokumentus.

9. Tiekėjas privalo parengti Kokybės užtikrinimo planą pagal VĮ IAE nustatytus reikalavimus (VĮ IAE saugai svarbių produktų tiekėjų ir subtiekėjų vertinimo bei jų veiklos kontrolės tvarkos aprašas, DVSta-1708-4 (https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103)). Parengtą Kokybės užtikrinimo planą tiekėjas privalo suderinti su VĮ IAE ne vėliau kaip per 30 kalendorinių dienų nuo sutarties įsigaliojimo. Kokybės užtikrinimo plano forma patalpinta adresu: https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103.

10. Reikalavimai dėl Kokybės užtikrinimo plano rengimo ir derinimo netaikomi, jei siūlomos standartinės, serijinės gamybos prekės (angl. COTS – comercial off-the-shelf products), t. y. prekės, pritaikytos ir parduodamos plačiai visuomenei, kurioms pagaminti nereikia papildomo projektavimo ir specialaus pritaikymo konkrečiam užsakovui.

V. REIKALAVIMAI DARBŲ/PASLAUGŲ BEO AIKŠTELĖJE PIRKIMUI

11. Tiekėjo (ir visų lygių subtiekėjų) personalas prieš pradėdamas vykdyti veiklą VĮ IAE priklausančiose BEO aikštelėse, privalo VĮ IAE:

11.1. Žmonių ir organizacijos vystymo skyriaus Kompetencijų centre išklausyti saugos kultūros ir fizinės saugos mokymų kursus;

11.2. Saugos priežiūros ir kokybės valdymo skyriaus Saugos priežiūros grupėje išklausyti įvadinį instruktažą apie civilinę saugą ir avarinę parengtį.

11.3. Žmonių ir organizacijos vystymo skyriaus Kompetencijų centre būti apmokytas ir atestuotas gaisrinės ir radiacinės saugos (radiacinės saugos mokymai būtini tuo atveju, jei gaunamas Lietuvos Respublikos įgaliotos institucijos išduodamas dokumentas, suteikiantį teisę vykdyti veiklą jonizuojančios spinduliuotės aplinkoje branduolinės energetikos objekte) klausimais pagal Rangovinių organizacijų, vykdančių darbus IAE, personalo mokymo programą, MC-1410-23.

12. Teikdamas paslaugas BEO kontroliuojamoje zonoje, teikėjas privalo vadovautis šių dokumentų aktualiomis redakcijomis:

12.1. 1999 m. sausio 12 d. Lietuvos Respublikos radiacinės saugos įstatymu Nr. VIII-1019 (Žin., 1999, Nr. 11-239);

12.2. Branduolinės saugos reikalavimais BSR-2.1.2-2010 „Bendrieji atominių elektrinių su RBMK-1500 tipo reaktoriais saugos užtikrinimo reikalavimai“;

12.3. Branduolinės saugos reikalavimais BSR-1.4.1-2016 „Vadybos sistema“;

12.4. Branduolinės saugos reikalavimais BSR-1.9.3-2016 „Radiacinė sauga branduolinės energetikos objektuose“;

12.5. IAE radiacinės saugos instrukcija, DVSed-0512-2 (https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103);

12.6. Radiacinės saugos užtikrinimo, dirbant kontroliuojamoje zonoje, instrukcija, DVSed-0512-7 (https://www.iae.lt/teisine-informacija/vidiniai-teises-aktai/103);

13. Paslaugų teikėjas (ir visų lygių subteikėjai), vykdysiantis veiklą jonizuojančios spinduliuotės aplinkoje branduolinės energetikos objekte:

13.1. gali vykdyti veiklą, turėdami Lietuvos Respublikos įgaliotos institucijos išduotą dokumentą, suteikiantį teisę vykdyti veiklą jonizuojančios spinduliuotės aplinkoje branduolinės energetikos objekte;

13.2. neturintiems Lietuvos Respublikos įgaliotos institucijos išduoto dokumento, suteikiančio teisę vykdyti veiklą jonizuojančios spinduliuotės aplinkoje branduolinės energetikos objekte, paslaugų teikėjo (ir visų lygių subteikėjų) personalui bus taikomi apribojimai ir reikalavimai:

13.2.1. paslaugų teikėjo personalui bus taikoma gyventojams nustatyta metinės efektinės apšvitos dozės ribinė 1 mSv per metus vertė. Pasiekęs šią vertę, darbuotojas negalės einamais metais tęsti darbų kontroliuojamoje zonoje;

13.2.2. paslaugų teikėjas, prieš pradėdamas darbus kontroliuojamoje zonoje, turi nedelsdamas pateikti kiekvieno siunčiamo darbuotojo duomenis apie einamaisiais metais gautas dozes, atliekant darbus ne VĮ IAE;

13.2.3. paslaugų teikėjo personalui bus išduodami leidimai, suteikiantys teisę patekti į branduolinės energetikos objektų apsaugos zonas tik su palyda.

14. Tiekėjo (ir visų lygių subtiekėjų) personalui, kuris pagal sutartį dėl jiems priskirtų funkcijų ar pavesto darbo turi įgyti teisę be palydos patekti į branduolinės energetikos objekto apsaugos zonas (išskyrus riboto patekimo zoną) ir (ar) branduolinės energetikos objekto aikštelę, leidimas gali būti suteiktas tik atlikus fizinių asmenų patikrinimą Branduolinės energijos įstatymo numatyta tvarka, pateikiant nustatytos formos dokumentus VĮ IAE Fizinės saugos skyriui. Patikrinimas ir sprendimo išduoti leidimą priėmimas trunka iki 40 darbo dienų, nuo visų reikiamų dokumentų pateikimo dienos.

15. Paslaugos, susijusios su radioaktyviai užteršta įranga, turi būti teikiamos IAE kontroliuojamos zonos ribose.

16. Radioaktyviai užteršta įranga ir įrankiai paslaugų teikėjui negrąžinami ir už juos nebus kompensuojama ar kitaip atlyginama.

VI. DOKUMENTAI

17. Tiekėjas pasiūlyme turi nurodyti pagal šios techninės specifikacijos 1, 3-7 lentelių techninius reikalavimus siūlomų bei visos kitos įrangos, kuri bus pateikta (fotografavimo įrangos, durų procesorių, spausdintuvų ir t.t.) prekių gamintojus ir modelius.

18. Kartu su pasiūlymu Tiekėjas turi pateikti prekių gamintojo parengtus techninius aprašus ir/ar analogiškus gamintojo parengtus dokumentus, įrodančius siūlomų prekių, nurodytų šios techninės specifikacijos 1, 3-7 lentelėse techninių parametrų atitikimą šios techninės specifikacijos reikalavimams.

19. Kartu su prekėmis Tiekėjas turi pateikti siūlomų prekių gamintojų techninius aprašus ir 1 lentelėje nurodytų prekių gamintojų numatytą eksploatavimo (vartojimo) instrukciją (lietuvių ir anglų kalba).

VII. REIKALAVIMAI DĖL ĮDIEGIMO, PRISTATYMO IR PRIĖMIMO-PERDAVIMO

20. Visos prekės turi būti pristatytos ir sumontuotos VĮ Ignalinos atominės elektrinės pagrindinėje aikštelėje, Panaudoto branduolinio kuro saugyklos aikštelėje ir Laikinosios panaudoto branduolinio kuro saugyklos aikštelėje Drūkšinių k., 31152 Visagino sav.

VIII. ĮRANGA

21. Tiekėjas užtikrina, kad turės pakankamai sutarties įgyvendinimui reikalingų priemonių ir įrangos.

22. Pagal šią sutartį perkančiosios organizacijos vardu negali būti perkama ar baigus vykdyti sutartį perkančiajai organizacijai perduodama jokia techninė įranga, reikalinga sutarties įgyvendinimui.

IX. KITOS IŠLAIDOS

23. Visos kitos išlaidos, susijusios su sutarties įgyvendinimu, turi būti įskaičiuotos į bendrą sutarties kainą. Jokios papildomos išlaidos, neįskaičiuotos į sutarties kainą, kompensuojamos nebus.

X. APLINKOS APSAUGOS KRITERIJŲ REIKALAVIMAI

24. Maksimaliai mažinamas popieriaus sunaudojimas dokumentams, dokumentų kopijavimui ir spausdinimui, teikiant pirmenybę skaitmeninėms dokumentų kopijoms, siunčiant elektroniniu paštu, pasinaudojant elektroninio parašo funkcijos galimybėmis ar kitais būdais. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka žaliojo pirkimo reikalavimus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakyme Nr. Dl-508 „Dėl Produktų, kurių viešiesiems pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos turi taikyti pirkdamos prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“.

XI. APMOKYMAI

25. Tiekėjas turi apmokyti Užsakovo darbuotojus vykdyti programinės įrangos administravimo (5 darbuotojus), naudojimo (5 darbuotojus) bei tiekiamos techninės įrangos aptarnavimo bei gedimų šalinimo darbus.

XII. KITI REIKALAVIMAI

26. Visoms siūlomoms prekėms turi būti taikoma ne trumpesnė nei 24 mėnesių garantija nuo perdavimo-priėmimo akto pasirašymo dienos.

27. Garantiniu laikotarpiu, esant prekių defektams, Užsakovas kreipiasi į Tiekėją su prašymu atvykti šalinti gedimus telefonu arba el. paštu. Defektų šalinimo paslaugos pradedamos teikti darbo dienomis ne vėliau kaip per 48 valandas nuo prašymo atvykti gavimo momento, jei prašyme atvykti nenustatyta vėlesnė data. Tiekėjas užtikrina atsiradusių defektų pašalinimą savo sąskaita ne vėliau kaip per 30 kalendorinių dienų nuo kreipimosi dienos.

28. Garantija – tai laikotarpis, per kurį išaiškėjus pateiktų prekių trūkumams/defektams, jie turi būti pašalinti prekių tiekėjo sąskaita. Pakeistoms naujoms įrangos dalims turi būti taikoma ne mažesnė kaip gamintojo garantija nuo remonto paslaugų perdavimo-priėmimo akto pasirašymo dienos.

29. Visos siūlomos prekės turi būti naujos, nenaudotos.

_____

VALSTYBĖS ĮMONĖ
IGNALINOS ATOMINĖ ELEKTRINĖ

CVP IS tiekėjai

CVP IS priemonėmis

2025-05- Nr. ĮS-

Į _____ Nr. _____

DĖL PIRKIMO DOKUMENTŲ PAAIŠKINIMO IR PATIKSLINIMO

Informuojame, kad tarptautinio viešojo pirkimo „Pateikimo kontrolės sistemos pirkimas“, vykdomo atviro konkurso būdu (pirkimo ID 1984530, toliau – Pirkimas), metu Centrinės viešųjų pirkimų informacinės sistemos priemonėmis gauti tiekėjo(-ų) prašymai paaiškinti / patikslinti Pirkimo dokumentus.

VĮ Ignalinos atominės elektrinės Viešųjų pirkimų komisija (toliau – Komisija) teikia atsakymus į pateiktus klausimus.

Eil.	Prašymai (kalba netaisyta):	Atsakymai į Prašymus:
1.	Prašome paaiškinti kaip suprantamas apibrėžimas “darbo stotys (9vnt)? Ar tai reiškia sistemos administratoriaus/operatoriaus nuotolinė darbo vieta? Kokį sistemos funkcionalumą galima atlikti naudojantis darbo stotimi: kurti vartotojus, administruoti vartotojus, valdyti įrenginius ir kt?	Darbo stotis tai kompiuteris su Windows operacine sistema (Pastaba. IAE naudojamos ne žemesnės kaip **Windows 11** x64 operacinės sistemos versijos), kurioje turi būti įdiegta patekimo kontrolės sistemos programinė įranga, kurioje gali prisijungti tiek administratorius, tiek operatorius. Tačiau trys darbo stotys turi turėti administratoriaus ir operatoriaus funkcionalumą, t. y. turi būti galimybė kurti vartotojus, administruoti vartotojus, valdyti įrenginius ir turėti visas administratoriaus teises. O šešios darbo stotys privalo turėti operatoriaus funkcionalumą, t. y. turi turėti galimybę minimaliai atlikti šiuos veiksmus: sukurti leidimą, keisti leidimo prieigos teises, atspausdinti leidimą, keisti leidimų tvarkaraščius, matyti pranešimus, matyti leidimų patekimo vietą realiu laiku, realiu laiku keisti leidimo būklę (blokuoti/atblokuoti, pakeisti leidimo zoną), dirbti su ataskaitomis,

		tačiau gali turėti platesnes teises priklausomai nuo siūlomo sprendimo.
2.	Sistemos specifikacijoje nėra aprašyta kaip sistema turi veikti esant “offline” režimui. Prašome patikslinti ar reikalingas sistemos veikimas neprisijungus (offline režimu), t. y. ar sistemos įvykiai turi būti išsaugomi kontroleriuose dingus ryšiui?	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus, keliamus sistemos veikimui ir nustatome, kad sistema (įskaitant kontrolerius) privalo veikti “offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai turėtų vykdyti praleidimą pro duris, kurias jie kontroliuoja bei vykdyti sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio turi būti sinchronizuoti.
3.	Sistemos specifikacijoje nėra keliamas reikalavimas šifruoti duomenis, nors skaitytuvų techniniuose reikalavimuose numatytas OSDP šifruotas protokolas. Prašome patikslinti ir/ar nurodyti ar turi būti užtikrintas AES šifravimas? Ir kokio lygio?	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus, ir nustatome, kad turi būti naudojamas šifravimo protokolas su ne trumpesniu nei 128 bitų raktu.
4.	Prašome patikslinti kaip suprantamas ir kokį funkcionalumą turi atlikti 1.3. punkte minimas prieigų planavimo modulis. Koks konkretus funkcionalumas turi būti išpildytas?	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus, ir nustatome, kad prieigų planavimo modulis turi leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius.
5.	Prašome patikslinti kaip suprantamas ir kokį funkcionalumą turi atlikti 1.5. punkte aprašytas generuojamas aliarminis pranešimas? Ar tai suprantama kaip pranešimas sistemoje? ar garsinis signalas?	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus, ir nustatome, kad generuojamas aliarminis pranešimas - pranešimas sistemoje, kurį galėtų pamatyti operatorius, su garsiniu signalu.
6.	Prašome paaiškinti ir patikslinti 4.10 punkte aprašytą vartelių blokavimo mechanizmą. Koks veikimo principas? Ar teisingai suprantame, kad tai aukščiausias užrakinimo statusas (net jeigu vartotojas turi teisę praeiti, programiškai galima apriboti durų atidarymą?)	Vartelių blokavimo mechanizmą rangovas galės pasirinkti savo nuožiūra (elektromagnetinė spyna, elektromagnetas ir pan.) priklausomai nuo konkrečios situacijos (konkrečių vartelių). Vartelių blokavimo mechanizmai turėtų blokuoti vartelius elektroniniu būdu (negalima jų mechaniškai – su raktu ar kaip kitaip, atidaryti). Varteliai atsiblokuoti turi jei vartotojas su teise praeiti pasinaudos skaitytuvais, kurie kontroliuoja vartelių atidarymą. Programinis vartotojo, turinčio teisę praeiti, blokavimo funkcionalumas nereikalaujamas.
7.	Prašome paaiškinti ir patikslinti 4.11 punkte aprašytą durų blokavimo mechanizmo veikimo principą.	Žr. Atsakymą į 6 klausimą.
8.	Prašome patikslinti ir paaiškinti 6 lentelės 4 punkte aprašytos “Specializuota spausdintuvo programinė įranga” funkcionalumą ir veikimo principą. Ar tai reiškia, kad kortelės dizainas, formatavimas ir spausdinimas turi būti	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus dėl 6 lentelės 4 punkte aprašytos “Specializuotos spausdintuvo programinės įrangos” funkcionalumo ir nustatome, kad kortelės

	atliekamas praėjimo sistemos programinėje įrangoje?	dizainas, formatavimas ir spausdinimas **turi būti** atliekamas praėjimo sistemos programinėje įrangoje. Specializuota spausdintuvo programinė įranga turi būti suprantama, kaip spausdintuvo tvarkyklės reikalingos spausdintuvo prijungimui prie darbo stoties su Windows operacine sistema (Pastaba. IAE naudojamos ne žemesnės kaip **Windows 11** x64 operacinės sistemos versijos).
9.	7 lentelė. Prašome patikslinti ar vartotojo foto nuotrauka turi būti saugoma praėjimo sistemos programinės įrangos duombazėje prie vartotojo? Ar pridėjus kortelę prie skaitytuvo sistemoje bus matoma darbuotojos fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės? (vizualinė darbuotojų patikra)	Atsakydami į šį klausimą, patiksliname Techninės specifikacijos reikalavimus, ir nustatome, kad Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka turi būti saugoma praėjimo sistemos programinės įrangos duomenų bazėje prie vartotojo. Pridėjus kortelę prie skaitytuvo sistemoje turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).
10.	Prašome patikslinti prie kokios įrangos bus prijungti fotografavimo įrenginiai? Ar teisingai suprantame, kad jie bus prijungti prie vienos iš “darbo stoties”?	fotografavimo įrenginiai (2 vnt.) turi būti prijungti prie skirtingų darbo stočių (2 vnt.)
11.	Ar praėjimo sistemos vartotojai turi būti sinchronizuojami su kitomis duombazėmis ar vartotojų sąrašais? Pvz. MS Active Directory	Tokio funkcionalumo reikalavimas nėra numatytas Pirkimo dokumentuose, tačiau jis nėra draudžiamas.
12.	Kadangi šiuo metu PO (perkančioji organizacija) naudoja dvigubos autentifikacijos (2FA) metodą kortelė+pin kodas patekimui į patalpas, o konkurso specifikacijoje yra numatyta įsigyti kortelių skaitytuvus su klaviatūromis, prašome patikslinti ar perkama įeigos kontrolės sistema turi palaikyti 2FA ar MFA (multifactor authentification) funkcionalumą? Jeigu toks funkcionalumas numatytas ar visur bus naudojama tik kortelė + pin kodas, ar gali/turi būti naudojami ir kiti identifikatoriai (pvz biometriniai duomenys, žetonai, mobilūs raktai)?	Sistema turi turėti dvigubos autentifikacijos metodo (kortelė+pin) funkcionalumą. Kiti metodai nėra reikalaujami, bet gali būti siūlomi kaip papildomi (pvz biometriniai duomenys, žetonai, mobilūs raktai), tačiau visais atvejais privalo būti užtikrintas dvigubos autentifikacijos metodo (kortelė+pin) funkcionalumas su perkamais skaitytuvais su klaviatūra.
13.	Papildymas 8 klausimui. a. Jeigu PO nereikalauja, kad kortelės maketavimas turi vykti vienoje sistemoje, tokiu atveju prašome nurodyti techninius reikalavimus vartotojų duomenų perkėlimui tarp sistemų: i. Koks turi būti duomenų šifravimas? ii. Ar duomenys (ir kiek laiko) turi būti saugomi kortelių maketavimo sistemoje?	i. Koks turi būti duomenų šifravimas? Žr. Atsakymą į 3 klausimą. ii. Ar duomenys (ir kiek laiko) turi būti saugomi kortelių maketavimo sistemoje? Kortelių maketavimo sistemoje turi būti saugomi kortelių šablonai, bet ne vartotojo asmeniniai duomenys. Duomenų saugojimo laikas neribojamas, kiek būtina pagal galiojančius t. aktus.

14.	Ar sistemoje turi būti numatyta galimybė palaikyti valstybinių numerių atpažinimo funkcionalumą?	Šis funkcionalumas nereikalaujamas, tačiau nėra draudžiama siūlyti šio papildomo funkcionalumo.
15.	VĮ Ignalinos atominės elektrinės pagrindinėje aikštelėje esančioje instaliacijoje panaudotas FKAR-PG 2x2x0,5 kabelis neatitinka OSDP v2 standartui keliamo reikalavimo naudoti vytos poros kabelį. Ar esant nekorektiškam sistemos veikimui, Perkančioji Organizacija atliks kabelio keitimą savo lėšomis ?	Perkančioji organizacija neprisiima rizikos dėl nekorektiško sistemos veikimo, net ir esant kabelių neatitikimui siūlomai sistemai, todėl tiekėjai turi siūlyti suderinamas sistemas su turima infrastruktūra arba pasirūpinti esamos infrastruktūros pritaikymu siūlomai sistemai (pvz. įskaičiuoti kabelių keitimo išlaidas į savo pasiūlymą ir pan.).

Taip pat Komisija po Pirkimo paskelbimo be po gautų tiekėjų klausimu pastebėjo netikslumus / neaiškumus Pirkimo dokumentuose (toliau tekste – PD), t. y. „*Pateikimo kontrolės sistemos pirkimo techninėje specifikacijoje*“, todėl vadovaujantis PD A dalies 15.3 p. „*Nesibaigus pasiūlymų pateikimo terminui, perkančioji organizacija savo iniciatyva turi teisę paaiškinti (patikslinti) PD* <...>“, savo iniciatyva tikslina PD.

Tikslinami PD E dalies, t. y. „*Pateikimo kontrolės sistemos pirkimo techninės specifikacijos“ (toliau – TS)*“ (toliau – TS) dalis punktų, išdėstomi nauja redakcija ir/ar papildomi naujais reikalavimais.

Keičiami TS 1 lentelės 2, 5 ir 10 p. išdėstomi nauja redakcija:

2.	Prieigų planavimo modulis (turi leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius)	Turi būti

<...>

5.	Modulis, generuojantis aliarminius pranešimus (pranešimas sistemoje, kurį galėtų pamatyti operatorius, su garsiniu signalu): bandymas patekti neturint leidimo ir pan.	Turi būti

<...>

10.	Programinė įranga ne mažiau kaip 9 darbo stotims (3 (trys) darbo stotys turi turėti administratoriaus ir operatoriaus funkcionalumą, 6 (šešios) darbo stotys privalo turėti operatoriaus funkcionalumą). Pastaba. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos.	Turi būti

TS 1 lentelė yra papildoma naujais reikalavimais ir jie yra išdėstomi taip:

12.	Sistema (įskaitant kontrolerius) privalo veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai turėtų vykdyti praleidimą pro duris, kurias jie kontroliuoja bei vykdyti sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio turi būti sinchronizuoti.	Turi būti
13..	Duomenų šifravimui naudojamas šifravimo protokolas su ne trumpesniu nei 128 bitų raktu	Turi būti
14.	Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka turi būti saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).	Turi būti

TS 4 lentelė yra papildoma nauju reikalavimu (4 lentelės 10 punktas) ir jis yra išdėstomas taip:

10.	Galimybė naudoti dvigubos autentifikacijos metodą (kortelė+pin)	Turi būti

Atitinkamai su pranešimu bus pridėta bei paviešinta CVP IS prie PD *patikslinta Tiekėjo pasiūlymo forma (*docx),* kurioje tiekėjas turi uždeklaruoti atitikimą šiam TS reikalavimui.

<u>Pirkimo dokumentuose nustatytų terminų tikslinimas</u>:

Atsižvelgiant į tai, kad buvo padaryti Konkurso pirkimo dokumento pakeitimai, Komisija priėmė sprendimą **pakeisti Pirkimo dokumentų** A dalies 2.1 p. nustatytus terminus ir šis punktas išdėstomas taip:

„2.1.1. Susitikimas su tiekėjais bus organizuojamas 2025-04-28 - 2025-05-02 dienomis.

*2.1.2. Perkančioji organizacija prašymą paaiškinti pirkimo dokumentus turi gauti ne vėliau kaip iki **2025-05-13 imtinai**.*

*2.1.3. Atsakymas į tiekėjo prašymą paaiškinti pirkimo dokumentus turi būti siunčiamas taip, kad tiekėjas jį gautų ne vėliau kaip iki **2025-05-20 imtinai**.*

*2.1.4. Pasiūlymų pateikimo termino pabaiga: **2025-05-27 10:00 val.***

*2.1.5. Pradinio susipažinimo su pasiūlymais posėdžio data: **2025-05-27**.“*

Pridedama. Tiekėjo pasiūlymo forma (patikslinta), 7 lapai.

Viešųjų pirkimų komisijos pirmininkė

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	VĮ Ignalinos atominė elektrinė (102 / 103) 255450080, Elektrinės g.4, K 47, Drūkšinių k., 31152 Visagino sav., Lietuvos Respublika
Dokumento pavadinimas (antraštė)	DĖL PIRKIMO DOKUMENTŲ PAAIŠKINIMO IR PATIKSLINIMO
Dokumento registracijos data ir numeris	2025-05-08 Nr. ĮS-1830(13.66E)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	2025-05-08 10:57:11 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-05-08 10:57:24 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2020-08-28 17:14:12 – 2025-08-27 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Ignalinos atominė elektrinė, VĮ, į.k. 255450080 LT", sertifikatas galioja nuo 2024-12-18 09:12:37 iki 2027-12-18 09:12:37
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.63
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2025-05-08 11:03:48)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2025-05-08 11:03:49 Dokumentų valdymo sistema Avilys

VALSTYBĖS ĮMONĖ
IGNALINOS ATOMINĖ ELEKTRINĖ

CVP IS tiekėjai

CVP IS priemonėmis

2025-05- Nr. ĮS-

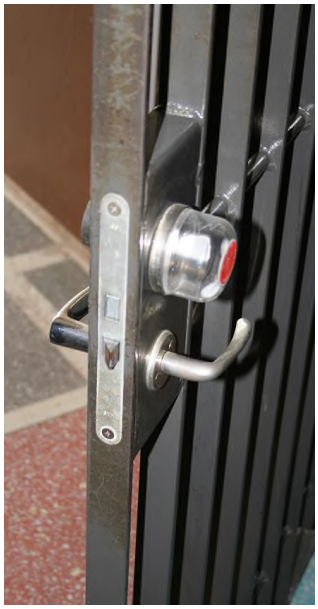
Į _____ Nr. _____

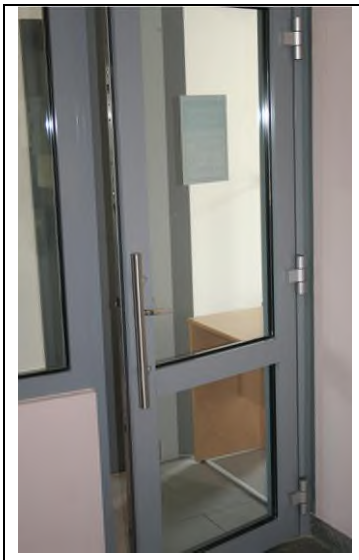
DĖL PIRKIMO DOKUMENTŲ PAAIŠKINIMO

Informuojame, kad tarptautinio viešojo pirkimo „Pateikimo kontrolės sistemos pirkimas“, vykdomo atviro konkurso būdu (pirkimo ID 1984530, toliau – Pirkimas), metu Centrinės viešųjų pirkimų informacinės sistemos priemonėmis gauti tiekėjo (-ų) prašymas (-ai) paaiškinti / patikslinti Pirkimo dokumentus.

VĮ Ignalinos atominės elektrinės Viešųjų pirkimų komisija (toliau – Komisija) teikia atsakymus į pateiktus klausimus.

Eil. Nr.	Prašymai (kalba netaisyta):	Atsakymai į Prašymus:
1.	Prašome patikslinti ar esama patekimo kontrolės sistema turi įrengtus durų padėties daviklius (magnetinius kontaktus). Jei taip, tai ar jie lieka (nebus demontuoti) ir ar juos reikės prijungti prie naujos sistemos?	Esamoje sistemoje neįrengti durų padėties davikliai.
2.	Ar rangovas turi įsivertinti ir naujus durų padėties daviklius (magnetinius kontaktus) vietose, kur naujai įrengiama (jei tokių vietų yra) patekimo kontrolės sistema?	Durų padėties daviklių įsivertinti nereikia, kadangi tokio funkcionalumo, t. y. durų padėties daviklių įrengimo, nereikalaujame.

3.	Prašome pateikti informaciją (aprašymus) kokio tipo užblokavimo mechanizmai yra sumontuoti išnaudojami duryse/varteliuose su patekimo kontrolės sistema.	Šiuo metu naudojamose duryse / varteliuose yra sumontuotos paprastos raktu rakinamos spynos.
4.	Prašome pateikti informaciją (aprašymus, nuotraukas) apie vartelius, kuriems rangovas, pagal TS (techninė specifikacija) punktą Nr. 4.10, turi numatyti užblokavimo mechanizmus.	Standartiniai varteliai atrodo taip (nuotraukos pridedamos): 1 variantas:   2 variantas:  

5.	Prašome pateikti informaciją (aprašymus, nuotraukas) apie duris, kurioms rangovas, pagal TS punktą Nr. 4.11., turi numatyti užblokavimo mechanizmus.	Durys atrodo taip (nuotraukos pridedamos): Durys Nr. 1   Durys Nr. 2  

6.	Prašome pateikti informaciją (aprašymus, nuotraukas) kaip šiuo metu ant/prie turniketų yra sumontuoti skaitytuvai, kokie laikikliai naudojami, kad įvertinti naujus reikiamus laikiklius.	Šiuo metu sumontuoti skaitytuvai atrodo taip (nuotraukos pridedamos): Skaitytuvas Nr. 1   Skaitytuvas Nr. 2  
7.	Pagal TS punktą Nr. 6.2.2. rangovas turės pateikti ir sumontuoti vartų valdymo pultą (vartų ir anti-taraninių vartų valdymui). Ar nuo vartų iki pulto vietos yra įrengtas reikiamas kabelių kiekis ar rangovas turi juos nusimatyti ir turės juos įrengti naujai?	Komunikacinės linijos nuo vartų / antitaraninių įrenginių yra nutiestos iki operatorinės. Reikėtų įsivertinti esamų kabelių prailginimą (iki 5 metrų kiekvieną kabelį) nuo sienos operatorinėje iki stalo, ant kurio turės būti sumontuotas valdymo pultas.

8.	Pagal TS punktą Nr. 6.2.4 rangovas turės atlikti 7 vartelių skaitytuvų sumontavimą ir komunikacijų pratiesimo darbus. Taip pat reikia numatyti užrakinimo mechanizmus. Atsižvelgiant į tai, kad reikia naujų komunikacijų ir užrakinimo mechanizmų, bei todėl, kad TS punkte Nr. 5 esama PKS nėra minimi varteliai, ar teisingai suprantame, kad šiuose varteliuose šiuo metu nėra įrengta pateikimo kontrolės sistema ir ją reikėtų įrengti naujai? Jei taip, tuomet prašome nurodyti kiek ir kokio įrangos (skaitytuvai, magnetiniai kontaktai ir pan.) reikia numatyti.	Minimuose varteliuose šiuo metu nėra įrengtų patekimo kontrolės sistemos elementų. Būtų reikalingi skaitytuvai (įskaičiuoti į TS tiekimo apimtį) bei durų procesoriai. Durų padėties daviklių nereikalaujame.
9.	Pagal TS punktą Nr. 6.2.6 rangovas turės atlikti 2 durų į patalpas skaitytuvų sumontavimo ir komunikacijų pratiesimo darbus, įtraukiant į tiekimo apimtį durų užrakinimo mechanizmus, valdomus per skaitytuvus. Atsižvelgiant į tai, kad reikia naujų komunikacijų ir užrakinimo mechanizmų, ar teisingai suprantame, kad šiose duryse šiuo metu nėra įdiegta pratekimo kontrolės sistemos ir ji būtų diegiama naujai? Jei taip, tuomet prašome nurodyti kiek ir kokio įrangos (skaitytuvai, magnetiniai kontaktai ir pan.) reikia numatyti.	Analogiškai kaip atsakyme į 8 klausimą.
10.	Prašome patikslinti kas turima omenyje, kai sakoma: "durų mechanizmus, valdomus per skaitytuvus"? Panašiu atveju TS punkte 6.2.4 nurodoma, kad vartelių užrakinimo	Paaiškiname, kad reikalavimas “durų mechanizmus, valdomus per skaitytuvus“ turi būti suprantamas kaip “durų mechanizmus, valdomus per durų kontrolerius (=procesorius)”.

	mechanizmai turi būti valdomi per durų procesorius.	
11.	TS punkte 6.2.7 nurodoma, kad užbaigus sistemos diegimo darbus turi būti parengtas su Užsakovu suderintas techninis darbo projektas. Prašome patvirtinti, kad techninis darbo projektas turės būti parengtas remiantis STR reikalavimais. Taip pat atkreiptinas dėmesys, kad įprastai projektas yra rengiamas prieš darbų pradžią.	Techninis darbo projektas turi būti suprantamas kaip visų atliktų darbų aprašymas ir sumontuotos įrangos išdėstymo schemos pateikimas, t. y. jis neprivalo būti parengtas remiantis STR reikalavimais**.**
12.	Prašome informuoti ar po esamos įrangos demontavimo, kurią atliks Užsakovo darbuotojai, kaip nurodoma TS punkte Nr. 6.2.1., bus sužymėti kabeliai?	Demontavimo metu esami kabeliai bus sužymėti. Taip pat pažymime, kad demontavimas ir montavimas turėtų būti vykdomas tuo pačiu metu, t. y. atjungus ir demontavus esamą skaitytuvą jo vietoje turėtų būti montuojamas naujas bei prijungiamas prie naujo durų kontrolerio. Visame tame procese dalyvaus Užsakovo atstovai, kurie operatyviai spręs tokio tipo klausimus.
13.	Prašome informuoti, ar Užsakovas garantuoja, kad esami kabeliai yra tinkami naudoti, ar rangovas turi įsivertinti ir kabelių testavimą prie prijungiant naują įrangą?	Užsakovas negali garantuoti, kad esami komunikaciniai kabeliai (nuo durų kontrolerių iki skaitytuvų) tiks siūlomai sistemai (negalime žinoti kokia sistema bus pasiūlyta). Turėtų būti pasiūlyta tokia sistema ir tokia įranga, kuriai esami komunikaciniai kabeliai tiktų.
14.	Prašome nurodyti kokiame aukštyje ir kokiomis konstrukcijomis bus/būtų klojami naujai kabeliai?	Jei kalbame apie nauju kabelius prijungti duris/vartelius – situacija yra pakankamai skirtinga visiems objektams, todėl negalime nurodyti konkrečiai. Didesnė dalis kabelių tikriausiai būtų klojama virš pakabinamų lubų įprastinio aukščio patalpose

Atsižvelgiant į tai, kad Pirkimo dokumentai aiškinami PD nustatytais terminais, PD A dalies 2 punkte nustatyti terminai nesikeičia.“

Viešųjų pirkimų komisijos pirmininkė

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	VĮ Ignalinos atominė elektrinė (102 / 103) 255450080, Elektrinės g.4, K 47, Drūkšinių k., 31152 Visagino sav., Lietuvos Respublika
Dokumento pavadinimas (antraštė)	DĖL PIRKIMO DOKUMENTŲ PAAIŠKINIMO
Dokumento registracijos data ir numeris	2025-05-19 Nr. ĮS-1969(13.66E)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-05-19 13:22:39 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2020-08-28 17:14:12 – 2025-08-27 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Ignalinos atominė elektrinė, VĮ, į.k. 255450080 LT", sertifikatas galioja nuo 2024-12-18 09:12:37 iki 2027-12-18 09:12:37
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.63
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2025-05-19 13:54:26)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2025-05-19 13:54:26 Dokumentų valdymo sistema Avilys

T33238

C. TIEKĖJO PASIŪLYMAS 1-AI PIRKIMO DALIAI

Patekimo kontrolės sistemos pirkimas

2025-05-26
(Data)

Kaunas
(Vieta)

Tiekėjo pavadinimas [jei tai tiekėjų grupė, nurodyti: jungtinės veiklos sutarties pagrindu veikianti tiekėjų grupė, sudaryta iš: [nurodyti visų partnerių pavadinimus]]	Spectra Baltic UAB
Atsakingasis partneris [nurodyti atsakingojo partnerio pavadinimą, jei pasiūlymą teikia tiekėjų grupė]	
Tiekėjo adresas [jei pasiūlymą teikia tiekėjų grupė, nurodyti visų partnerių adresus]	Baltų pr. 145, LT-47125 Kaunas
Už pasiūlymą atsakingo asmens vardas, pavardė	
Telefonas, el. pašto adresas	

Šiuo pasiūlymu pažymime, kad sutinkame su visomis šio pirkimo sąlygomis, nustatytomis pirkimo dokumentuose.

Siūlomos šios prekės ir

prekių pristatymą, montavimą, paleidimą, derinimą, personalo apmokymą (toliau vadinama – prekės)
:

						Valiuta: Eurai	
Eil. Nr.	**Prekės pavadinimas[1]**	**Prekės gamintojas**	**Prekės modelis**	**Mato vnt.**	**Vieneto įkainis be PVM**	**Preliminarus kiekis[4]**	**Preliminari suma be PVM[2]**
1	Patekimo kontrolės sistemos (toliau - PKS) programinė įranga serveriui (1 vnt.) ir darbo stotims (9 vnt.)	Inner range (Australija)	996901C; 996940-60;995200PEEU3; 996018PCBK; 996535PCBK;	kompl.	42954,66	1	42954,66
2	PKS leidimų kortelė	Inner range (Australija)	994610	vnt.	4,80	3000	14400,00
3	PKS skaitytuvas su klaviatūra	Inner range (Australija)	994725MF + 999046	vnt.	347,10	78	27073,80

4	PKS skaitytuvas be klaviatūros	Inner range (Australija)	994720MF + 999037	vnt.	132,50	67	8877,50
5	PKS kortelių spausdintuvas	FARGO (JAV)	DTC1250e	vnt.	3982,90	2	7965,80
6	Vartų valdymo pultas	Spectra Baltic UAB (Lietuva)	Nestandartinė, pagal spec. užsakymą gaminama prekė	vnt.	2500,00	1	2500,00
7	Fotografavimo įrenginiai su tvirtinimo prie sienos laikikliais	Hewlett-Packard (JAV)	HP 950 4K	kompl.	200,00	2	400,00
8	Vartelių užblokavimo mechanizmai, valdomi per durų procesorius	Eff-Eff (Vokietija)	118E.13---A71 PROFIX2	vnt.	60,00	7	420,00
9	Durų užblokavimo mechanizmai, valdomi per durų procesorius	Eff-Eff (Vokietija)	E7	vnt.	28,50	2	57,00
10	Įrangos montavimo, paleidimo, derinimo ir darbuotojų apmokymo paslaugos [5]	Spectra Baltic UAB (Lietuva)	Įrangos montavimo, paleidimo, derinimo ir darbuotojų apmokymo paslaugos	kompl.	30000,00	1	30000,00
						Bendra preliminari kaina be PVM[2]:	134648,76
						PVM (21%) kaina[3]:	28276,24
						Bendra preliminari kaina su PVM[2]:	162925,00
Bendra preliminari kaina su PVM žodžiais: Vienas šimtas šešiasdešimt du tūkstančiai devyni šimtai dvidešimt penki eurai							

Jei suma skaičiais neatitinka sumos žodžiais, teisinga laikoma suma žodžiais.

[1] - prekės (-ių) pavadinimas turi atitikti techninėje specifikacijoje nurodytą prekės (-ių) pavadinimą.
[2] - kainos nurodomos suapvalintos, paliekant du skaitmenis po kablelio.
[3] - tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, jis atitinkamų skilčių nepildo ir nurodo priežastis, dėl kurių PVM nemoka.
[4] **- kiekvienoje pozicijoje nurodytas kiekis yra maksimalus.**
[5] - Į paslaugų kainą yra įskačiuotos visos išlaidos susijusios su perkamos įrangos montavimu, paleidimu, derinimu bei darbuotojų apmokymu, taip pat į šią kainą yra įskaičiuota tiekiamų durų procesorių (TS 4.6. p.) ir kompiuterių tinklo komutatorių (TS 4.7.p.) kaina, kurių kiekis priklauso nuo siūlomos įrangos tipo, todėl yra parinktas tiekėjo savarankiškai taip, kad patekimo kontrolės sistema funkcionuotų tinkamai).

Siūlomos prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus ir jų charakteristikos pateikiamos pasiūlymo priede Nr. 1.

Teikdami šį pasiūlymą, mes patvirtiname, kad į mūsų siūlomą kainą įskaičiuoti visi mokesčiai bei visos sutarties vykdymo išlaidos ir kad mes prisiimame riziką už visas išlaidas, kurias, teikdami pasiūlymą ir laikydamiesi techninės specifikacijos sąlygų, privalėjome įskaičiuoti į pasiūlymo kainą.

Informacija apie sutarties vykdymo metu numatomus pasitelkti subtiekėjus ar specialistus ir ekspertus: *(Pildoma, jei tiekėjas ketina sutarties vykdymui pasitelkti subtiekėją ar specialistus ir ekspertus, kurie pasiūlymo pateikimo metu nėra tiekėjo ar jo pasitelkiamo (-ų) subtiekėjo (-ų), darbuotojai, tačiau laimėjimo atveju bus įdarbinti)*:

Eil.Nr.	Subtiekėjo pavadinimas, specialistų ir/ar ekspertų vardas, pavardė	Įsipareigojimų dalis, nurodant konkrečius pagal sutartį prisiimamus įsipareigojimus, kuriai ketinama pasitelkti subtiekėją, ir/ar kvalifikacijos reikalavimas (-ai), kuriam (-iems) pagrįsti bus remiamasi nurodytu subtiekėju, specialistu ir/ar ekspertu

Kartu su pasiūlymu pateikiami **pasiūlymo 1 priedas ir** šie dokumentai:

Eil.Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	...Tiekėjo deklaracija	...2
2.	...Nacionalinio saugumo deklaracija	...2
3.	...ESPD deklaracija	...17

Pasiūlymas galioja 180 kalendorinių dienų nuo pasiūlymų pateikimo termino pabaigos.

Nurodome, kad šiose pasiūlymo dalyse (dokumentuose) yra pateikta konfidenciali informacija:

Eil.Nr.	Konfidencialios pasiūlymo dalies (konfidencialaus dokumento) pavadinimas

Teikdami šį pasiūlymą, patvirtiname, kad:

- **tiekėjui, subrangovams, tiekėjams ir subjektams, kurių pajėgumais remiamasi (tais atvejais, kai jiems tenka 10 % sutarties vertės) netaikomi ribojimai, nustatyti 2014 m. liepos 31 d. Tarybos reglamentu (ES) Nr. 833/2014 dėl ribojamųjų priemonių atsižvelgiant į Rusijos veiksmus, kuriais destabilizuojama padėtis Ukrainoje[1], įskaitant 2022 m. balandžio 8 d. Tarybos reglamentu 2022/576[2] padarytus pakeitimus;**
- **tiekėjui netaikomi ribojimai, nustatyti 2014 m. kovo 17 d. Tarybos reglamentu (ES) Nr. 269/2014 dėl ribojamųjų priemonių, taikytinų atsižvelgiant į veiksmus, kuriais kenkiama Ukrainos teritoriniam vientisumui, suverenitetui ir nepriklausomybei arba į juos kėsinamasi[3], įskaitant pakeitimus, padarytus 2022 m. balandžio 8 d. Tarybos reglamentu (ES) Nr.2022/581[4].**

[1] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A02014R0833-20220413

[2] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32022R0576
[3] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A02014R0269-20220421
[4] https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32022R0581&from=LT

1-os pirkimo dalies pasiūlymo priedas Nr. 1.

Siūlomos prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus ir jų savybės yra tokios:

Eil. Nr.	Prekės pavadinimas	Techninės charakteristikos pavadinimas	Siūlomos prekės techninės charakteristikos vertė	Atitikimą įrodančio dokumento pavadinimas ir puslapio Nr.
1.	Patekimo kontrolės sistemos (toliau - PKS) programinės įrangos (toliau - PĮ) serveriui (1 vnt.) ir darbo stotims (9 vnt.)			
		1.1. Vartotojų valdymo modulis	Vartotojų valdymo modulis	https://www.innerrange.com/products/software-licenses/996901c
		1.2. Prieigų planavimo modulis (turi leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius)	Prieigų planavimo modulis (leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius	https://www.innerrange.com/products/software-licenses/996901c
		1.3. Prieigų planavimo modulis	Yra prieigų planavimo modulis	https://www.innerrange.com/products/software-licenses/996901c
		1.4. Modulis, leidžiantis rengti leidimų "panaudojimo" ataskaitas, pagal duomenis esančius PKS	Modulis, leidžiantis rengti leidimų "panaudojimo" ataskaitas, pagal duomenis esančius PKS	https://www.innerrange.com/products/software-licenses/996901c
		1.5. Modulis, generuojantis aliarminius	1.5. Modulis, generuojantis aliarminius	https://www.innerrange.com/products/software-licenses/996901c

		pranešimus (pranešimas sistemoje, kurį galėtų pamatyti operatorius, su garsiniu signalu): bandymas patekti neturint leidimo ir pan.	pranešimus (pranešimas sistemoje, kurį gali pamatyti operatorius, su garsiniu signalu): bandymas patekti neturint leidimo ir pan.	
		1.6. Modulis, leidžiantis atlikti įrenginių konfigūravimą	Modulis, leidžiantis atlikti įrenginių konfigūravimą	https://www.innerrange.com/products/software-licenses/996901c
		1.7. Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams	Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams	https://www.innerrange.com/products/software-licenses/996901c
		1.8. „Anti-passback“ funkcija	Yra „Anti-passback“ funkcija	https://www.innerrange.com/downloads/programming_manual-integriti_guide_global_anti_passback
		1.9. Duomenų bazės tipas SQL	Duomenų bazės tipas SQL	Integriti Hardening Guide
		1.10. Programinė įranga ne mažiau kaip 9 darbo stotims (3 (trys) darbo stotys turi turėti administratoriaus ir operatoriaus funkcionalumą, 6 (šešios) darbo stotys privalo turėti	1.10. Programinė įranga ne mažiau kaip 30 darbo stotims. Kiekvieną darbo stotį galima suprogramuoti kad turėtų administratoriaus ir/arba operatoriaus funkcionalumą. Darbo stotyse instaliuotos Windows 11 x64	https://www.innerrange.com/products/software-licenses/996901c

		operatoriaus funkcionalumą). Pastaba. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos.	operacinės sistemos.	
		1.11. Licencija (jei reikalinga) prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 10 durų su skaitytuvais papildomai	Licencija prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 60 durų su skaitytuvais papildomai	Inner Range| 996940Integriti Door License
		1.12. Sistema (įskaitant kontrolerius) privalo veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai turėtų vykdyti praleidimą pro duris, kurias jie kontroliuoja bei vykdyti sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio turi	1.12. Sistema (įskaitant kontrolerius) gali veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai vykdo praleidimą pro duris, kurias jie kontroliuoja bei vykdo sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio bus sinchronizuoti.	https://www.innerrange.com/products/software-licenses/996901c a8357f_9b86fb5bac5240ee90a08431400d53f7.pdf

		būti sinchronizuoti.		
		Duomenų šifravimui naudojamas šifravimo protokolas su ne trumpesniu nei 128 bitų raktu	Duomenų šifravimui naudojamas šifravimo protokolas su 128 bitų raktu	https://www.innerrange.com/products/software-licenses/996901c
		Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka turi būti saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).	Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka yra saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).	https://www.innerrange.com/products/software-licenses/996901c
2.	PKS leidimų kortelė			
		2.1. Veikimo dažnis 13,56MHz	Veikimo dažnis 13,56MHz	Inner-Range-994610-ISO-Card-Data-Sheet.pdf
		2.2. DESFire® EV3 lustas	DESFire® EV3 lustas	Inner-Range-994610-ISO-Card-Data-Sheet.pdf

		2.3. Palaikomas standartas	*Standartas Mifare DESFire©*	Inner-Range-994610-ISO-Card-Data-Sheet.pdf
		2.4. Spalva	*Spalva balta*	Inner-Range-994610-ISO-Card-Data-Sheet.pdf
		2.5. Galimybė veikti -25° iki +40° temperatūros intervale	Veikia -25° iki +40° temperatūros intervale	Inner-Range-994610-ISO-Card-Data-Sheet.pdf
3.	PKS skaitytuvas su klaviatūra			
		3.1. Klaviatūra	Yra klaviatūra	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.2. Šviesos indikatoriai	*Programuojamas LED indikatorius*	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.3. Garsinis signalas	Programuojamas pypeklis	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.4. 13,56MHz perdavimo dažnis	13,56MHz perdavimo dažnis	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.5. Darbinė įtampa	*11-14V DC*	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.6. Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas	Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.7. OSDP duomenų perdavimo protokolas	OSDP duomenų perdavimo protokolas	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.8. Atsparumo aplinkos poveikiui klasė	Atsparumo aplinkos poveikiui klasė IP67	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.9. Galimybė veikti -20° iki +60° temperatūros intervale	Veikia -25° iki +60° temperatūros intervale	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf
		3.10. Galimybė naudoti dvigubos	Galima naudoti dvigubos autentifikacijos	a8357f_696cb4cb1c144d048a6d41a198da888f.pdf

		autentifikacijos metodą (kortelė+pin)	metodą (kortelė+pin	
4.	PKS skaitytuvas be klaviatūros			
		4.1. Šviesos indikatoriai	*Programuojamas LED indikatorius*	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.2. Garsinis signalas	Programuojamas pypeklis	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.3. 13,56MHz perdavimo dažnis	13,56MHz perdavimo dažnis	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.4. Darbinė įtampa	*11-14V DC*	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.5. Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas	Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.6. OSDP duomenų perdavimo protokolas	OSDP duomenų perdavimo protokolas	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.7. Atsparumo aplinkos poveikiui klasė	Atsparumo aplinkos poveikiui klasė IP67	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
		4.8. Galimybė veikti -20° iki +60° temperatūros intervale	Veikia -25° iki +60° temperatūros intervale	a8357f_1f965cdc55e74eabb22ab7b720bb0637.pdf
5.	PKS kortelių spausdintuvas			
		5.1. USB, Ethernet jungtys	*USB 2.0 Ethernet jungtis*	HID FARGO DTC1250e Printer Datasheet | HID Global
		5.2. Galimybė spausdinti spalvotai	Yra galimybė spausdinti spalvotai	HID FARGO DTC1250e Printer Datasheet | HID Global

		5.3. Spalvoto spausdinimo rezoliucija	Spalvoto spausdinimo rezoliucija 300dpi	HID FARGO DTC1250e Printer Datasheet | HID Global
		5.4. Specializuota spausdintuvo programinė įranga	Specializuota spausdintuvo programinė įranga Asure ID™ Enterprise	https://www.hidglobal.com/products/enterprise
		5.5. Eksploatacinės medžiagos 3000 spalvotų kortelių spausdinimui	*YMCKO-250* x 12 vnt	https://www.spectrabaltic.lt/Ieigos-kontrole/Korteliu-gamybos-iranga-deklai/Juosteles-ir-laminatai-korteliu-spausdintuvams/045000-Fargo-YMCKO-250-spausdintuvo-kasete-tinkama-DTC1000-DTC1250e.html
		5.6. Galimybė spausdinti ant leidimų kortelių su šios techninės specifikacijos 3 lentelėje nurodytais parametrais	Yra galimybė spausdinti ant leidimų kortelių su šios techninės specifikacijos 3 lentelėje nurodytais parametrais	HID FARGO DTC1250e Printer Datasheet | HID Global
6.	Fotografavimo įrenginys su tvirtinimo prie sienos laikikliais			
		6.1. Maksimali vaizdo raiška	4K	HP 950 4K Webcam | HP® Official Site
		6.2. Matymo kampas (Field of View - FOV)	Matymo kampas 102.7 laipsnių	b12871fff4473bed0937128722dbf22eb7c9.pdf
		6.3. Jungties tipas USB	Jungties tipas USB	b12871fff4473bed0937128722dbf22eb7c9.pdf

VALSTYBĖS ĮMONĖ
IGNALINOS ATOMINĖ ELEKTRINĖ

UAB „Sectra Baltic“

CVP IS priemonėmis

_____ Nr. ĮS-_____

Į _____ Nr. _____

DĖL PATEIKTO PASIŪLYMO PAAIŠKINIMO (PIRKIMO NR. 1984530)

VĮ Ignalinos atominės elektrinės Viešųjų pirkimų komisija, įvertinusi Jūsų pasiūlymo, pateikto tarptautiniame viešajame pirkime „Patekimo kontrolės sistemos pirkimas“, vykdomame atviro konkurso būdu (pirkimo Nr. 1984530, toliau – Pirkimas), techninę dalį, nustatė, kad pasiūlymas yra **neaiškus**.

Vadovaudamasi Lietuvos Respublikos viešųjų pirkimų įstatymo (Pirkimo paskelbimo metu aktualios redakcijos) 45 straipsnio 3 dalimi ir Pirkimo dokumentų A dalies 17.4 punktu, prašome ne vėliau kaip iki **2025-07-16 (imtinai)** CVP IS priemonėmis paaiškinti/patikslinti, kaip Jūsų siūlomos prekės atitinka tokius „Patekimo kontrolės sistemos pirkimas pirkimo techninės specifikacijos‘ (toliau – TS) reikalavimus:

TS reikalavimas	Pasiūlymo neaiškumai ir prašymas juos paaiškinti
TS 1 lentelė – **Patekimo kontrolės sistemos (toliau - PKS) programinė įranga serveriui (1 vnt.) ir darbo stotims (9 vnt.)**	Modeliai- 996901C; 996940-60; 995200PEEU3; 996018PCBK; 996535PCBK;* ***Neaišku.** Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų **prekių gamintojų aprašymus**.
1.2. Prieigos kontrolės modulis – turi būti	Pasiūlymo formos 1 priede nurodote – <Prieigų planavimo modulis (leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant gamintojų aprašymus ir/arba lygiaverčius gamintojų parengtus ir/ar patvirtintus dokumentus, įrodančius atitiktį šiam TS reikalavimui (-ams) (toliau tekste - **Įrodymai**)
1.3. Prieigų planavimo modulis (turi leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius) - Turi būti	Pasiūlymo formos 1 priede nurodote – <Yra prieigų planavimo modulis> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c

	patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.7. Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams - Turi būti	Pasiūlymo formos 1 priede nurodote – <Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.8. „Anti-passback“ funkcija - Turi būti	Pasiūlymo formos 1 priede nurodote – <Yra „Antipassback“ Funkcija> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Tokia funkcija Integrity nurodyta šiame apraše https://www.innerrange.com/downloads/programming_manual-integriti_guide_global_anti_passback Tačiau iš pateiktų dokumentų neaišku, ar įranga komplektuojama būtent tokiu kontroleriu (šiame apraše pagal nuorodą minima kontrolierių serija Controller firmware V3.2.x.xxxxx). Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.9. Duomenų bazės tipas SQL - Turi būti	Pasiūlymo formos 1 priede nurodote – <Duomenų bazės tipas SQL> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda - Integriti Hardening Guide- neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.10. Programinė įranga ne mažiau kaip 9 darbo stotims (3 (trys) darbo stotys turi turėti administratoriaus ir operatoriaus funkcionalumą, 6 (šešios) darbo stotys privalo turėti operatoriaus funkcionalumą). Pastaba. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos – Turi būti	Pasiūlymo formos 1 priede nurodote – <1.10. Programinė įranga ne mažiau kaip 30 darbo stotims. Kiekvieną darbo stotį galima suprogramuoti kad turėtų administratoriaus ir/arba operatoriaus funkcionalumą. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos.> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.11. Licencija (jei reikalinga) prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 10 durų su skaitytuvais papildomai- Turi būti	Pasiūlymo formos 1 priede nurodote – <Licencija prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 60 durų su skaitytuvais papildomai>. Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda, pateikta Pasiūlymo Priede Nr. 1 – Inner Range| 996940Integriti Door License – neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams) Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.

1.12. Sistema (įskaitant kontrolerius) privalo veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai turėtų vykdyti praleidimą pro duris, kurias jie kontroliuoja bei vykdyti sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio turi būti sinchronizuoti - Turi būti	Pasiūlymo formos 1 priede nurodote – **<** 1.12. Sistema (įskaitant kontrolerius) gali veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai vykdo praleidimą pro duris, kurias jie kontroliuoja bei vykdo sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio bus sinchronizuoti.> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda, pateikta Pasiūlymo Priede Nr. 1 – a8357f_9b86fb5bac5240ee90a08431400d53f7.pdf – neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.13. Duomenų šifravimui naudojamas šifravimo protokolas su ne trumpesniu nei 128 bitų raktu - Turi būti	Pasiūlymo formos 1 priede nurodote – <Duomenų šifravimui naudojamas šifravimo protokolas su 128 bitų raktu> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
1.14. Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka turi būti saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra) – turi būti	Pasiūlymo formos 1 priede nurodote – < Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka yra saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
TS 2 lentelė **PKS leidimų kortelės**	Modelis – 994610 Gamintojas – Inner range (Australija)
2.1. Veikimo dažnis 13,56MHz Turi būti	Pasiūlymo formos 1 priede nurodote – < Veikimo dažnis-13,56MHz > Pasiūlymo formos 1 priede pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant įrodymus.
2.2. DESFire® EV3 lustas Turi būti	Pasiūlymo formos 1 priede nurodote – < DESFire® EV3 lustas > Pasiūlymo formos 1 priede pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams)

	Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.
2.3. Palaikomas standartas ISO14443A arba lygiavertis	Pasiūlymo formos 1 priede nurodote – <Standartas Mifare DESFire©> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams) Be to, jeigu siūlomas standartas pavadintas „Standartas Mifare DESFire“, todėl jeigu siūlomas ISO 14443A lygiavertis standartas, turite pateikti jo lygiavertiškumo įrodymus.
2.4. Spalva - Balta	Pasiūlymo formos 1 priede nurodote – < Spalva balta> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.
2.5. Galimybė veikti -25° iki +40° temperatūros intervale - Turi būti	Pasiūlymo formos 1 priede nurodote – < Veikia -25° iki +40° temperatūros intervale> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.
TS 3 lentelė- **Skaitytuvas su klaviatūra**	Modelis – 994725MF +999046 Gamintojas – Inner Range ***Neaišku.** Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų **prekių gamintojų aprašymus**.
3.6. Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas - Turi būti	Pasiūlymo formos 1 priede nurodote – <Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas> Nors pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (a8357f_696cb4cb1c144d048a6d41a198da888f.pdf) neatsidaro, todėl iš jos komisijos nepavyko įsitikinti dėl jūsų siūlomo skaitytuvo su klaviatūra atitikties TS reikalavimams, tačiau Komisijai pavyko surasti gamintojo svetainėje siūlomos įrangos aprašymą, iš kurio Komisijai pavyko įsitikinti dėl dalies reikalavimų. Tačiau, teikiant atsakymą prašome pateikti veikiančią nuorodą į gamintojo aprašymą ir/arba gamintojų aprašymus. Pažymėtina, kad iš viešai skelbiamos informacijos Komisija mato - < Credentials: Mifare DESFire© **EV1/EV2** with AES encryption > Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus, kad siūlomas skaitytuvas turi ne tik Kortelių su DESFire®EV1/EV2 lustų palaikymą, bet ir EV3 lustų palaikymą.
TS 4 lentelė- **Skaitytuvas be klaviatūros**	Modeliai: 994720MF + 999037* Gamintojas – Inner Range

	***Neaišku.** Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų **prekių gamintojų aprašymus**.
4.5. Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas - Turi būti	Pasiūlymo formos 1 priede nurodote – <Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas> Nors pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (a8357f_696cb4cb1c144d048a6d41a198da888f.pdf) neatsidaro, todėl iš jos komisijos nepavyko įsitikinti dėl jūsų siūlomo skaitytuvo su klaviatūra atitikties TS reikalavimams, tačiau Komisijai pavyko surasti gamintojo svetainėje siūlomos įrangos aprašymą, iš kurio Komisijai pavyko įsitikinti dėl dalies reikalavimų. Tačiau, teikiant atsakymą prašome pateikti veikiančią nuorodą į gamintojo aprašymą ir/arba gamintojų aprašymus. Tačiau iš šis viešai pasiekiamos informacijos Komisija mato – < Credentials: Mifare DESFire©EV1/EV2 with AES encryption > Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus, kad siūlomas skaitytuvas turi ne tik Kortelių su DESFire®EV1/EV2 lustų palaikymą, bet ir EV3 lustų palaikymą.

Taip pat primename, kad visi pateikiami dokumentai turi atitikti visus pirkimo dokumentų reikalavimus, tarp jų:

- A dalies 7.1. punkto reikalavimai: „Pasiūlymai turi būti rengiami lietuvių kalba. Pažymos, diplomai, sertifikatai, pagrindžiantys tiekėjų pašalinimo pagrindų nebuvimą, techniniai aprašai ir analogiški dokumentai, įrodantys siūlomų prekių techninių parametrų atitikimą techninių specifikacijų reikalavimams, priimami ir lietuvių ar anglų ar rusų kalba. Jeigu dokumentai yra išduoti kita kalba, tokiu atveju prie šių dokumentų turi būti pridedamas viso pateikiamo dokumento teisingas vertimas į lietuvių ar anglų ar rusų kalbą, patvirtintas vertėjo parašu“.

Papildomai primename, kad aiškindamas pasiūlymą, tiekėjas privalo laikytis Viešųjų pirkimų tarnybos direktoriaus 2022 m. gruodžio 30 d. įsakymu Nr. 1S-240 patvirtintų Taisyklių reikalavimų (plačiau žr. – 1S-240 Dėl Pasiūlymų patikslinimo, papildymo ar paaiškinimo taisyklių patvirtinimo).

Viešųjų pirkimų komisijos pirmininkė

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	VĮ Ignalinos atominė elektrinė (102 / 103) 255450080, Elektrinės g.4, K 47, Drūkšinių k., 31152 Visagino sav., Lietuvos Respublika
Dokumento pavadinimas (antraštė)	DĖL PATEIKTO PASIŪLYMO PAAIŠKINIMO (PIRKIMO NR. 1984530)
Dokumento registracijos data ir numeris	2025-07-09 Nr. ĮS-2759(13.66E)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	2025-07-09 13:30:24 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-07-09 13:30:40 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2020-08-28 17:14:12 – 2025-08-27 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Ignalinos atominė elektrinė, VĮ, į.k. 255450080 LT", sertifikatas galioja nuo 2024-12-18 09:12:37 iki 2027-12-18 09:12:37
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.79.2
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2025-07-09 13:40:22)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2025-07-09 13:40:26 Dokumentų valdymo sistema Avilys

Bureau Veritas Certification

Spectra Baltic, UAB

Baltų pr. 145, LT-47125 Kaunas

Šis sertifikatas apima daugiau nei vieną veiklos padalinį; kitas(-i) padalinys(-iai) nurodytas(-i) kitame(-uose) puslapyje(-iuose)

Šiuo sertifikatu Bureau Veritas Certification Holding SAS - UK Branch patvirtina, kad įvertino nurodytos organizacijos vadybos sistemą ir nustatė, jog ji atitinka toliau nurodyto vadybos sistemos standarto reikalavimus

ISO 9001:2015

Sertifikavimo sritis

Elektronikos, elektrotechnikos, silpnų srovių: apsaugos ir įeigos sistemų, vaizdo stebėjimo, informacinių technologijų, telekomunikacijų sričių prekių tiekimas, pardavimas, projektavimas ir techninė priežiūra

Pirmojo sertifikavimo ciklo pradžios data :	**11-10-2021**
Ankstesnio sertifikavimo ciklo pabaigos data:	**—**
Sertifikavimo (pakartotinio sertifikavimo) audito data:	**—**
Sertifikavimo (pakartotinio sertifikavimo) ciklo pradžios data:	**31-07-2023**
Organizacijos vadybos sistemai nuolat atitinkant nurodyto standarto reikalavimus, šis sertifikatas baigia galioti:	**30-07-2026**

Sertifikato Nr.: **LT006837** Ver.: **1** Išdavimo data: **31-07-2023**

UKAS MANAGEMENT SYSTEMS
0008

BVCH SAS UK Branch vardu

Sertifikavimo įstaigos adresas: 5th Floor, 66 Prescot Street, London, E1 8HG, Jungtinė Karalystė

Sertifikatą išdavė: Ukmergės g. 369A, LT-12142 Vilnius

Norėdami gauti daugiau informacijos apie šio sertifikato sritį ir galiojimą bei apie vadybos sistemos reikalavimų taikymą, prašom skambinti: +370 5 233 79 75

Bureau Veritas Certification

Spectra Baltic, UAB

ISO 9001:2015

Sertifikavimo sritis

Padalinio pavadinimas ir(arba) adresas	Padalinio adresas	Padalinio sertifikavimo sritis
Kauno centrinis padalinys	Baltų pr. 145, LT-47125 Kaunas	Elektronikos, elektrotechnikos, silpnų srovių: apsaugos ir įeigos sistemų, vaizdo stebėjimo, informacinių technologijų, telekomunikacijų sričių prekių tiekimas, pardavimas, projektavimas ir techninė priežiūra
Klaipėdos padalinys	Baltijos pr. 113, LT-93221 Klaipėda	Elektronikos, elektrotechnikos, silpnų srovių: apsaugos ir įeigos sistemų, vaizdo stebėjimo, informacinių technologijų, telekomunikacijų sričių prekių tiekimas, pardavimas ir techninė priežiūra
Vilniaus padalinys	T. Ševčenkos g. 20-44, LT-03111 Vilnius	

Sertifikato Nr.: **LT006837** Ver.: **1** Išdavimo data: **31-07-2023**

UKAS MANAGEMENT SYSTEMS
0008

BVCH SAS UK Branch vardu

Sertifikavimo įstaigos adresas: 5th Floor, 66 Prescot Street, London, E1 8HG, Jungtinė Karalystė

Sertifikatą išdavė: Ukmergės g. 369A, LT-12142 Vilnius

Norėdami gauti daugiau informacijos apie šio sertifikato sritį ir galiojimą bei apie vadybos sistemos reikalavimų taikymą, prašom skambinti: +370 5 233 79 75

IŠSAMI INFORMACIJA

PIRKIMO ID	1984530
PIRKIMO PROCESAS	1
PRANEŠIMO ID	280760
SIUNTĖJAS	Spectra Baltic
KONFIDENCIALU	Ne
TEMA	RE: Dėl pateikto pasiūlymo paaiškinimo
IŠSIŲSTA	15/07/2025 14:43
ATIDARYTA	15/07/2025 14:44
STATUSAS	Skaityti
PRIEDAI	Dokumentai pasiūlymo paaiškinimui siuntimui.zip (12.784145355224609375 MB)

TURINYS

On 09/07/2025, Valstybės įmonė Ignalinos atominė elektrinė wrote:
Žr. pridedamą dokumentą.

Laba diena,

Siunčiame jums mūsų pasiūlymo paaiškinimus

PRANEŠIMŲ ISTORIJA

10 Rezultatai viename puslapyje | Rodomos visos **2** atitiktys.

Vartotojas	Veiksmas	Data
	Peržiūrėti	15/07/2025 14:44
	Siųsti	15/07/2025 14:43

VALSTYBĖS ĮMONĖ
IGNALINOS ATOMINĖ ELEKTRINĖ
Elektrinės g. 4, K 47, Drūkšinių k.
31152 Visagino sav.

DĖL PATEIKTO PASIŪLYMO PAAIŠKINIMO (PIRKIMO NR. 1984530)
2025-07-15
Kaunas

Siunčiame jums kaip mūsų siūlomos prekės atitinka „Patekimo kontrolės sistemos pirkimas pirkimo techninės specifikacijos‘ (toliau – TS) reikalavimus:.

TS reikalavimas	Pasiūlymo neaiškumai ir prašymas juos paaiškint	Neaiškumų paaiškinimai
TS 1 lentelė – Patekimo kontrolės sistemos (toliau - PKS) programinė įranga serveriui (1 vnt.) ir darbo stotims (9 vnt.)	Modeliai 996901C; 996940-60; 995200PEEU3; 996018PCBK; 996535PCBK;* *Neaišku. Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų prekių gamintojų aprašymus.	Siunčiame nurodytų modelių gamintojų aprašymus: https://www.innerrange.com/products/software-licenses/996901c https://www.innerrange.com/products/software-licenses/996940 https://www.innerrange.com/products/enclosures-power/995200 https://www.innerrange.com/products/expansion-modules/996018pcbk https://www.innerrange.com/products/expansion-modules/996535pcbk
.2. Prieigos kontrolės modulis – turi būti	Pasiūlymo formos 1 priede nurodote – <Prieigų planavimo modulis (leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant gamintojų aprašymus ir/arba lygiaverčius gamintojų parengtus ir/ar patvirtintus dokumentus, įrodančius atitiktį šiam TS reikalavimui (-ams) (toliau tekste - Įrodymai)	Įrodymai, kad prieigų planavimo modulis leidžia konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius: Įrodymai yra surašyti prisegtuose dokumentuose: Integriti User Guide.pdf 8,9 psl. ir System Configuration Handbook.pdf 41 psl.
1.3. Prieigų planavimo modulis (turi leisti konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius) - Turi būti	Pasiūlymo formos 1 priede nurodote – <Yra prieigų planavimo modulis> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c Elektroninio dokumento nuorašas 2 patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Prieigų planavimo modulis leidžia konfigūruoti prieigų (kortelių) galiojimo tvarkaraščius: Įrodymai yra surašyti prisegtame dokumente: Integriti User Guide.pdf 10 psl.
1.7. Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams - Turi būti	Pasiūlymo formos 1 priede nurodote – <Modulis, leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Modulis leidžiantis realiu laiku stebėti visų sistemos įrenginių būseną bei siųsti komandas įrenginiams: Įrodymai yra surašyti prisegtame dokumente: Integriti User Guide.pdf 4, 21, 33 psl.
1.8. „Anti-passback“ funkcija - Turi būti	Pasiūlymo formos 1 priede nurodote – <Yra „Antipassback“ Funkcija> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Tokia funkcija Integrity nurodyta šiame apraše https://www.innerrange.com/downloads/programming_manualintegriti_guide_global_anti_passback Tačiau iš pateiktų dokumentų neaišku, ar įranga komplektuojama būtent tokiu kontroleriu (šiame apraše pagal nuorodą minima kontrolierių serija Controller firmware V3.2.x.xxxxx). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad įranga yra pasiūlyta su „Anti-passback“ funkcija: Įrodymai yra surašyti prisegtuose dokumentuose: System Configuration Handbook.pdf 41 psl, Guide - Global anti-passback.pdf visas dokumentas

1.9. Duomenų bazės tipas SQL - Turi būti	Pasiūlymo formos 1 priede nurodote – <Duomenų bazės tipas SQL> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda - Integriti Hardening Guide- neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Duomenų bazės tipas SQL: Įrodymai yra surašyti prisegtame dokumente: Hardware and Software Prerequisites.pdf -3 psl
1.10. Programinė įranga ne mažiau kaip 9 darbo stotims (3 (trys) darbo stotys turi turėti administratoriaus ir operatoriaus funkcionalumą, 6 (šešios) darbo stotys privalo turėti operatoriaus funkcionalumą). Pastaba. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos – Turi būti	Pasiūlymo formos 1 priede nurodote – <1.10. Programinė įranga ne mažiau kaip 30 darbo stotims. Kiekvieną darbo stotį galima suprogramuoti kad turėtų administratoriaus ir/arba operatoriaus funkcionalumą. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos.> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Programinė įranga yra 30 darbo stotims. Kiekvieną darbo stotį galima suprogramuoti kad turėtų administratoriaus ir/arba operatoriaus funkcionalumą. Darbo stotyse instaliuotos Windows 11 x64 operacinės sistemos: Įrodymai yra surašyti prisegtuose dokumentuose: apie 30 darbo vietų -Integriti License Change Release Notes.pdf - lentelė 2 psl.; apie operatorių rogramavimą:Guide - Operator Tenancies.pdf - visas failas, System Configuration Handbook.pdf 150 psl.; apie darbo stotis - Hardware and Software Prerequisites.pdf -5 psl
1.11. Licencija (jei reikalinga) prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 10 durų su skaitytuvais papildomai- Turi būti	Pasiūlymo formos 1 priede nurodote – <Licencija prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 60 durų su skaitytuvais papildomai>. Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą)- https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda, pateikta Pasiūlymo Priede Nr. 1 – Inner Range| 996940Integriti Door License – neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams) Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus	Įrodymai, Licencija prijungti prie šioje techninėje specifikacijoje nurodyto įrenginių kiekio ne mažiau kaip 10 durų su skaitytuvais: Įrodymai yra surašyti prisegtame dokumente: Integriti License Change Release Notes.pdf -2 psl Ir nuorodoje: https://www.innerrange.com/products/software-licenses/996940
1.12. Sistema (įskaitant kontrolerius) privalo veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai turėtų vykdyti praleidimą pro duris, kurias jie kontroliuoja bei vykdyti sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio turi būti sinchronizuoti - Turi būti	Pasiūlymo formos 1 priede nurodote – < 1.12. Sistema (įskaitant kontrolerius) gali veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai vykdo praleidimą pro duris, kurias jie kontroliuoja bei vykdo sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio bus sinchronizuoti.> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Kita nuoroda, pateikta Pasiūlymo Priede Nr. 1 – a8357f_9b86fb5bac5240ee90a08431400d53f7.pdf – neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Sistema (įskaitant kontrolerius) gali veikti „offline“ režimu, t. y. dingus ryšiui tarp kontrolerių ir serverio kontroleriai vykdo praleidimą pro duris, kurias jie kontroliuoja bei vykdo sisteminių įrašų archyvavimą. Ryšiui atsistačius sisteminiai pranešimai tarp kontrolerio ir serverio bus sinchronizuoti: Įrodymai yra surašyti prisegtame dokumente: Guide - ILAM Offline Operation.pdf 1 psl
1.13. Duomenų šifravimui naudojamas šifravimo protokolas su ne trumpesniu nei 128 bitų raktu -	Pasiūlymo formos 1 priede nurodote – <Duomenų šifravimui naudojamas šifravimo protokolas su 128 bitų raktu> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Duomenų šifravimui naudojamas šifravimo protokolas su 128 bitų raktu: Įrodymai yra surašyti prisegtame dokumente: Inner Range Integriti Cyber Security Summary May 2025.pdf. -

Turi būti		visas dokumentas ir Integriti - Encryption Overview.pdf. – visas dokumentas
1.14. Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka turi būti saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra) – turi būti	Pasiūlymo formos 1 priede nurodote – < Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka yra saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).> Tačiau gamintojo aprašyme (kuris pasiekimas pagal nuorodą) – https://www.innerrange.com/products/software-licenses/996901c patvirtinančios informacijos neradome. Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus	Įrodymai, kad yra Vartotojo atvaizdavimas sistemoje (Vartotojo foto nuotrauka yra saugoma patekimo sistemos programinės įrangos duomenų bazėje. Pridėjus kortelę prie skaitytuvo sistemos pranešimų lange turi būti matoma darbuotojo fotonuotrauka, kuri turi sutapti su foto nuotrauka ant kortelės (vizualinė darbuotojų patikra).: Įrodymai yra surašyti prisegtame dokumente: Guide - Operator Challenge.pdf 5 psl
TS 2 lentelė PKS leidimų kortelės	Modelis – 994610 Gamintojas – Inner range (Australija)	
2.1. Veikimo dažnis 13,56MHz Turi būti	asiūlymo formos 1 priede nurodote – < Veikimo dažnis13,56MHz > Pasiūlymo formos 1 priede pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Veikimo dažnis13,56MHz: Įrodymai yra surašyti prisegtame dokumente: Inner Range - Sifer Credentials.pdf visas failas ir nuorodoje: https://www.innerrange.com/products/user-interface/994610
2.2. DESFire® EV3 lustas Turi būti	Pasiūlymo formos 1 priede nurodote – < DESFire® EV3 lustas > Pasiūlymo formos 1 priede pateikta nuoroda į gamintojo aprašymą (Inner-Range-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams) 4 Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad Veikimo dažnis13,56MHz: Įrodymai yra surašyti prisegtame dokumente: Inner Range - Sifer Credentials.pdf visas failas ir nuorodoje: https://www.innerrange.com/products/user-interface/994610
2.3. Palaikomas standartas ISO14443A arba lygiavertis	Pasiūlymo formos 1 priede nurodote – <Standartas Mifare DESFire©> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (InnerRange-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams) Be to, jeigu siūlomas standartas pavadintas „Standartas Mifare DESFire“, todėl jeigu siūlomas ISO 14443A lygiavertis standartas, turite pateikti jo lygiavertiškumo įrodymus.	Įrodymai, kad yra palaikomas standartas ISO14443A yra pateikti oficialiame gamintojo laiške Sifer ISO Cards.pdf
2.4. Spalva - Balta	Pasiūlymo formos 1 priede nurodote – < Spalva balta> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (InnerRange-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams). Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus.	Įrodymai, kad spalva yra Balta yra pateikti oficialiame gamintojo laiške Sifer ISO Cards.pdf
2.5. Galimybė veikti -25° iki +40° temperatūros intervale - Turi būti	Pasiūlymo formos 1 priede nurodote – < Veikia -25° iki +40° temperatūros intervale> Pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (InnerRange-994610-ISO-Card-Data-Sheet.pdf) neatsidaro, todėl iš jos komisija taip pat negali įsitikinti dėl atitikimo TS reikalavimui (-ams).	Įrodymai, kad kortelės gali veikti -25° iki +40° temperatūros intervale yra pateikti oficialiame gamintojo laiške Sifer ISO Cards.pdf

	Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus	
TS 3 lentelėSkaitytuvas su klaviatūra	Modelis – 994725MF +999046 Gamintojas – Inner Range *Neaišku. Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų prekių gamintojų aprašymus	Siunčiame nurodyto modelio gamintojo aprašymą: https://www.innerrange.com/products/user-interface/994725
3.6. Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas - Turi būti	Pasiūlymo formos 1 priede nurodote – <Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas> Nors pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (a8357f_696cb4cb1c144d048a6d41a198da888f.pdf) neatsidaro, todėl iš jos komisijos nepavyko įsitikinti dėl jūsų siūlomo skaitytuvo su klaviatūra atitikties TS reikalavimams, tačiau Komisijai pavyko surasti gamintojo svetainėje siūlomos įrangos aprašymą, iš kurio Komisijai pavyko įsitikinti dėl dalies reikalavimų. Tačiau, teikiant atsakymą prašome pateikti veikiančią nuorodą į gamintojo aprašymą ir/arba gamintojų aprašymus. Pažymėtina, kad iš viešai skelbiamos informacijos Komisija mato - < Credentials: Mifare DESFire© EV1/EV2 with AES encryption > Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus, kad siūlomas skaitytuvas turi ne tik Kortelių su DESFire®EV1/EV2 lustų palaikymą, bet ir EV3 lustų palaikymą.	Įrodymai, kad skaitytuvas palaiko Kortelies su DESFire EV1/EV2/EV3 lustais šioje nuorodoje: https://www.innerrange.com/products/user-interface/994725
TS 4 lentelėSkaitytuvas be klaviatūros	Modeliai: 994720MF + 999037* Gamintojas – Inner Range 5 *Neaišku. Vadovaujantis Pirkimo dokumentuose nustatytais reikalavimais turite pateikti visų Pasiūlymo Lentelėje Nr. 1 siūlomų prekių gamintojų aprašymus	Siunčiame nurodyto modelio gamintojo aprašymą: https://www.innerrange.com/products/user-interface/994720
4.5. Kortelių su DESFire®EV1/EV2/EV3 lustais palaikymas - Turi būti	Pasiūlymo formos 1 priede nurodote – <Kortelių su DESFire EV1/EV2/EV3 lustais palaikymas> Nors pasiūlymo formoje pateikta nuoroda į gamintojo aprašymą (a8357f_696cb4cb1c144d048a6d41a198da888f.pdf) neatsidaro, todėl iš jos komisijos nepavyko įsitikinti dėl jūsų siūlomo skaitytuvo su klaviatūra atitikties TS reikalavimams, tačiau Komisijai pavyko surasti gamintojo svetainėje siūlomos įrangos aprašymą, iš kurio Komisijai pavyko įsitikinti dėl dalies reikalavimų. Tačiau, teikiant atsakymą prašome pateikti veikiančią nuorodą į gamintojo aprašymą ir/arba gamintojų aprašymus. Tačiau iš šis viešai pasiekiamos informacijos Komisija mato – < Credentials: Mifare DESFire©EV1/EV2 with AES encryption > Prašome paaiškinti Jūsų pasiūlymą, pateikiant Įrodymus, kad siūlomas skaitytuvas turi ne tik Kortelių su DESFire®EV1/EV2 lustų palaikymą, bet ir EV3 lustų palaikymą	Įrodymai, kad skaitytuvas palaiko Kortelies su DESFire EV1/EV2/EV3 lustais šioje nuorodoje: https://www.innerrange.com/products/user-interface/994720

Tikimės tolimesnio produktyvaus bendradarbiavimo.

(Parašas)

spectra baltic
UAB Spectra Baltic
Įmonės kodas 304635904
PVM kodas LT100012460119
Baltų pr. 145,
LT-47125 Kaunas
+370 37 334 074
info@spectrabaltic.lt
www.spectrabaltic.lt

Back

Integriti Corporate Edition

996901C

The Corporate Edition takes everything from Professional and Business and adds the ability to have up to 30 operators utilising the system at the same time as well as the ability to connect an unlimited number of CCTV cameras.

Advanced security applications for organisations requiring a high level of security and advanced onsite guarding features are also included such as Advanced Alerts, Operator Challenge, Guard Tour and SNMP Health monitoring.

Business to Corporate Upgrade – 996901UPGC

Features | Related products | Ordering Options | Documents | Software & Firmware | Media

Included Features

- User Management, System Programming, System Status, Programming History (Audit Trail)
- Hassle Free IP Connection with SkyTunnel *a
- Software Operator Permissions
- GateKeeper – A Dedicated Application for Daily End User Operations
- Additional Workstations / Clients (Floating or Fixed)
- Support for Multiple Controllers
- Schematic Graphical Maps with Scalable Vector based graphics
- Alarm Management
- Smartphone-Server Interface
- Communicator - Email, SMS & Pager
- Photo ID Card Design
- Dynamic User Import Module (DUIM)
- Advanced Reports
- Web-based Client for Desktop or Mobile Devices (Responsive)
- CCTV Integration *b
- CCTV Licence Plate Recognition Integration
- Active Directory Integration - Operators
- Active Directory Integration - Users
- User Qualifications Manager
- Advanced Alarm Management, Alarm Escalation, Response Plans & Operator Challenge. *c
- SNMP & Health Monitor
- Guard Tour Manager

Optional Features

- 3rd Party Door Integration
- Event Review I/O Communications
- Milestone XProtect Access ACM Integration
- Mobile Credential Management Integration
- Modbus BMS Integration
- KeyLocker / Locker Integration
- Elevator Management Integration (Lift HLI)
- Additional Server Node - HA / Load Spreading
- Inner Range Mobile Reader Application
- Biometric Management Integration
- Intercom Integration
- Visitor Management Integration
- VingCard Integration
- RightCrowd Enterprise Integration
- Real-Time Location System (RTLS) Integration
- Active User Rotation Module (AURM)
- XML Integration (Technology Partner Program)

a. - SkyTunnel provides non-permanent connections between Integriti Controllers, Integriti software and the Integriti Mobile App.
b. - Businness Edition includes 32 Cameras, which can be expanded further.
c. - Basic alert functionality is included as standard with the Professional & Business Editions. However, advanced alert functions such as Response Plans, Alert Escalations, Alert Reporting
and Operator Challenge requires the Corporate Edition.

Back

Address
1 Millennium Court Knoxfield, Victoria, 3180, Australia

Call Us
+61 3 9780 4300

Mail Us
sales.au@innerrange.com

Back

Integriti Door License

996940

The base packages of Integriti Professional, Business and Corporate include the connection of the first 16 Doors. Additional Door licenses are required (per door). where more than 16 Doors are needed.

The Integriti server totals the number Doors across all Controllers that are connected to the server.

Related products | Ordering Options | Documents

	Global
Integriti Door License	996940

Back

Address
1 Millennium Court Knoxfield, Victoria, 3180, Australia

Call Us
+61 3 9780 4300

Mail Us
sales.au@innerrange.com

Back

Small Enclosure

995200

The Small Enclosure is a universal sturdy metal enclosure designed for general purpose installation of small size Inner Range modules and equipment. In addition to the power supply PCB, 1 x "B" size or 2 x "C" size PCB's may be fitted per enclosure.

A range of powered or non-powered versions are available.

The Small Enclosure's low profile side elevation protrudes less than 90mm from the mounting surface.

Features | Related products | Ordering Options | Documents

Enclosure Features:

- Robust metal enclosure
- Mounting option for a 9Ah Lead Acid Battery
- Low Profile design Size 252(L) x 358(W) x 85(D) (mm)

Back

Address
1 Millennium Court Knoxfield, Victoria, 3180, Australia

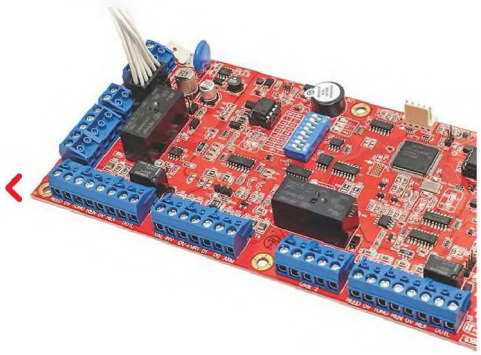
Call Us
+61 3 9780 4300

Mail Us
sales.au@innerrange.com

Back

Intelligent LAN Access Module (ILAM)

996018PCB&K



The Intelligent LAN Access Module (ILAM) can be used to control and monitor up to 8 Doors or Lift cars on the Inner Range RS-485 LAN, or via IP LAN if connected using Ethernet Bridge or CLOE devices. The base module supports 2 doors/2 readers and is expandable up to 8 doors/8 readers with the simple addition of 2 Door expander boards via the UniBus in-cabinet expansion interface.

The Intelligent LAN Access Module offers a complete suite of programmable options to provide advanced high-security access control, security area control and door alarm monitoring functions.
Offline intelligence is also provided via the on-board database to provide access control functionality and event logging even if communications to the master controller are severed. Upon reconnection, all buffered events and any programming changes are automatically synchronised with the main Controller.

The ILAM is also used for integration of wireless door locking systems from Assa Abloy Aperio, SimonsVoss or Salto Sallis.

Intelligent LAN Access Module with UniBus In-Cabinet Expansion

- Up to 8 Doors
- Up to 8 Wiegand readers or 16 SIFER RS-485 Readers
- Up to 8 Lift cars

Features | Related products | Ordering Options | Documents | Software & Firmware | Media

Module Features

- RS-485 LAN connectivity
- RS-485 Reader connectivity (up to 16 SIFER or third party OSDP Readers)
- Reader options to control Doors, Lifts, Areas and User Logon
- Supports Wiegand card readers up to 88bits
- Reader outputs with individual self-resetting overcurrent protection
- UniBus in-cabinet expansion interface
- Dedicated lock power input
- External Inner Range power supply connection
- Full monitoring of external Inner Range power supply
- Heavy duty lock relays
- Reader Valid & Invalid outputs
- Door reed & tongue sense inputs per door
- Door request to enter & exit inputs per door
- DOTL relay outputs per door
- Dedicated cabinet tamper input
- Small PCB size 200 x 95mm
- Over-The-Wire firmware upgradable
- Built-in module locater buzzer

Doors, Expansion & Integration Options

- Expandable to 8 Doors (2 Doors on-board)
- Expandable to 16 Inner Range SIFER or third party OSDP RS-485 readers via the dedicated RS-485 reader port
- Expandable to 8 Wiegand Readers (2 Readers on-board)
- Five enclosure sizes allow 2, 4, 6 or 8 Door/Reader configurations

- Three plug on external power supply options (2A, SMART 3A or SMART 8A Switch Mode)
- Aperio, SimonsVoss, Salto Sallis integration - up to 8 Doors via RS-485 Reader port
- Lift button I/O interfacing via optional UniBus Lift interface card (Up to 96 Floors)

Offline Intelligence

- Offline intelligence provided for all Wiegand readers and standard lock outputs
- Offline Access Control database for 100,000 users with Integriti and 10,000 users with Inception
- Offline time periods
- Offline event database of 100,000 events

Back

Australia / NZ | Asia | Canada | Middle East | UK / Europe | USA

Address
1 Millennium Court Knoxfield, Victoria, 3180, Australia

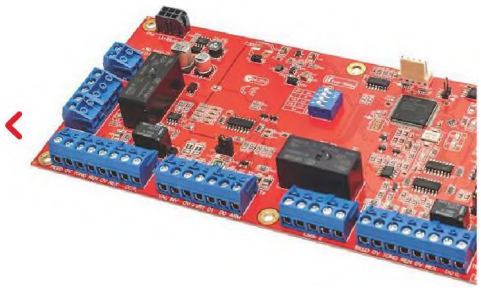
Call Us
+61 3 9780 4300

Mail Us
sales.au@innerrange.com

Back

UniBus 2 Door 2 Reader Expander

996535PCB&K



The UniBus 2 Door / 2 Reader Expander can be used to provide control and monitoring of 2 additional Doors or Readers on a compatible UniBus host module. When connected to the Intelligent LAN Access Module, the UniBus 2 Door / 2 Wiegand Reader expander can provide installation configurations for 4, 6 or 8 doors. SIFER or third party OSDP RS-485 readers can be assigned via the host module for Read In & Read Out access control on each door.

The UniBus 2 Door / 2 Reader Expander is designed for installation within the same tamper-protected enclosure as its UniBus host module. The UniBus device is connected directly to the host module or daisy-chained to another UniBus device via the UniBus patch cable supplied. Up to 3 UniBus 2 Door / 2 Reader Expander devices can be connected.

Host Module Compatibility
The UniBus 2 Door / 2 Reader Expander is compatible with the following UniBus Host Modules:

- Intelligent LAN Access Module (Part. 996018PCB&K)
- Integriti IAC Controller (Part. 996035PCB&K)

Features Related products Ordering Options Documents Software & Firmware

Module Features

- Provides an additional 2 Doors / 2 Wiegand Readers for Host Module
- Assign Read In & Read Out SIFER or third party OSDP RS-485 readers for each door via the Host Module
- UniBus connectivity to Host Module
- Reader options to control Doors, Lifts, Areas and User Logon
- Supports Wiegand card readers up to 88bits
- Reader outputs with individual self-resetting over current protection
- UniBus loop-through connectors
- LED Status & Fault Indicators
- Dedicated lock power input
- Heavy duty lock relays
- Reader Valid & Invalid Outputs
- Door reed & tongue sense inputs per door
- Door request to enter & exit inputs per door
- DOTL relay outputs per door
- Integriti "B" size footprint 200 x 94mm
- Over-The-Wire firmware upgradable

Back

INTEGRITI USER GUIDE

www.innerrange.com

inner range

Intelligent Security Solutions

TABLE OF CONTENTS

TABLE OF CONTENTS

INTEGRITI SOFTWARE

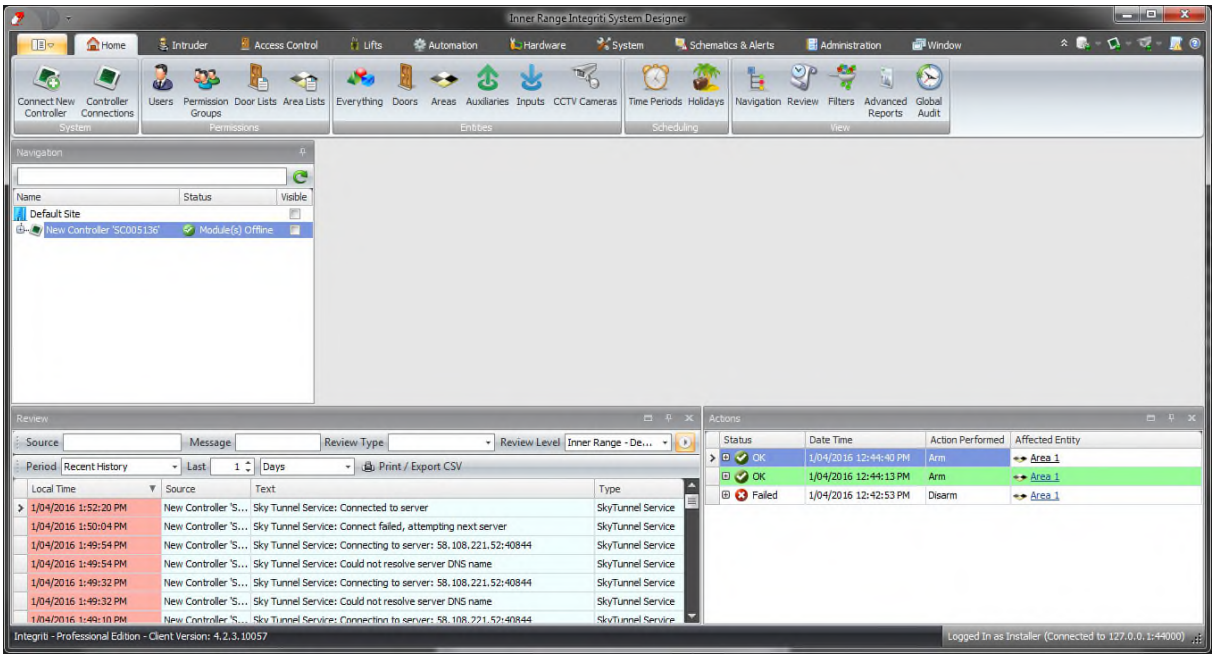
SOFTWARE APPLICATIONS

The Integriti software suite includes two applications:

- Integriti System Designer for system programming and configuration.
- Integriti GateKeeper for everyday control and monitoring.

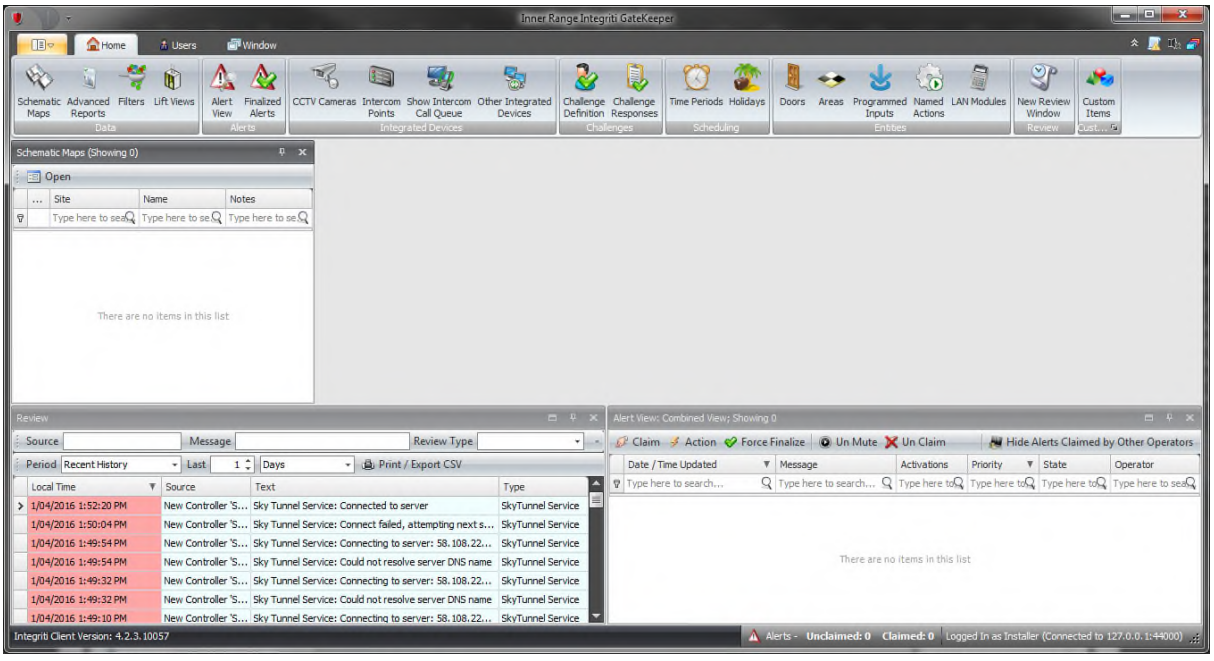
INTEGRITI SYSTEM DESIGNER

Integriti System Designer is commonly used to configure and administer your site; this application contains setting and options that if changed can affect the overall functionality of the site. In most cases System Designer is used by your Installer to commission the system or to perform maintenance. Your site administrator may need access to Integriti System Designer to make programming changes.



INTEGRITI GATEKEEPER

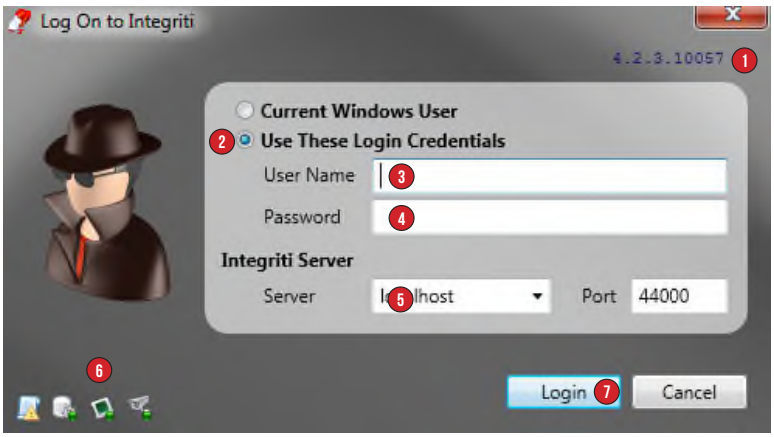
Integriti GateKeeper provides you with a simplified version of System Designer, which only shows items commonly used to monitor your site. GateKeeper does not allow you to access options that if changed would affect the overall security of the site. GateKeeper is commonly used to monitor and change the state of areas or doors and programme users.



LOGIN WINDOW

To launch System Designer or GateKeeper, navigate to the **Start Menu > All Programs > Inner Range** folder and click the applications icon. Once an application is launched a login window will appear, this window is identical for System Designer and GateKeeper. To log into the application, enter your operator name and password then click the **Login** button.

The **Login** window contains the following options:



1. The **Software Version** number identifies which version of the software you have installed.

2. The default method for logging into System Designer and GateKeeper is **Use These Login Credentials.** This method allows you to login by entering your user name and password. If your software has been configured to use the **Current Windows User** option, you can login without needing to enter a user name and password. This login option is configured by your installer and requires additional licenses.

3. Enter your **User Name** in this field.

4. Enter your **Password** in this field.

5. Do not change the **Integriti Server** settings unless instructed to do so by your Installer.

6. The **Server Icons** show the status of the servers that are required for the software to operate.

INTEGRITI SERVERS

The Integriti servers are required for System Designer and GateKeeper to run, connect to controllers and CCTV systems.

Before you login to System Designer or GateKeeper make sure the Integriti servers are started, this is indicated by a green dot. If they have not started, right-click the **Servers Icon** and click **Start**.

If the integriti servers are not visible you may be on a client workstation or the application was not launched with administrator privileges.

The table below shows all the possible states for the Integriti servers.

	Stopped	Stopping	Starting	Started
Integriti Application Server				
Integriti Controller Server				
Integriti Integration Server				

SOFTWARE NAVIGATION

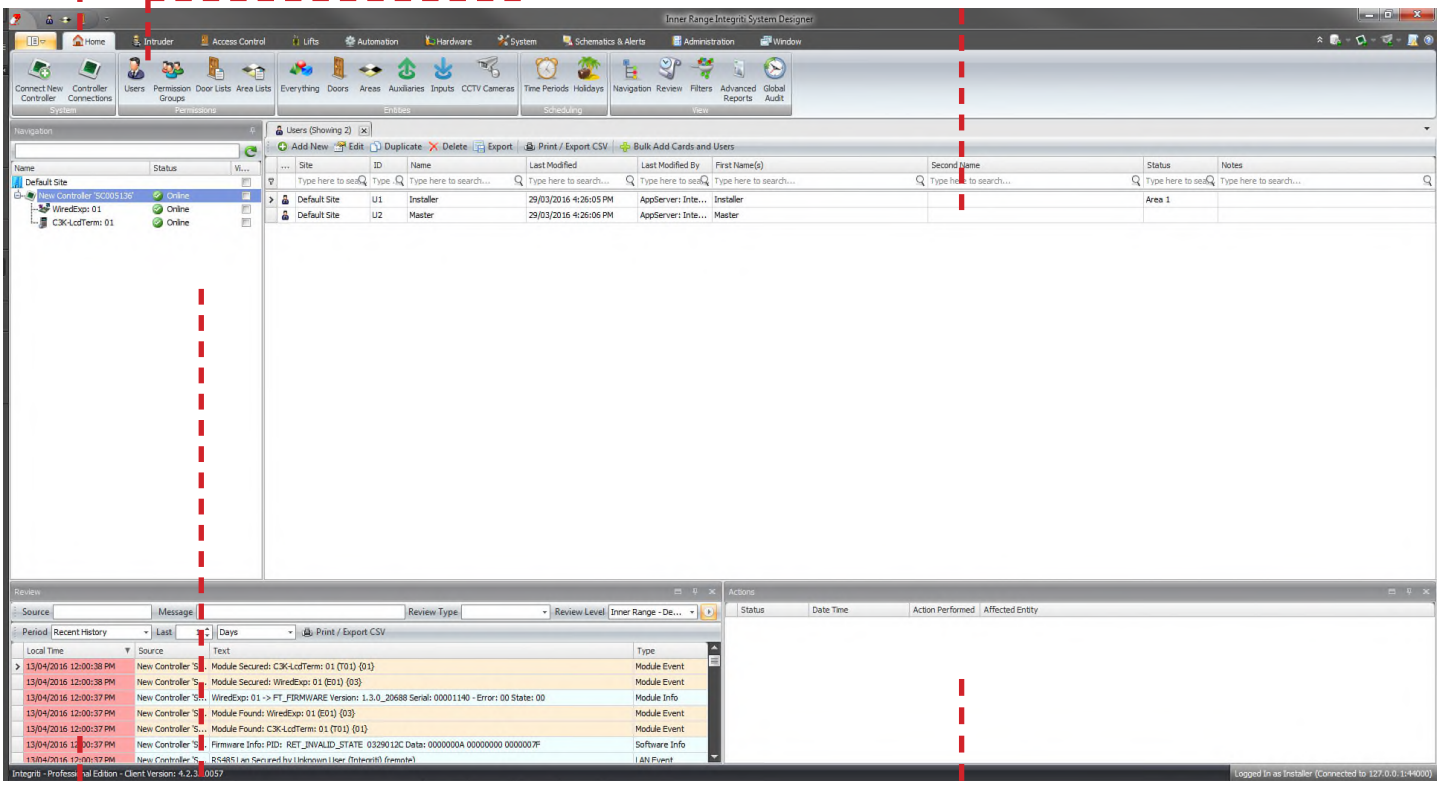
USER INTERFACE

The default layout for System Designer and GateKeeper share common elements. Below is a breakdown of the System Designer interface.

Quick Access Tool-bar

Ribbon

Workspace



Review Panel

Navigation Panel

Actions Panel

RIBBON

The Ribbon is designed to help you quickly find the items you need to programme or monitor the system. Items are organized into logical groups, which are collected under tabs. Each tab relates to a type of function, such as Intruder or Access Control tabs.

Tabs

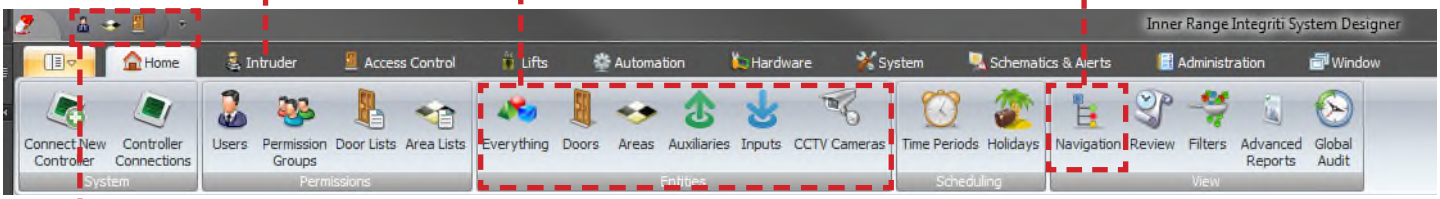
The tabs arrange all the items by category. The **Home Tab** has the most commonly used items.

Groups

Each tab is divided into smaller groups based on their function

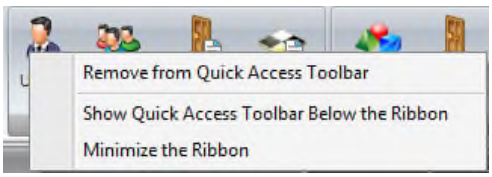
Icons

Each icon relates to a specific system item that can be programmed or monitored.



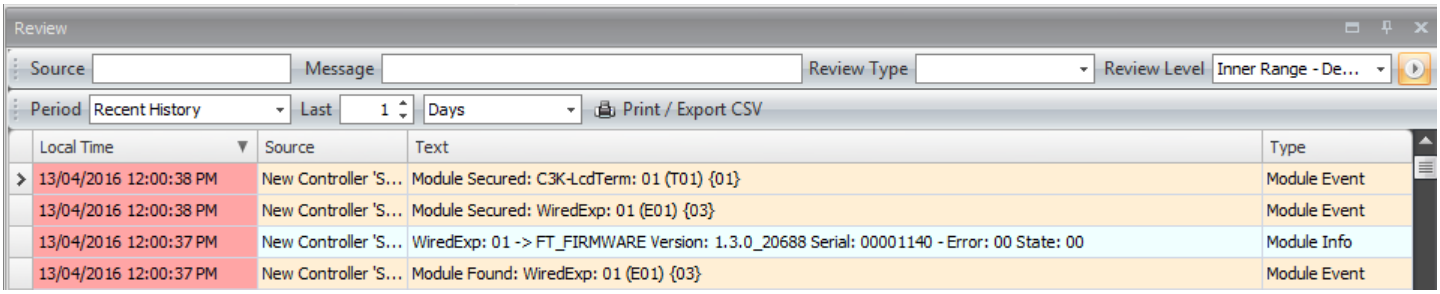
Quick Access Toolbar

The Quick Access Toolbar provides a location that you can save commonly used items so that they can be opened without navigating through the ribbon. Right-click on any icon and select the **Add to Quick Access Toolbar** option to display the item in the Quick Access Toolbar.



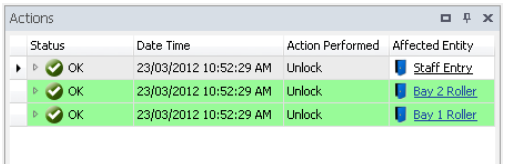
REVIEW PANEL

The **Review** panel is located at the bottom left of the Integriti System Designer window by default. Review is a historical log of the events that have occurred on the security controller or within the software.



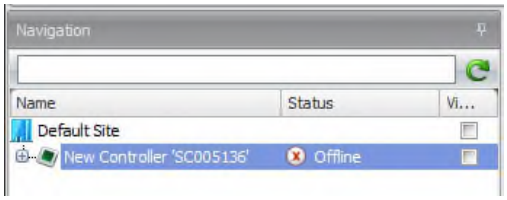
ACTIONS PANEL

The **Actions** panel displays actions that are performed by an operator from the software. The action list will display if the action was successful or failed.



NAVIGATION PANEL

The **Navigation** panel displays the sites, sub-sites, controllers and hardware modules on the system. This display can be used to view the state of controllers and modules or to trigger commands such as connecting or disconnecting a controller.



EDITOR WINDOW

When an item such as a user, area or door is edited, all the options and properties appear in an Editor Window. There are some common elements between editor windows for different items.

Tool Bar

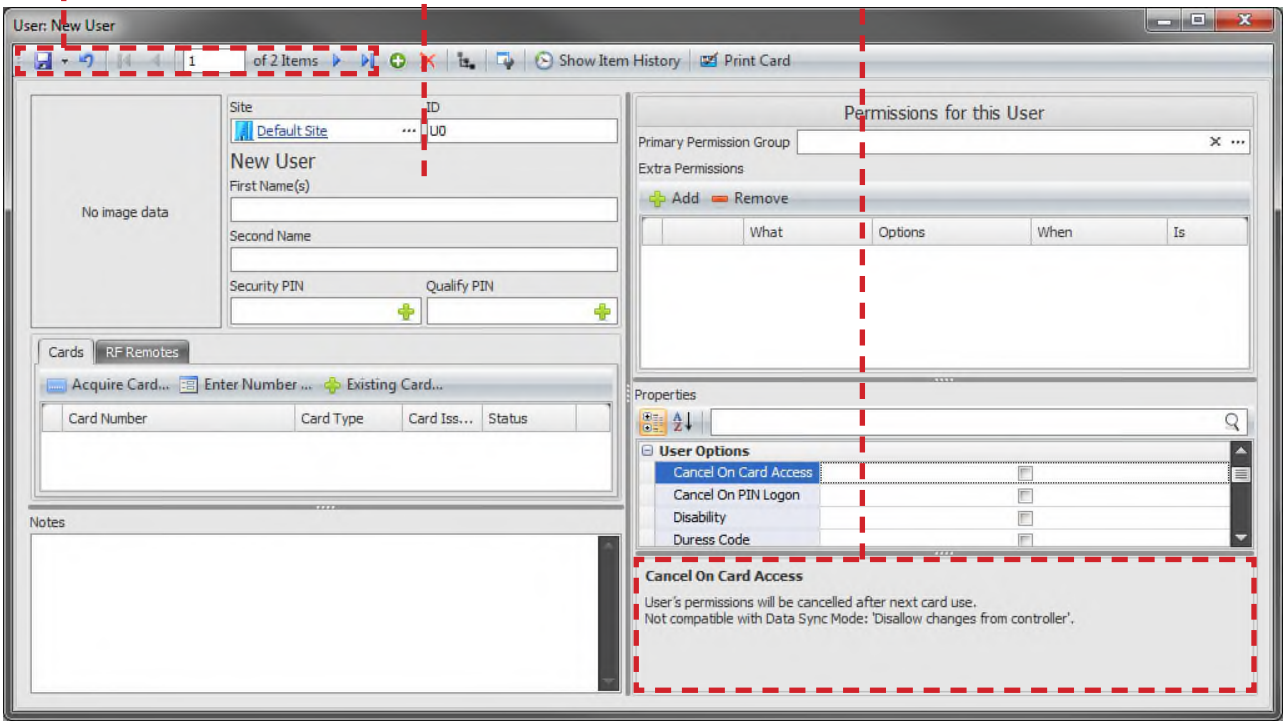
Most of the toolbar icons appear on every editor window.

Properties / Options

The main part of the editor window displays all the properties for the item you are editing.

Context-based Help

The help displayed will change based on the selected property or option.

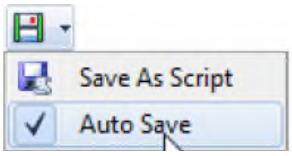


EDITOR WINDOW TOOL BAR

The toolbar contains the following buttons:

1. The **Save** button will save the item that is currently displayed in the editor window.
2. The **Undo** button will revert the last change since the editor window was opened.
3. The **First Item** button will move backwards to the first item in the list.
4. The **Previous Item** button will move backwards one item.
5. The **Item Number** field displays what number that current item is in the series. You can type in a number to jump to a particular item.
6. The **Next Item** button will move forward one item.
7. The **Last Item** button will move forward to the last item in the list.
8. The **Create New** button will make a new blank item.
9. The **Delete** button will remove the currently selected item.
10. The **Show Cross References** button will open a window that shows the other system items that relate to the currently displayed item.
11. The **Show Item History** will open a window that shows the entire history of the item.
12. The **Item Specific Commands** will change based on the item you have open.

You can toggle the automatic save feature by clicking the **Save** button drop-down and selecting the **Auto Save** option. The **Save** icon will change to a green icon when the automatic save feature is active. When you make a programming change to an item and close the window or navigate to the next item, your changes will automatically be saved.

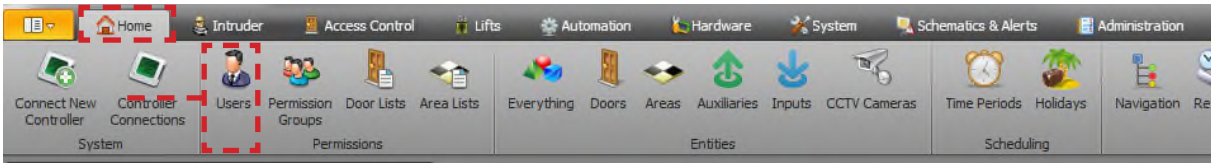


USER PROGRAMMING

CREATING A USER

A user is any person that will interact with the Integriti system via a keypad or card reader. The **User Editor** window allows you to assign the user a PIN number, access card, user permissions or even a photo.

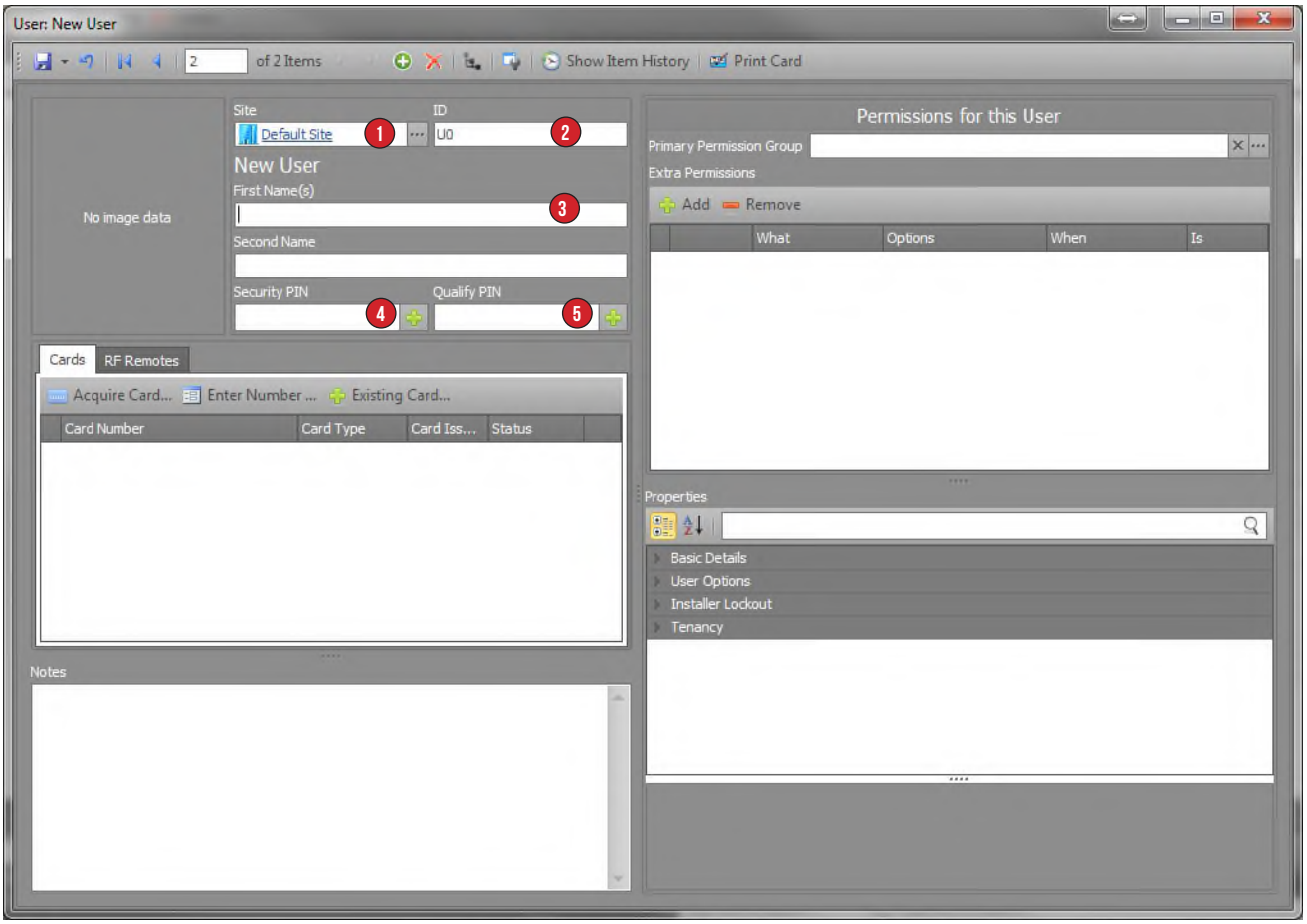
To create a new user from System Designer, navigate to the **Home** tab then click the **Users** icon, this will open the **Users List**. Click the **Add** button to open the User Editor window containing a blank user record.



To create a new user from GateKeeper, navigate to the **Users** tab then click the **Users** icon, this will open the **Users List**. Click the **Add** button to open the **User Editor** window containing a blank user record.

USER EDITOR WINDOW

The top left section of the **User Editor** window contains the basic user information.



1. The **Site** field is used to associate a user with a site or sub-site, this will not have any impact on the user. The user will only be visible in the software if the operator logged in has permission to view users from that sub-site.
2. The **ID** field is a unique number that you can use to identify the users. Each time you add a new user, the user will be given the next available number. The ID field is just a number that has no effect on the user.
3. The **First & Second Name** fields are where you enter the user's first and last name.

4. The **Security PIN** is required for a user to interact with the Integriti system via a keypad. If the user needs to be able to arm or disarm areas from the keypad, you will need to assign the user a security PIN and a menu group. There is no minimum or maximum length for a Security PIN by default; however your system may have been configured to have a fixed PIN code length. If you enter a Security PIN that is either too long or too short the following error will occur.

5. The **Qualify PIN** can be used instead of the **Security PIN** when entering a door that requires the user to enter a PIN to unlock. The qualify PIN is used so that the PIN number that is used for keypad access can be different to the PIN number used for door access. Please check with your installer if you are unsure if you need to use the qualify PIN.

INTRODUCTION TO PERMISSIONS

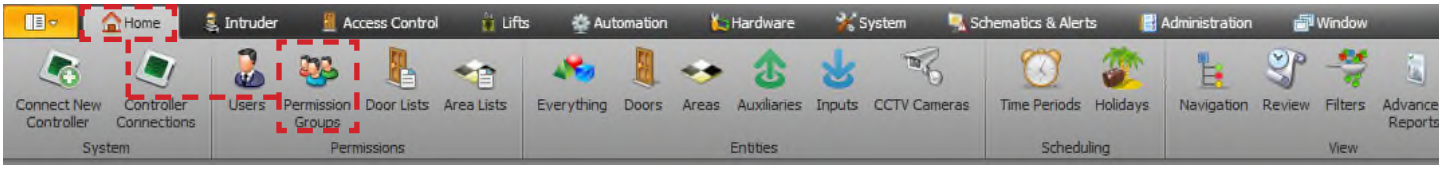
It is important to understand how user permissions are structured before assigning permissions to a user. A permission is an item that you assign to a user to allow or deny that user the ability to interact with the item. Permissions include doors, areas, floors, lift cars and menu groups. In most cases more than one door or area is assigned to a user. It is recommended that you use a list of items such as area lists, door lists or floor lists when assigning permissions for many of the same item.

PERMISSION GROUPS

A permission group is a collection of permissions that can be assigned to one or more users. Many organizations have an internal structure where users share similar roles, for example, Warehouse Staff. It is easier to assign a single permission group to all of the Warehouse Staff rather than adding individual areas, doors or menu groups to each user. In most cases, the permission groups will closely match the roles within the company. Permission groups make it easier for you to add a single door to a group of users as it only requires the change to be made to a permission group and it will affect all users assigned that permission group.

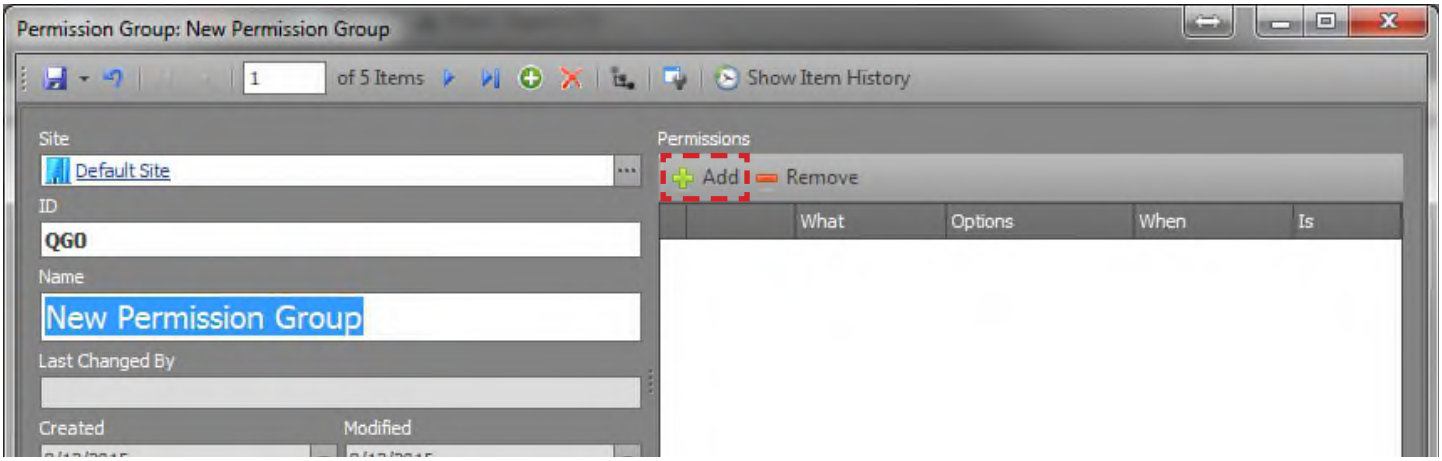
CREATING A PERMISSION GROUP

Permission groups can only be created or edited from System Designer. To create a new permission group, navigate to the **Home** tab and click the **Permission Group** icon. Click the **Add New** button to open the **Permission Group Editor** window.

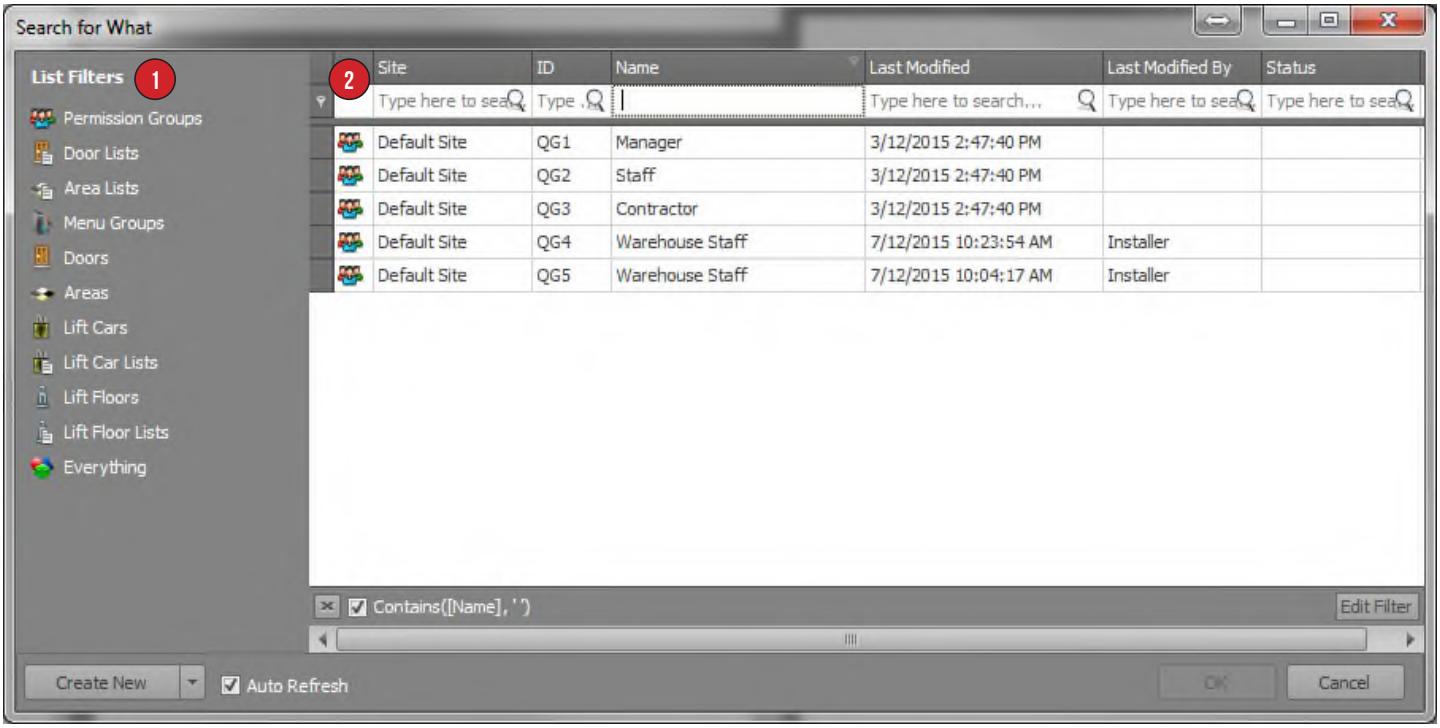


PERMISSION GROUP EDITOR WINDOW

The **Permission Group Editor window** only contains a **Name** field and it is primarily used to add or remove permissions. To add a permission to a permission group click the **Add** button.



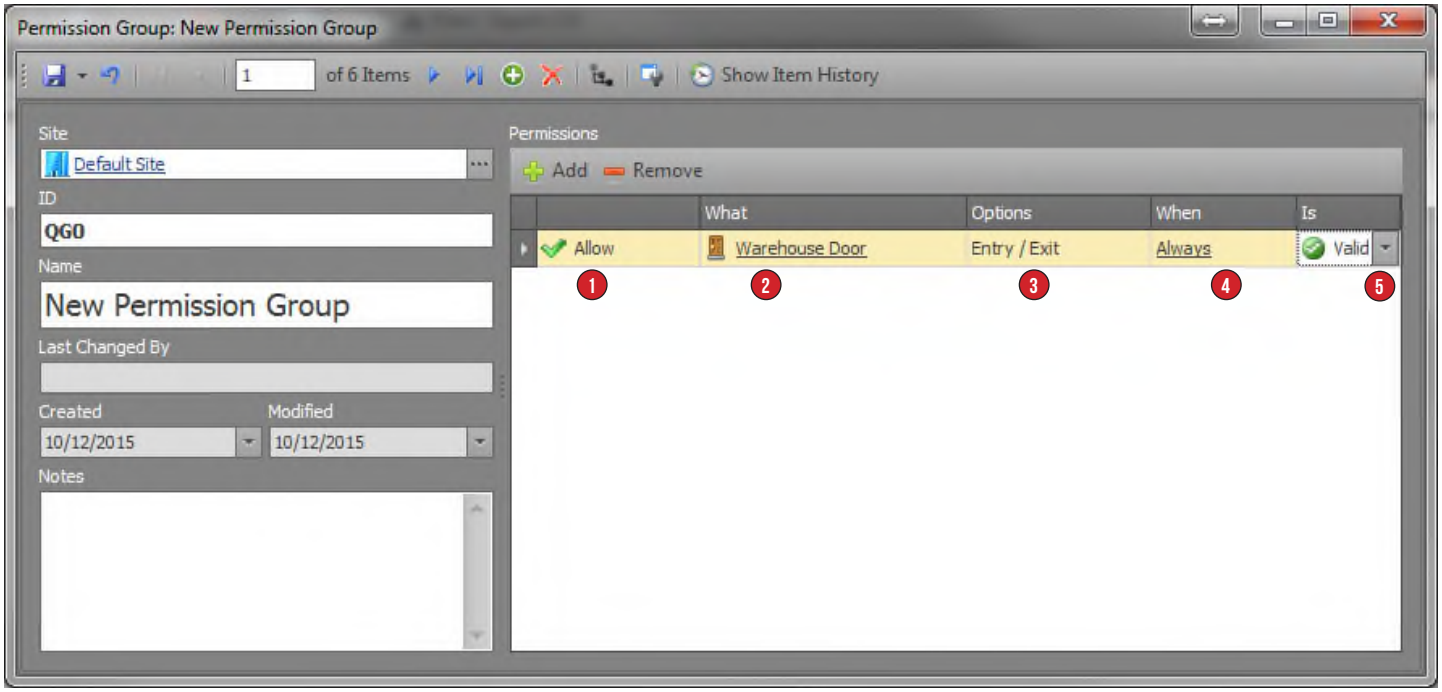
The **Search for What** window will open, this window has two sections:



1. The **List Filter** allows you to filter all the available items that can be assigned to a user as a permission based on the item type.
2. The **Filtered Item** list allows you to choose one or more items to assign to the user. To select more than one item at a time, hold down the **CTRL** button and click multiple items.

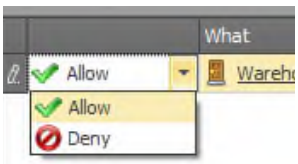
PERMISSION STRUCTURE

Once you have selected an item from the **Search for What** window click the **OK** button to add it to the permission group. The item is then displayed in the **Permission Group** editor window and has the following options:



1 : ALLOW OR DENY

This column determines if the permission is allowing or denying access to the item. Please note that if you deny an item that has already been allowed within the permission group, the deny will override the allow.

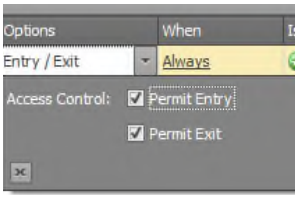


2 : WHAT

The **What** column is used to determine which item the permission refers to. Clicking the ellipsis, (button with three dots) will open the **Search for What** window allowing you to select a different item.

3 : OPTIONS

The **Options** column is used to determine how the user can interact with the assigned item. This allows you to assign a user permissions only to arm a particular area and not disarm it. Alternatively, you can assign the user permissions to only enter or exit a door.

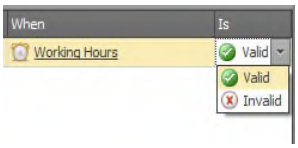


4 : WHEN

The **When** column is used to provide conditional permission to an item. This is most commonly used to assign a user with permission to an item but restrict its access to certain times of the day. For example, you may have a user that is only allowed to access a door during working hours. This can be achieved by adding the Working Hours time period to the **When** column.

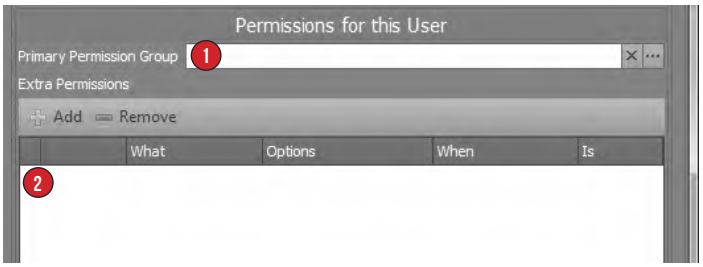
5 : IS

The **Is** column is used to reverse the condition that is used in the **When** column. If you only wanted a user to have access to a door after working hours you could put the Working Hours time period time in the **When** column and set the **IS** column to invalid. This is easier than creating a new time period called Non-Working Hours.



ASSIGNING USER PERMISSIONS

The **Permissions for this User** window is divided into two sections, the Primary Permission Group and the Extra Permissions. It is important to understand the structure of permissions before assigning permissions to a user



1 : PRIMARY PERMISSION GROUP

The **Primary Permission Group** option is where a user's permissions are usually assigned. This field only allows you to assign a single permission group, in most cases a user will be assigned a primary permission group based on their role in the company.

2 : EXTRA PERMISSIONS

The **Extra Permissions** section lets you allow or deny permissions for items independent of the primary permission group. This feature is commonly used to reduce the number of permission groups within the Integriti system.

If two users have similar roles, for example Warehouse Staff and Warehouse Manager, they can both be assigned the same primary permission group. You would then add extra permissions for the additional doors and areas that the Warehouse Manager needs.

The extra permissions use the same **What & When** structure as in the permission group programming.

USER PROPERTIES

There are many settings found in the **Properties** section of the **User Editor** window, most of these options are rarely used and should not be edited unless instructed to do so by your installer.

Below are three more commonly used options:

1 : USER CANCELED

If flagged, the user's permissions will be disabled. The user will not be able to interact with the Integriti system via a keypad or an access control door.

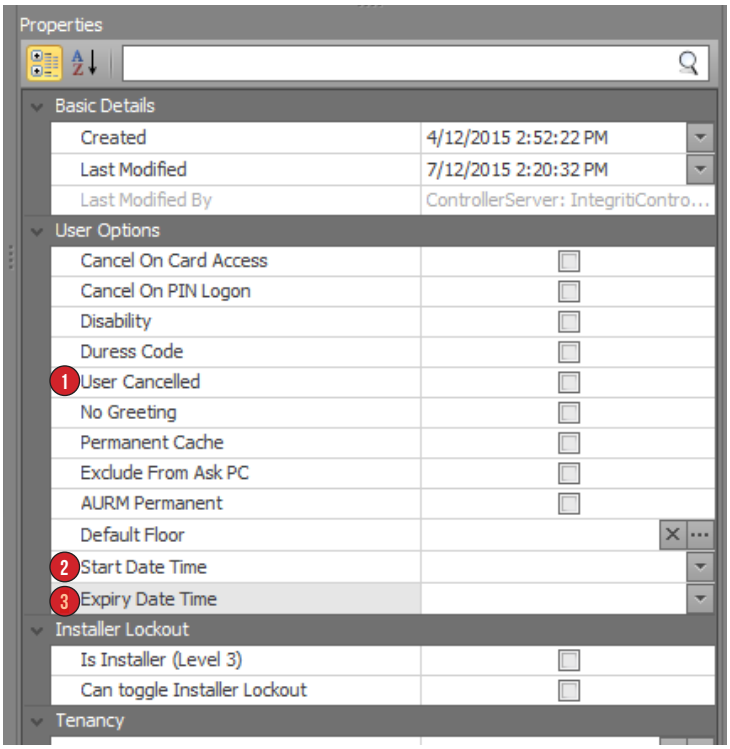
2 : START DATE TIME

The **Start Date Time** option prevents the user from interacting with the Integriti system until the date and time specified.

3 : EXPIRY DATE TIME

The **Expiry Date Time** option prevents the user from interacting with the Integriti system past the date and time specified.

The **Start Date Time** and the **Expiry Date Time** can be used separately or combined. For example, a visitor that attends a site for a set duration of time between two dates. The **Start Date Time** will ensure that visitor will not be able to access the site early and the **Expiry Date Time** will ensure that the card can not be used past the end of the visit.



ASSIGNING CARDS TO USERS

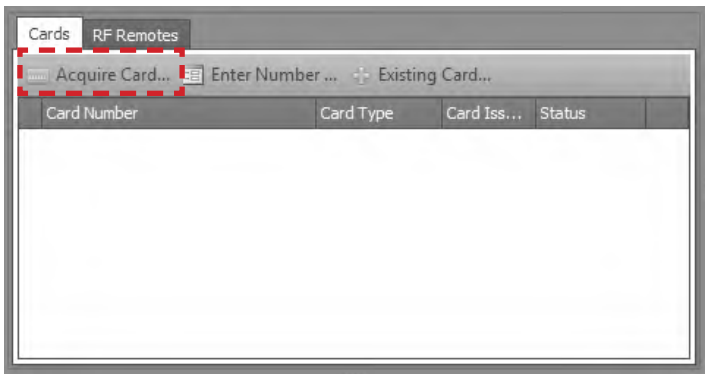
Once a user has been created and programmed, the next step is to assign them a card. There are numerous card formats and card types in Integriti, therefore, there is more than one way for you to assign a card to a user.

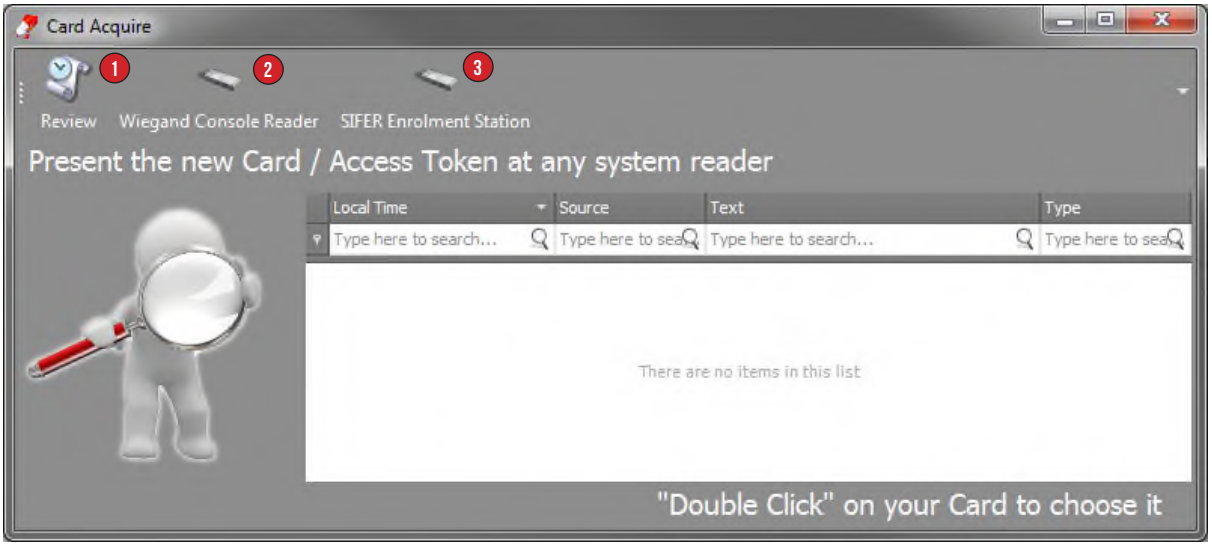
The following methods for assigning cards will depend on the types of cards you currently use on-site. Check with your installer to confirm which method is correct for you.

DIRECT ENTRY

Direct Entry is a method of using the raw information that is read from a card by a reader. Integriti does not interpret the raw information. **Direct Entry** cards can not be preprogrammed in Integriti as every card needs to be badged to read its information.

To assign a direct entry card to a user, click the **Acquire Card** button found in the **Cards** section of the **User Editor** window. The **Acquire Card** window provides you three methods to acquire a card.





1. **Review:** Selecting this option will scan for review messages of card badges at any reader on the site. Simply badge the card you want to assign to a user at a reader, once it appears in the list double click it to assign it to the user.
2. **Wiegand Console Reader:** If many direct entry cards are going to be assigned, it may be easier to use a Wiegand Console Reader method. The Wiegand Console Reader method uses the enrollment station that attaches to the PC via a serial port. To assign a card to a user, badge a card at the enrollment station and double-click the most recent card information.
3. **SIFER Enrollment Station:** If SIFER Cards and readers are being used, the SIFER enrollment station can be attached to a PC via a USB port to make the enrollment of many SIFER cards easier.

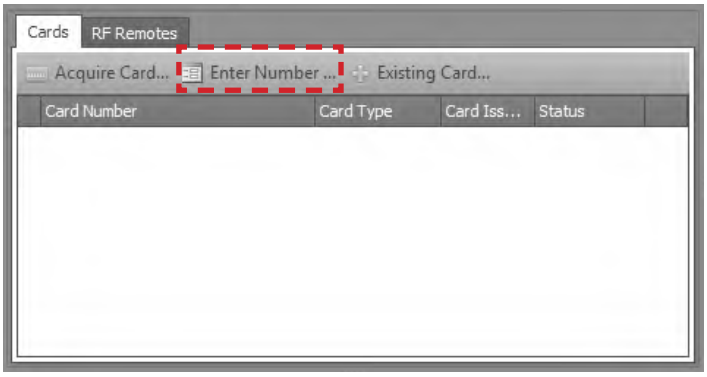
Once the card has been double clicked the card will appear in the **Cards** section of the user programming.

SITE CODED CARDS

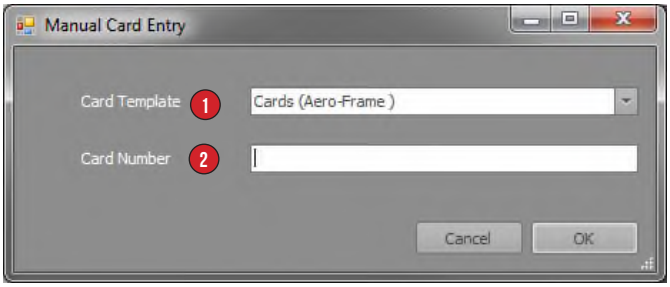
Site Coded cards unlike Direct Entry cards can be pre-programmed on the Integriti System and do not require you to badge the card to assign it to a user. In some cases, the number will be printed on the card itself.

If your system has been configured by your installer for site code, you will be able to enter the card number rather than badging the card to assign it to a user.

To assign a Site Coded card to a user, click the **Enter Number** button in the **Cards** section, this will open the **Manual Card Entry** window.



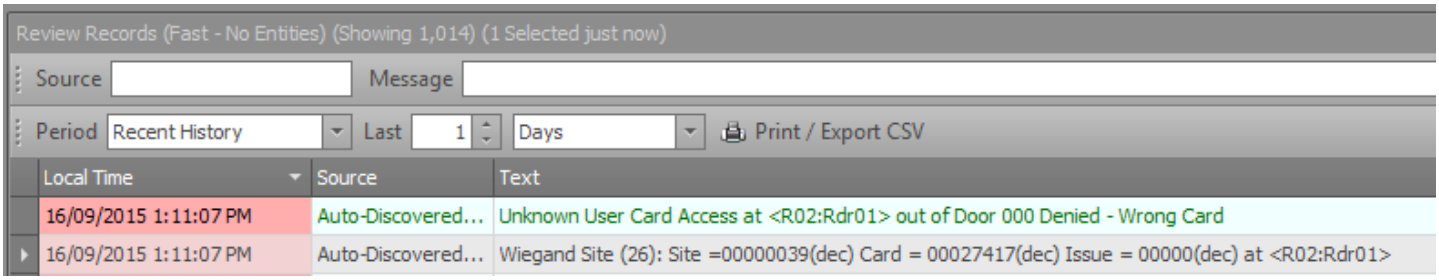
The **Manual Card Entry** window contains two fields that are required to assign a card to a user.



1. The **Card Template** is used to define what type of card you are assigning. In some cases there may be more than one template, this usually occurs when a combination of new and old cards are being used on a site.

2. The **Card Number** field is were you enter the unique card number. In some cases the number will be printed on the card, if it is not printed you may need to badge a card at a reader to view the card details.

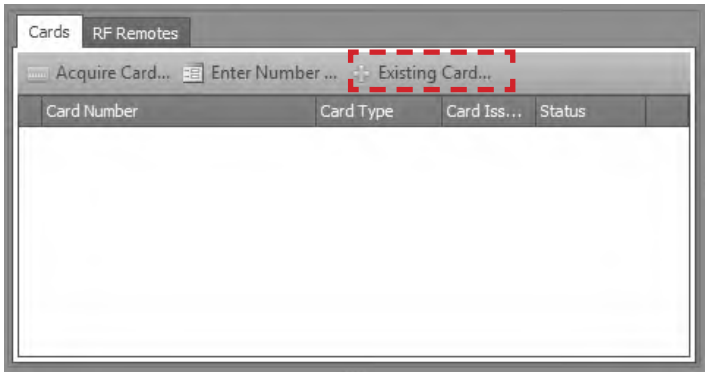
Below is a review message that contains the card information. The card number is 00027417.



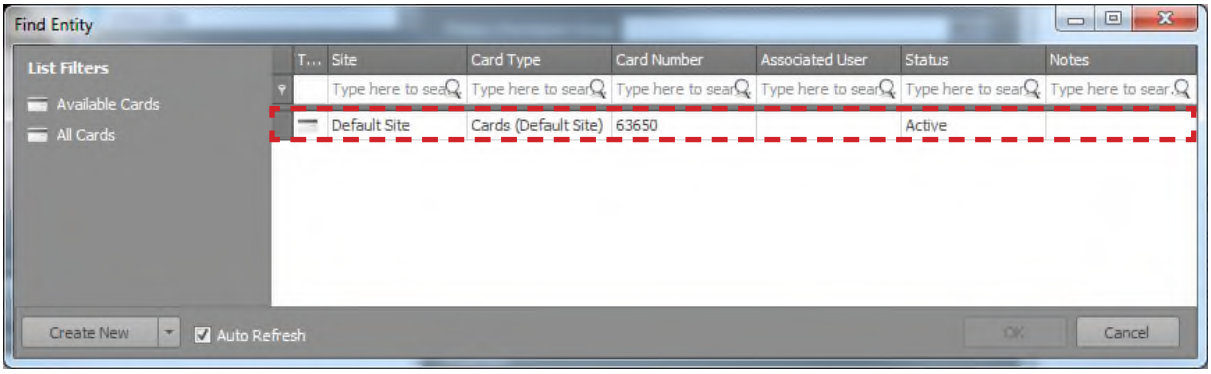
EXISTING CARD

When users that have cards assigned to them are deleted from the Integriti System, the card remains behind with an unallocated status.

This unallocated card can be assigned to a new user.
To assign an existing card to a user, click the **Existing Card** button in the **Cards** section.



This will open the **Find Entity** window that displays all the unallocated cards. Select a card from the **Available Cards** list and click the **OK** button to assign it to the user.



DOOR LISTS

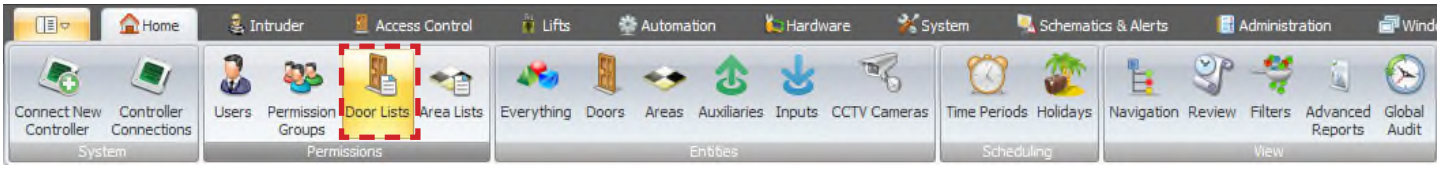
INTRODUCTION TO DOOR LISTS

A door list is a collection of doors that can be used for user permissions, door control or automation. When assigning multiple doors to a user, it is easier to assign a single door list.

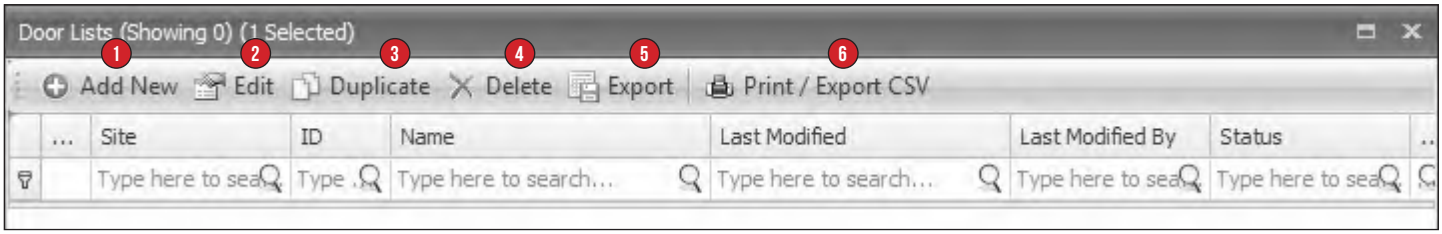
An operator can lock or unlock a door list, instead of having to control doors one at a time. The Integriti controller can be configured to automatically lock or unlock a door list.

THE DOOR LISTS MENU

To program a door list, navigate to the **Home** tab and click the **Door Lists** icon.



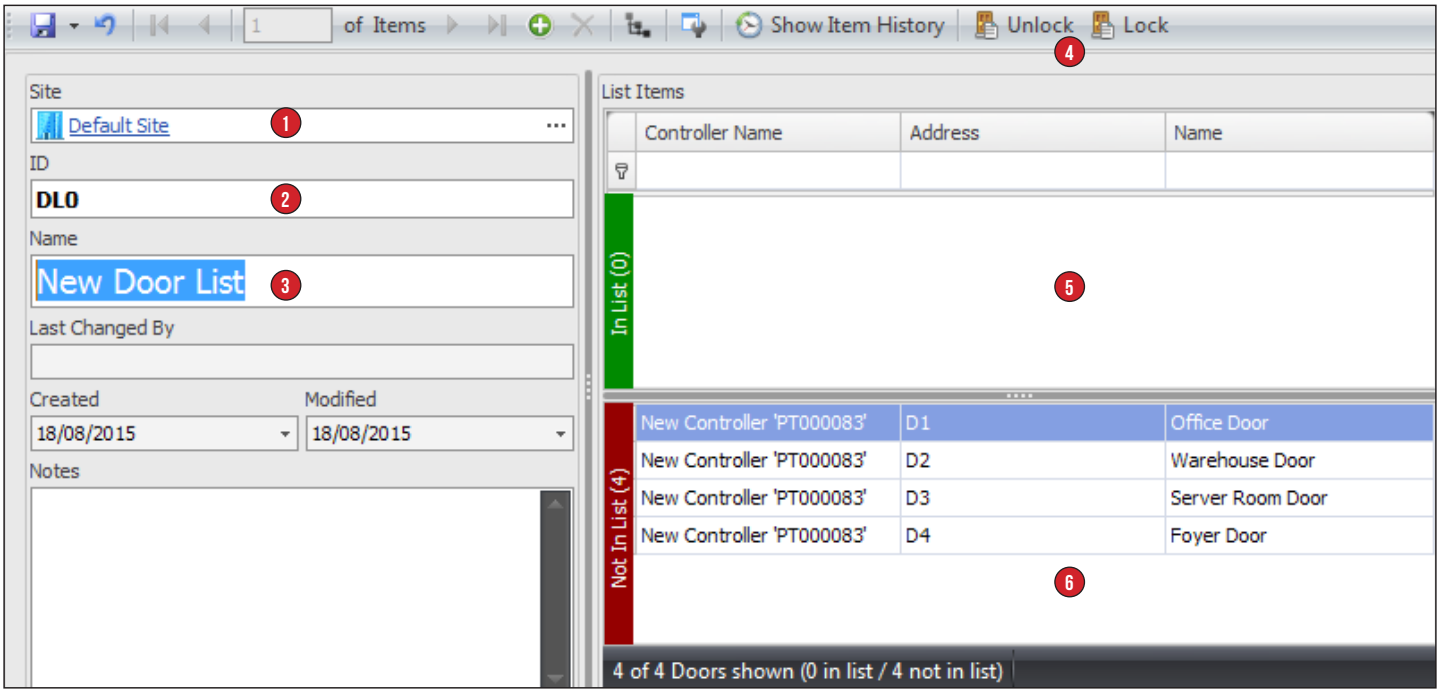
The **Door Lists** menu will open; this list contains all the currently programmed door lists.



1. The **Add New** button will create a new blank door list.
2. The **Edit** button will open the selected door list for programming changes.
3. The **Duplicate** button will create a new door list that is identical to the selected door list.
4. The **Delete** button will delete the selected door list(s).
5. The **Export** button saves the selected door list(s) as an IR-Entities file.
6. The **Print/Export CSV** button provides a printable version of the contents of the Door Lists window.

CREATING A NEW DOOR LIST

Click the **Add New** button to open the **Door Lists Editor** window.

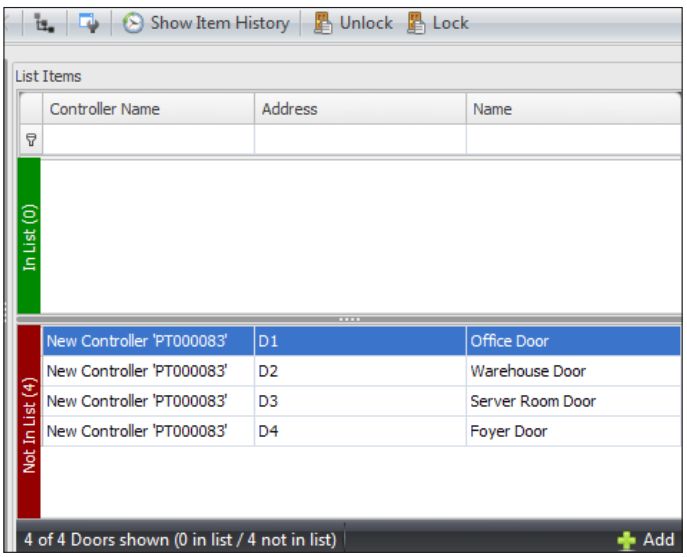


1. The **Site** field determines which site this door list will be associated with.
2. The **ID** field displays the unique identification code for each door list, this ID cannot be changed.
3. The **Name** field is where a name can be assigned to the door list.
4. The **Unlock** and **Lock** buttons will control all of the doors assigned to the door list.
5. The **In List** section displays all doors that are assigned to the door list.
6. The **Not In List** section displays all of the doors that are not assigned to the door list.

ADDING/REMOVING A DOOR FROM A DOOR LIST

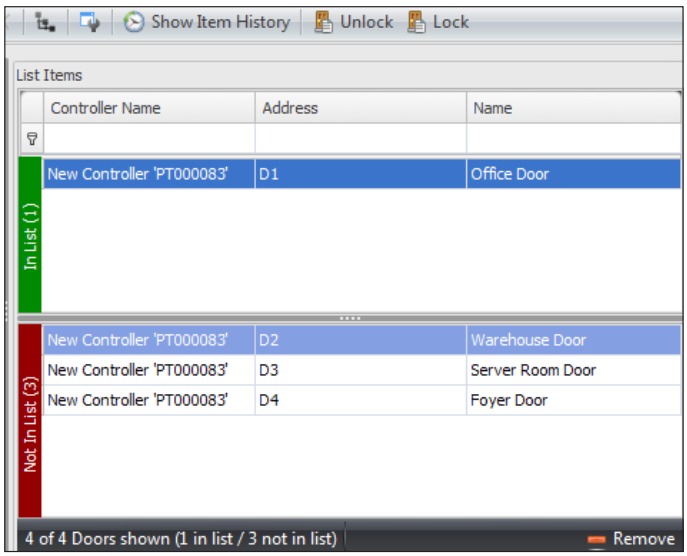
ADDING A DOOR

1. Select one or more doors from the **Not In List** section.
2. Click the **Add** button to add the door(s) to the door list.
3. The door will move from the **Not In List** section to the **In list** Section.



REMOVING A DOOR

1. Select one or more doors from the **In List** section .
2. Click the **Remove** button to remove the door(s) from the door list.
3. The door will move from the **In List** section to the **Not In list** Section.



AREA LISTS

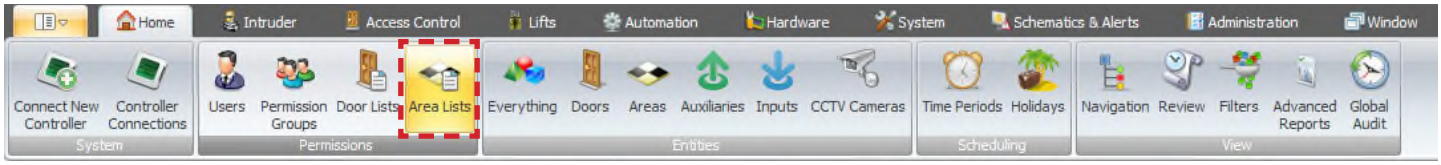
INTRODUCTION TO AREA LISTS

An area list is a collection of areas that can be used for user permissions, area control or automation. When assigning multiple areas to a user, it is easier to assign a single area list.

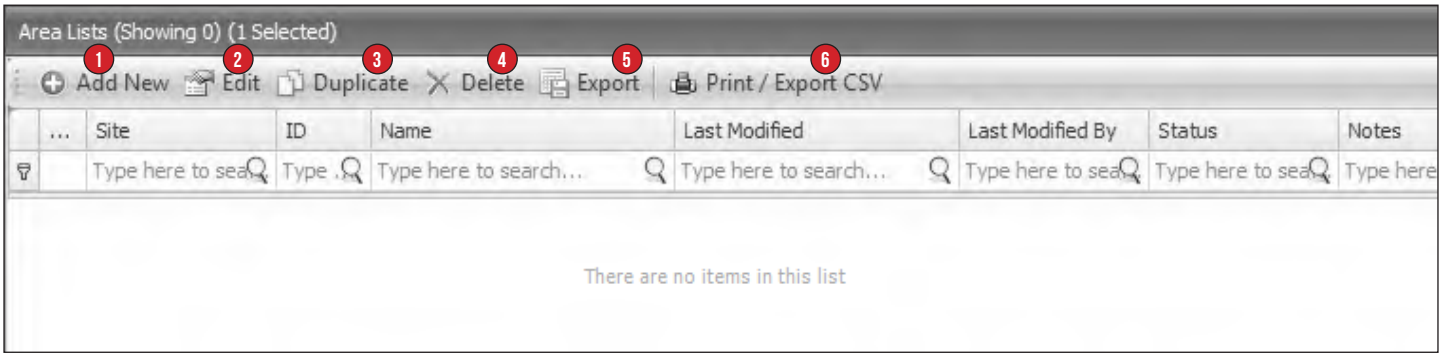
An operator can arm or disarm an area list instead of having to control areas one at a time. The Integriti controller can be configured to automatically arm or disarm an area list.

THE AREA LISTS MENU

To program an area list, navigate to the **Home** tab and click the **Area Lists** icon.



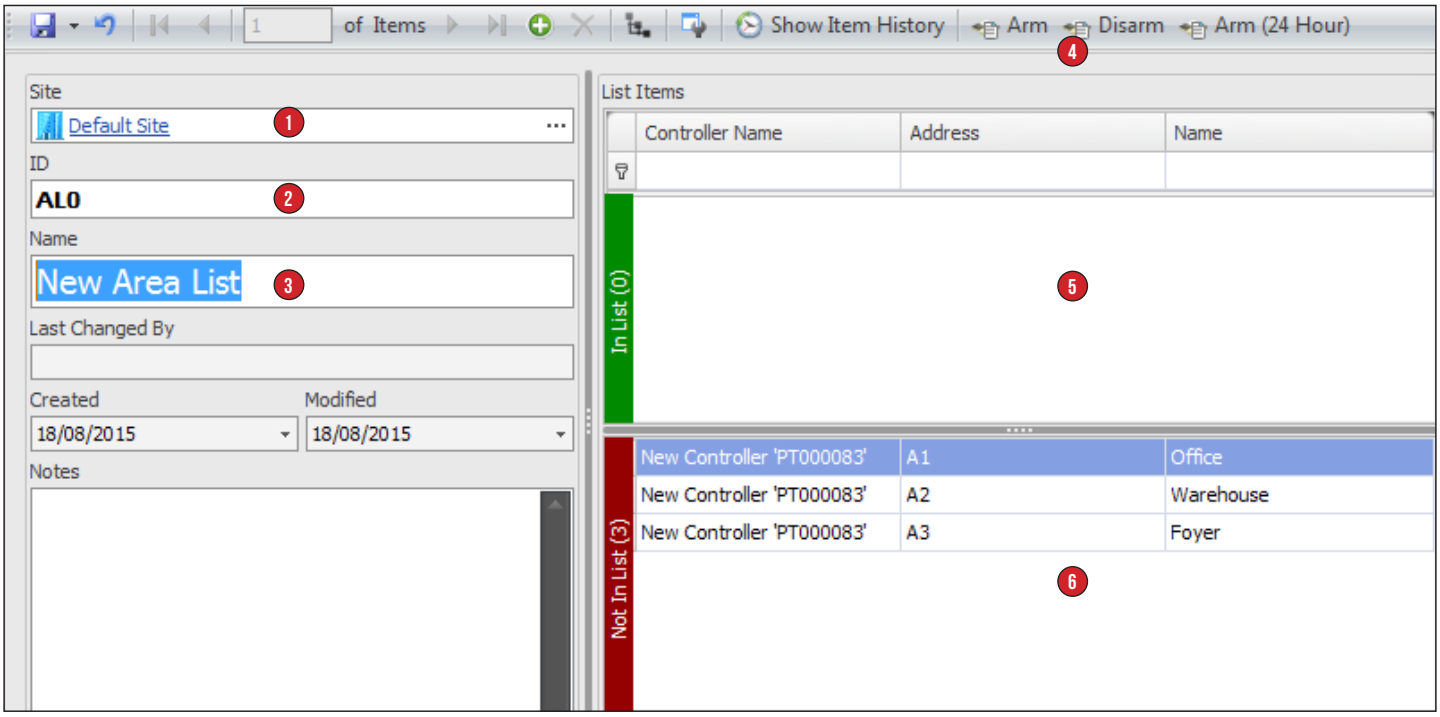
The **Area Lists** menu will open; this list contains all the currently programmed area lists.



1. The **Add New** button will create a new blank area list.
2. The **Edit** button will open the selected area list for programming changes.
3. The **Duplicate** button will create a new area list that is identical to the selected area list.
4. The **Delete** button will delete the selected area list(s).
5. The **Export** button saves the selected area list(s) as an IR-Entities file.
6. The **Print/Export CSV** button provides a printable version of the contents of the **Area Lists** window.

CREATING A NEW AREA LIST

Clicking the **Add New** button will open the **Area Lists Editor** window.

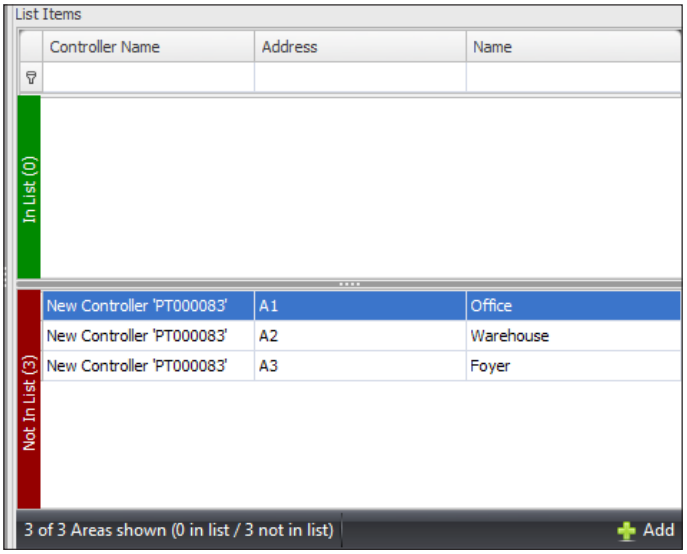


1. The **Site** field determines which site this area list will be associated with.
2. The **ID** field displays the unique identification code for each area list - this cannot be changed.
3. The **Name** field is where a name can be assigned to the area list.
4. The **Arm** and **Disarm** buttons will control all the areas assigned to the area list.
5. The **In List** section displays all the areas that are assigned to the areas list.
6. The **Not In List** section displays all the areas that are not assigned to the area list.

ADDING/REMOVING AN AREA FROM AN AREA LIST

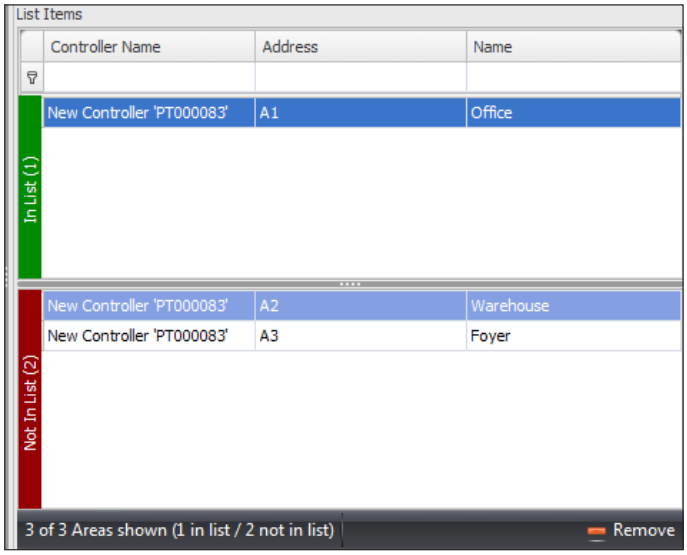
ADDING AN AREA

1. Select one or more areas from the **Not In List** section.
2. Click the **Add** button to add the area(s) to the area list.
3. The area will move from the **Not In List** section to the **In list** Section.



REMOVING AN AREA

1. Select one or more areas from the **In List** section .
2. Click the **Remove** button to remove the area(s) to the area list.
3. The door will move from the **In List** section to the **Not In list** section.



ALERTS

INTRODUCTION TO ALERTS

An alert is a notification that draws an operator's attention to an event or alarm.

For example, when a duress panic/duress button is pressed by a user it will require a guard to respond in person. Without an alert the event may be completely missed or actioned too late.

Alerts are viewed and actioned from Integriti GateKeeper. The alert will remain in the software until it is finalized by an operator.

USING AN ALERT

Alerts are usually configured by your installer, as an end user you will interact with alerts from an **Alert View** window. An alert view is a collection of different types of alerts, in some cases the alerts that you are able to see and respond to may differ from other operators.

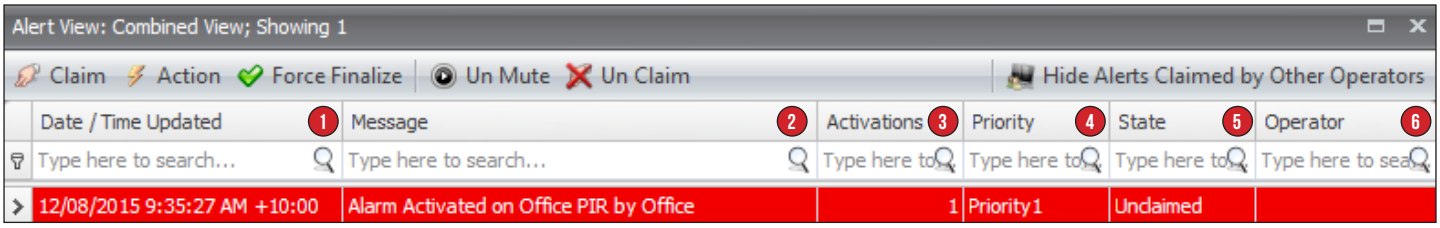
Alert views are only visible in Integriti GateKeeper and are part of the default layout. If the alert views are not visible, navigate to the **Home** tab and then click the **Alert Views** icon.

ALERT CREATION

When the event that triggers an alert occurs, the alert is created and appears in the **Alert View** window. The appearance of the alert is determined by how it is configured. Alerts can be configured to have different foreground and background colors, this allows the you to easily identify the type of event that has occurred.

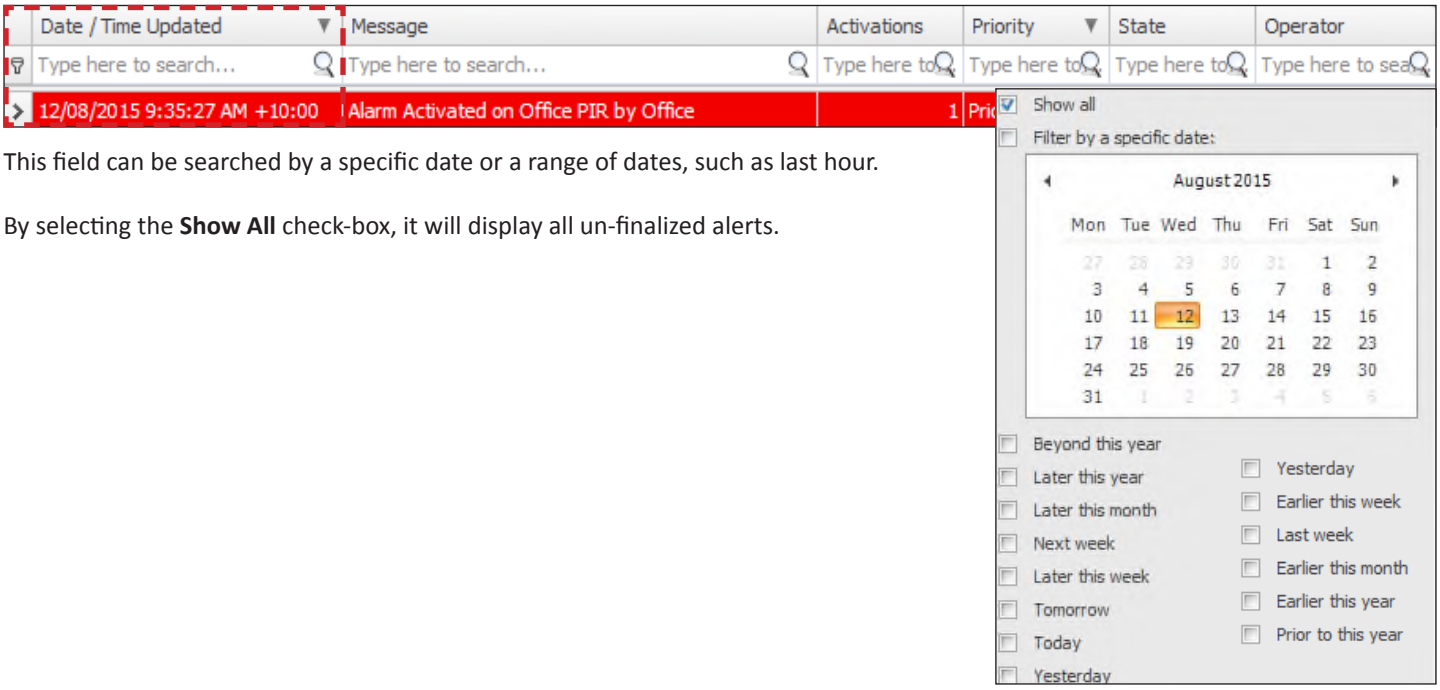
READING ALERT INFORMATION

The **Alert** window has multiple columns that contain information to help you identify the alert priority, what triggered the alert and when the alert was generated. These columns can be used to filter the currently displayed alerts.



1 : DATE / TIME UPDATED

This displays the most recent occurrence of the event that triggered the alarm.



This field can be searched by a specific date or a range of dates, such as last hour.

By selecting the **Show All** check-box, it will display all un-finalized alerts.

2 : MESSAGE

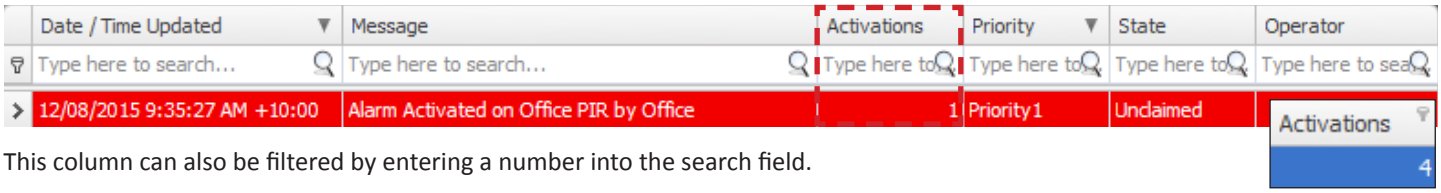
This provides a summary of the event(s) that have occurred to trigger the alert.

The **Message** field is a basic text-based filter that you can use to filter the displayed alerts by typing the name of an item, for example: office.

This would filter the alerts to only display the ones that contain the word office in the **Message** field.

3 : ACTIVATIONS

Alerts can be grouped by the input, area or review message that created them. The Activations column provides a count of how many times the event has occurred, rather than having individual alerts for each event.



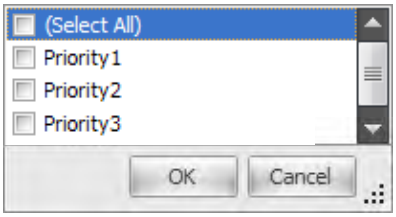
This column can also be filtered by entering a number into the search field.

4 : PRIORITY

An alert can be configured to have a priority; you can use this priority to determine which event to action first. The priority scale is from 1 (high) to 16 (low).

The **Priority** column can be filtered by selecting one or more of the check boxes.

You can view all alerts by checking the **(Select All)** check box.

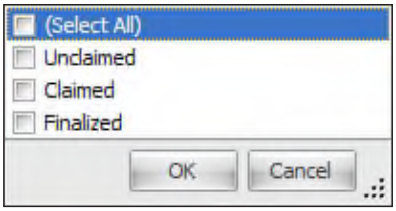


5 : STATE

The state of an alert will either be Unclaimed, Claimed or Finalized; this allows you to identify which alert to action in order to avoid two operators dealing with the same alert.

The **State** column can be searched by selecting one or more of the check boxes.

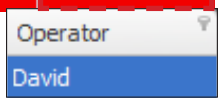
You can view all alerts by checking the **(Select All)** check box.



6 : OPERATOR

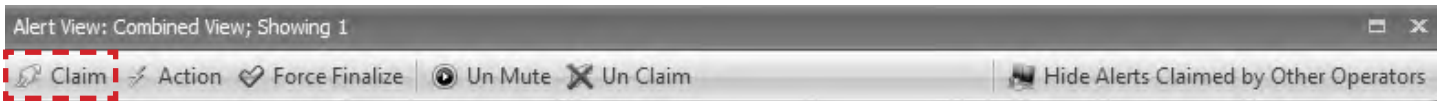
Once an alert has been claimed by an operator, the operator's name will appear in the Operator column.

The **Operator** column has a basic text-based search field; you can filter the alerts by typing the name of an operator, for example, David.

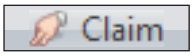


CLAIMING ALERTS

Integriti GateKeeper can have multiple operators logged in who can view and action alerts at the same time. Claiming alerts is a way to identify who is dealing with an alert, this prevents two operators both actioning on the same alert.



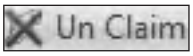
CLAIMING ALERTS



The **Claim** button is used to assign the alert to yourself; this will change the state from unclaimed to claimed.

Additionally your operator name will appear in the **Operator** column in the alert view. Once claimed, only that operator can action and finalize the alert.

UNCLAIMING ALERTS



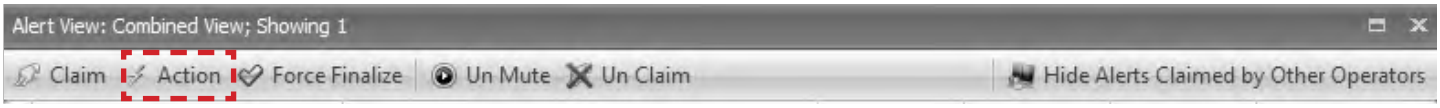
Once an alert is claimed, the **Claim** button will change to an **Un Claim** button

If you have claimed an alert and needed another operator to action it, you can unclaim the alert by clicking the **Unclaim** button in the alert view.

Note: Claiming an alert will only work if each operator logs in with a unique operator name.

ACTIONING ALERTS

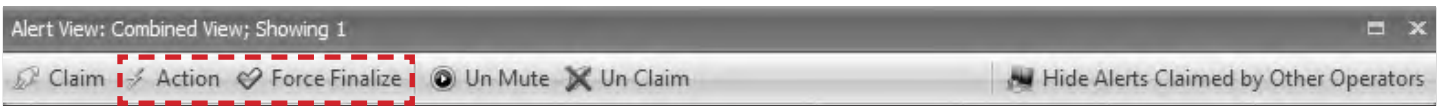
Once an alert has been claimed, the next step is to action it. The **Action** button opens the **Finalize Response** window.



The **Finalize Response** window is used to enter a summary of how you responded to the alert and the alerts outcome.

FINALIZING ALERTS

The last step in actioning an alert is to finalize the alert; this removes the alert from the alert view permanently. Finalized alerts are viewable by clicking the **Finalized Alerts** icon in the **Home** tab.



There are two methods for finalizing an alert:

FINALIZE

You can click the **Finalize** button on the **Finalize Response** window when actioning an alert

FORCE FINALIZE

Force Finalize allows more than one alert to be finalized by an operator, this is used to clear multiple alerts at once.

To force finalize select one or more alerts from the alert view and click the **Force Finalize** button.

The Finalize Response window will open allowing you to submit a response for all the selected alerts.

THE ALERT LIFESPAN

Alerts can be configured to perform actions at specific stages of its lifespan.

These actions may occur when the alert is created, claimed or finalized.

The most common alert action draws the attention of an operator to the workstation when the alert is first created. This can be done by performing one of the following actions:

PLAYING A SOUND

The alert can control a workstation and play an audio file such as a siren sound.

The alert may be configured to play the sound continuously, the sound can be muted by clicking the **Mute** button in the **Finalize Response** window when actioning an alert.

DISPLAYING A SCHEMATIC MAP

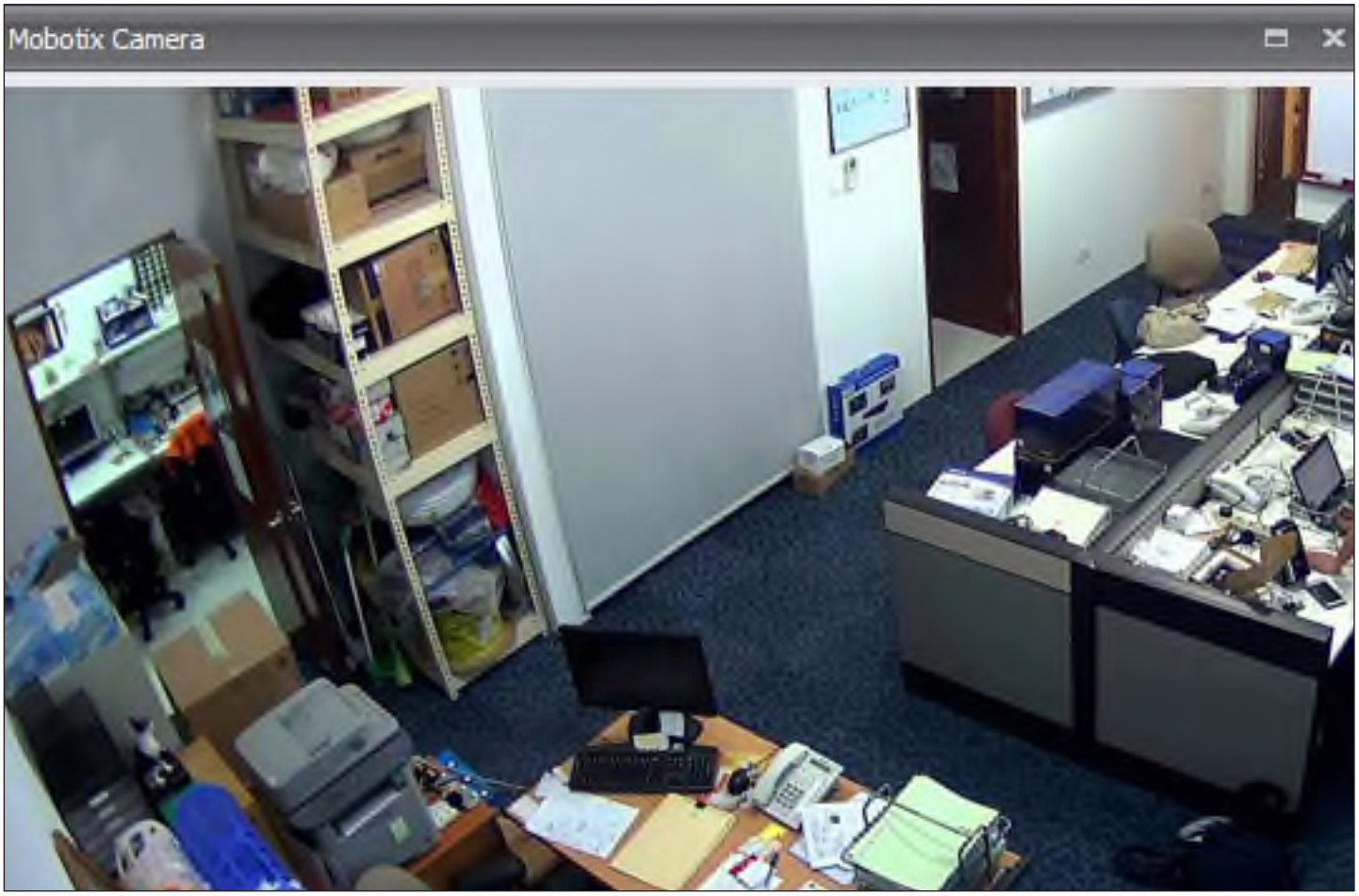
The alert can control a workstation and launch a schematic map.

This is commonly used to show the operator a map relating to the alarm.

DISPLAYING CCTV FOOTAGE

The alert can control a workstation and launch CCTV footage.

This is commonly used to show the operator live footage from a camera relating to the Alarm.



SCHEMATIC MAPS

INTRODUCTION TO SCHEMATIC MAPS

Schematic maps are a graphical representation of your site; they allow you to control and view the state of areas, doors, inputs, auxiliaries and many more items.

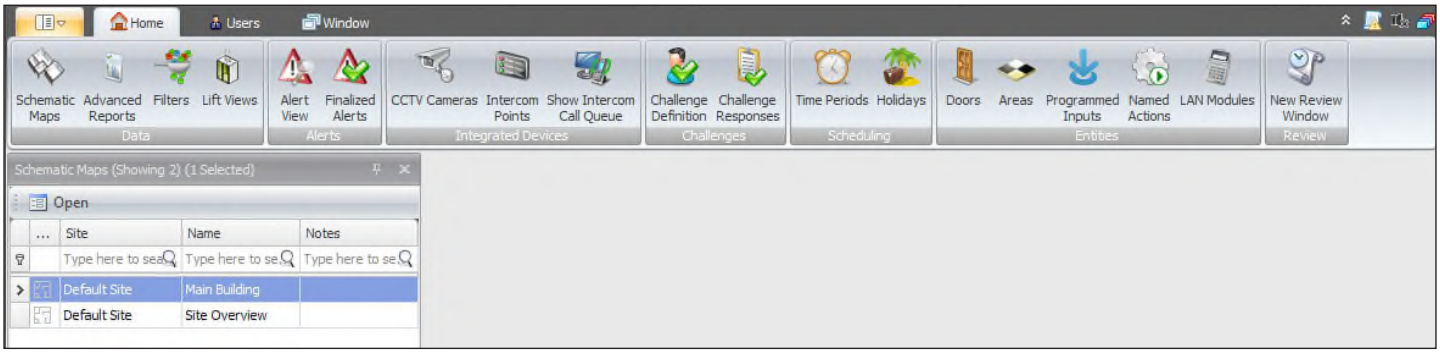
A schematic map may be as simple as a single map containing a floor plan with a couple of icons representing detectors or as complex as multiple maps that are navigated for more detailed views.

Schematic maps are usually created and configured by the installer.

OPENING SCHEMATIC MAPS

Schematic maps are usually viewed from Integriti GateKeeper, the **Schematic Maps** item list is a part of the default layout.

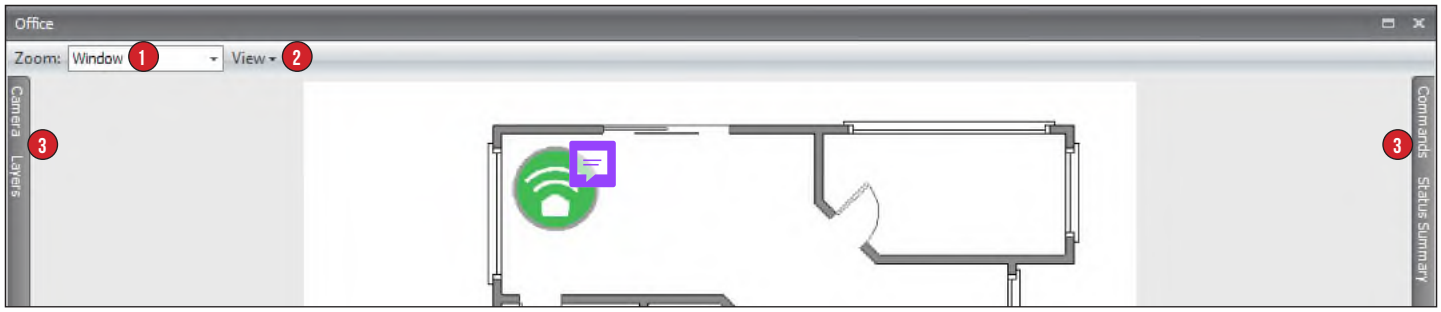
To open a Schematic map select a map from the **Schematic Maps Item** list and click the **Open** button. You can also open a schematic map by double-clicking on it.



If the **Schematic Map Item** list is not visible, click the **Schematic Map** icon in the **Home** tab.

TOOLBAR & NAVIGATION

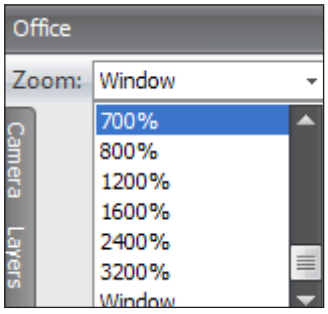
The schematic map window is made up of three sections:



1 : ZOOM

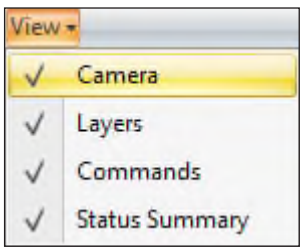
The **Zoom** option allows you to set a zoom percentage, this determines how close or far away you are from the displayed map.

The **Window** option will fit the map in the current window, if the window is resized, the map will resize.



2 : VIEW

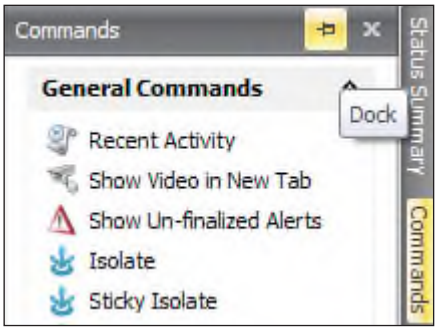
The **View** menu toggles the visibility of the **Camera**, **Layers**, **Commands** and **Status Summary** windows.



DOCKED WINDOWS

The four docked windows are used to interact with the map, see the status of entities, toggle the visibility of layers and view CCTV footage.

The purpose of these docked windows are explained later in this guide. By default the **Commands** and **Status Summary** windows are visible and the **Layers** and **Camera** windows are hidden.



To dock or auto-hide a window, click on the **Drawing Pin** icon.

Dock Panel: 

Auto-Hide: 

If set to Auto-Hide, the window will collapse once the operator selects a different window or an item on the map.

MAP ELEMENTS

Elements are shapes, icons, text or images that are placed on a schematic map. These elements can be static or dynamic.

Static elements are used for design or labeling purposes. For example, a label displaying the name of a map would not need to change, so this would be a static element.

Dynamic elements are used to display the state of item within the Integriti system. For example, an icon representing a particular door will change as the doors state changes from locked to unlocked.

Dynamic elements have an associated or linked item that can be configured when the map is created or edited.

ELEMENT TYPES

There are four element types that you may have on your schematic maps:

- Shapes
- Icons
- Labels
- Images

SHAPES

Shapes are used when the associated entity cannot be represented by an icon, for example, a perimeter fence or a large area.

In addition to this, shapes are commonly used for design elements such as map legends or buttons.

There are five different shapes in schematic maps, they all differ in appearance but have some common features. All shapes have interior and exterior colors. However, the interior color of lines and multi-segment lines are not visible. The **Line Size** setting determines the thickness of the outline.

All shapes have an Opacity setting which determines their level of transparency. These settings are configured when creating or editing the schematic maps.

1. **Rectangle**
   The rectangle is used as a representation of an area, button or border.

2. **Ellipse**
   The ellipse is used as a button.

3. **Line**
   The line is used as a representation of a fence line or as a border.

4. **Multi-Segment Line**
   The multi-segment line is used as a representation of a complex fence line or an area without an internal color.

5. **Freeform**
   The freeform shape is used as a representation of a complex area.

ICONS

Icons provide a simple, dynamic and flexible means of representing system items.

A schematic map can contain hundreds of icons and can still be easily understood as the icons change in appearance as the associated items change state.

A map will never have an icon that is not linked to an entity, but in some cases the map legend may contain what appears to be an icon. The legend only uses the image that is contained within the icon for a particular state.

It would not be appropriate for the key to change state.

LABELS

Labels are elements that display text on a schematic map.

When configured as a static element, the text appearance and contents will not change - this is commonly used for map legends.

The label element can be configured as a dynamic element - doing so will cause its appearance and contents to change based on the state of the entity it is associated with. E.g.: A temperature sensor's label could display 'Server Room Temp: 18.5 degrees C'.

IMAGES

Images can only be used as static elements; they are generally used for design purposes, such as adding a company logo to the map.

ELEMENT STATUS

When an element is linked to an entity, it will change in appearance based on the entity's state.

Each entity in the system has a set of rules that determine its appearance depending on whether it is displayed as a shape, icon or label.

The most commonly found entities on a map are doors, areas, inputs and outputs. In most cases, areas will be displayed as a shape due to the fact that an area does not have a single point location that an icon can represent.

Below are the states for the most commonly used elements:

DOORS

State	Icon	Description
Door Locked		The door is currently locked.
Unlocked		The door is currently unlocked.
Forced		The door is currently locked and has been forcefully opened.
DOTL		The door was unlocked, opened then relocked, but has not been closed for a long time. This state requires numerous other settings to work, not all doors will show DOTL.
Timed Unlocked		The door has been unlocked for a set period of time.
Has Alarms		The door is referenced in an alert; see the alerts section for more details.

INPUTS

State	Icon	Description
Sealed		The PIR detector does not sense movement.
Alarm		The PIR detector senses movement.
Isolated		The PIR detector has been isolated to ignore the alarm and tamper states.
Tamper		The cover of the PIR detector has been removed or someone has tampered with the cabling.

OUTPUTS

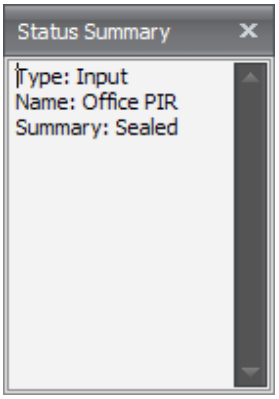
State	Icon	Description
On		The auxiliary is on.
Off		The auxiliary is off.

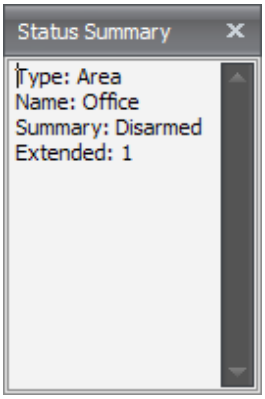
AREAS

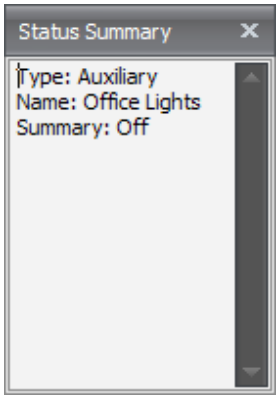
State	Shape Option 1	Shape Option 1	Description
Disarmed			The area is currently disarmed.
Armed			The area is currently armed.
Alarm			The area is referenced in an alert.

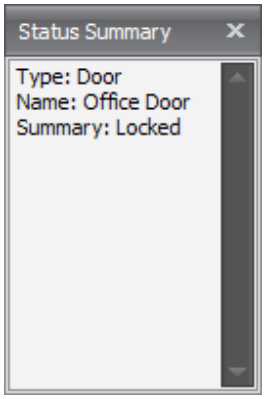
STATUS SUMMARY

The **Status Summary** window provides a summary of the item linked to the map element. This summary includes the type, name and the current status:









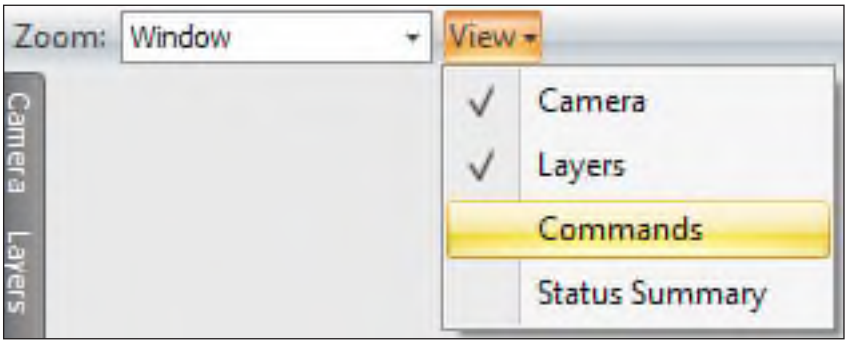
COMMANDS

Each element on a map that is linked to a door, area, input or auxiliary is accompanied with a list of commands.

These commands include viewing review, showing videos and controlling the item. The control commands will change based on the type of item you have selected.

The commands are accessed in one of two ways:

1. Clicking an element on the map will display the commands in the **Commands** window if it is visible. If the Commands window is not visible, click the **View** button and select the **Commands** option.
2. Right click an element on the map to display the **Commands** menu.

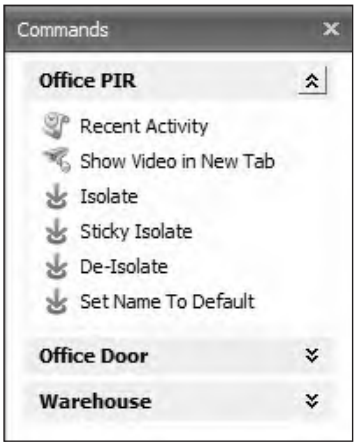


More than one element can be selected by holding the **CTRL** button and clicking the elements you wish to select.

If all of the selected elements are linked to the same type of entity (i.e. areas), the commands will apply to all the selected areas.

There will also be an individual area command that will appear under the areas name (right).

If more than one element is selected and they are not linked to the same entity type (i.e. a door and an area), the commands window will display a drop down menu for each of the selected elements (below).



GENERIC COMMANDS

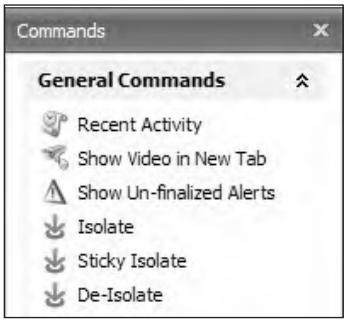
There are three commands that appear for most items that are displayed on schematic maps.

Recent Activity
This displays all review messages that relate to the selected entity for the last hour. This allows you to easily see the recent activity for an area or door.

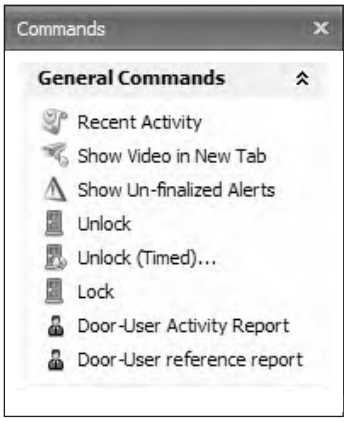
Show Video in New Tab
If you have the CCTV Integration license, you can launch CCTV footage from cameras that are associated to items on your map. The video will open in a new tab and the schematic map will remain open in the background.

Show Un-Finalized Alerts
If alerts have been configured on your system for the items displayed on your map, clicking this option will display the alerts that are still outstanding for the selected item.

Area Commands	Descriptions
Arm	This will arm the selected area or areas.
Disarm	This will disarm the selected area or areas.
Arm (24 Hour)	This will arm the 24 hour part of the selected area or areas.
Disarm (24 Hour)	This will disarm the 24 hour part of the selected area or areas.



Area Commands	Descriptions
Isolate	This ignores state changes for the input until the area is re-armed.
Sticky Isolate	This ignores state changes for the input until de-isolated.
De-Isolate	This reverses the isolate & sticky isolate command.



Area Commands	Descriptions
Unlock	This unlocks the door indefinitely.
Unlock (Timed)...	This unlocks the door for the specified amount of time, at the end of the time the door will relock.
Lock	This locks the door.
Door-User Activity Report	This generates a review report of all users that have accessed the door in the last day.
Door-User Reference Report	This generates a report that contains all the users that have permission to access the door.

Area Commands	Descriptions
On	This turns the auxiliary on indefinitely.
On (Timed)...	This turns the auxiliary on for the specified amount of time, at the end of the time the auxiliary will turn off.
Off	This turns the auxiliary off.
Set Analogue Value ...	Not commonly used.

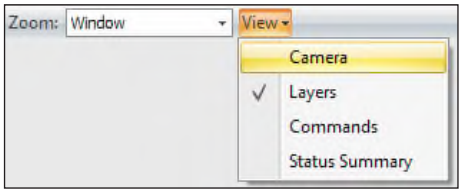
CAMERA

If you are licensed for CCTV integration and have a CCTV system enrolled, you can view video footage from within the **Schematic Map** window.

Cameras can be placed on a schematic map as an icon; the icon provides you with the following commands:

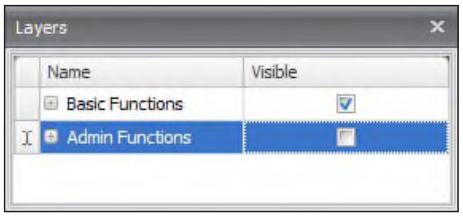
- Invoke Command
- Show Video in New Tab
- Show Video in Side Panel

Show Video in Side Panel
This will display live footage from the camera in the Camera tab. If any other camera icon is clicked, the window will automatically change to the selected camera.
If the camera window is not visible in the **Schematic Map** window, click the **View** button and select **Cameras**.



LAYERS

Schematic maps can be configured to contain layers. Layers are a way to group and stack elements on a map. A layer can be made visible or hidden by selecting the **Visibility** check-box.



On a busy schematic map with a large number of icons/shapes, you can hide layers to simplify the map and shift the operators focus on more important items.

You can restrict the layers an operator can view and therefore add or remove map items and commands for an operator. For example, a map can have an administrator layer that has controls and buttons that most operators can not see.

MAP LINKS

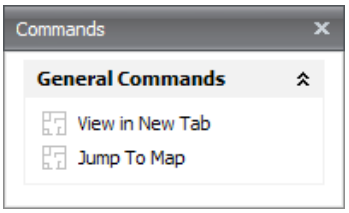
If you have more than one schematic map, you may want to navigate from one map to another rather than opening a map from the **Maps** item list.

Some schematic maps are setup so that each map is zooming in or out from the previous map, navigation can be simplified by having a button that returns you to the home/site map.

Map links are a shape, icon, label or image that allow you to navigate between schematic maps.
The following commands are available for map links:

View in New Tab
Opens the linked map in a new tab and the original map remains in the background.

Jump to Map
Opens the linked map in the current tab and replaces the original map.



ADDITIONAL MAP FUNCTIONALITY

Depending on how your schematic maps have been setup, the following features may be available to you:

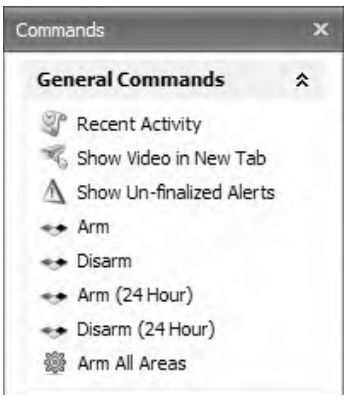
ADDITIONAL COMMANDS

Additional commands can be used to add extra control options to an element on a schematic map.

For example, an image of a large red button could have an additional command to lock down the entire site.

In the Commands window, additional commands will appear at the bottom of the default commands for the linked item.

By default, an additional command will be displayed as a cog icon.



SINGLE CLICK ACTIONS

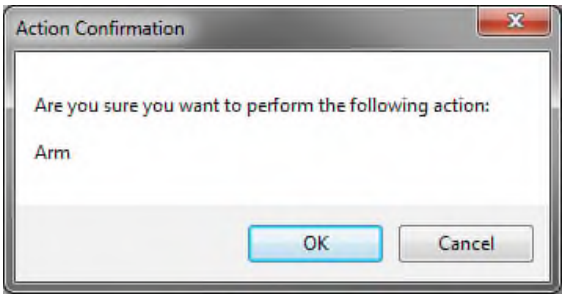
Single click actions trigger an item action or additional command with a single mouse click; this is useful if the map is displayed on a touchscreen. The default commands are still available by right-clicking the element.

ACTIONS AND COMMANDS REQUIRE VALIDATION

The **Action and Commands Require Validation** option is used to verify that the operator wants to perform the command they clicked.

When the operator attempts to perform a command that is using this feature, the system will prompt them with a confirmation window.

This feature can be applied to only certain elements on a schematic map.



NAVIGATION PANEL

INTRODUCTION TO THE NAVIGATION PANEL

The **Navigation** panel is an ordered list of all the sites, sub-sites, controllers and LAN modules. This panel is only visible in System Designer

The **Navigation** panel allows you to easily find a module, identify its state and make programming changes.

Initially, the Navigation view only contains the default site, as additional sites and controllers are added, the navigation tree will expand.

NAVIGATION PANEL BREAKDOWN

1. The **Docking PIN** determines if the navigation bar automatically hides when not in use.
2. The **Search** field filters the items within the **Navigation** panel to entered text
3. The **Refresh** button will refresh the **Navigation** panel if there has been a change made that is not being displayed.
4. The **Name** column contains the names of the site, keywords, controllers and LAN modules.

   All entities in the Navigation panel can be sorted by name in ascending or descending order by clicking on the column heading.
5. The **Status** column displays the state of the Integriti control module, LAN modules and Unibus expanders. This is explained further in the next section.
6. The **Visible** check-box will filter item list to the selected site, controller or module.

   This makes finding an item that relates to a particular site, controller or module much easier.

MODULE STATUS

The **Navigation** panel will display the following status:

Module online

Module offline

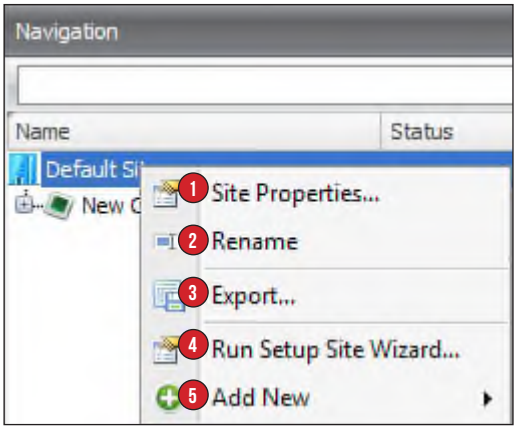
Controller online with modules offline

Controller offline

Controller syncing

Controller with warnings

SITE OPTIONS



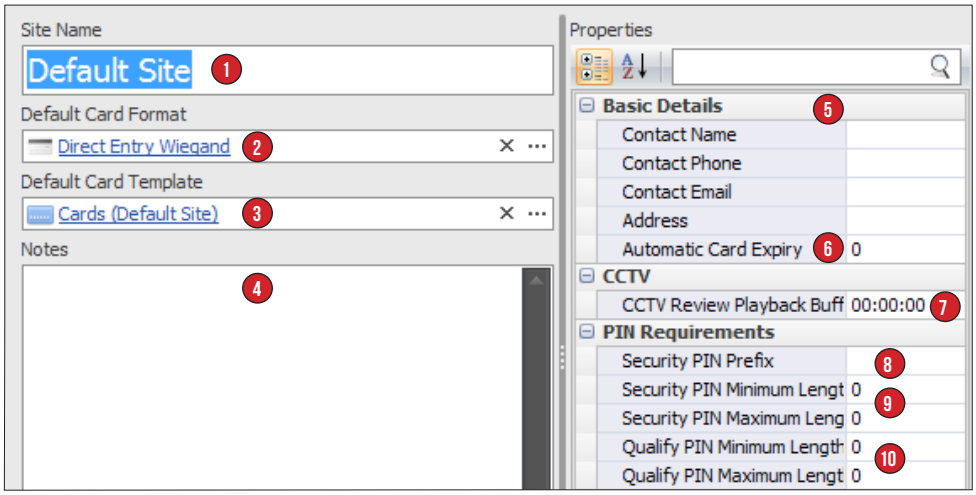
Right clicking on a site will present you with the following options:

1. The **Site Properties** option opens a menu containing basic site details, CCTV playback buffer and PIN requirements.
2. The **Rename** option allows you to rename the site.
3. The **Export** option will create an IR.Entities file containing all the programming relating to this site. This includes all sub-sites, keywords and controllers.

   This export will not contain software related entities such as operators and operator types.
4. The **Run Site Setup Wizard** option launches the site setup wizard allowing you to configure access cards. This allows you to specify a card template, card format and site code for the site. Any changes will be applied site-wide. In addition to this, the site setup wizard will prompt you to enroll a controller, change the installer password and setup regular backups.
5. The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.

SITE PROPERTIES MENU

The Site Properties menu contains the following settings:

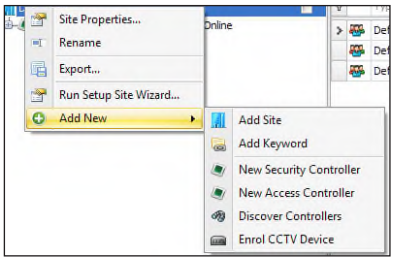


1. The **Site Name** field is used to set the name for the site.
2. The **Default Card Format** field lets you define the card format that will automatically be selected when assigning new cards to users.
3. The **Default Card Template** field lets you define the card template that will automatically be selected when assigning new cards to users.
4. The **Notes** field is used to record any notes for the site.
5. The **Basic Details** section lets you assign contact information for the site including a contact's name, phone number, email and address.
6. The **Automatic Card Expiry** field sets the number of days that a card, when assigned, will remain valid for before automatically expiring. If this value is set to zero, access cards will not automatically expire.
7. The **CCTV Review Playback Buffer** determines how much footage prior to an event is displayed when viewing old footage.

   For example: if this option is set to 10 seconds the footage will start 10 seconds before the event.
8. The **Security PIN Prefix** is used to add a prefix to the start of the security PIN for all users on the site.
9. The **Security PIN Minimum Length** and **Security PIN Maximum Length** fields are used to restrict the length of users security PIN to a specific number of digits.
10. The **Qualify PIN Minimum Length** and **Qualify PIN Maximum Length** fields are used to restrict the length of users qualify PIN to a specific number of digits.

ADD NEW OPTIONS

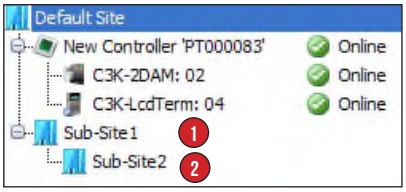
The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.



The options available are:

ADD SITE

The **Add Site** option will create a new unnamed sub-site.



1. Once named, the sub site will be located in the hierarchal view below the default site.
2. If a sub site is added to an existing sub site, it will appear nested within the first.

ADD KEYWORD

This option creates a keyword that is located in the selected site.

NEW SECURITY CONTROLLER

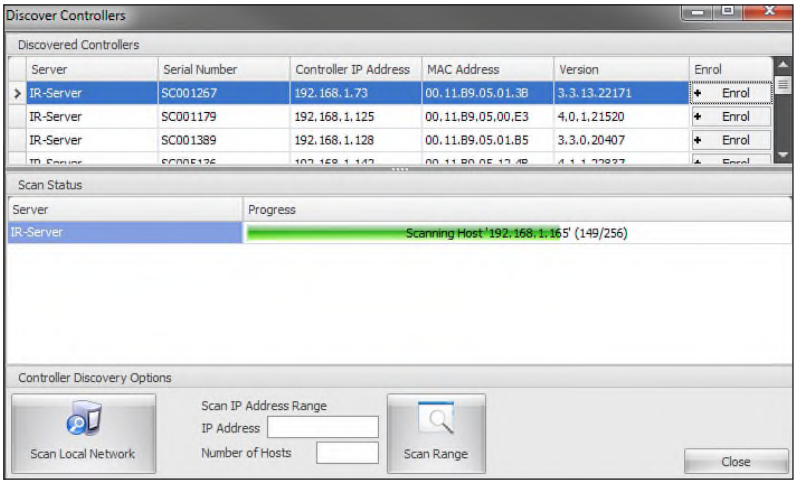
This option opens the **Controller Editor** window where a new Integriti Security Controller (ISC) can be programmed.

NEW ACCESS CONTROLLER

This option opens the **Controller Editor** window where a new Integriti Access Controller (IAC) can be programmed.

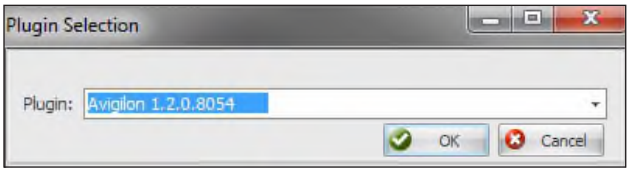
DISCOVER CONTROLLERS

This option opens the **Discover Controllers** window and will automatically start scanning the local network for controllers.



ENROLL CCTV DEVICE

This option launches the **Plug-in Selection** window where the CCTV system can be selected and then configured.



SUB-SITE OPTIONS

The right-click options for a sub-site are identical to a normal site with one exception:

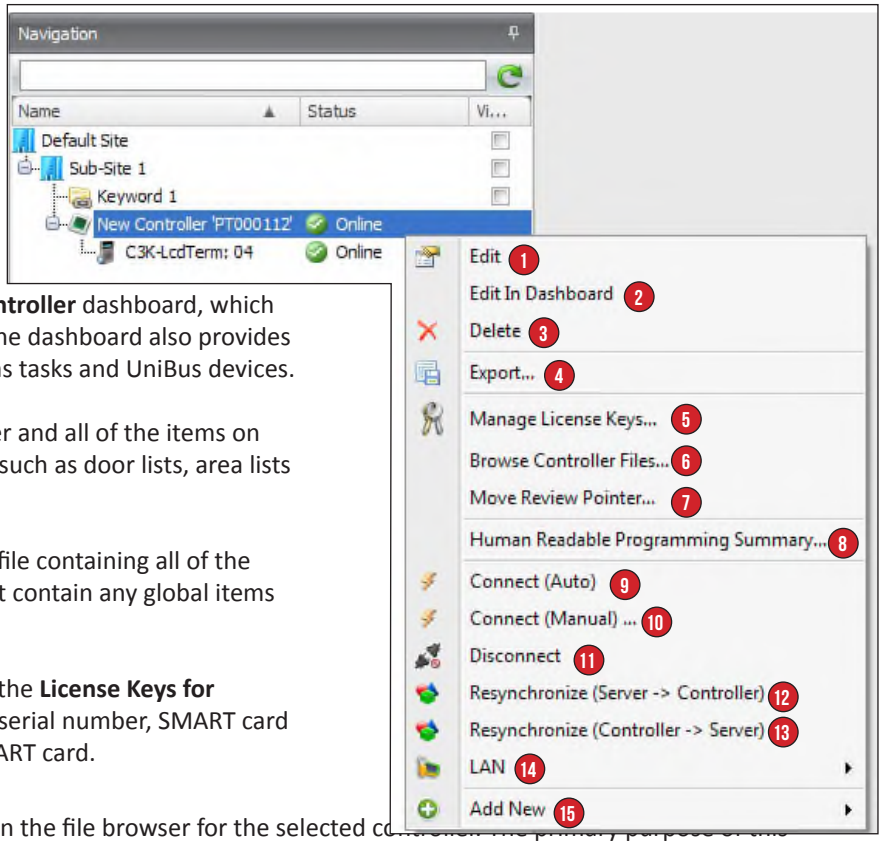
DELETING SUB-SITES

The Delete option will remove the sub-site from the Navigation panel. Since the sub-site may reference a number of other entities within the software, you may find it hard to delete a sub-site.

To solve this you can move entities that reference the sub-site to another site or sub-site.

CONTROLLER OPTIONS

Right clicking a controller will present you with the following options:



1. The **Edit** option will open the **Controller Editor** window allowing you to make programming changes to the controller options.
2. The **Edit in Dashboard** option will open the **Controller** dashboard, which simplifies the programming of the controller. The dashboard also provides the status panel entities such as macros, comms tasks and UniBus devices.
3. The **Delete** command will remove the controller and all of the items on the controller. This will not delete global items such as door lists, area lists or users.
4. The **Export** command will create an IR.Entities file containing all of the Items contained within the panel. This does not contain any global items such as door lists, area lists or users.
5. The **Manage License Keys** command will open the **License Keys for Controller** window that displays the controller serial number, SMART card serial number and the licenses held on the SMART card.
6. The **Browse Controller Files** command will open the file browser for the selected controller. The primary purpose of this window is to upload, rename or delete files located on the controllers Serial Flash, SD Card or a USB Flash Drive.

   A common use for the **Browse Controller Files** command is to clear the previous versions of firmware stored on the serial flash. If the serial flash storage on the controller is full, no additional files can be copied to this location. This stops any future firmware updates.

   In addition to file management, you can use this window to test, install or install and default the controller firmware.

7. The **Move Review Pointer** command will synchronize the specified number of review events on the controller.

   This is commonly used if there is a synchronize issue where some review messages are generated by the panel, but do not appear in the software.

   The review pointer can be moved back to a certain time or number of events.

8. The **Human Readable Programming Summary** command will generate a full programming summary of your Integriti controller. This will include the inputs, areas, doors etc.

   Once generated, the programming summary can be saved or printed.

9. The **Connect (Auto)** command reconnects the panel with the last used connection method.

10. The **Connect (Manual)** command launches the **Connect to Controller** window allowing you to choose the connection method.

11. The **Disconnect** command disconnects the controller from the Integriti software, this includes USB connections.

12. The **Resynchronize (Server -> Controller)** command resynchronizes the current programming held within the Integriti software with the Integriti controller.

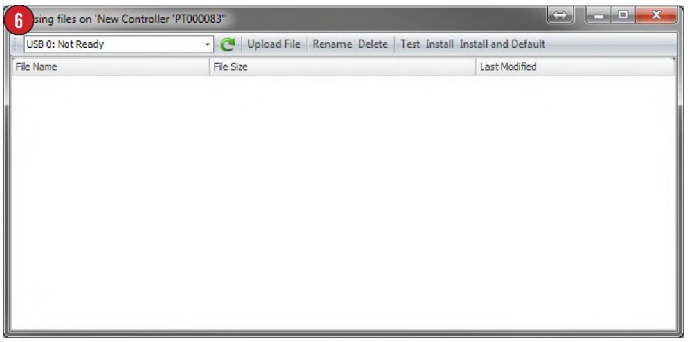
13. The **Resynchronize (Controller - > Server)** command resynchronizes the current programming held within the Integriti controller with the Integriti software.

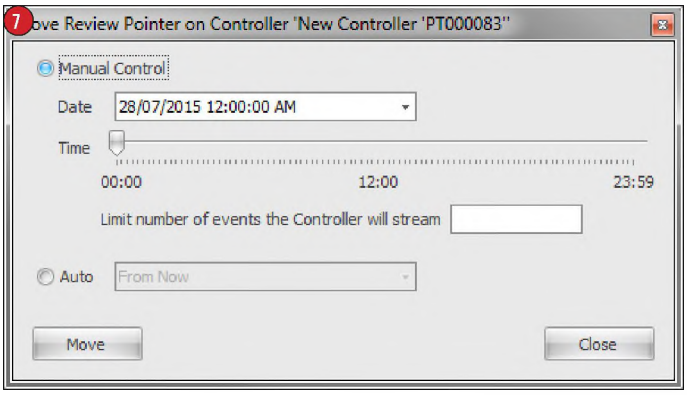
14. The **LAN** menu provides multiple LAN related commands for the currently selected controller.

15. The **Add New** menu allows you to add additional modules to the Integriti controller without having the physical module.

    This can be used to create and program a new module before physically connecting it.

    Once the module is selected, it will appear in the **Navigation** panel and all related items (such as inputs, auxiliaries etc.) will be created.





MANAGE LICENSE KEYS MENU

The Manage License Keys menu contains the following:

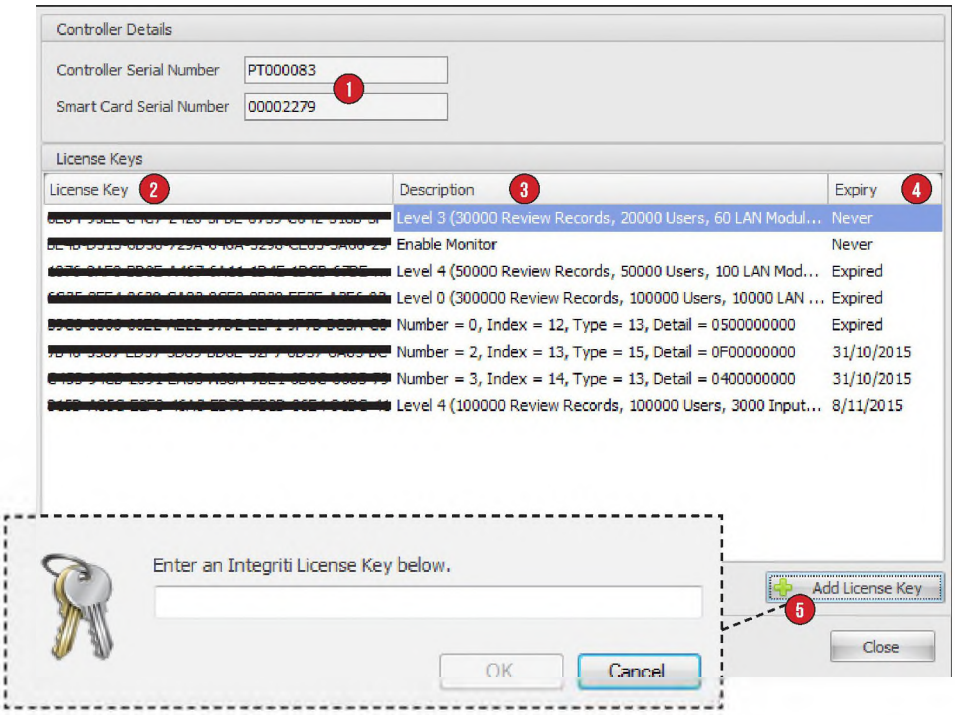
1. The **Controller Serial Number** and **Smart Card Serial Number** are both displayed in this menu.

2. The **License Key** column contains the unique key associated with each license.

3. The **Description** column provides additional information relating to the licenses.

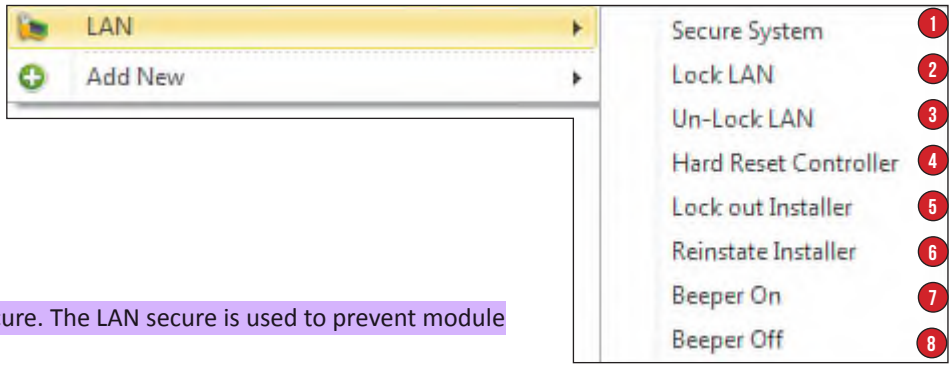
4. The **Expiry** column displays the expiry information for the licenses.

5. The **Add License Key** button is used to input new license keys.



LAN OPTIONS

The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.



The options available are:

1 : SECURE SYSTEM

This command performs a controller LAN secure. The LAN secure is used to prevent module substitution on the Integriti controller.

The **System Secure** command is the same as the LAN secure function accessible through the LCD terminal (menu 7 - 8 - 1 then 9) for the controller.

2 : LOCK LAN

The **Lock LAN** command prevents any newly attached module from connecting to the Integriti controller.

Modules that are not present at the time the LAN was locked will be ignored by the controller.

To add new modules to the controller, the LAN will need to be unlocked.

3 : UNLOCK LAN

The **Unlock LAN** command removes the LAN lock and will allow new modules to be added to the Integriti controller.

4 : HARD RESET CONTROLLER

The **Hard Reset Controller** command will perform a reset of the selected controller. This function is similar to physically power cycling the controller to reset it.

5 : LOCKOUT INSTALLER

This command is used to stop the installer logging onto a keypad, this is only used in the UK.

6 : REINSTATE INSTALLER

This command is used to allow the installer to log onto a keypad, this is only used in the UK.

7 : BEEPER ON

This command is used to start a beeping noise that can be used to find the control module.

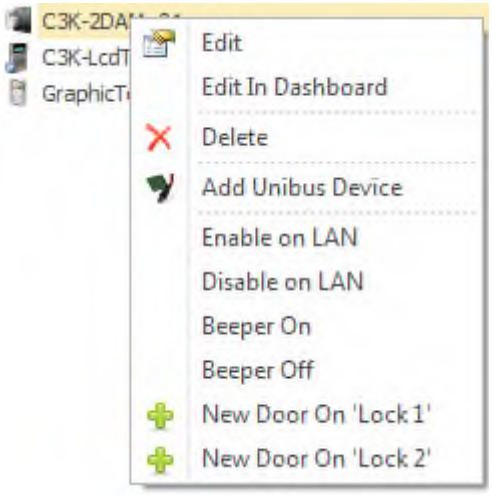
The Integriti Security Controller is not fitted with a beeper, this command will work on an Integriti Access Controller.

8 : BEEPER OFF

This will turn the controllers beeper off.

LAN MODULE OPTIONS

Most of the options in the right-click menu for a LAN module are the same as the right-click options for the Integriti controller.



Some of the options that are unique to certain modules are:

ENABLE ON LAN

This command reverses the **Disable on LAN** command and restores the module functionality.

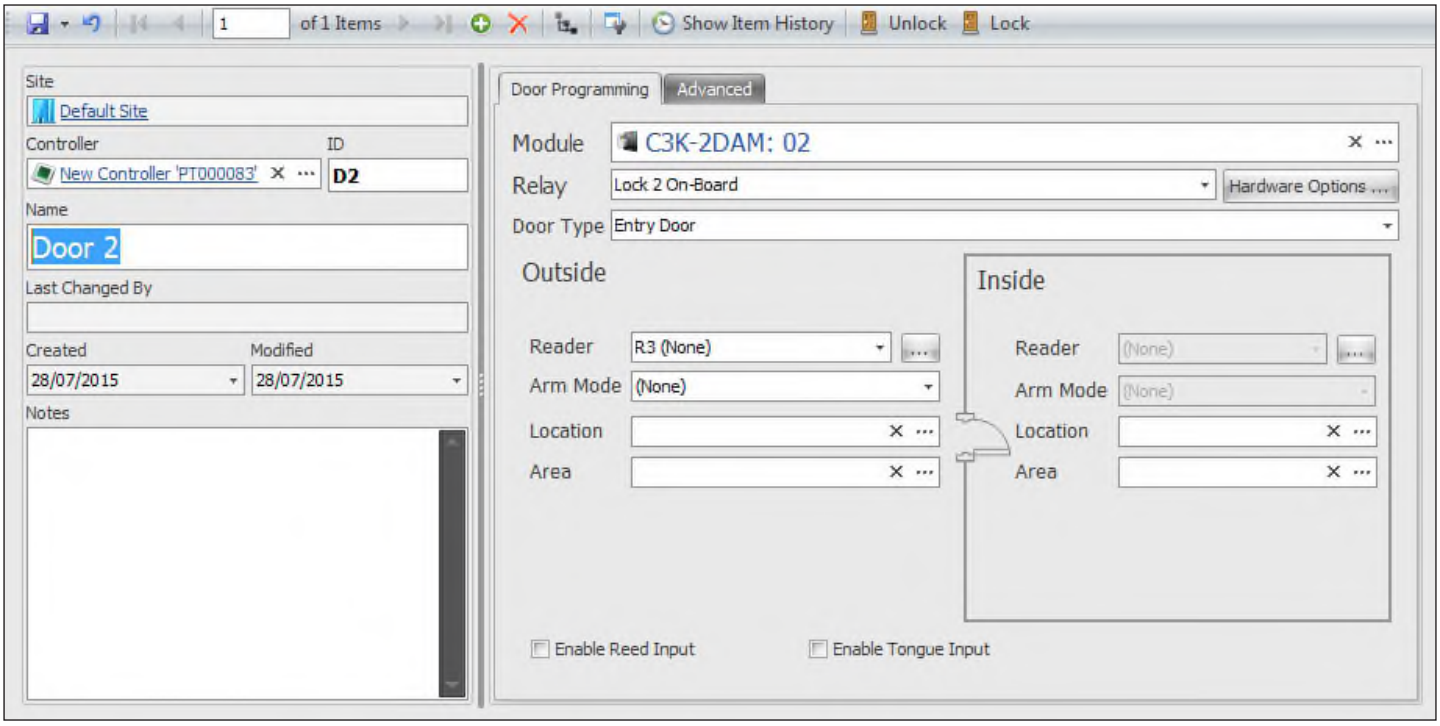
DISABLE ON LAN

This command allows you to disable the LAN module, this will cause the Integriti controller to ignore the module and the module itself will become unresponsive.

If you disable an Integriti module, the **Enable on LAN** command will restore the modules functionality. However if you disable a older Concept module, the module will need to power cycle the module.

NEW DOOR ON 'LOCK 1/LOCK 2'

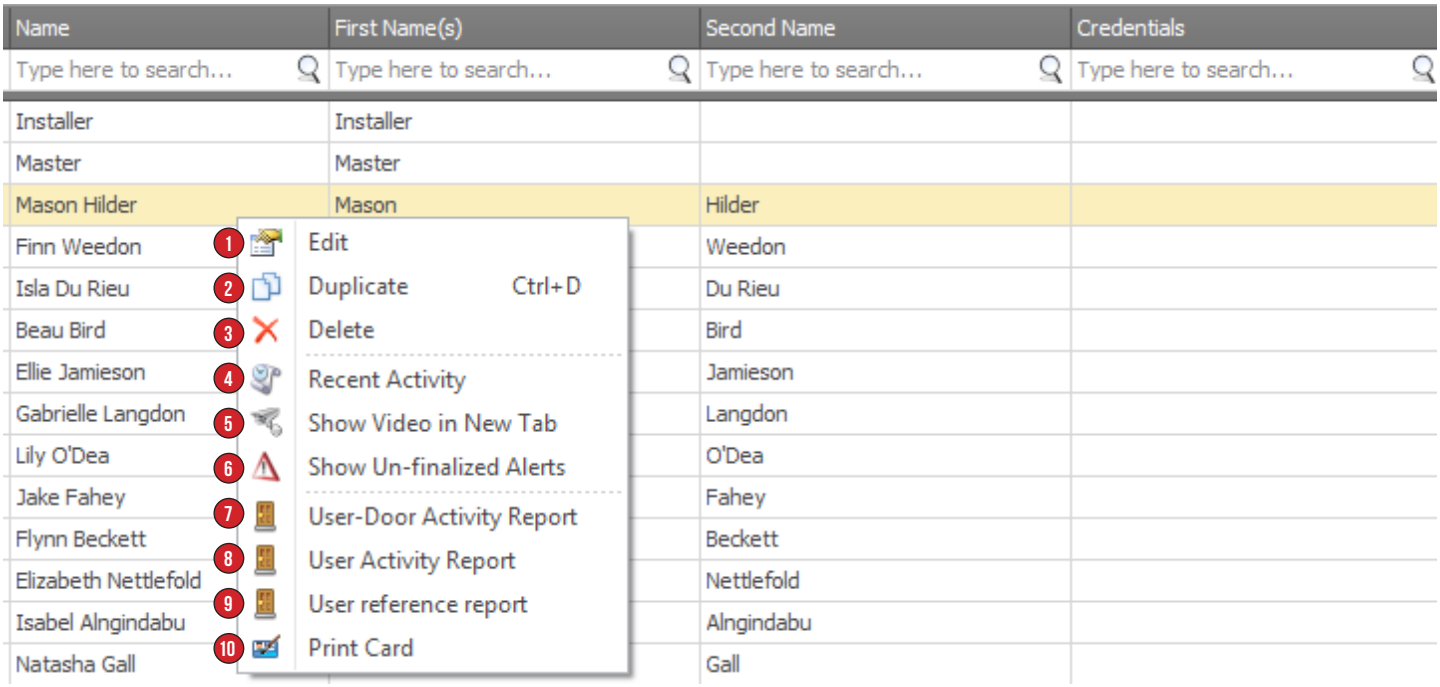
This command is available for Access Control modules and keypads. Selecting this command will open the **Door Editor** window, allowing the programming of the door on the selected module, using the selected lock.



USER COMMANDS (GATEKEEPER)

INTRODUCTION TO USER COMMANDS

Right-clicking a user in GateKeeper will display the following user commands.



1. The **Edit** command will open the **User Editor** window allowing you to make programming changes for the selected user.

2. The **Duplicate** command creates a copy of the currently selected user in the **User Editor** window. This can be used to streamline programming by duplicating similar users and making some minor changes. Be careful not to leave the card number or security PIN the same, as this will cause a credential clash.

3. The **Delete** command will permanently remove the user from the system. You will be presented with a conformation dialogue after clicking the **Delete** command.

4. The **Recent Activity** command provides a filtered review report containing all of the events that relate to the selected user or users for the last one hour. From this window, the duration of the report can be changed and the report can be printed or exported.

5. The **Show Video in New Tab** command will open a new window containing live footage of the associated camera or cameras. This will only work if the selected user is associated to a CCTV camera.

6. The **Show Un-finalized Alerts** command will open a window containing any un-finalized alerts relating to the selected user.

7. The **User-Door Activity Report** command provides a filtered review report containing all of the access events that relate to the selected user or users for the last one hour. This does not contain any review for the lock state or card data. From this window, the duration of report can be changed and the report can be printed or exported.

8. The **User Activity Report** command provides a filtered review report containing all the events that relate to the selected user or users for the last one hour. From this window, the duration of report can be changed and the report can be printed or exported.

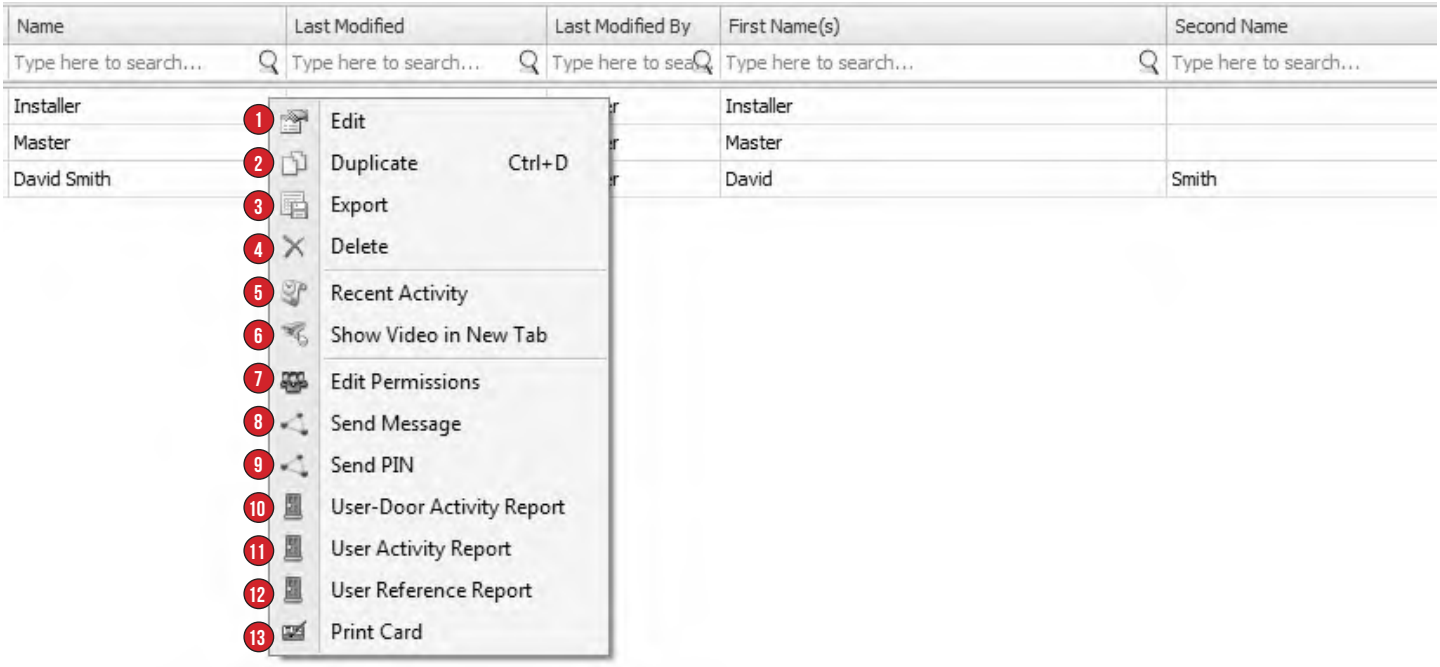
9. The **User Reference Report** command provides a report containing all the items that the selected user or users have permission to access; this includes areas, area lists, doors, door lists, permissions groups, menu groups etc.

10. The **Print Card** command uses the **Photo ID** license and allows you to print photo ID cards for users. Clicking the **Print Card** command will open the **Card Print Preview** window.

USER COMMANDS (SYSTEM DESIGNER)

INTRODUCTION TO USER COMMANDS

Right-clicking a user in System Designer will display the following user commands.



1. The **Edit** command will open the **User Editor** window allowing you to make programming changes for the selected user.

2. The **Duplicate** command creates a copy of the currently selected user in the **User Editor** window. This can be used to streamline programming by duplicating similar users and making some minor changes. Be careful not to leave the card number or security PIN the same, as this will cause a credential clash.

3. The **Export** button will export the selected user(s) as an IR-entities file.

4. The **Delete** command will permanently remove the user from the system. You will be presented with a conformation dialogue after clicking the **Delete** command.

5. The **Recent Activity** command provides a filtered review report containing all of the events that relate to the selected user or users for the last one hour. From this window, the duration of the report can be changed and the report can be printed or exported.

6. The **Show Video in New Tab** command will open a new window containing live footage of the associated camera or cameras. This will only work if the selected user is associated to a CCTV camera.

7. The **Edit Permissions** option will open the **User Permissions** window, allowing the primary permission group and the extra permissions to be edited without the **User Editor** window being opened. This is used to change the permissions for multiple users at the same time.

8. The **Send Message** command will send an SMS, email or pager message to the selected user or users. This functionality requires the **Communicator** license.

9. The **Send PIN** command will send the security PIN number to the selected user or users. The PIN can be sent as an email or SMS and requires the **Communicator** license.

10. The **User-Door Activity Report** command provides a filtered review report containing all of the access events that relate to the selected user or users for the last one hour. This does not contain any review for the lock state or card data. From this window, the duration of report can be changed and the report can be printed or exported.

11. The **User Activity Report** command provides a filtered review report containing all the events that relate to the selected user or users for the last one hour. From this window, the duration of report can be changed and the report can be printed or exported.

12. The **User Reference Report** command provides a report containing all the items that the selected user or users have permission to access; this includes areas, area lists, doors, door lists, permissions groups, menu groups etc.

13. The **Print Card** command uses the **Photo ID** license and allows you to print photo ID cards for users. Clicking the **Print Card** command will open the **Card Print Preview** window.

CCTV

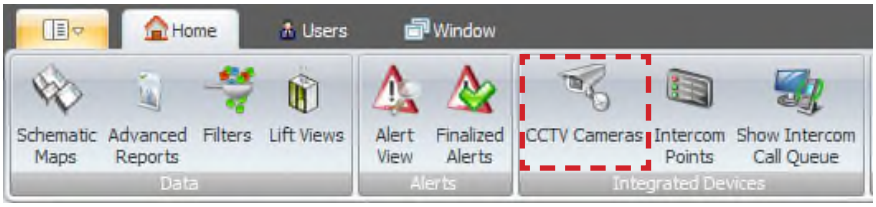
INTRODUCTION TO CCTV INTEGRATION

The CCTV Integration allows some of the functionality of a third party camera system to be incorporated into the Integriti Software. This allows an operator to view live and historical CCTV camera footage and even control PTZ cameras.

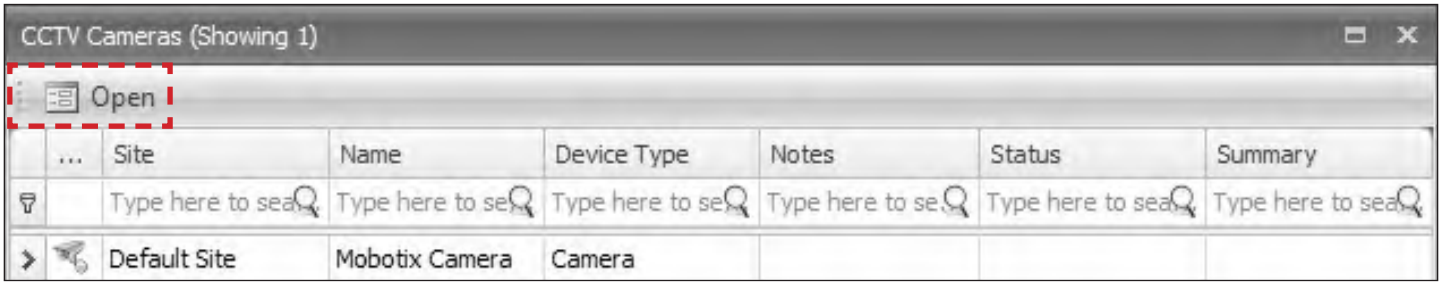
The setup and configuration of the CCTV Integration is usually done by a Certified Technician.

VIEWING CCTV FOOTAGE FROM A CAMERA

To view the live footage from a CCTV camera in GateKeeper, select the Home tab and click on the CCTC Cameras icon.

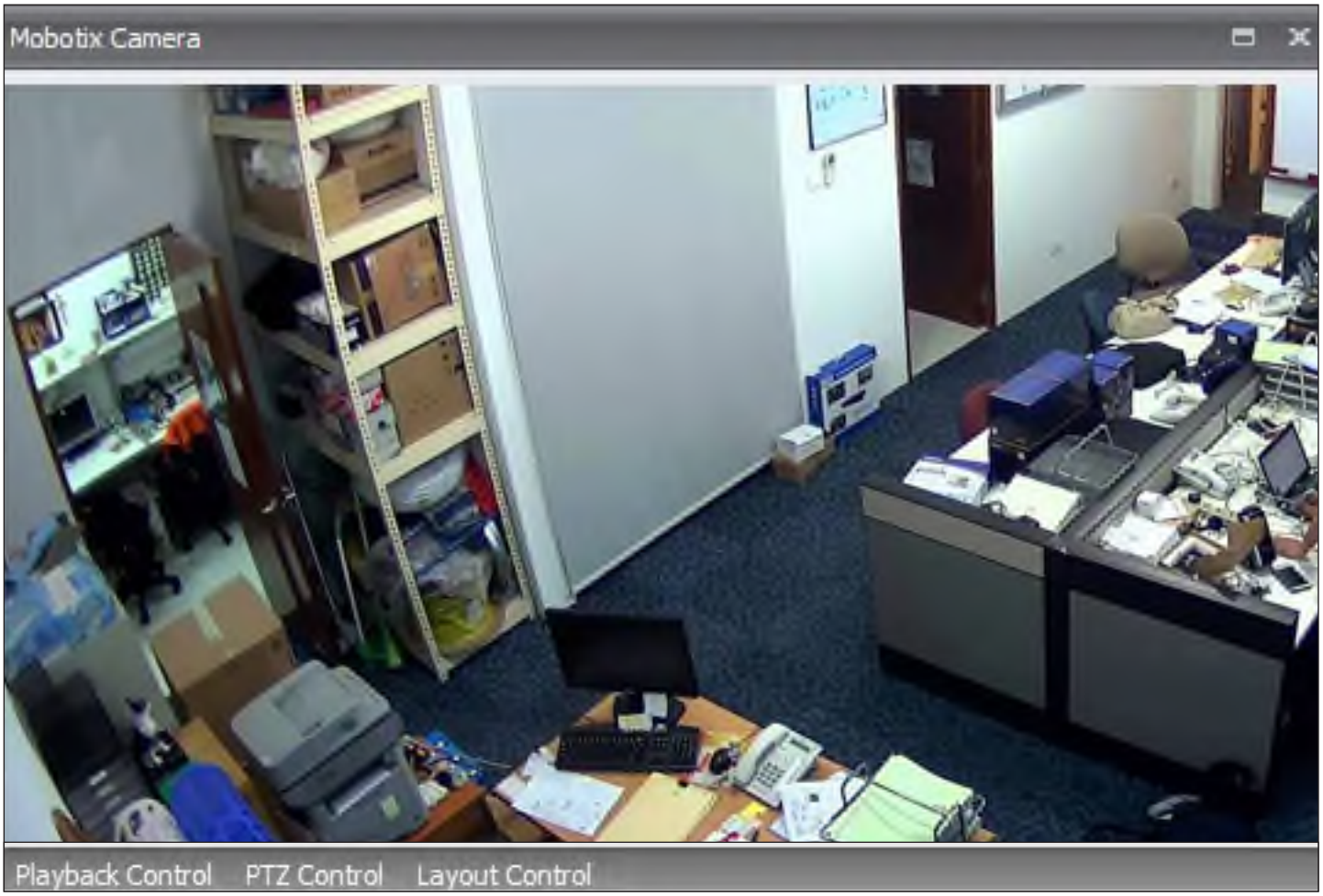


This will launch the CCTV Cameras list that contains all of the cameras that can be viewed by the operator.



To view the live footage from a camera, select the Camera and click the **Open** button or double-click on the camera.

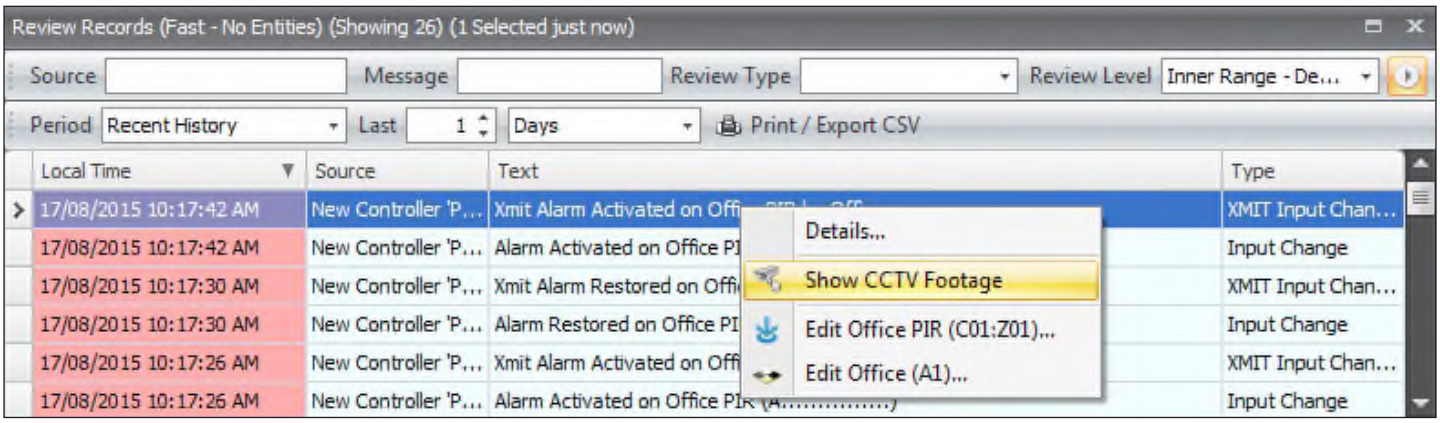
A new window will open containing the live footage.



VIEWING HISTORICAL FOOTAGE

In some cases, the CCTV cameras are associated to areas, doors, inputs or outputs in your system. You can view historical footage from the camera by finding the event you would like to see in the **Review** window.

Once you have found the event, right-click the Review Record and select the **Show CCTV Footage** option.



A new window will open containing the historical footage that matches the date and time that the event occurred.

This will only work if there is footage available to view, this may be restricted by the storage space available to the CCTV system.

AUTOMATIC CCTV POP-UPS

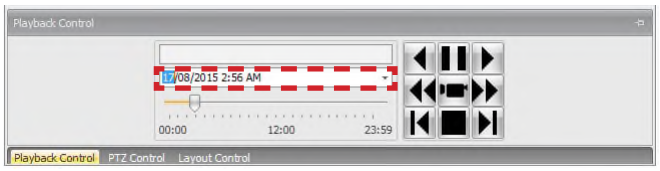
If configured, live CCTV footage can pop-up in the Integriti GateKeeper software, this pop-up is based on a particular event. This is commonly used when live footage is required to be seen by an operator for an event such as a duress or panic button being pressed. This functionality requires that either alerts or scheduled tasks are configured.

CONTROLLING THE PLAYBACK OF FOOTAGE

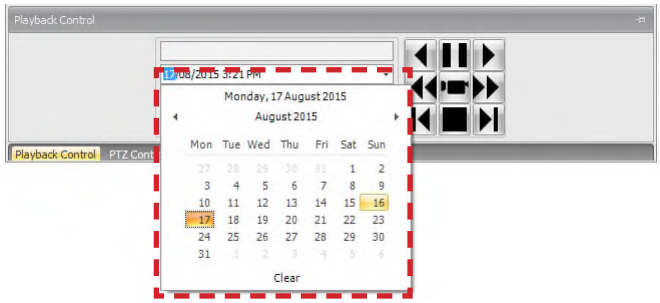
Once you open the camera window, the footage can be controlled with the playback controls, found in the **Playback Control** tab.

DATE & TIME SELECTOR

The **Date & Time** field is used to retrieve footage from a certain time by entering the date and time of the event.

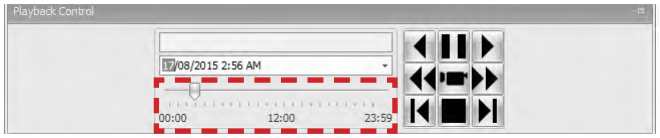


Alternatively the **Date & Time** drop down is used to select the date using a calendar preview.



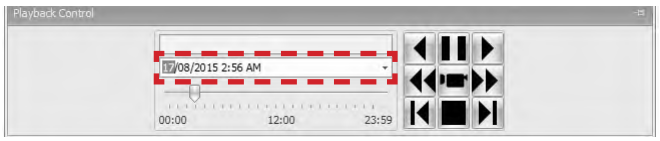
Once the date has been set, the time can be set using the **Time** slider.

Drag the slider to the nearest time to the time the event occurred. The time slider is in a 24-hour format.



As the time slider is changed, the date and time selector will update.

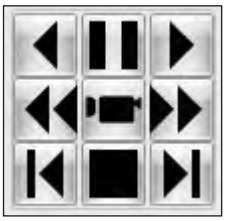
This is the start time that is used when using the other playback controls.



PLAYBACK BUTTONS

The playback buttons allow you to easily play, rewind, fast-play and pause CCTV footage.

The controls below will differ from one CCTV system to another.



PLAY

This button plays the footage forward at normal speed.

FAST FORWARD

This button plays the footage forward at high speed; each click increases the speed of playback.

REWIND

This button plays the footage backwards at normal speed.

FAST REWIND

This button plays the footage backwards at high speed; each click increases the speed of playback.

PAUSE

This button will pause the footage on the current frame.

LIVE VIEW

This button display live footage from the CCTV camera.

STEP FORWARD

This button advances the footage one frame at a time.

STOP

This will stop the current footage stream.

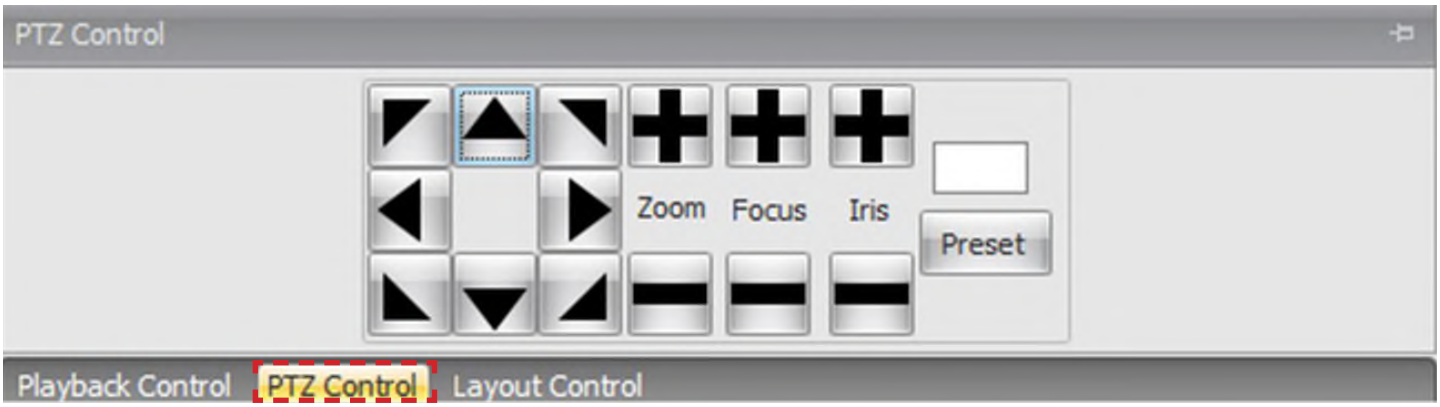
STEP BACKWARD

This button rewinds the footage one frame at a time.

CONTROLLING A PTZ CAMERA

If you have a PTZ (Pan, Tilt and Zoom) CCTV camera you can control the PTZ functionality via Integriti GateKeeper or System Designer.

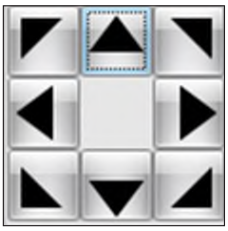
Select the **PTZ Control** tab to view the PTZ controls, some of these commands may not work based on your camera's capabilities.



PLAYBACK BUTTONS

The directional arrows are responsible for the pan and tilt of the camera. Single-clicking an arrow will move the camera in the direction you clicked.

If the arrow is clicked and held down, the camera will move until the button is released.



ZOOM

The zoom buttons control the amount that the camera is zoomed in or out.

The "+" button increases the amount of zoom and the "– "button decreases the amount of zoom.

FOCUS

The focus buttons control the area that the camera is focused on, this may be used to bring a foreground object into focus.

The "+" and "–" buttons shift the focal area forward or backward.

IRIS

The iris control will result in more or less light entering the camera through the lenses. This is used to increase or decrease the brightness of the camera footage.

The "+" button increases the amount of light reaching the camera and the "–" button decreases it.

PRESET

If the CCTV camera has been configured to use preset locations, you can trigger the camera to move to a preset by using the preset field.

Once a preset number has been entered, clicking on the Preset button will result in the camera moving to that particular preset location.

VIEWING MULTIPLE CAMERAS

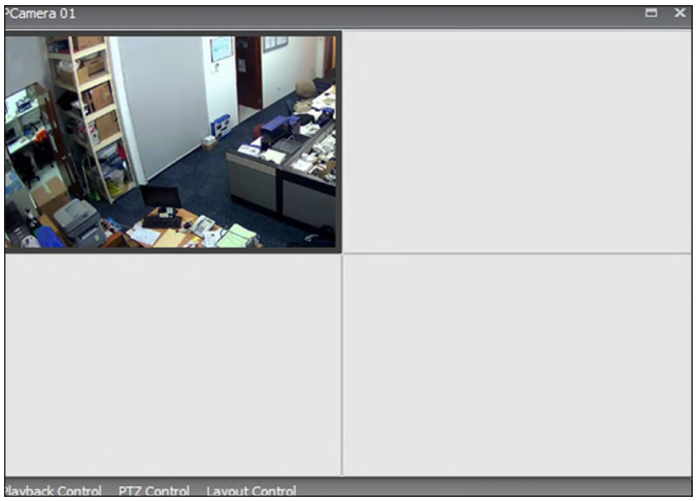
In some cases an area, door, input or auxiliary may be associated to more than one camera, when viewing historical footage the **Camera** window will contain more than one camera.

The number of cameras viewed at once can be changed by using the **Layout Control** tab found in the **Camera** window, this will work for historical and live footage.

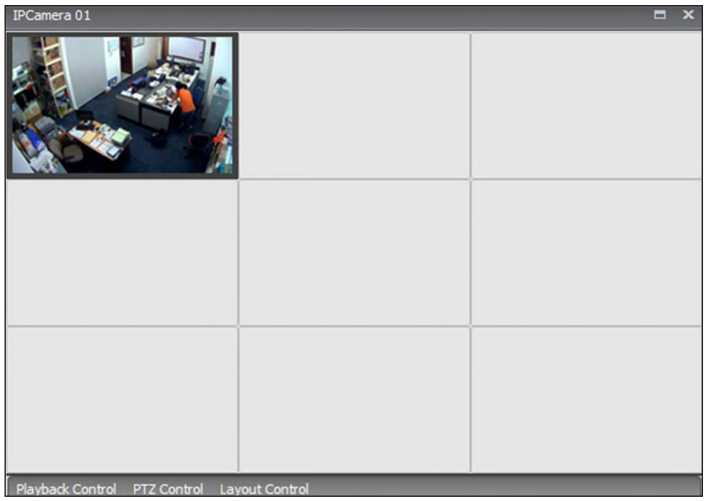
The layout of the camera window can be set to: 1x1, 2x2, 3x3 or 4x4.

1X1

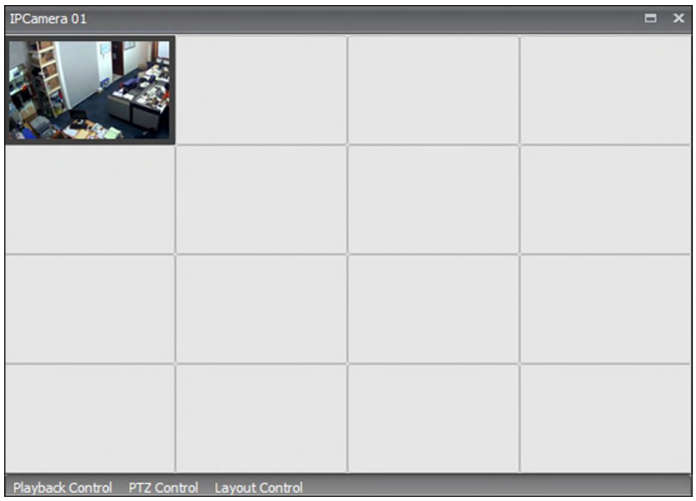
2X2



3X3



4X4



Once you have selected a camera layout, drag additional cameras onto the **Camera** window to be displayed. Closing the **Camera** window will reset the layout.

OPERATORS

INTRODUCTION TO OPERATORS

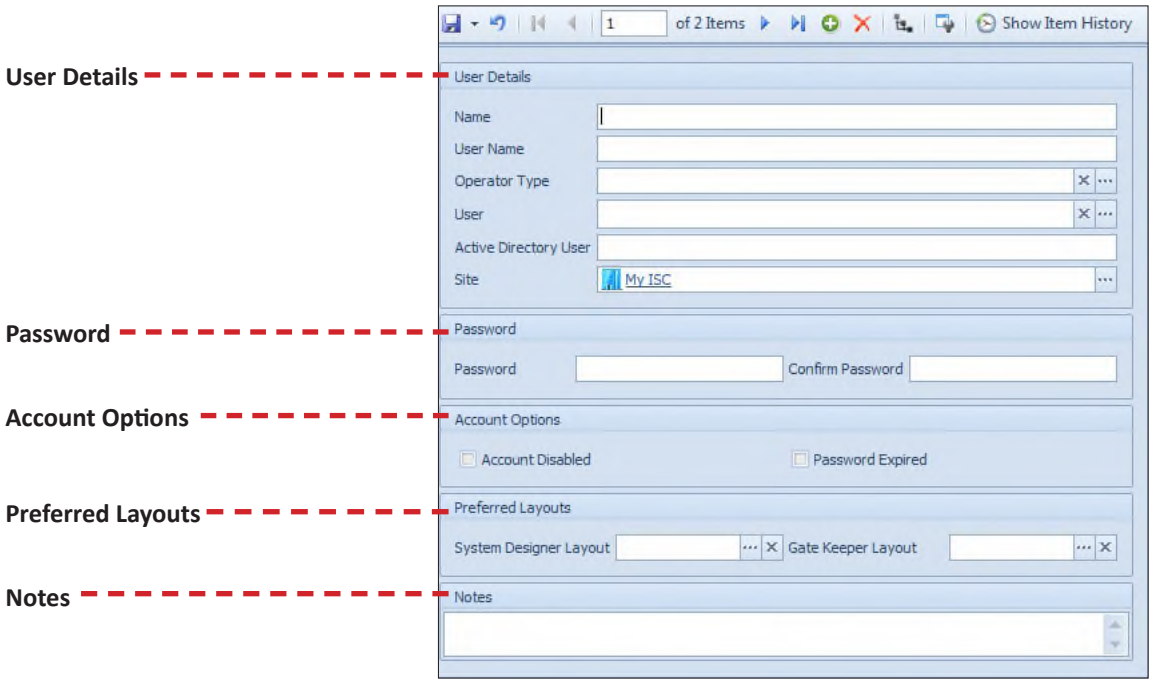
Operators are the users who login to the Integriti System Designer or GateKeeper software.

Most programming changes to the Integriti system are audited, this audit includes the operator that made the change. It is recommended that each user logging into the software has a unique operator name and password.

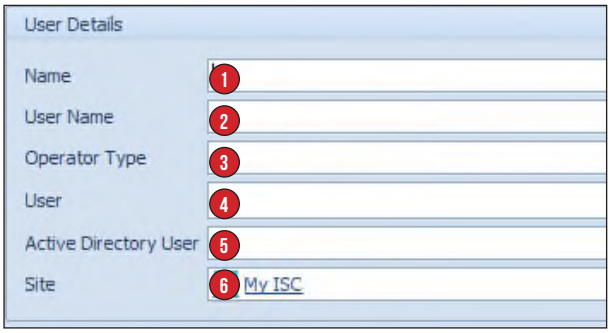
To view, edit, create or delete operators navigate to the **Administration** tab and click the **Operators** icon.

OPERATOR EDITOR WINDOW

The **Operator Editor** window is broken down into five sections:



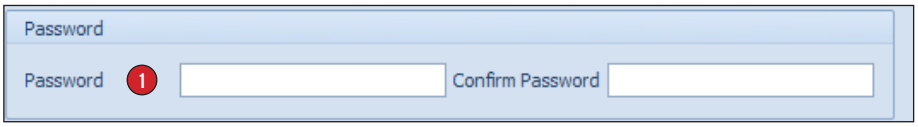
USER DETAILS



1. The **Name** field is used to identify the operator.
2. The **User Name** field is used by the operator to log-in to the Integriti Professional or GateKeeper software.
3. The **Operator Type** determines the permissions/access levels that the operator has.
4. The **User** field allows a user in the controller to be assigned to the operator. The operator will only be able to control items as assigned to the user.
5. **Active Directory User** allow users to login to the Integriti software using their window credentials. Active Directory is a licensed feature
6. The **Site** field sets the default site for any entities that the operator creates (areas, doors, etc.)

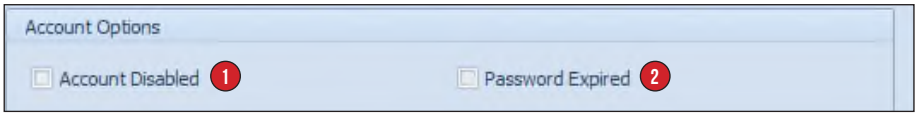
PASSWORD

1. The **Password** and **Confirm Password** fields are used in conjunction with the User Name field to allow operators to log into the Integriti Professional or Integriti GateKeeper software.



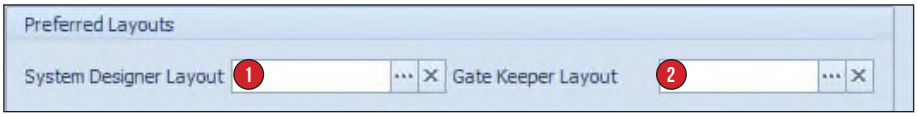
ACCOUNT OPTIONS

1. Enabling the **Account Disabled** option will disable the operator and prevent them from logging in.
2. Enabling the **Password Expired** option will force the operator to change their password the next time they log in.



PREFERRED LAYOUTS

The Preferred Layouts are used to define the default layout for the operator when they first log in.



1. The **System Designer Layout** field defines the default layout for the Integriti Professional software.

2. The **GateKeeper Layout** field defines the default layout for the Integriti GateKeeper software.

ASSIGNING USERS TO OPERATORS

The user section allows a user in the system to be assigned to the operator, the operator will only be able to control the items that are assigned to the users permissions. When user is assigned to an operator and the operator controls an item such as a door, the system will generate a review message that contains the user. Below are examples of an operator unlocking a door from the software with and without a user assigned.

WITHOUT AN ASSIGNED USER

8/07/2015 4:29:01 PM	SAMSUNG INC	Front Door Unlocked by Comms Task 01 (Integriti CT) (Integriti) (remote) (D022)

The message describes the event correctly, however there is no information regarding the individual responsible for remotely unlocking the door.

WITH AN ASSIGNED USER

07/2015 4:32:26 PM	SAMSUNG INC	Front Door Unlocked by Rob Steed (Integriti) (remote) (D022)

The review message now contains both the event and the user responsible. For tracking and auditing purposes, it's recommended that all operators who control system entities, such as areas, doors, lift cars etc have an associated user.

If the operator attempts to control an item that their assigned a user does not have permission to control, the following review message will be generated:

9/07/2015 8:56:28 AM	SAMSUNG INC	Area Action by Rob Steed (Integriti) (remote) failed in queue 4 because Not Allowed

ACTIVE DIRECTORY USERS

If **Active Directory Operator** authentication is enabled it will allow users to sign on with their currently logged-on windows account or with the provided Active Directory credentials. This can provide a single sign on (SSO) type functionality to the Integriti software. An Active Directory Operator License is required.

There are two methods that can be used to link Active Directory users to Integriti Operators:

Via Operators
Individual operator records can be manually linked to a domain account.

Via Operator Types
Active Directory Groups can be linked to Integriti Operator Types. Operators are created and controlled by domain administrators.

OPERATOR TYPES

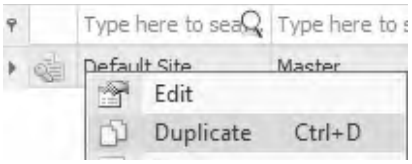
INTRODUCTION TO OPERATORS TYPE

Operator Types determine what items and features an operator can access within the Integriti System Designer or GateKeeper software. The relationship between an operator and the operator type is similar to the relationship between the user and a permission group.

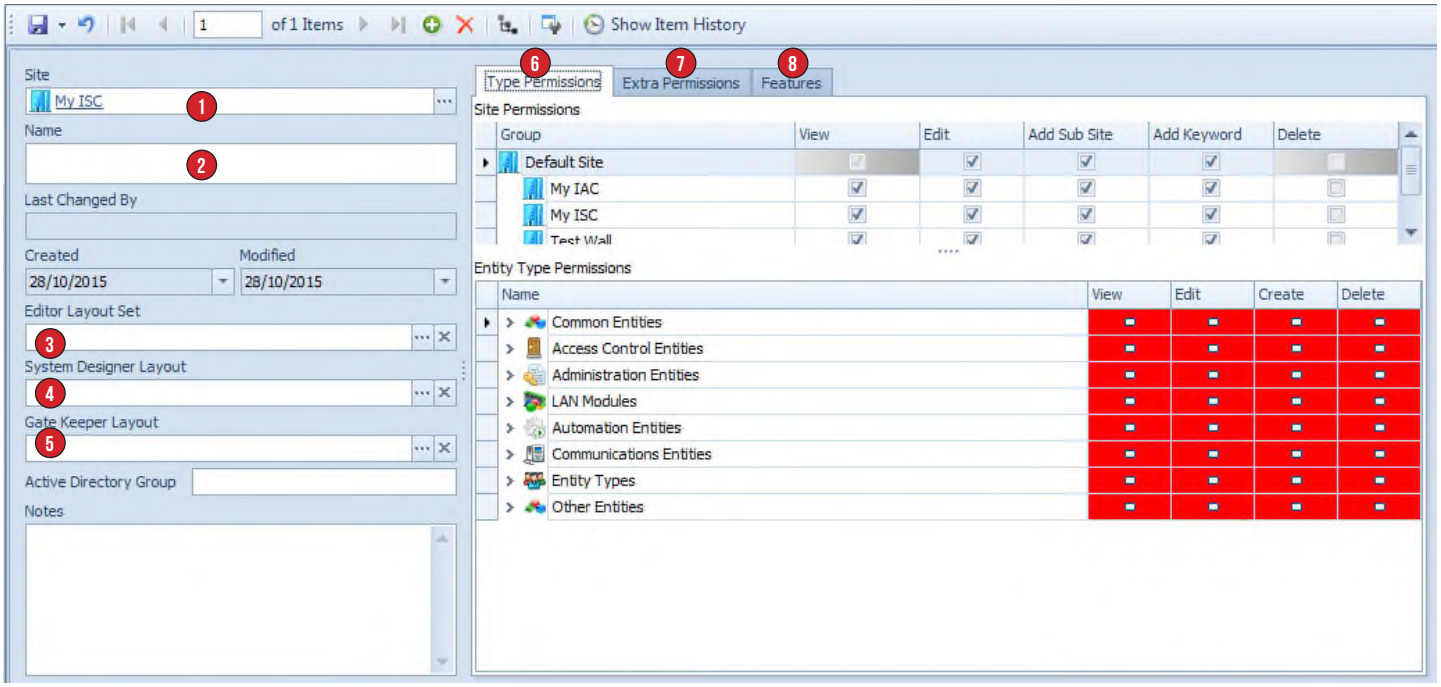
To create, edit or delete an operator type navigate to the **Administration** tab and click the **Operator Types** icon.

CREATING AN OPERATOR TYPE

It is quicker to duplicate an operator type such as **Master** and edit it rather than adding a new operator type and starting from scratch.



Right-click an operator type and select **Duplicate**, this will create an unnamed copy. The **Operator Type** window contains the following items:



1. The **Site** field is used to identify which site the operator type belongs to.

2. The **Name** field is used to identify the purpose and contents of the operator type. i.e. Security Guard

3. The **Editor Layout Set** determines the appearance of the editor window for each item. This editor layout will load for any operator assigned this operator type. If left empty the default editor layout is used.

4. The **System Designer Layout** determines the appearance of the System Designer software. This layout will load for any operator assigned this operator type. If left empty the default System Designer layout is used.

5. The **GateKeeper Layout** determines the appearance of the GateKeeper software. This layout will load for any operator assigned this operator type. If left empty the default System Designer layout is used.

6. The **Type Permissions** tab determine the groups of items an operator can view, edit, create or delete. Permissions for items can be assigned separately for sites and sub-sites.

7. The **Extra Permissions** tab allows you to set permissions for individual items such as specific door or a specific user.

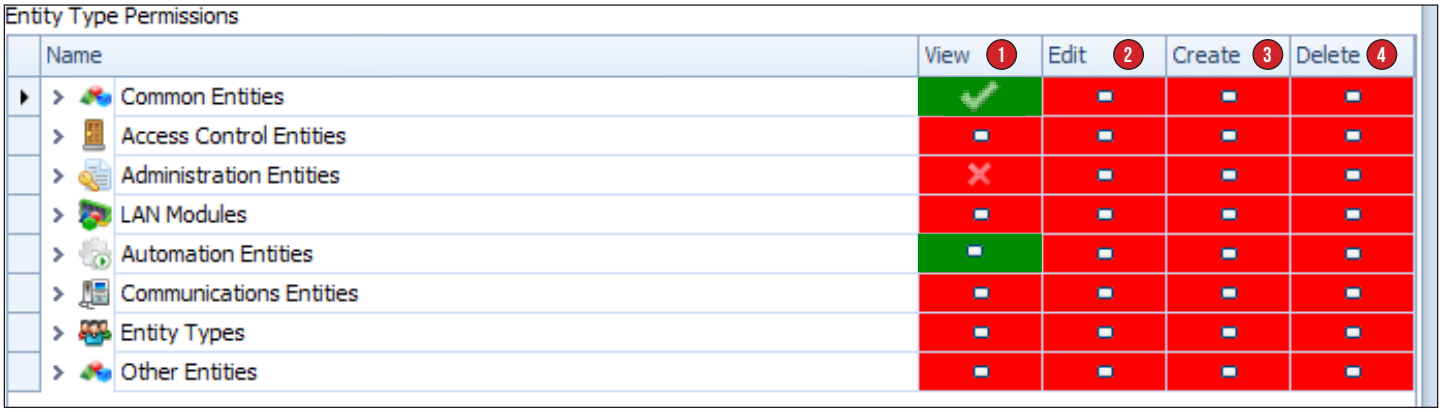
8. The **Features** tab determine the additional functionality the operator will have in the System Designer or GateKeeper software.

THE TYPE PERMISSIONS TAB

SITE PERMISSIONS

1. Enabling the **View** option allows the Operator to see the site in the **Navigation** panel. The **View** option can not be disabled for the default/top site.
2. Enabling the **Edit** option allows the operator to edit the properties of the site such as the site name.
3. Enabling the **Add Sub Site** option allows the operator to add sub-sites to the selected site.
4. Enabling the **Add Key Word** option allows the operator to add a keyword the site.
5. Enabling the **Delete** option allows the Operator to delete the site. The **Delete** option can not be enabled on the default/ top site.

ENTITY TYPE PERMISSIONS



1. The **View** check-box allows the operator to view the item for the currently selected site.
2. The **Edit** check-box allows the operator to edit the item for the currently selected site.
3. The **Create** check-box allows the operator to create the item for the currently selected site.
4. The **Delete** check-box allows the operator to delete the item for the currently selected site.

You will notice there is 4 selectable options to choose from:

Allow

Inherit Allow (this inherits permissions from the parent site)

Deny

Inherit Deny (this inherits permissions from the parent site)

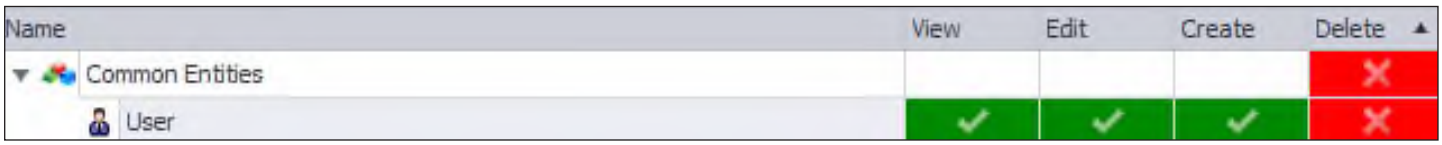
EXTRA PERMISSIONS TAB

The **Type Permissions** tab provides an operator permission to view, edit, create or delete an entire group of items. This means that if an operator is provided the permission to edit users there is no restriction on which users they can edit.

The **Extra Permission** tab is used to add and remove permissions for single items. For example, you may have an operator that has permission to edit users, however you want to stop them from editing the **Installer** user. To do this, add an extra permission that denies the edit permission for the **Installer** user.

The example below demonstrates how to restrict an operator from viewing a single user:

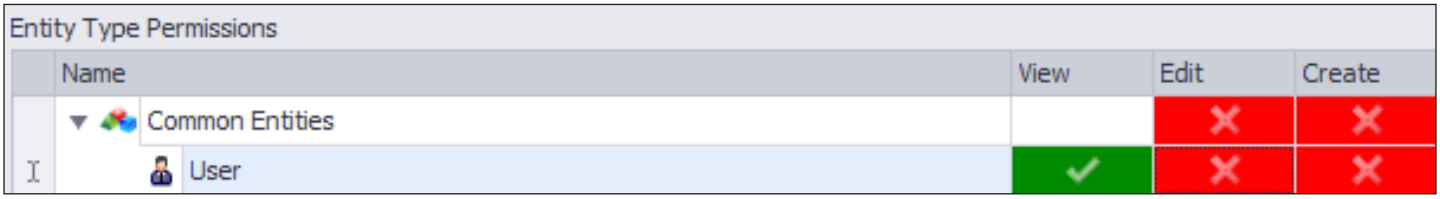
1. In the **Type Permissions** tab the **Common Entities > User** options to view, edit and create users are enabled. This allow the operator to view and edit all users.



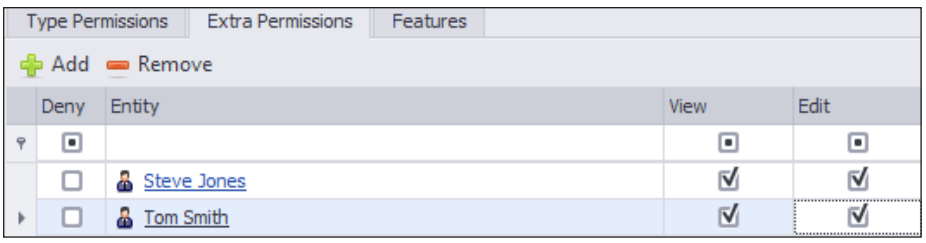
2. In the **Extra Permissions** tab the **Installer** user is added and the **Deny** and **View** options are enabled to stop the operator viewing the Installer user.

The example below demonstrates how to increase an operators permissions using extra permissions.

1. In the **Type Permissions** tab the **Common Entities > User** option only allow the operator to view users. The operator can open and view users however changes will not be saved.



2. In the **Extra Permissions** tab two users are added and the **View** and **Edit** options are enabled. This allows the operator to edit just these two users.



FEATURES TAB

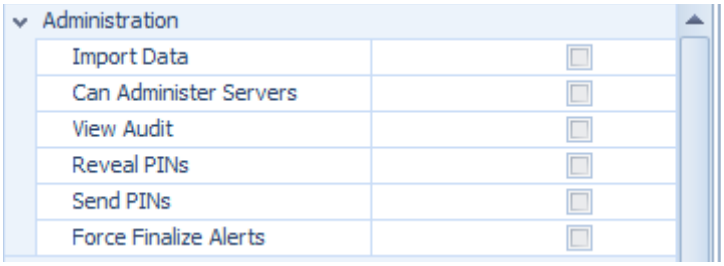
The **Features** tab allows you to enable access to specific features within the System Designer and GateKeeper software.

These features are broken up into seven sub-categories:

1. Administration
2. Review
3. Controllers
4. Licensing
5. Layout
6. Integration
7. Software Modules

ADMINISTRATION

The **Import Data** option allows operators to access the **Import Data** feature from the **Administration** tab.



The **Can Administer Servers** option allows operators to view servers, workstations and client connections from the **Administration** tab.

The **View Audit** option allows operators to view a historical log of all programming changes to system items.

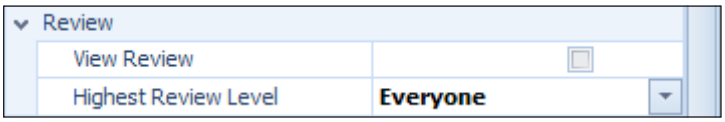
The **Reveal PINs** option allows an operator to view other users PINs.

The **Send PINs** option allows an operator send a PINs to users via e-mail or SMS, this feature is used when a user forgets their PIN. A license is required to send SMS or emails from the Integriti software.

The **Force Finalize Alerts** option allows an operators to finalize (close) one or more alerts without writing a response.

REVIEW OPTIONS

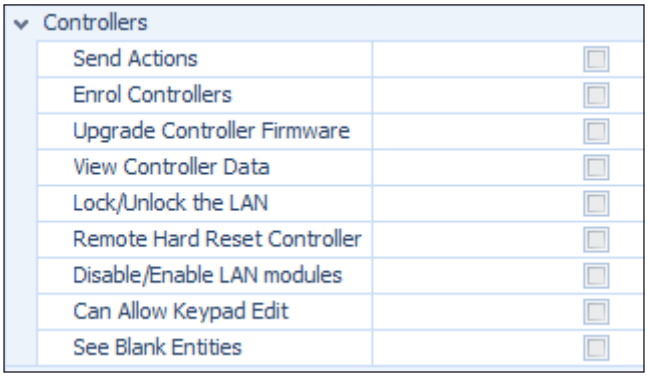
The **View Review** option allows operators to see review.
The **Highest Review Level** determines the highest level of review that the operators will have permission to view.
The review levels are:



1. Everyone
2. User - Essential
3. User – Standard
4. User – Detailed
5. Installer – Detailed
6. Inner Range - Debug

CONTROLLERS OPTIONS

The **Send Actions** option allows operators to control items such as areas, doors or outputs from the System Designer or GateKeeper software.



The **Enroll Controllers** option allows operators to add new controllers to the site from the System Designer software.

The **Upgrade Controller Firmware** allows the operator to upgrade the firmware of the Integriti controller and hardware modules.

View Controller Data allows operators to view controller related information and data such as hardware licenses.

The **Lock/Unlock LAN** option allows operators to perform a LAN lock on integriti controllers, once the LAN is locked no modules can be added to the system until the operator unlocks the LAN. This option should only be enabled for the Installer or site administrator.

The **Remote Hard Reset Controller option** allows operators to reset on a controller via the Integriti software. A hard reset will disable all security and access control for about a minute. This option should only be enabled for the Installer or site administrator.

The **Disable/Enable LAN Modules** option allows operators to disconnect or connect a LAN modules to the Integriti controller. Disabling a LAN module may result in doors, inputs or automation not working correctly. This option should only be enabled for the Installer or site administrator.

The **Can Allow Keypad Edit** option allows operators to change the data synchronization mode for a controller; this can be used to enable or disable programming changes from a keypad. This option should only be enabled for the Installer or site administrator.

The **See Blank Entities** option allows operators to see a list of all blank entities currently present in the system.

LICENSING

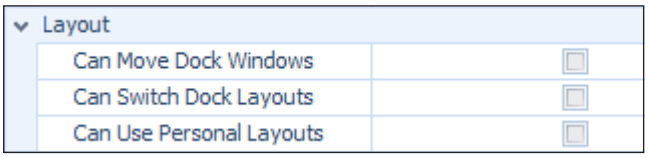
The **Can Manage Licenses** option allows operators to add software and hardware licenses to the Integriti System Designer software. To add licenses click the **Administration** tab and select **License Manager**.

LAYOUT

The **Can Move Dock Windows** option allows operators to change the location of windows for the Integriti System Designer and GateKeeper software.

The **Can Switch Dock Layouts** option allows operators to load System Designer or GateKeeper layouts.

The **Can Use Personal Layouts** option allows operators to keep the changes they make to a layout after exiting the software. Their personal layout will automatically be loaded when they next login to the software



INTEGRATION

The Enroll Integration Device option allows operators to enroll new third party devices such as CCTV recorders or intercom systems.

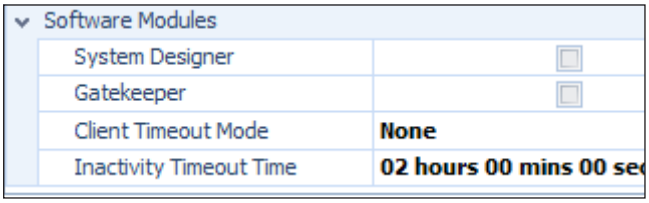
SOFTWARE MODULES

The **System Designer** option allows the operator to log into the System Designer software. This option can be disabled to provide the operator with access to only GateKeeper.

The **GateKeeper** option allows the operator to log into the GateKeeper software. This option can be disabled to provide the operator with access to only System Designer.

The **Client Timeout Mode** is used to automatically log an operator out of the Integriti software. The mode can be set to auto log-out after no system activity, this mode uses the time specified in the **Inactivity Timeout Time.**

The **Inactivity Timeout Time** determines how long the operator needs to be inactive before the system automatically logs them out.

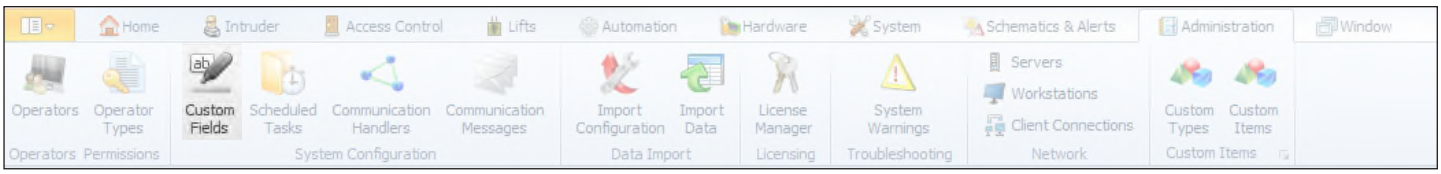


CUSTOM FIELDS

INTRODUCTION TO CUSTOM FIELDS

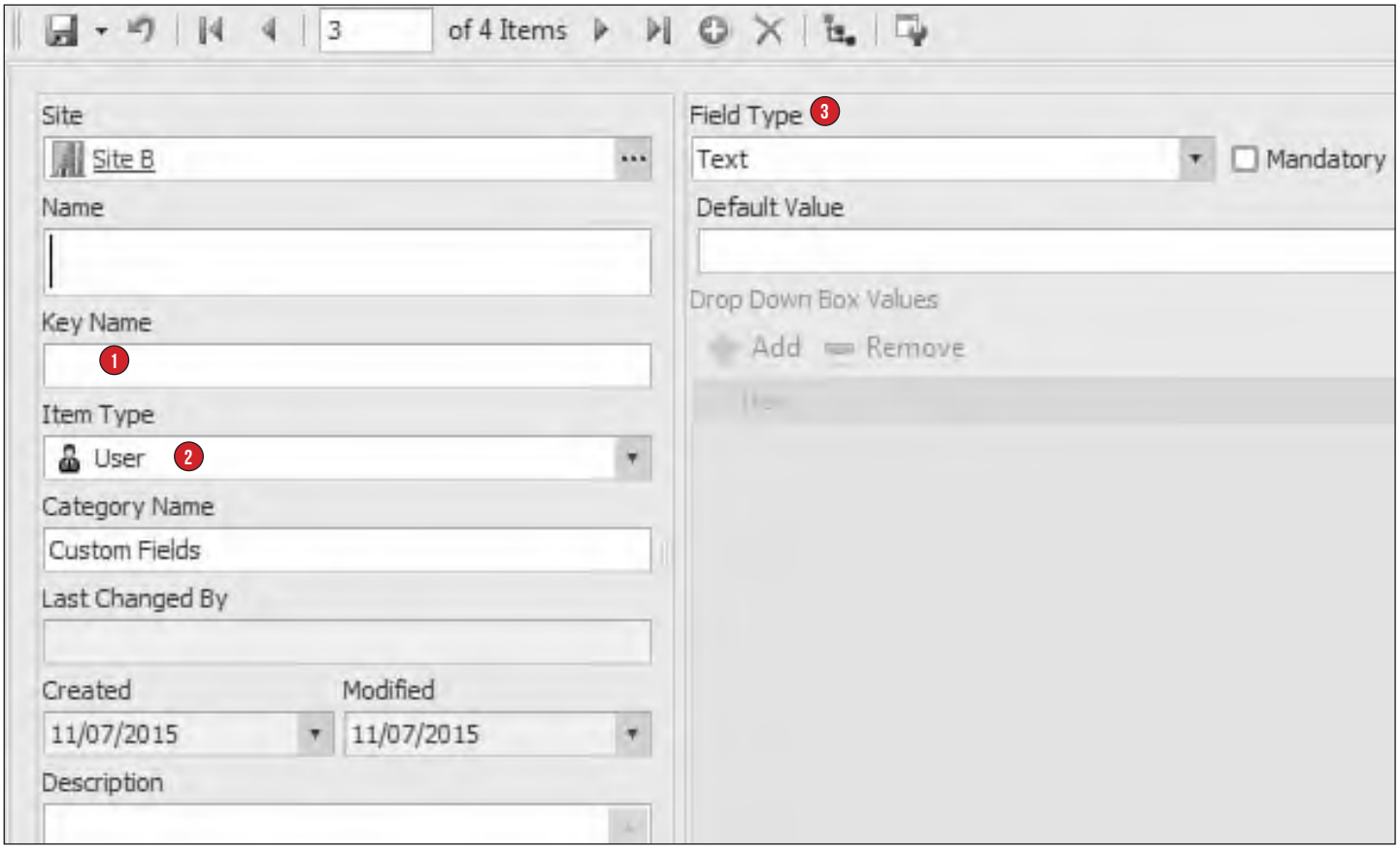
Custom fields allow you to add fields to almost any programmable item in the Integriti Software. These custom fields allow you to capture or display extra information that is otherwise not present in the default Integriti menus. For example: a users date of birth or driver's license number.

To access the Custom Fields menu, you must navigate to the **Administration** tab and select **Custom Fields**



CREATING A CUSTOM FIELD

When creating a custom field, you will be presented with the following menu:



1. The **Key Name** field allows you to create a database name for this custom field. This is particularly useful if you are going to use this custom field in a report. It is a recommended standard that all custom field key names contain the cf_ prefix.

2. When creating a custom field you have the option of selecting an **Item Type**. This will determine where the field will appear.

3. **Field Type** setting allows you to define the type of data that the custom field will contain. These field types ensure that operators are capturing the data in the correct format.

FIELD TYPES

Field Types allow you to define the type of data that the custom field will contain. These field types ensure that operators are capturing the data in the correct format. Below is a list of available field types:

Text	A simple text field up to 8000 Characters.
Notes	A multi-line text box with up to 8000 Characters.
Integer	A number ranging from -2,147,483,648 to 2,147,483,647
Decimal	A number with 15-16 decimal places
Currency	A monetary value
Date and Time	A combination of the following 2 field types
Date	A date selector From 01/01/0001 to 31/12/9999
Time	A time selector Hours, minutes, seconds, AM/PM
Image	A BMP, GIF, JPG, JPEG, ICO or PNG image
Check Box	Ticked or not ticked
Editable Drop Box	A drop down list of selectable items, you may enter custom text
Drop Down Box	A drop down list of selectable items
Email Address	An Email address field
Telephone Number	A Telephone number field (no spaces required)

DEFAULT VALUE

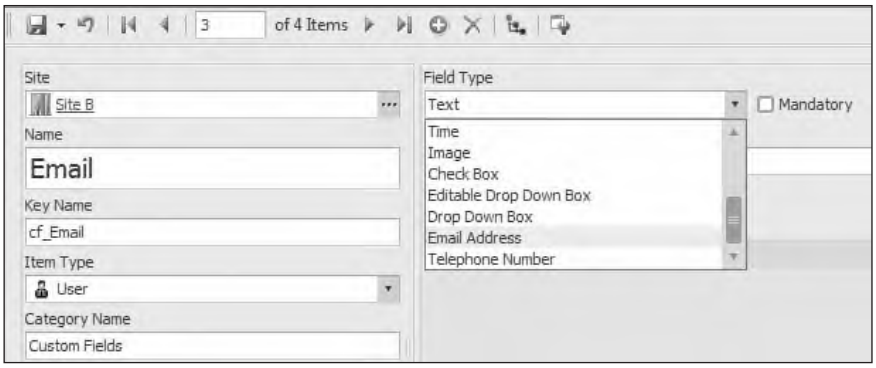
If you specify a Default value then this will be displayed in the field unless changed by the operator.

MANDATORY

If the Mandatory check box is enabled an operator will not be able to save the changes to an item without entering the custom field.

CUSTOM FIELD EXAMPLE

A commonly used custom field is a users email address. The **Email Address** field can be used to send the user emails containing their PIN number or alert messages.



Creating email custom field:

1. Name the custom field.
2. Select **Email Address** from the **Field Type** option.
3. If the field has to be entered by an operator flag the **Mandatory** field.

The **Email** custom field bellow will appear in the **User Editor** window

BUILT IN REPORTS

INTRODUCTION TO BUILT IN REPORTS

You can run basic user or door reports from the Integriti Software. These reports can identify what doors a user can access or which users have accessed a door in the last 24 hours.

RUNNING A USER BUILT IN REPORT

Select one or more users and right click to view the user options. The following user reports are available:

USER DOOR ACTIVITY REPORT

This report displays review events for each time the selected user or users accessed a door in the period specified. This includes door access events where the user is granted access or denied.

USER ACTIVITY REPORT

This report displays all the review events that relate to the selected user or users in the period specified. This includes door access events, keypad login and logout.

USER REFERENCE REPORT

This report displays the permissions assigned to the selected user or users.

RUNNING A DOOR BUILT IN REPORT

Select one or more doors and right-click to view the door options. The following user reports are available:

DOOR USER ACTIVITY REPORT

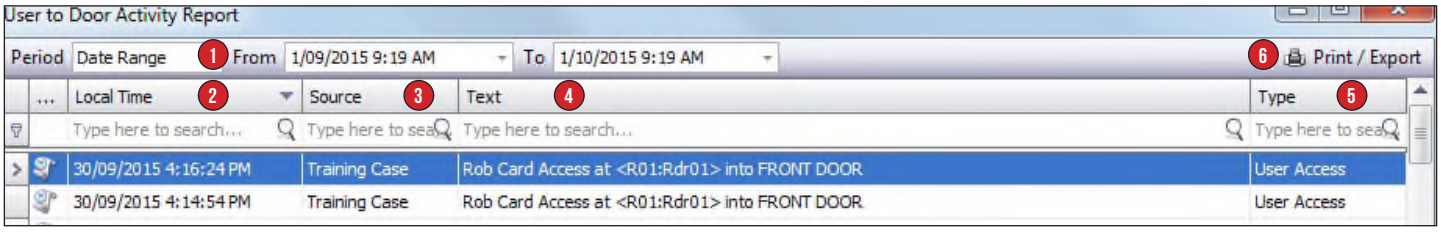
This report displays review events for each time a user accesses the selected door in the period specified. This includes door access events where the user is granted access or denied.

DOOR USER REFERENCE REPORT

The report displays the users with permission to access the selected door or doors.

BUILT IN REPORTS WINDOW

Once you select a report; the report window will open. Below is an example of the User-Door Activity Report:



1. The **Period** filter sets the range of dates and times that the report includes. You can select either a date range or number of days.
2. The **Local Time** column shows the date that the event occurred.
3. The **Source** column displays the controller that generated the review message.
4. The **Text** column displays the logged information for the event that occurred.
5. The **Type** column displays the category of the review event.
6. The **Print/Export** button will print or save the contents of the report to a PDF or CSV file.

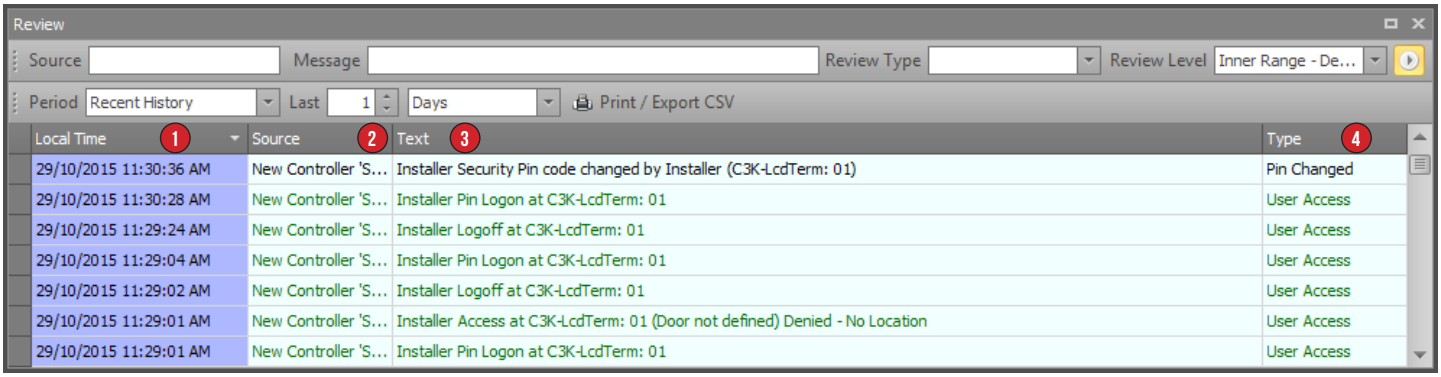
REVIEW

INTRODUCTION TO REVIEW

Review is a historical log of the events that occur in the Integriti System. These events can be created by the Integriti controllers, the Integriti application or even third party devices such as CCTV systems.

Review is commonly used to find historical evidence of an event, such as finding out which users accessed a particular door on a particular date. Review can also be used to generate advanced reports such as **Time on Site** reports for payroll.

The **Review** window below appears in System Designer and GateKeeper by default.



1. The **Local Time** column displays the date and time that the review event was generated.
2. The **Source** column displays the name of the device that generated the review event. Controller based events will display the name of the controller. Alternatively, there may be review events generated by the Integriti application which will have the source AppServer: IntegritiApplicationServer.
3. The **Text** column contains the review message.
4. The **Review Type** column displays the category of the review message. Every review message falls into a single category, this includes User Access, Card Info and Area Change etc.

REVIEW FILTERS

Located at the top of the **Review** window are a series of filter options that will assist you in locating review records of particular interest.

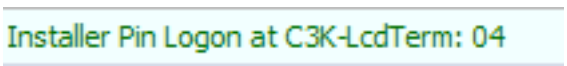
SOURCE

The **Source** text box is used to filter review based on the controller or application that created the event. This is commonly used on sites with many Integriti controllers to filter review to a single panel.

MESSAGE

The **Message** text box is a quick way to filter review if you know part of the message you are searching for. This method of searching review can often return records that may match your entry but aren't exactly what you're looking for.

For more accurate search results, you will need to use a wild-card. A wild-card is a placeholder symbol that represents one or more characters in the message. In Integriti the wild-card symbol is the % character.
Below is an example of how a wild-card is used:



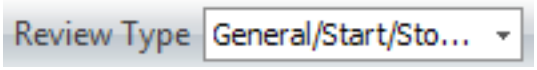
Entering the text **Installer** or **Inst%** will show this review message.

Entering the text **Installer Logon** will not show this review message as the text does not contain the word **PIN.**

A wild-card can be used to replace words between **Installer** and **Logon**; entering **Installer%Logon** will show this review message.

REVIEW TYPE FILTERING

The **Review Type** filter allows you to display review records based on one or more **Review Type** categories. This can be used to display all records of a particular type, for example **User Access** events.



REVIEW LEVEL FILTERING

The **Review Level** filter allows you to filter review record to different levels. The lowest review level is Everyone, this level will show the least number of review events. The highest review level is Inner Range - Debug, this level will display every generated review message.

PLAY / PAUSE REVIEW BUTTON

On sites that generate a large amount of review messages it is difficult to read review messages before they are replaced by new events. The **Play / Pause** button will start and stop new review messages from appearing in the **Review** window. When in the play mode the button will appear highlighted.

PERIOD FILTERING

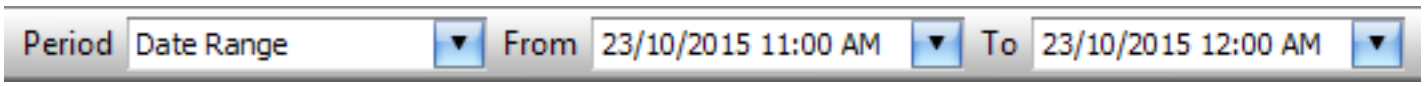
The **Period** is a time-based filter that filters the review messages based on the date and time setting specified.

The three period filters are:

Live: This option will clear all review events from the review window and only display new events as they are created. If you wish to clear the review window a second time, click the **Refresh Live** button.

Recent History: This filter allows you search historic review based on a last number of weeks, days, hours or minutes. Below is an example of a recent history filter set to one day:

Date Range: This filter allows you to search historic review based on events occurring between to specified dates and times. Below is an example of a **Date Range** filter containing a one hour period of time on a particular day:

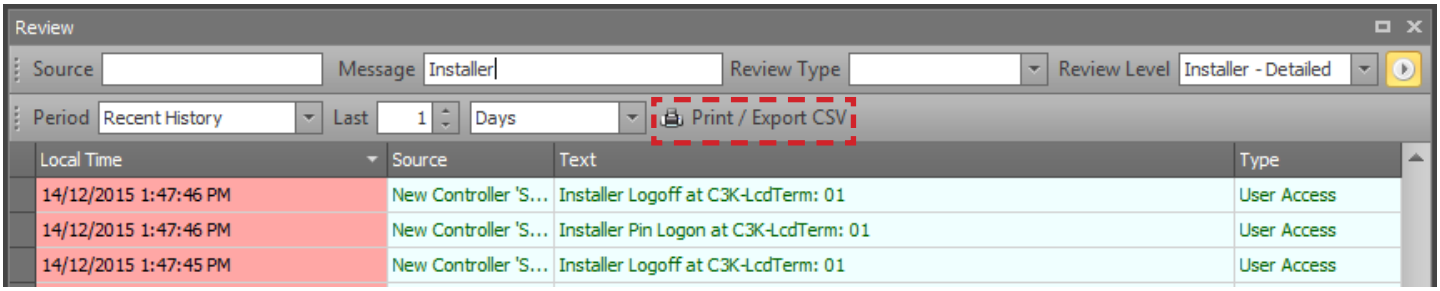


RIGHT CLICK OPTIONS

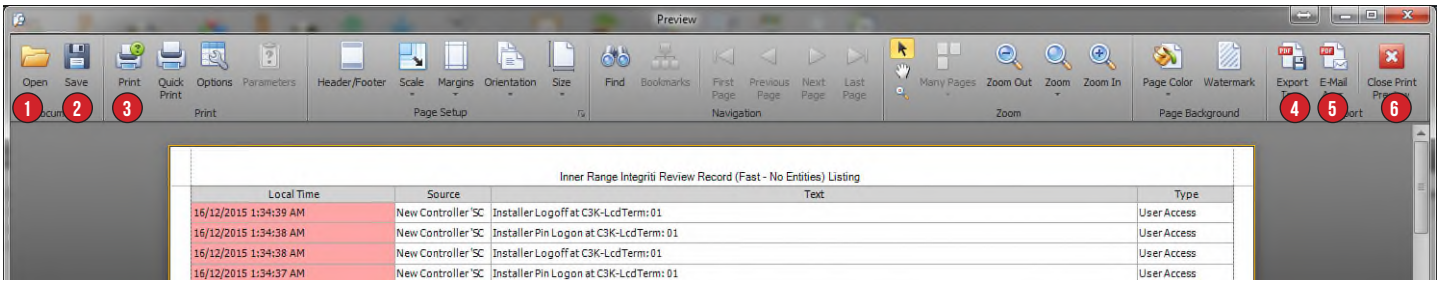
Right-clicking on a review message will open a list of all the system entities that were involved in generating this review message. Each of the items listed is a hyper-link to the editing screen for that item, this allows you to easily jump to that item to edit it.

EXPORTING REVIEW

In some cases you may need to provide a copy of the review to someone else in a particular format. Once you have filtered the review records review you can export these review records in the format of your choice. To export review click the **Print Export** button, this will open the **Preview** window.



The **Preview** window contains a number of options, the most commonly used ones are:



1. The **Open** command is used to open and view a preview that was saved in the native format using the **Save** command.
2. The **Save** command is used to save the contents of the preview window in the native .prnx file. This file can be opened at a later date using the Open command.
3. The **Print** command will open the **Windows Print** window allowing you to select a printer and set the appropriate printing options.
4. The **Export To** command allows you to save the contents of the **Preview** window in the file format of your choice. Commonly used formats are PDF, XLS or CSV. After selecting a format the **Format Options** window will open, these setting are best left as default.
5. The **Email As** command works the same as the **Export To** command, however, once the file is saved it will be attach to a blank email in your default mail client.
6. The **Close Print Preview** button will exit the **Preview** window without saving the contents.

integriti
INTEGRATED SOLUTIONS

SYSTEM CONFIGURATION HANDBOOK

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Certified System
Quality
ISO 9001

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

UPDATES AND ADDITIONAL INFORMATION:

Check the Website regularly for:

- Additional applications and tables not included in this manual.
- Updates and/or changes to existing documents.
- New documents added to this manual.

Advanced Tech Support:

- http://www.onlinetraining.innerrange.com/
  (Restricted downloads)
- http://www.onlinetraining.innerrange.com/login/signup.php
  (Restricted account creation)
- http://www.innerrange.com.au/support.php
  (Support contacts)

Home Page:

- http://www.innerrange.com

Please send or fax any comments regarding this manual to:

- "Publications" at the Head Office address. (See front cover)
  – Or –
- e-mail to: Publications@innerrange.com

Disclaimer:

1. The manufacturer and/or its agents take no responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from the correct or incorrect use of the Inner Range system and its peripherals.
2. Whilst every effort has been made to ensure the accuracy of this manual, Inner Range Pty Ltd assumes no responsibility or liability for any errors or omissions. Due to ongoing development the contents of this manual are subject to change without notice.

System Configuration Handbook

Table of Contents

1. Hardware and Software Prerequisites

The Integriti suite consists of Server and Client software. Integriti software installation files contain all of the client and server software in one package for easy deployment. The entire software suite can be installed on a single machine for typical installations or as one server and *n* clients.

For detailed information, please refer to the document titled 'Hardware and Software Prerequisites'.

2 Installing the Software

Before installing Integriti, please make sure your computer hardware specifications meet the minimum hardware requirements as explained in the document titled 'Hardware and Software Prerequisites'.

Integriti should only be installed by someone logged on to the machine locally as an administrative user.

2.1 Installation packages available

There are two installation packages available – the full installer and the web installer.

The full installer is the larger of the two and contains all of the files and resources required to install the Integriti software management suite on your computer without the use of internet connectivity.

The web installer is much smaller and quicker to download, but requires an internet connection for the duration of the installation process and may take a little longer to install depending on the dependencies required for your computer.

The web installer is a good option when upgrading an existing Integriti installation.

To begin the Integriti installation, double click the Integriti setup executable:

 Integriti_Pro_Full_x*xx*_setup_(*xxxxx*).exe – or –  Integriti_Pro_web_setup_(*xxxxx*).exe

Make sure you have the latest version of Integriti before installing. Visit http://www.onlinetraining.innerrange.com/login/index.php *(login required).*

2.2 Installation options

After accepting the license agreement and reviewing the release notes you will have the following options:

- Installation path
- Components to install
  - Server & Client
  - Client Only
  - Stand Alone Controller Server
- Where should setup create the database?
  - Upgrade my existing database
  - In a new SQL Express Instance

- I will specify an existing SQL Instance (advanced)

2.2.1 Registration

On first use of the Integriti management software, you will be presented with the software activation wizard. You will be required to enter a valid product key before continuing with the registration process.

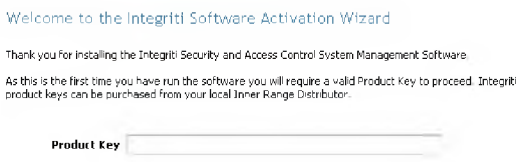


Figure 1

Upon entering your license key you will have the option of selecting from one of three registration methods:

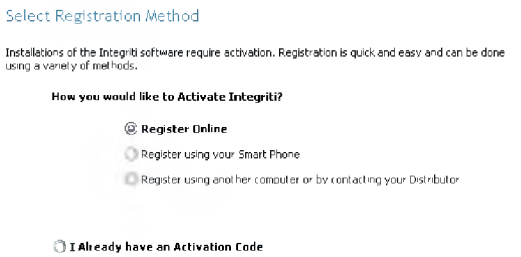


Figure 2

2.2.1.1 Register online (Default, recommended option).

If the machine has access to the internet, you can register online. Once you have provided some basic site details, the software will automatically register itself.

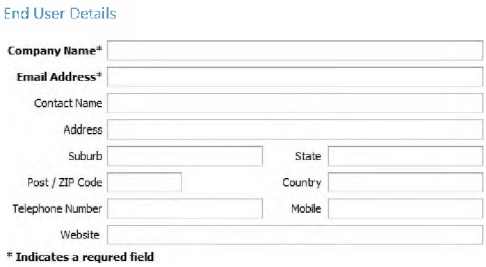


Figure 3

2.2.1.2 Register using your smart phone.

If the machine does not have access to the internet, you have the option to register the software using your mobile device.

Using your mobile device, take a photo of the QR code shown on the screen (not the one in this document). The QR code will translate to a URL on your mobile device. This web page will request the same information as if you were registering online.

Figure 4

When the registration page has been completed, you will be given a unique activation code. Enter this code in to register your copy of the software using the method below.

2.2.1.3 Register using another computer or by contacting your distributer.

If you are unable to register the software due to security or connectivity issues, this option allows you to go through the process by either contacting your distributor or by using another computer that has internet access.

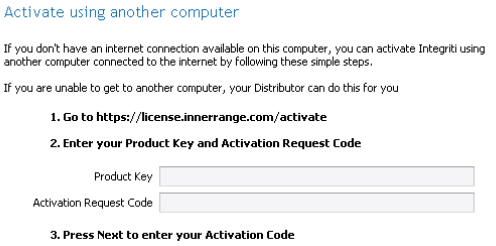


Figure 5

2.2.1.4 I Already have an Activation Code.

If you have already been through the registration process and have been given your activation code, you can select the 'I Already have an Activation Code' option to register your copy of the software.

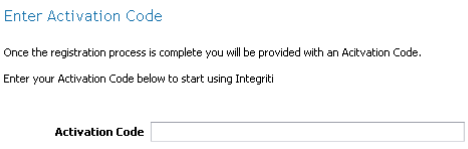


Figure 6

3 Login

Operators are presented with a login dialog when they run Integriti. To log in, simply enter your operator name and operator password then click the Login button.

Operator credentials are defined within the Integriti management software.

The default Integriti operator login is a user name of 'installer' with the default password of 'installer'. It is strongly recommended that you remove this operator or change the password as soon as possible.

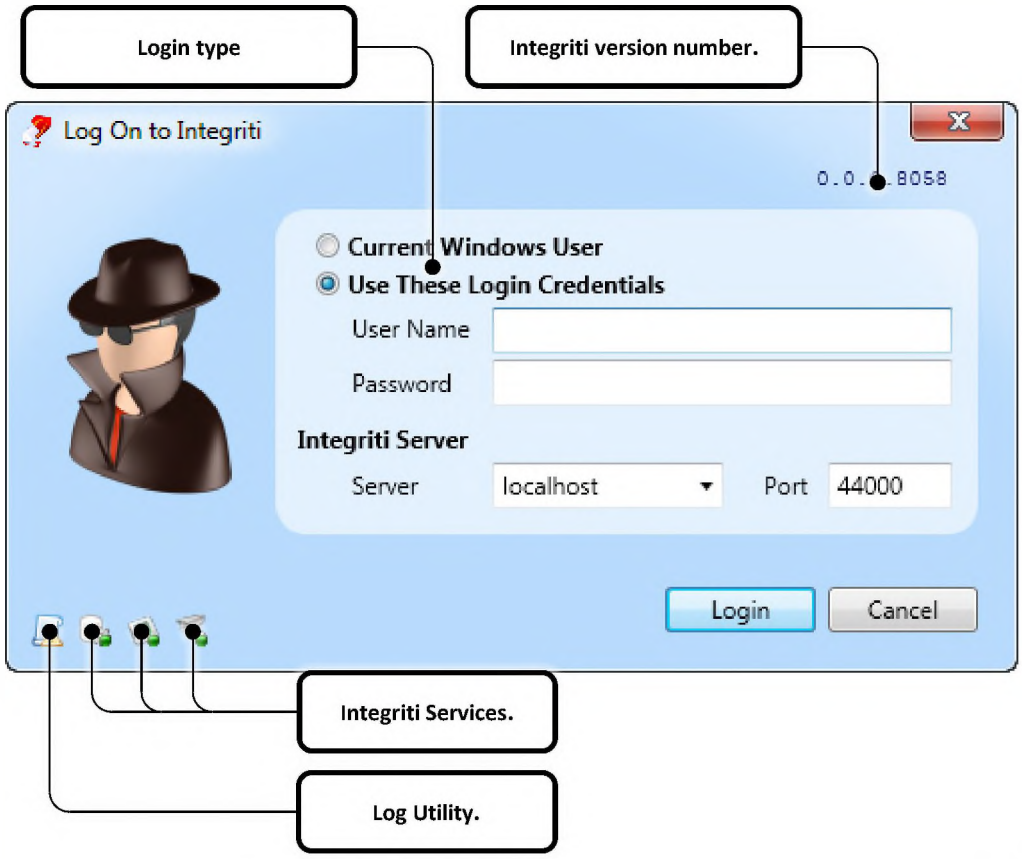


Figure 7

Make sure the Integriti services are running before you attempt to log in. *See Integriti Services on page 13.*

3.1 Integriti Services

The Integriti services should be running before you log in to Integriti. If they are not, right-click the service icon and click Start.

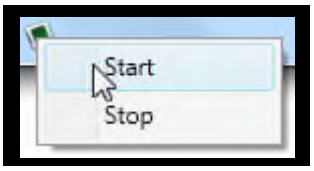


Figure 8

The service icon should appear solid (with a green indicator), indicating that the service is running:

	Stopped	Stopping	Starting	Running
Integriti controller server				
Integriti application server				
Integriti Integration server				

Table 1

3.2 Log Utility

The log utility is used for diagnostic / fault finding purposes. You can access the log utility by clicking the icon either in the login dialog or in the Integriti title bar. For more information on the log utility, see the section titled 'Integriti log viewer' towards the end of this document.

4 User Interface

Please read the document titled “Interface Elements for Integriti” for more information on how to make good use of the user interface.

4.1 The Review Panel

The review panel is located at the bottom left of the Integriti window by default. At a glance, operators can see events as they occur and action them if required.

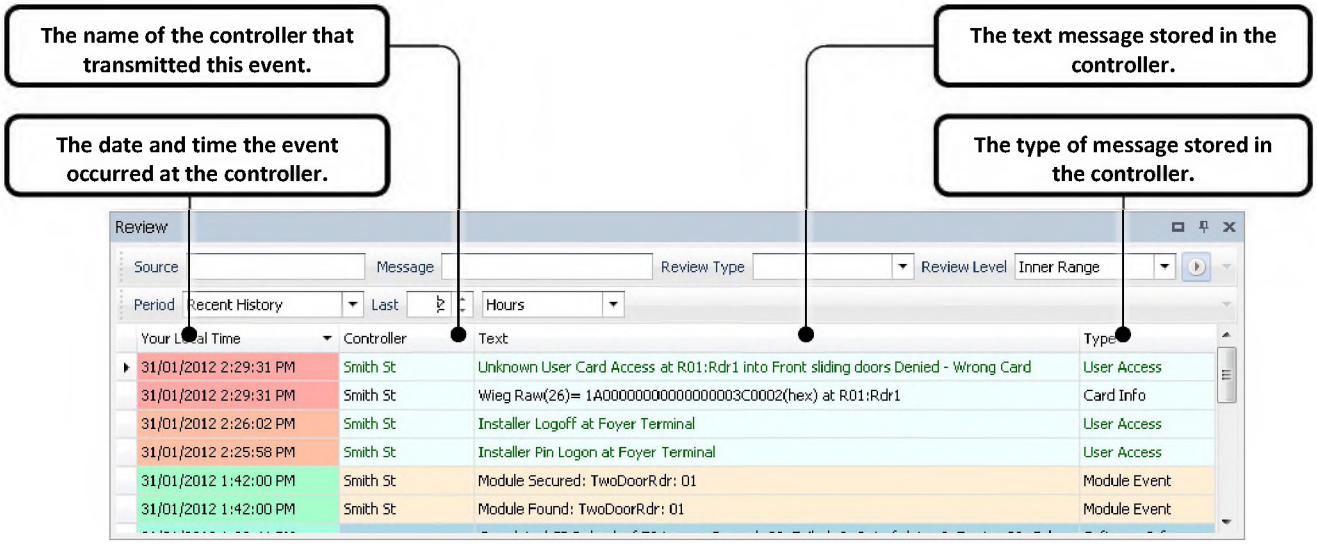


Figure 9

The review panel has a 'heat signature' feature which allows the operator to see the age of the displayed review events. The background colour of the review events in the first column 'Your Local Time' represents the age.

Your Local Time	Controller	Text
21/11/2011 8:33:50 AM		Controller 'New Controller (PT000031)' disconnect
21/11/2011 8:18:28 AM	New Controller (...	Module UnSecured: Front Entry & Car Park
21/11/2011 8:18:28 AM	New Controller (...	Module Found: Front Entry & Car Park
21/11/2011 8:03:16 AM	New Controller (...	System Date/Time set to Nov 21 2011 08:02:50 U
21/11/2011 8:03:16 AM	New Controller (...	Timezone set to UTC+11:00 by Integriti 01 (Integ
21/11/2011 8:03:16 AM	New Controller (...	Comms Task 02 (Integriti) - Integriti Connected du

Figure 10

The single greatest advantage of this feature is the ability to notice how review events are grouped without reading individual timestamps. ***Figure 10*** is a simple example of this feature.

Your Local Time	Controller	Text
21/11/2011 9:58:06 AM	New Controller (...	System Date/Time set to Nov 21 2011 09:58:36 U
21/11/2011 9:58:06 AM	New Controller (...	Timezone set to UTC+11:00 by Integriti 01 (Integ
21/11/2011 9:58:05 AM	New Controller (...	Comms Task 02 (Integriti) - Integriti Connected du
21/11/2011 9:00:00 AM	New Controller (...	Working Hours became Valid (TP00001)
21/11/2011 9:58:35 AM		Controller 'New Controller (PT000031)' connected

Figure 11

In the example above an older event has been placed in between newer events. This scenario can occur when communications to one or many controllers has been (re-)established. Review filtering and organisation occurs at the time the filter is applied.

4.2 The Actions Panel

The actions panel will display various action types as they occur and their status. For instance, if you were to upgrade the firmware of a controller, a progress bar will appear in the actions panel indicating the firmware upgrade progress.

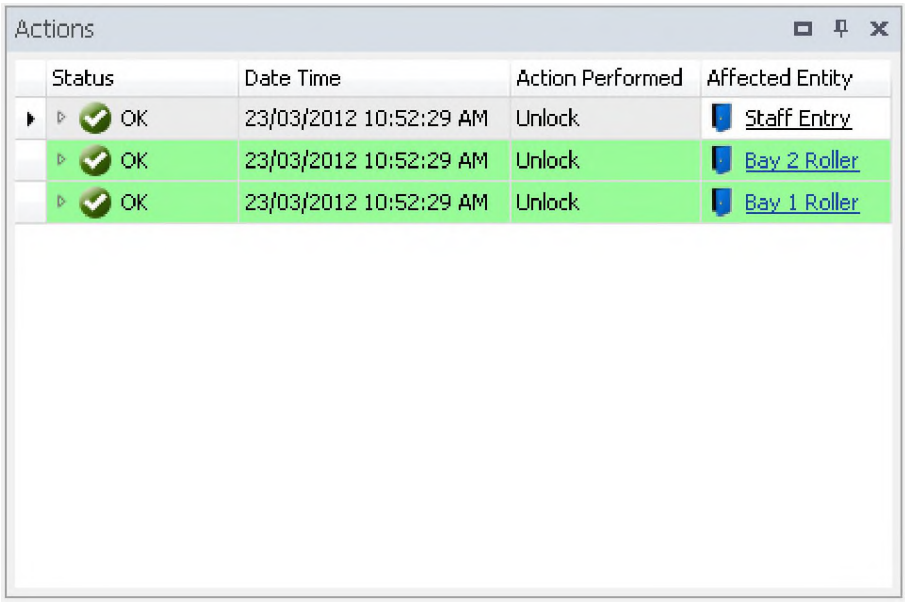


Figure 12

4.3 Editor windows

Most editor windows will look like the following example…

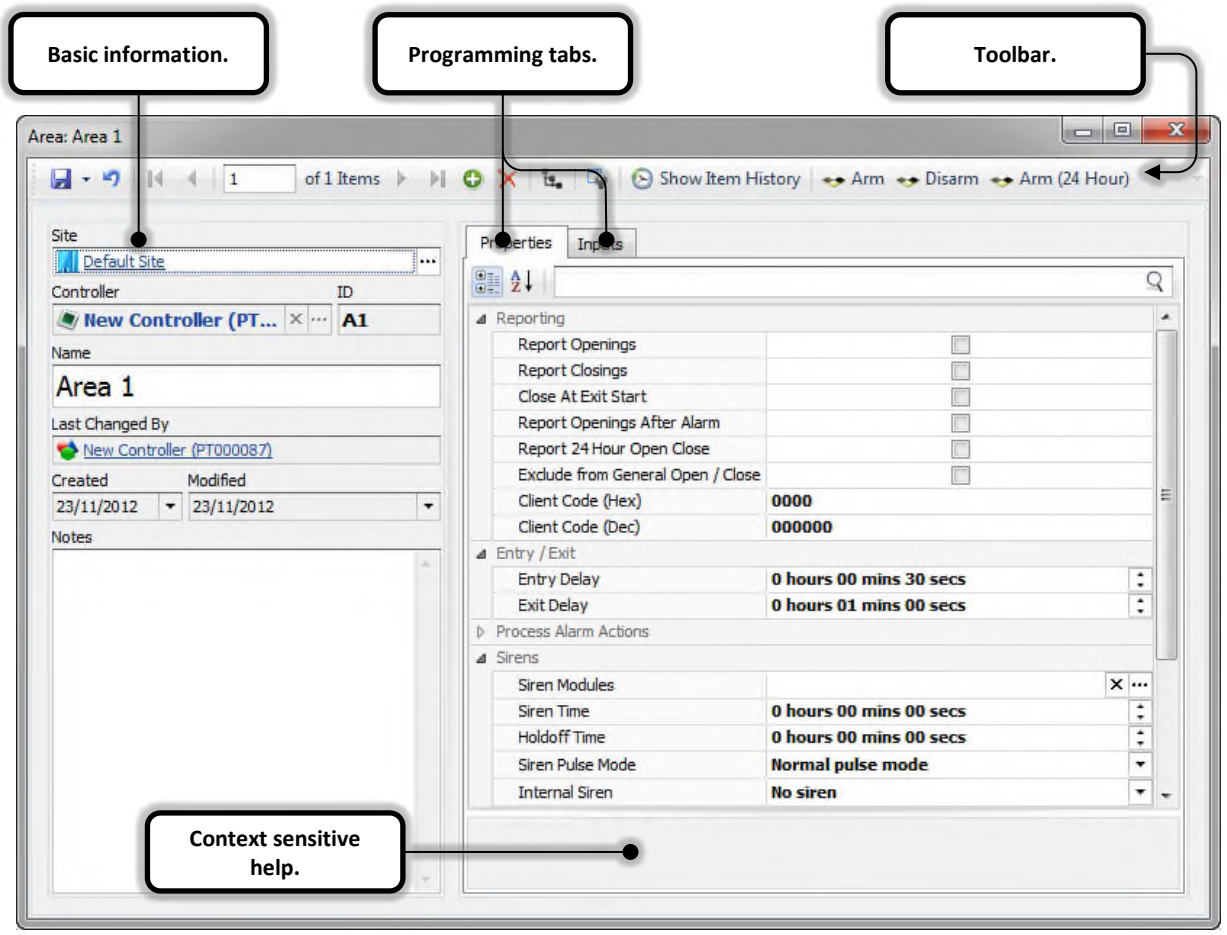


Figure 13

The left side of the editor window contains items relevant to all programmable entities within the Integriti management software.

The right side of the editor window contains a number of programming tabs (usually two). The first tab (e.g. 'Properties') will contain all of the required programmable items relevant to the entity. Other tabs will usually contain advanced options or lists to associate other entities with the currently programmed item (e.g. inputs to an area).

Context sensitive help will appear at the bottom right hand corner of the editor window for items selected under the programming tabs.

Depending on the editor window position and layout, not all of the information contained in the context sensitive help box may be visible. You can adjust the size of the context sensitive help box by clicking and dragging the top section of the box (*Figure 14*).

Figure 14

4.3.1 Toolbar

The toolbar contains the following buttons:

	Save	Save the currently displayed record settings.
	Undo	Undo the last change since the window was opened.
	First Record	Go to the first record in the series.
	Previous Record	Go back one record.
	Next Record	Go forward one record.
	Last Record	Go to the last record in the series.
	New Record	Create a new record.
	Delete Record	Delete the currently displayed record.
	Property page view	Change the view to the default property page layout.
	Show Cross References	Open a dialog with a tree view that displays the references to and references from this entity.
	Show Synchronisation Warnings	Displays the synchronisation warning panel.
	Audit	Open a new window displaying the entire history of changes made to this record.
	Customize Layout	Change the layout of the editor window.

Table 2

Other buttons specific to the current entity may be visible on the toolbar.

You can toggle an automatic save feature by clicking on the save button dropdown followed by 'Auto Save'. The Save icon will change to a green icon when the automatic save feature is active.

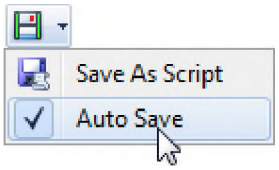


Figure 15

4.3.2 Hyperlinks

Integriti has the added convenience of hyperlinks. Hyperlinks are blue text labels that allow you quickly navigate between related items, without using the ribbon and panels to manually locate them. To follow a hyperlink, simply click on it. Clicking on a hyperlink will open a window with the properties for the clicked item.

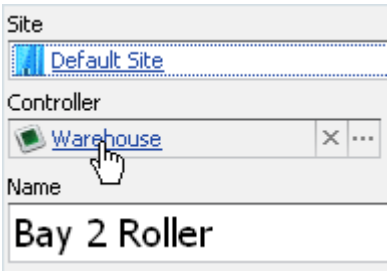


Figure 16

5 Setting up an intruder system

The following will step you through what is required to commission a basic intrusion system.

It is assumed that the operator is logged in to the System Designer. An Integriti controller with the necessary modules attached should already be online, communicating with the server.

The instructions provided are based on the default layout.

5.1 Introduction and programming summary

Areas

Security management operation is designed around the concept of Areas. Areas are groups of Inputs such as movement detectors that can be collectively enabled when the Area is turned on or disabled when the Area is turned off.

The system determines which Areas each User can control during which times and with which options.

Inputs

An Area can contain one or more detection devices or other devices (wired to Zone Inputs) and/or one or more System Inputs. If a Zone detects an intruder or a System Input is activated (e.g. Low Battery, Cabinet Tamper, etc.) it will only be actioned if the Area that the Input is in, is turned on. The action which is taken when an Input is activated in a particular Area (e.g. activate Siren/s, activate Auxiliaries, report to Central Station, etc.) is determined by how that Input is programmed in that particular Area.

An Input can be programmed into more than one Area. The Alarm action taken by an Input when in the Alarm condition is dependent on how that Input is programmed in each Area, and on the Area/s being turned on.

This allows a particular Input alarm to be actioned in different ways depending on what Areas it is assigned to, and which of those Areas are on.

Process Groups

Defining how an Input will be actioned in each Area is primarily done by allocating an appropriate Process Group, to every Input in each Area that it is assigned to. Process Group programming includes defining the Input states (Seal/Alarm/Tamper/Isolate/...) that will be recognised, Entry/Exit delay processing options, Reporting & message options, and Auxiliary and Siren control options.

Programming summary

Inputs are assigned to areas with a process group. Input programming records cover the physical attributes of the input on the module. Process group programming records contain the rules that govern how the input will behave within the assigned area.

Recommended programming sequence:

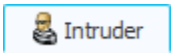
- Configure Inputs
- Create and populate Areas
  - Set up Area reporting
  - Assign Sirens to Areas
  - Assign Inputs to Areas and Assign Process Groups
- Create Telephone Number records
- Configure a Communications Task for monitoring
  - Assign Telephone Numbers to a Communications Task
- Create an Area List
- Create a Menu Group
  - Give arming permissions to a Menu Group
- Create a Permission Group
  - Adding Areas and Area Lists
  - Adding Menu Groups
- Create Users
- Assigning Permissions to Users
  - User PIN codes

5.2 Inputs & input behaviour

On some Modules, a number of the Zone Inputs have pre-defined functions. These can only be used as general purpose Zone Inputs if the operation relating to the pre-defined function is not being implemented.

5.3 Setup inputs

All inputs should be named according to their application and some additional options may need setting.

1. Click on the 

tab followed by 

.
2. Double-click an input to program. The Editor Window for the input should appear.
3. Change the name of the input to something more appropriate.
   - e.g. "`Front Door Reed Switch`"
4. On the right-hand side of the window, expand-out Options.

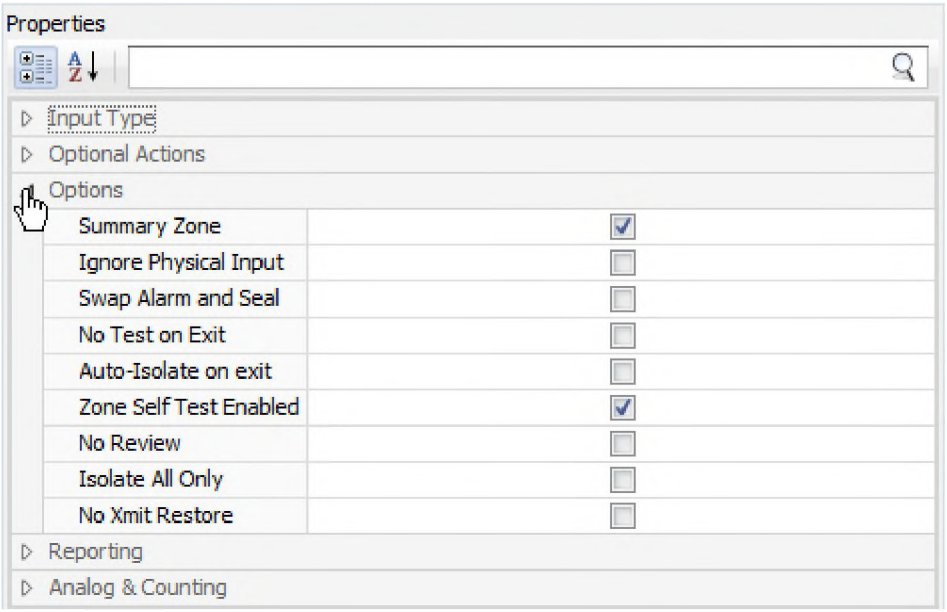


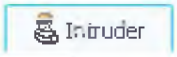
Figure 17

5. If there is a possibility that the input will be in an unsealed state at the time of arming, then click "No test on exit".
6. If the input is physically wired to a normally open device then you might need to tick the "Swap Alarm and Seal" option.
7. Save and close the editor window for the Input.
8. Repeat steps **2** - **6** for the other inputs you are using.

The input item editor, like all item editor windows in Integriti contains a context sensitive help box at the lower right which can help remind users of the effect of each option.

5.4 Set up areas

Once all of the Inputs have been programmed, you can configure the Areas.

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new area should appear.
3. Give the Area a name.

Under the 

tab…

4. Expand-out reporting.
   a. If openings for the area should be reported, click the "Report Openings" option.
   b. If closings for the area should be reported, click the "Report Closings" option.
   c. Enter the Client Code in "Client Code" field provided by the monitoring centre.
5. Expand-out Entry / Exit.

a. If an entry delay is required, fill in the “Entry Delay” option.
b. If an exit delay is required, fill in the “Exit Delay” option.

6. Expand-out Sirens

a. To make use of the sirens, click on the ··· to the right of Siren Modules.

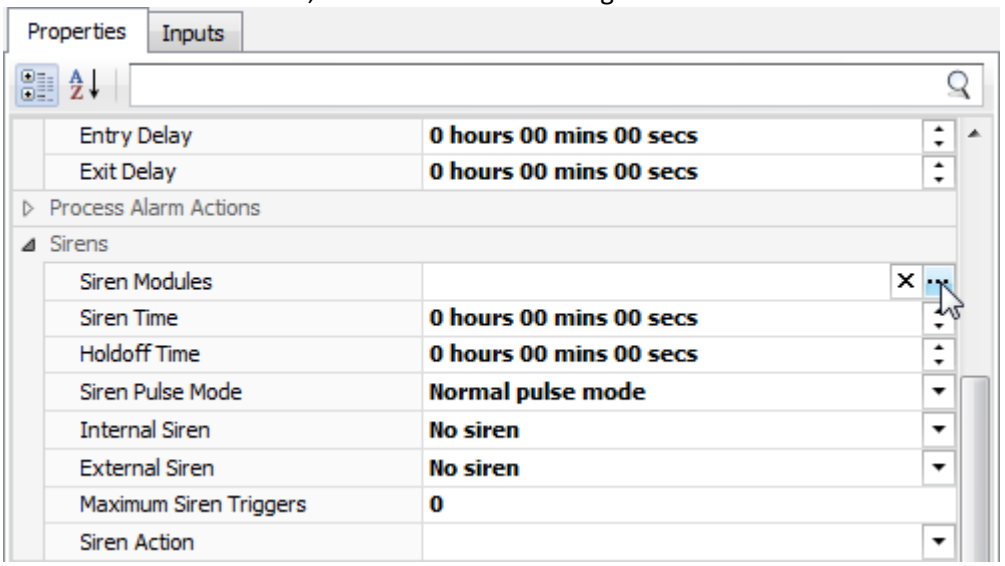


Figure 18

b. A new window “Siren Modules” should appear. Click on the Add button.
c. From the window that appears, select the required siren module(s) and click OK.
d. Verify that all of the required siren modules have been selected and click OK.
e. Change the siren time option as required. (Note local laws etc…)
f. Click on the “Internal Siren” drop-down and select the mode of operation for the siren modules internal siren.
g. Click on the “External Siren” drop-down and select the mode of operation for the siren modules external siren.
h. If required, adjust the “Maximum Siren Triggers” that can occur before a siren is disabled.

Under the Inputs tab…

7. Click on Add to add inputs to the area.

8. From the window that appears, select the input(s) you want to add to the area and click OK. If you have a large list of available inputs, you may wish to filter the list by typing into the filter row at the top of the Input selection window. The Controller, ID, and Name fields are particularly useful here.
Pick a Process Group that defines how each input will operate. See the section titled ‘Default entities’ for a summary of the process groups and their behaviour.

9. Change the Process Group of an input (if required) by selecting the input and clicking Change Process Group.

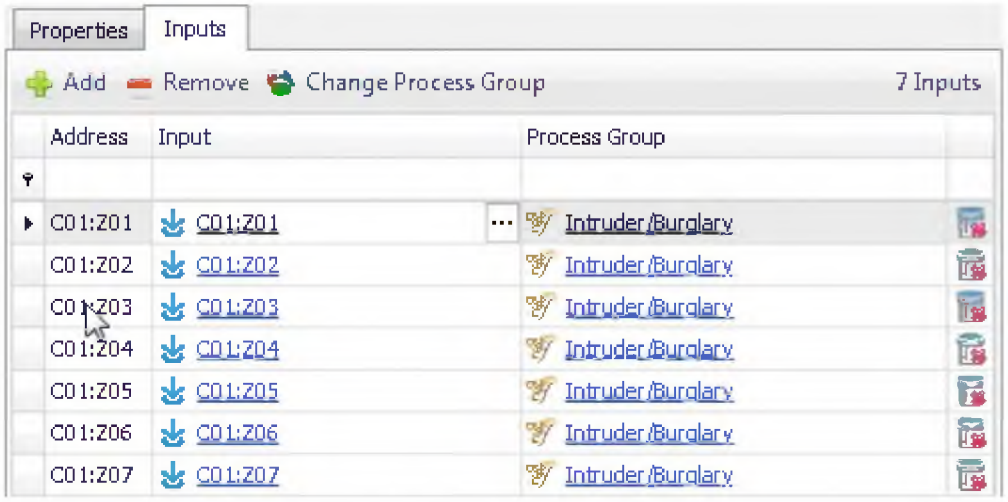


Figure 19

Figure 20

10. Save and close the editor window for the area.

5.5 Set up a System Area

The Integriti security controller has various system input types which should be placed in to an area for local alarms and reporting purposes. Alarms such as AC failure, Low battery, LAN communications failure and cabinet tampers are some of the types of system inputs that should be included in a system area.

Integriti has a feature in area programming that allows you to automatically populate a designated system area with the inputs you specify. To do this you will need to create a Systems area and using the 'Assign System Inputs' feature, enter the systems input types for all of the required Integriti/Concept 4000 LAN modules.

This systems area can be any area you choose, and the below step by step guide shows you how to create this Systems area.

Creating a new System Area…

1. Click on the Intruder tab followed by Areas.
2. Click Add New. The Editor Window for a new area should appear.
3. Give the area a name such as 'System Area'.
4. Give the Area a new name and enter any necessary notes in the Notes field.
5. Establish what Systems inputs will be required for available LAN modules. Refer to the 'System Input Process Group Defaults' in the appendix for more information on what process group is appropriate for each individual system input.
6. Click on the Inputs tab.
7. Click on Assign System Inputs. The following window should appear…

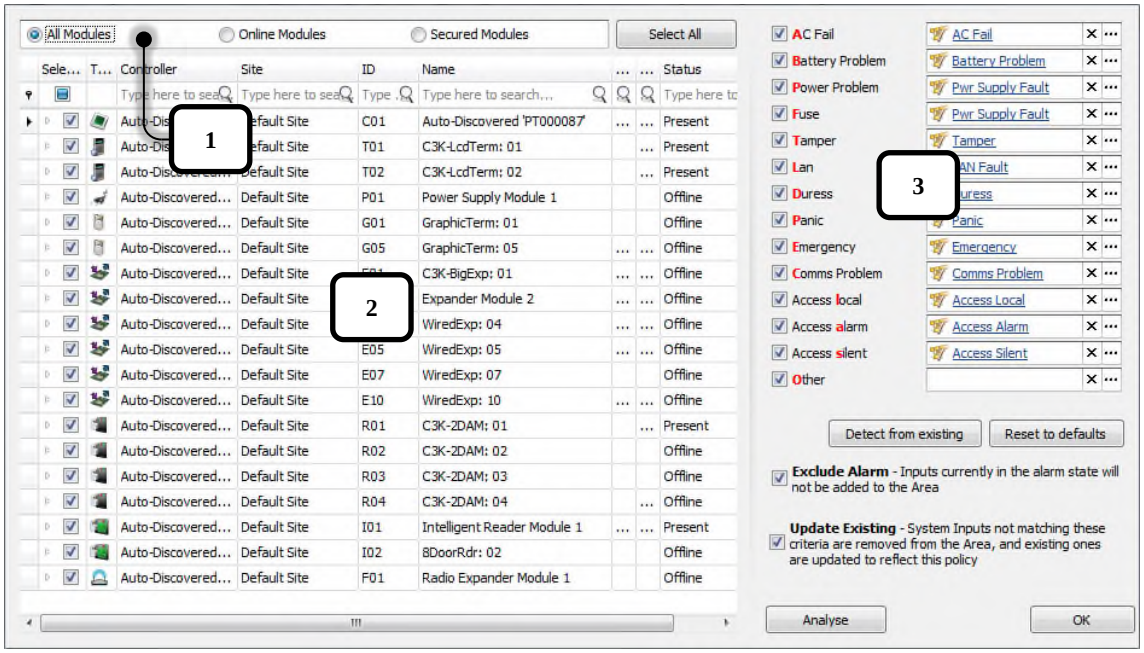
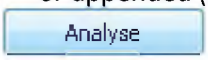
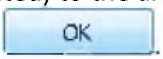


Figure 21

8. Select what module category you will be assigning inputs from (1).
9. Select (or unselect) modules as required in the list below (2).
10. Select the Process Groups based the various input types you want to assign to this area (3). Usually intrusion and access system inputs are divided in to two separate system areas for easier system wide control and monitoring.
    - Detect from existing is used in cases where system inputs are being updated or appended to an area with pre-existing inputs. If the Process Group selected for a particular type of input was something other than factory default, Integriti will use that Process Group instead (e.g. The 'Duress' Process Group was used for 'Panic' Inputs).
    - Clicking Reset to defaults will change the Process Groups for the various input types to factory default.

- Checking the Exclude Alarm option will exclude any inputs that are in alarm at the time the button was pressed from the area.
- If Update Existing is checked, inputs assigned to this area will be updated or appended (if they do not already exist).

11. Click 

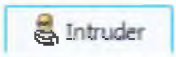
to display a total of all of the inputs that will be added (or updated) to the area. Totals for each Input type will also appear.
12. Click 

.
13. Add any additional area processing you may require, such as reporting options for open and close etc...
14. Ensure access to the System Area is restricted to the integrator and/or on site technician.
15. Save and close the editor window for the system area.

5.6 Configure PSTN reporting

To setup reporting via the telephone dialler you will need to configure Telephone Number(s) and a Communications Task.

Configuring the Telephone Number...

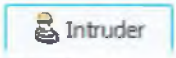
1. Click on the 

tab followed by 

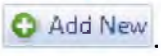
.
2. Click 

. The Editor Window for a new phone number should appear.
3. Give the telephone a name.
4. Enter the phone number on the right-hand side of the phone number editor window.
5. Save and close the editor window for the telephone number.
6. Repeat steps **1** - **5** if additional telephone numbers are required.

Configuring the Communications Task...

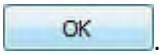
1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new communications task should appear.
3. Give the communications task a name.
4. On the right-hand side under Comms Task Setup, click on the "Type" dropdown and select "Dialler".
5. On the right-hand side under Dialler Programming.
6. Expand-out Reporting.
   a. Change the "Format" to "Contact ID".

Contact ID is common however; IRFast is preferred when the Central Station supports it as more information is available to aid in achieving an appropriate response. SIA, 4+2 and other less common formats are also available if desired.

b. Enter the Client Code in "Client Code" field provided by the monitoring centre.
c. Click on the  to the right of the Telephone number fields to open the Telephone number selection window.
d. Select the Telephone number from the list and click  .
e. Repeat for the second phone number if required.

7. Expand-out Contact ID.
a. The "Standard" map is the default used for Contact ID. If necessary, change the format here.

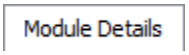
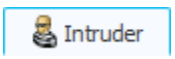
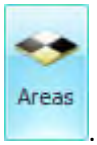
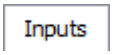
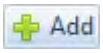
8. Save and close the editor window for the Communications Task.

5.7 Configuring dialler test reports

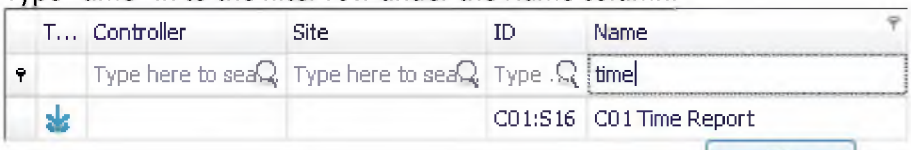
Monitoring centres usually ask for a routine dialler test to be configured on the controller to test the integrity of the communications path and to ensure the controller is still online and functional.

To configure the Integriti controller for a dialler test report you will need to change controller settings, program an area and assign the Time Report input to the area.

Configuring the Time Report…

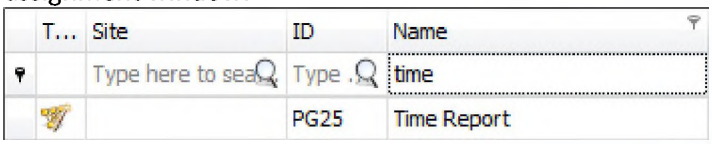
1. Click on the  tab followed by  .
2. Double-click the controller. The Editor Window for the controller should appear.
3. Click on the  tab.
4. Expand-out Time Report.
5. Enter the hour of the day that the controller should send a dialler test report to the monitoring centre.
6. Tick the day(s) of the week that the controller should send dialler test reports to the monitoring centre.
7. Tick Holidays to allow dialler test reports on holidays.
8. Save and close the editor window for the controller.
9. Click on the  tab followed by  .
10. Click  . The Editor Window for a new Area should appear.
11. Give the Area a new name and enter any necessary notes in the Notes field.
12. Click on the  tab.
13. Click the  to open the Input selection window.

14. Type “time” in to the filter row under the Name column.



15. Select the Time Report system input from the list and click OK.

16. Type “time” in to the filter row under the Name column of the process group assignment window.



17. Select the Time Report process group from the list and click OK.

18. Save and close the editor window for the area.

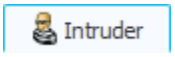
5.8 User security permissions

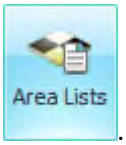
5.8.1 Area Lists

Area lists provide convenience and functionality. Example usage of area lists:

- Assigning the same areas to a number of users.
- Assigning many areas (more than 8) to users.
- Controlling a number of areas using a named action.

Creating Area Lists…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new area list should appear.
3. Give the Area List a name.

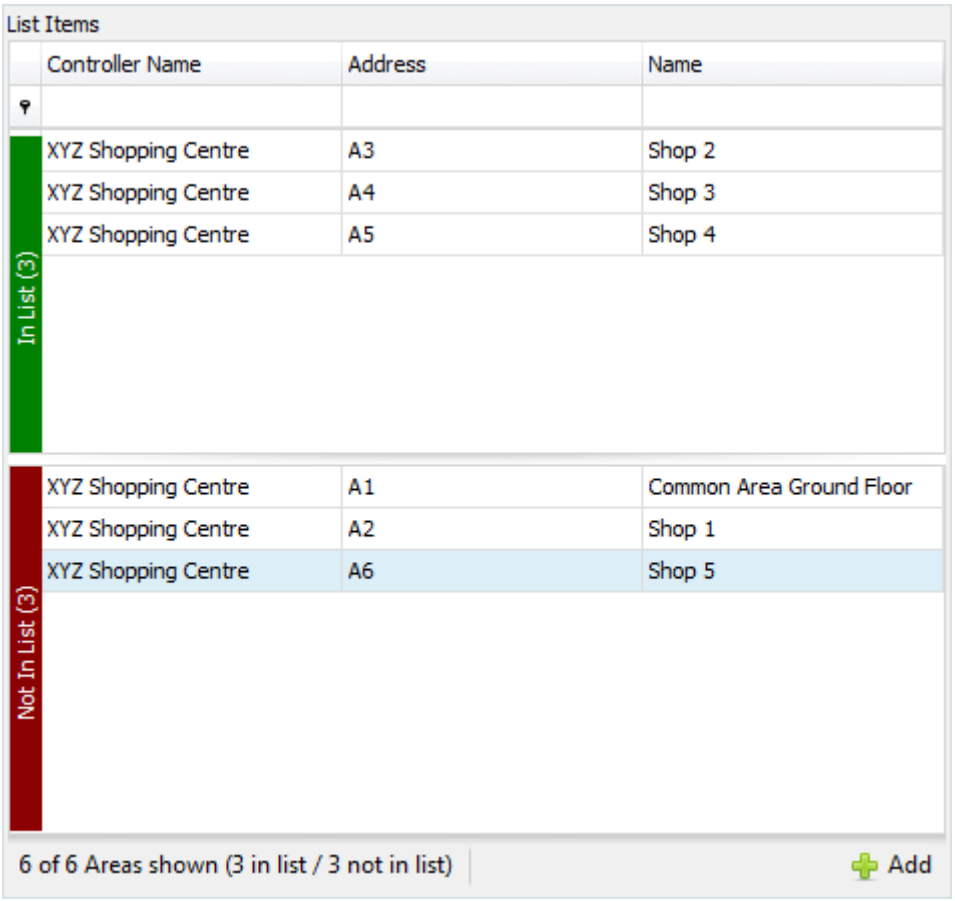


Figure 22

4. Items in the top section of the window are in the area list. Items in the bottom section are not. Double click items to move them from one section to the other.
5. Save and close the editor window for the Area List.

5.8.2 Menu Groups

Menu Groups are permission sets used to grant or deny user's terminal access to the Integriti controller.

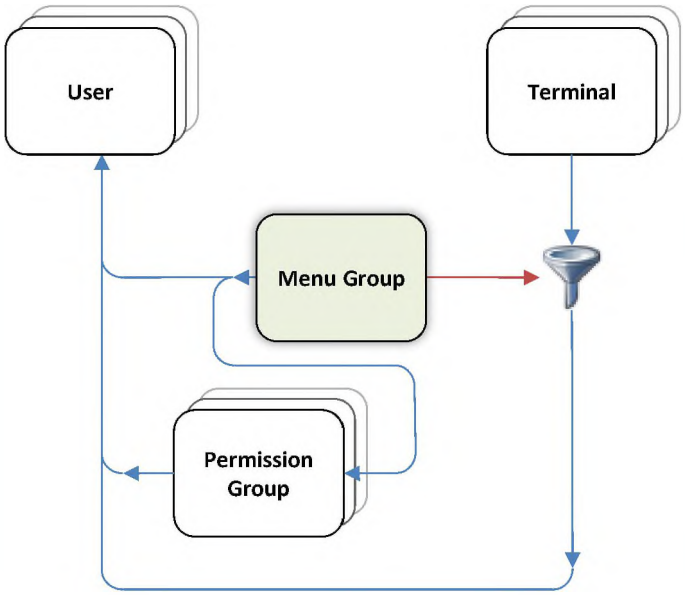
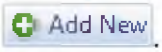


Figure 23

Menu groups can be assigned to compound entities, permission groups and users.

Menu Groups...

1. Click on the  tab followed by  .
2. Click  . The Editor Window for a new menu group should appear.
3. Give the Permission Group a name.
4. On the right-hand side under Properties.
5. Expand-out Main Menu Items.
   a. Tick the "Area" option.
6. Save and close the editor window for the Menu Group.

5.8.3 Permission Groups

A permission group can contain a list of areas, area lists, doors, door lists, menu groups and other permission groups from all of the accessible controllers within Integriti.

Instead of individually assigning the same individual permissions to every user, you can assign these permissions to a permission group. The permission group is then assigned to

users. Changing the permissions for all of the users with the same permission group is simple as the only change required is in the permission group.

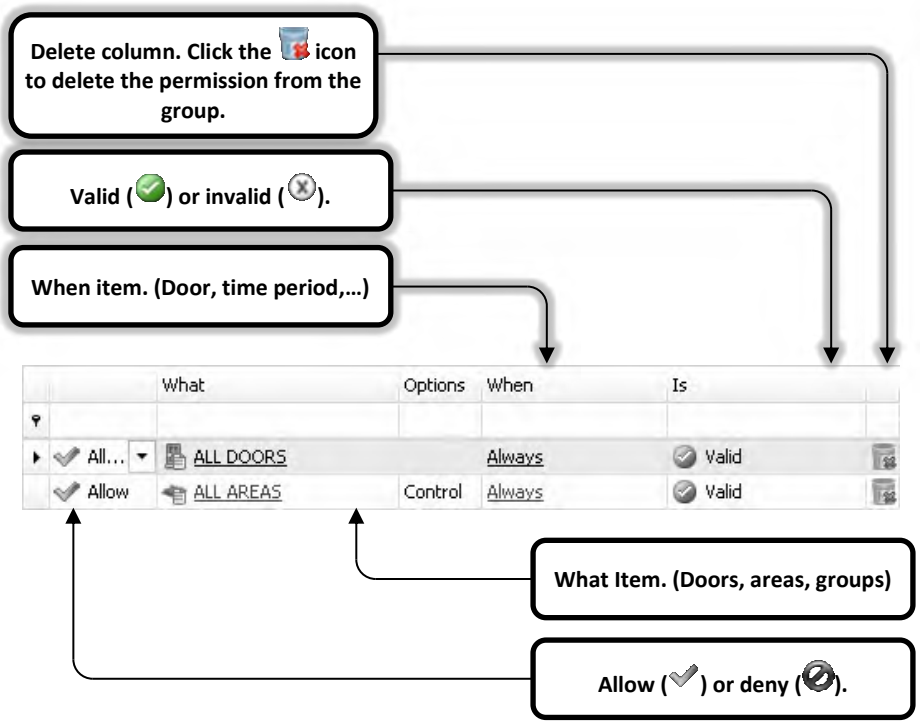


Figure 24

Permission Groups can have a maximum of 16 permissions.

Permission Groups can contain other permission groups but they are not permitted to create cyclic references.

Permission Groups can only go 4 levels deep from the top level entity.

Example:

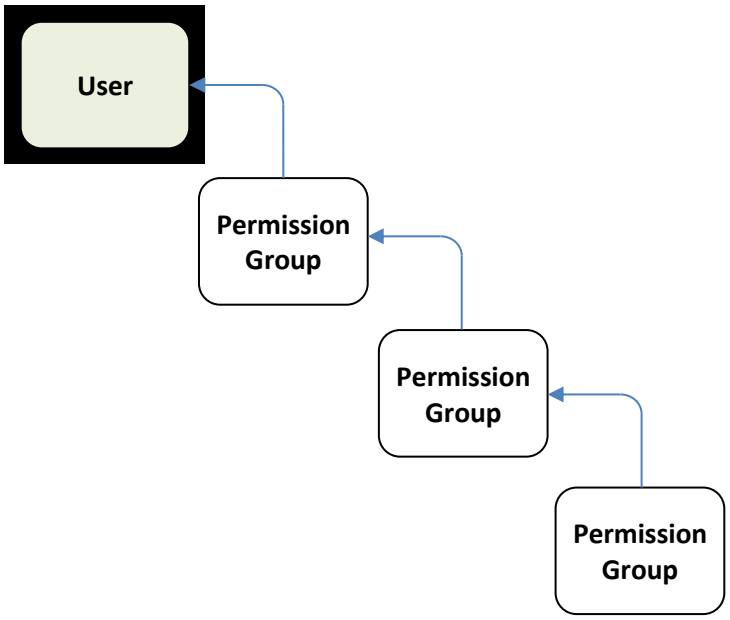


Figure 25

5.8.3.1 *Using Allow and Deny permissions*

Most permission groups will only contain 'allow' permissions as they are created for a large group of users that need these permissions assigned to them. There may be applications where the permission group could be assigned to other users but might include a few too many permissions.

This can be solved by assigning the permission group to the user and then adding an extra deny permission to filter out the permission.

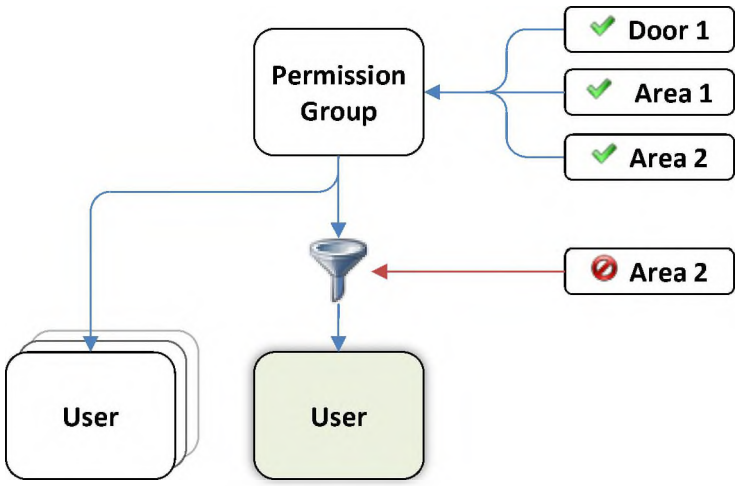


Figure 26

The highlighted user in the figure above has the same permission group as other users. However, the extra deny permission for area 2 will ensure the highlighted user only has access to Door 1 and Area 1.

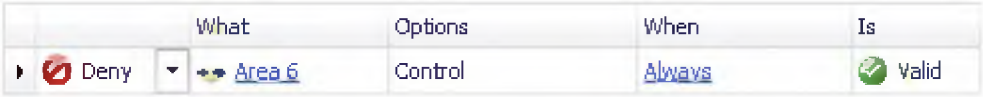
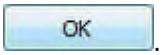


Figure 27

1. Click on the Intruder tab followed by Permission Groups.
2. Click Add New. The Editor Window for a new permission group should appear.
3. Give the Permission Group a name.
4. On the right-hand side, click on Add. A new window should appear.
5. On the left side of the window, select Areas or Area Lists.

6. Select the area / area list on the right side and click 

.
7. The permission group will have a new row added to it under permissions. In the left-hand column, select whether the permission is allowing access or denying it.
8. The "What" column is the selected door, door list, area, etc…
9. Depending on the entity selected in the "What" column, the "Options" column may have a drop-down selection available. ***Figure 28*** is an example of the area control options.

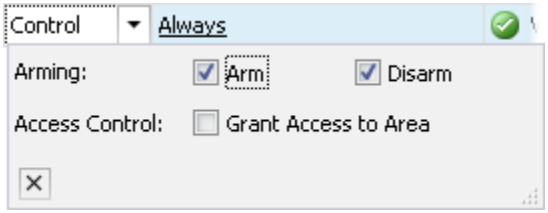


Figure 28

10. The "When" column is an optional qualifier for the permission itself. Its default value is "always". Permissions are often qualified by times (e.g. Time Periods or Holidays, but can also be qualified by many other things, like the state of doors or areas.
11. The "Is" column determines whether the optionally selected qualifier ("When") needs to be valid or invalid. Permission
12. Repeat steps **4** - **12** and make sure you add the Menu Group you created earlier. If additional areas or area lists are required, repeat the steps again accordingly.
13. Save and close the editor window for the Permission Group.

5.8.4 Users

Users within the Integriti management software are global. This means that the user record is only created the one time and individual permissions will tie the user to one or many controllers.

Qualify PIN codes may be used in association with cards for access control to provide a "something you have plus something you know" method of user authentication, in a card and PIN system. Many users can have the same Qualify PIN codes (just like an ATM card).

Security PIN codes are unique codes (passwords) used to identify users. These PIN codes are used to log in to the Integriti controller and perform various tasks. Because individual PIN codes are used to identify users at the controller, duplicate PIN codes are not permitted.

You can add individual permissions to a user by clicking the 

button within the User Programming dialog or if many users are likely to have the same permissions, permission groups should be used.

Permissions that can be added to a user are Doors, Door Lists, Areas, Area Lists, Menu Groups and Permission Groups.

Each User record has a default Permission Group. Permission Groups are an optional resource used for organisation of granular user permissions.

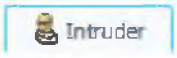
There are two methods used to create new users:

Creating a new user by duplicating an existing record:

If an existing user has the same configuration as the new user you are about to create then the easiest method of creating that new user is by clicking the existing user you want to duplicate followed by the 

button. A new dialog window will appear with the new user details.

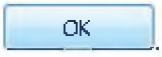
Assigning permissions to users…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new user should appear.
3. Give the User a name.
4. Give the user a Security PIN.
   Users have two PIN codes. The Qualify PIN is used for access control purposes where a PIN qualification is required for access control. This number can be duplicated across the system.
   The purpose of the Security PIN is to log in to the terminal. This PIN code must be unique. If a duplicate PIN is entered, the PIN will not be allowed and the original owner of the PIN will be notified when they log in next that their PIN has been discovered.
5. On the right-hand side of the window, click on the 

to the right of Primary Permission Group.
   The primary permission group should contain most (if not all) of the required permissions for the user to control areas, doors and other items with relevant access from a terminal or external interface (e.g. web interface).
6. Select the Permission Group you created earlier from the window that appears and click 

.
   In cases where the primary permission group does not cover all of the required permissions for the user, extra permissions can be used to give additional permissions or deny permissions that were allowed but not required within the primary permission group.
7. Save and close the editor window for the User.

5.9 Using the intrusion system

5.9.1 Arming / Disarming…

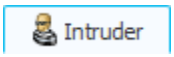
5.9.1.1 Terminal access

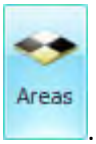
Arming an area from the terminal…

1. Enter your PIN followed by OK: **[0], [1], [Ok]**
2. Go in to the area menu: **[Menu], [0]**
3. Use the up/down directional arrows to select an area: **[▲] / [▼]**
4. Turn the area on by pressing ON: **[On]**

5.9.1.2 Software access

Arming Areas…

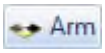
1. Click on the 

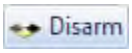
tab followed by 

.

- Method 1
  2. Right-click an area from the list.
  3. Click 

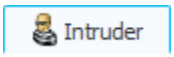
or 

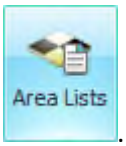
.
- Method 2
  2. Double-click the area from the list.
  3. Click 

or 

in the toolbar.

Arming Area Lists…

1. Click on the 

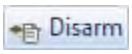
tab followed by 

.

- Method 1
  2. Right-click an area from the list.
  3. Click 

or 

.
- Method 2
  2. Double-click the area from the list.
  3. Click 

or 

in the toolbar.

24 Hour Areas…

Arming and disarming 24 hour areas is the same as the procedures listed above for arming and disarming areas.

5.9.2 Isolating

There are three isolation options available, isolate, sticky isolate and de-isolate. When an input is isolated its states are ignored.

Isolating an input will result in states of that input being ignored until any area that the input is associated with is disarmed.

Sticky Isolation is more permanent. By sticky isolating an input, the input will remain isolated until something or someone de-isolates it.

Isolating the input…

1. Click on the Intruder tab followed by Inputs.

- Method 1
  2. Right-click an input from the list.
  3. Click Isolate, Sticky Isolate or De-Isolate.
- Method 2
  4. Double-click the input from the list.
  5. Click Isolate, Sticky Isolate or De-Isolate in the toolbar.

5.10 Advanced

5.10.1 Auto arm / disarm by Time Period

Automatic arming and disarming of an area can be achieved by using named actions. You will need to create a time period defining the when the area will automatically arm and/or disarm before creating the named action.

Creating a Time Period…

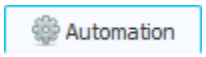
1. Click on the Home tab followed by Time Periods
2. Click Add New. The Editor Window for a new Time Period should appear.
3. Give the Time Period a name.

Under the Time Periods **tab…**

4. Click on Add to create a new row for the Time Period.

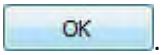
5. Click on the Start Time and enter the time that the area should arm.
6. Click on the End Time and enter the time that the area should disarm.
7. Click on the days which this time should apply to. Note that you can enter any number of start / stop time pairs and that these can occur on different days if desired (e.g. 9am – 12pm and 1pm to 5 pm on weekdays and 9am to 12:30 pm Saturday)
8. If this time is to ignore holidays then tick the Ignore Holidays check box at the end of the row.
9. Save and close the editor window for the Time Period.

Creating a Named Action…

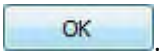
1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action.
   a. Click on the drop-down arrow to the right of Action to Take.
   b. Select Control Area from the list that appears.
   c. Click on the  to the right of the Area field to open the Area selection window.
   d. Select the Area from the list and click 

.
6. Expand-out Optional Trigger.
   a. Click on the  to the right of the Entity field to open the Entity selection window.
   b. Click on 

on the left side of the window.
   c. Select the Time Period that was created earlier from the list and click 

.
7. Save and close the editor window for the Time Period.

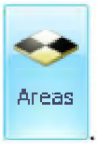
5.10.2 Defer area arming

Defer area arming is used in applications where automatic re-arming of an area is required to ensure an area remains secure. Users with defer arming enabled will be able to disarm areas but will start a timer that when expired will re-arm said area. This is also often used as an alarm in a lone worker scenario.

The following procedure assumes that an area has already been created and a user has access to this area.

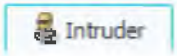
Enabling Defer arming for the Area…

1. Click on the 

tab followed by 

.
2. Double-click the area to enable defer arming on. The Editor Window for the area should appear.
3. On the right-hand side under Properties.
4. Expand-out General.
   a. Tick the Defer Area check box.
   b. Change the Defer Time to an appropriate value. Make sure you factor in the exit delay time for the area (if any).
5. Save and close the editor window for the Area.

Enable Defer arming for the Menu Group…

1. Click on the 

tab followed by 

.
2. Double-click the Menu Group given to the users that have permissions to disarm the area to be Defer armed. The Editor Window for the Menu Group should appear.
3. On the right-hand side under Properties.
4. Expand-out Area Control Permissions.
   a. Tick the Initiate Defer check box.
5. Save and close the editor window for the Menu Group.

5.10.3 Process Groups

Defining how an Input will be actioned in each Area is primarily done by allocating an appropriate Process Group to every Input in each Area that it is assigned to. Process Group programming includes defining the Input states (Seal/Alarm/Tamper/Isolate/…) that will be recognised, Entry/Exit delay processing options, Reporting & message options, and Auxiliary and Siren control options.

Figure 29

A large number of predefined process groups exists (see 'Default entities') for common use cases or you can create your own process group if unusual functionality is desired.

5.10.4 24 Hour Areas

Each individual area has its own 24 hour area. The 24 hour area is for inputs using a process group with the Process 24 Hour option set.

Normally, zone inputs and system inputs that require the alarm condition to be processed 24 hours a day (e.g. Smoke detectors, duress buttons, LAN communications problems, AC failure, etc…) must be assigned to an area that is always turned on.

Inputs associated with an area using the process group option “Process 24 Hour” allows a zone input alarm to be processed in an area that is off; or a system input alarm to be processed as an alarm rather than a tamper in an area that is off. If the process group option “Process 24 Hour” is set, then an alarm condition on the zone/system input is processed as an alarm even if the area is turned off.

This option allows for 24 Hour alarm inputs such as fire, duress, emergency, etc… to be assigned to the same area as other inputs (e.g. intruder alarms) that are only processed when the area is on.

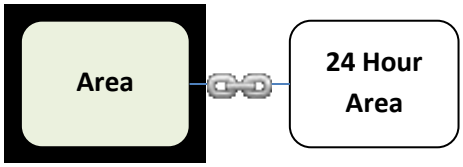


Figure 30

6 Setting up an Access System

The following will step you through what is required to commission a basic access control system.
It is assumed that the operator is logged in to the System Designer. An Integriti controller with the necessary modules attached should already be online, communicating with the server.
The instructions provided are based on the default layout.

6.1 Introduction and programming summary

The Integriti range of products integrates Access Control, Security Management and Building Automation. Access Control functionality and Building Automation operations can be kept completely separate from Security Management or can be fully integrated, if desired. Access Control operation is designed around the concept of Doors. The system simply determines which Users are allowed to use which Doors, at which times and with which options or restrictions.
Security Management operation is designed around the concept of Areas. Both Access Control and Security come together at Doors. For each Door in the system, one side is defined as the "outside" Area and the other side as the "inside" Area. Each Door can optionally be programmed as to which Area is on the outside and/or inside of the Door. If Area/s are programmed at a Door, then access at that Door will also be controlled by security considerations (via Areas).
e.g.

1. A User requiring access at a Door may be denied access because the Area they are about to enter is turned on, and they are not allowed to turn that Area off. If the User was allowed to turn that Area OFF then this may be done automatically on un-locking the Door, if programmed.
2. A User requesting access at a Door may be denied because the system has not seen the User leave the Area they are attempting to enter (Anti-Passback).

Doors

When designing an access system, Doors are the logical place to start. Each Door is numbered from Door 001 (D001), to the maximum available on your system. Each Door is individually programmed to define the functionality (via an Access Group) and the related Area/s, Auxiliaries and Timers, etc.

Access Modules

These Modules are required whenever access Cards are required, such as Proximity, Wiegand, Mag swipe, etc.

- Single Door Access Modules can control 1 Door with an Entry Reader.
- 2 Door Access Modules can control either 1 Door fitted with Entry and Exit Readers OR 2 Doors with Entry Readers.
- Intelligent 4 Door Access Modules can control 4 Doors with Entry and/or Exit Readers for all 4 Doors.

Each Access Module is individually programmed to define the Door/s controlled, Off-line operation, Zone input and Auxiliary options, Area control options and the direction (in or out), format, read mode, etc. for each Reader.

LCD Terminals

LCD Terminals can be used for Door Access Control if access to a Door is to be gained via a PIN code. Each Terminal may be individually programmed to define the Door controlled, Zone input & Auxiliary options & the direction (in or out).

Access Groups when Applied to Doors

Access Groups are a set of options that can be applied as a group to a Door. The typical system may have up to 32 Access Groups (depending upon system configuration) and each group may be individually programmed. A Door is assigned one of these Access Groups to use in determining the basic access control at the Door. The basic options that can be programmed for each Access Group are the modes of operation for Entry and Exit readers, Anti-passback options, REN/REX button options, Area control options, etc.

Time Periods

A Time Period can be used by any programming item that needs to be made Valid/Invalid according to the time of day and/or day of the week. A Time Period, once programmed, can be assigned to more than one item.

Holidays

A holiday comprises a start date and an end date and is used to set specified Time Period in-valid when a holiday occurs.
Each holiday can be defined as to which Time Period it will effect.

Programming summary

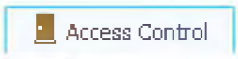
This section will take you through the creation of a basic access control system.

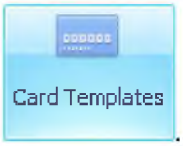
- Card template
- Door configuration
    - Reader module selection
    - Door types
- Reader module configuration
- User access permissions
    - Door lists
    - Permission Groups
    - Menu Groups
    - Credentials

6.2 Card Template

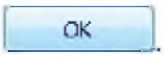
In cases where proximity technologies are used, a card template is required to define how the data on the proximity device will be interpreted. Card Templates also store the Site Code.

Creating a card template…

1. Click on the 

tab followed by 

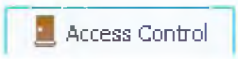
.
2. Click 

. The Editor Window for a new Card Template should appear.
3. Give the Card Template a name.
4. On the right-hand side under Properties.
5. Expand-out Card Format.
   a. Click on the  to the right of the Format field to open the Card Format selection window.
   b. Select the Card Format from the list and click 

.
6. Expand-out Site Code.
   a. Enter the Site Code in decimal or hexadecimal in either one of the Number fields.
7. Save and close the editor window for the Card Template.

6.3 Door configuration

Creating a door…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new Door should appear.
3. Give the Door a name.

Under the 

tab…

4. Click on the  to the right of the Module field to open the Reader Module selection window.
5. Select the Reader Module from the list and click 

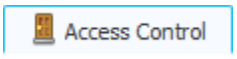
.
6. Click on the  to the right of the Relay field and select the desired lock relay from the list.
7. Click on the  to the right of the Door Type field and select the desired door type from the list.
8. Under the Outside heading
   a. Click on the  to the right of the Reader field and select the desired reader (or PIN device) from the list.

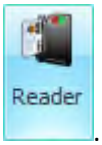
9. If you have chosen an Internal (Read In / Read Out Door) you will want to set up the internal reader or PIN Device as well.
10. Save and close the editor window for the Door.

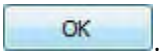
6.4 Reader module configuration

Reader modules usually require little or no configuration changes. Most of the programming had been taken care of when the Door was created and assigned to the reader module.

Reader Module configuration…

1. Click on the 

tab followed by 

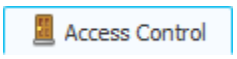
.
2. Double-click a Reader Module. The Editor Window for the Reader Module should appear.
3. Give the Reader Module a name.
4. On the right-hand side under Properties.
5. Expand-out Readers followed by Reader 1.
   a. Click on the  to the right of the Card Format field to open the Card Format selection window.
   b. Select the Card Format from the list and click 

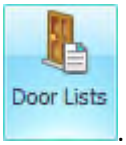
.
6. Save and close the editor window for the Reader Module.

6.5 User access permissions

6.5.1 Door Lists

Creating a Door List…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new Door List should appear.
3. Give the Door List a name.

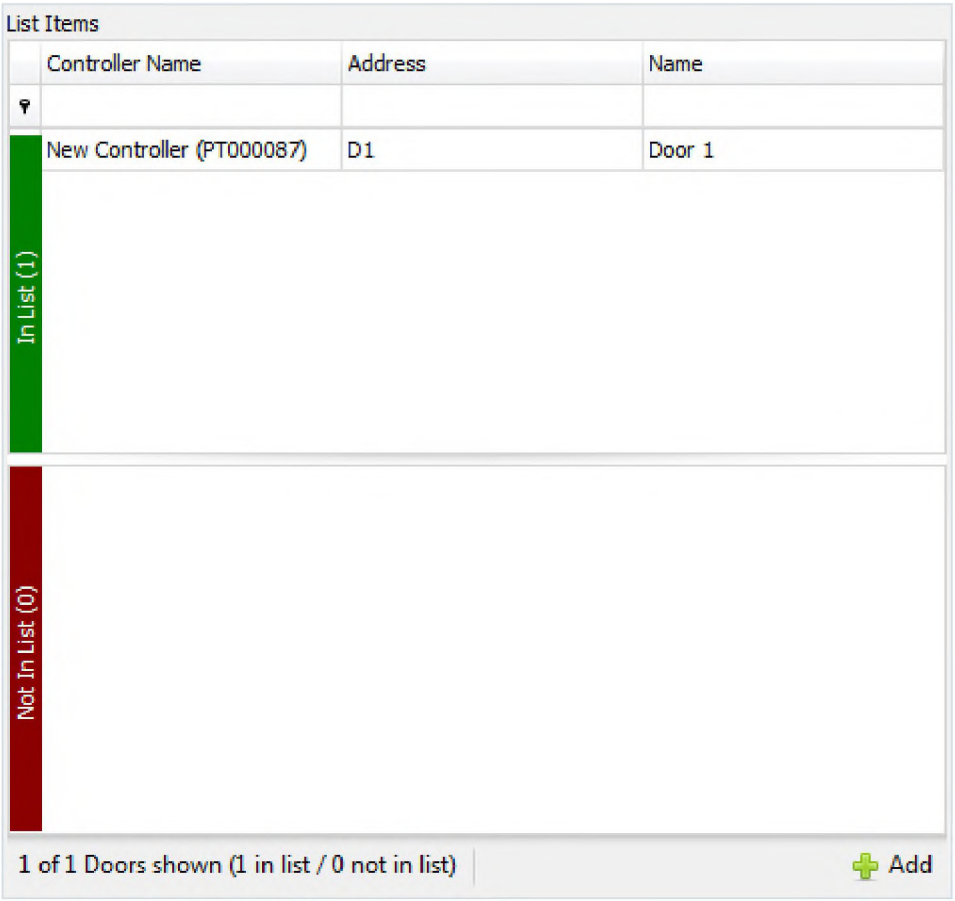


Figure 31

4. Items in the top section of the window are in the Door List. Items in the bottom section are not. Double click items to move them from one section to the other.
5. Save and close the editor window for the Door List.

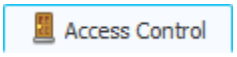
6.5.2 Menu Groups

Menu Groups…

1. Click on the Access Control tab followed by Menu Groups.
2. Click Add New. The Editor Window for a new menu group should appear.
3. Give the Permission Group a name.
4. On the right-hand side under Properties.
5. Expand-out Main Menu Items.
   a. Tick the “Access” option.
6. Save and close the editor window for the Menu Group.

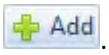
6.5.3 Permission Groups

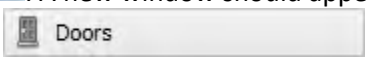
Creating Permission Groups…

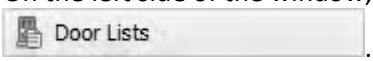
1. Click on the 

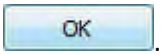
tab followed by 

.
2. Click 

. The Editor Window for a new permission group should appear.
3. Give the Permission Group a name.
4. On the right-hand side, click on 

. A new window should appear.
5. On the left side of the window, select 

or 

.
6. Select the Door / Door List on the right side and click 

.
7. The permission group will have a new row added to it under permissions. In the left-hand column, select whether the permission is allowing access or denying it.
8. The “What” column is the selected door, door list, area, etc…
9. Depending on the entity selected in the “What” column, the “Options” column may have a drop-down selection available. ***Figure 32*** is an example of the Door control options.

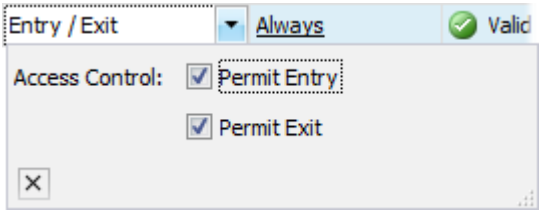


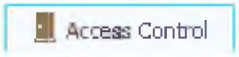
Figure 32

10. The “When” column is an optional qualifier for the permission itself. Its default value is always.
11. The “Is” column determines whether the optionally selected qualifier (“When”) needs to be valid or invalid.
12. The last column is a button to allow you to remove the individual permission. Double-click this if you want to remove the row.
13. Repeat steps **4** - **12** and make sure you add the Menu Group you created earlier. If additional areas or area lists are required, repeat the steps again accordingly.
14. Save and close the editor window for the Permission Group.

6.5.4 Credentials (Cards & RF fobs)

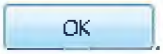
You can associate multiple credentials with a single user. A credential can be one of a number of things including but not limited to a swipe card, proximity card or wireless fob.

Assigning permissions to users…

1. Click on the 

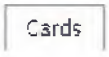
tab followed by 

.
2. Click 

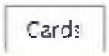
. The Editor Window for a new user should appear.
3. Give the User a name.
4. Give the user a Security PIN.
5. On the right-hand side of the window, click on the  to the right of Primary Permission Group.
6. Select the Permission Group you created earlier from the window that appears and click 

.

To add a new credential to a user:

- Click on the 

tab for swipe/proximity cards or 

tab for wireless devices.
- If you selected the 

tab you have 3 options for adding a credential to the user record.
  - Using 

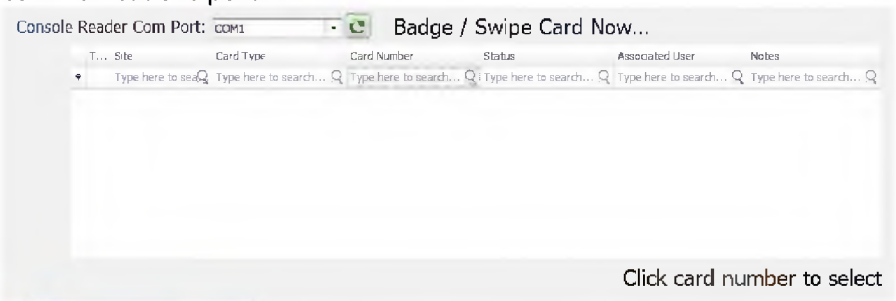
.
    1. Clicking 

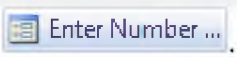
will open a new window where you have the option to select cards from 

or from a 

. Select one of these two items.
    2. If you selected 

, You might need to change the serial communications port.



  - Using 

.
    1. Selecting this option allows you to directly enter the card number.

Figure 33

2. Select the desired card template.
3. Enter the card number.
4. Click OK.

- Using Existing Card....
  1. Clicking this button will open a new window. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.
  2. Select a card from the list and click OK.

Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.

- If you selected the RF Remotes tab.
  - Using From Review....
    1. A find remote window will appear.
    2. Once the window is open, press a button on the remote. It should then appear in the list.
    3. Double-click the remote in the list.
  - Using Existing Remote....
    1. A find remote window will appear.
    2. Select a remote from the list and click OK.

Removing a credential from a user is as simple as double-clicking on the button to the right of the credential. Click the button to commit these changes.

7. Save and close the editor window for the User.

6.6 Using the access control system

6.6.1 Locking / Unlocking

Locking Doors...

1. Click on the Access Control tab followed by Doors.

- Method 1
  2. Right-click an door from the list.
  3. Click Unlock, Unlock (Timed) or Lock.
- Method 2
  2. Double-click the door from the list.
  3. Click Unlock, Unlock (Timed) or Lock in the toolbar.

Unlocking Doors...

1. Click on the Access Control tab followed by Door Lists.

- Method 1
  2. Right-click an door from the list.
  3. Click Unlock, Unlock (Timed) or Lock.
- Method 2
  2. Double-click the door from the list.
  3. Click Unlock, Unlock (Timed) or Lock in the toolbar.

6.7 Advanced access control

6.7.1 Time based door control

Timed door access requires the configuration of a Time Period and a Named Action. The Named Action will use the Time Period as an optional trigger to control the Door (or Door List).

Creating a Time Period…

1. Click on the Home tab followed by Time Periods.
2. Click Add New. The Editor Window for a new Time Period should appear.
3. Give the Time Period a name.
   See "Time Periods" for details on setting up a time period.

Under the Time Periods tab…

4. Click on Add to create a new row for the Time Period.
5. Click on the Start Time and enter the time that the area should arm.
6. Click on the End Time and enter the time that the area should disarm.
7. Click on the days which this time should apply to.
8. If this time is to ignore holidays then tick the Ignore Holidays check box at the end of the row.
9. Save and close the editor window for the Time Period.

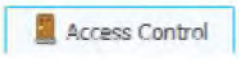
Creating a Named Action…

1. Click on the Automation tab followed by Named Actions.
2. Click Add New. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action.
   a. Click on the drop-down arrow to the right of Action to Take.
   b. Select Control Door from the list that appears.
   c. Click on the ··· to the right of the Door field to open the Door selection window.
   d. Select the Door from the list and click OK.
6. Expand-out Optional Trigger.
   a. Click on the ··· to the right of the Entity field to open the Entity selection window.
   b. Click on Time Qualifiers on the left side of the window.
   c. Select the Time Period that was created earlier from the list and click OK.
7. Save and close the editor window for the Time Period.

6.7.2 Disabled access

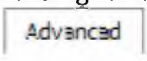
To give a disabled user extended access to a door you will need to configure the Handicapped Unlock Time of the Door and change the User to a Handicapped User.

Change the Handicapped Unlock Time of a Door…

1. Click on the 

tab followed by 

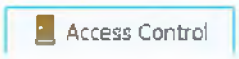
.
2. Double-click a Door to program. The Editor Window for the Door should appear.
3. On the right-hand side under Properties.

Under the 

tab…

4. Expand-out Advanced Door Configuration.
   a. Change the Handicapped Unlock Time.
5. Save and close the editor window for the Door.

Changing a User to a disabled User…

1. Click on the 

tab followed by 

.
2. Double-click a User to program. The Editor Window for the User should appear.
3. On the right-hand side under Properties.
4. Expand-out User Options.
   a. Click on Handicapped User.
5. Save and close the editor window for the Time Period.

7 Credentials

This section covers the creation and management of credentials. You can associate multiple credentials with a single user. A credential can be one of a number of things including but not limited to a swipe card, proximity card or wireless fob.

7.1 Card Format

Within each card format is a card type, and this will tell the reader how to operate, including whether to expect Magnetic card data or Wiegand card data, whether it needs to convert the raw data to site code, card number and issues number, or if it needs to hash or decrypt the card data. Some of these operations are done by the reader module and some by the control module. Different Card Types selected in the Card Format dialog of the software should display different fields where relevant, i.e. display site code bit lengths and offsets for Wiegand Custom Sitecodes and display Secure 40 scheme type for IR Secure 40.

All Card Formats that use a Wiegand type can also take a parameter called Wiegand Card Type. This can be N Bit meaning any bit length is allowed or it can be set to a particular bit length. N Bit will always return all the bits read. For fixed bit lengths, the behaviour varies between legacy Concept and new Integriti modules. For legacy modules, for cards equal to or longer than the bit length, it will return the first n bits, as if the card read were n bits long. If the card is shorter than the bit length, it is ignored. For Integriti modules if the card is not equal to the bit length, it is ignored completely.

Most of the common card formats have been added to the Integriti System Designer for convenience.

Card Types…

None	The Card Format will be unusable with this setting.
Wiegand Raw	For direct entry wiegand cards of any length. Credential is number of bits read followed by 11 bytes of data with the card data right justified and the rest of the filled padded with 0's. If no format is specified on the door then this is the format that will be used.

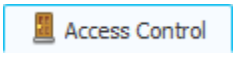
Wiegand Site	Allows user credentials to be entered as site code and card number providing the format is known for that user (i.e. HID 26 bit H10301), including migrations from Concept and other systems. Assumes that the bits that don't form the site code and card number (i.e. start and stop parity bits) conform to a manufacturer's specification that Inner Range was aware of at the time we implemented the SW/FW. There is an option in these formats called "encoding" which allows for different parity schemes than the standard one we assume from a particular card length, although none have been added as yet. All the underlying credentials are actually compared and stored as wiegand Raw.
Wiegand Custom Sitecode	Allows for site code formats unknown to Inner Range. This is now the recommended format when only one card format is used throughout the system. User credential stored is actually just the site code, card number and issue number, not the raw data. Parity and other unused bits are discarded and not compared.
Mag Raw 40	This magnetic swipe card format read the first 10 characters (40 bits) from a mag card, nibble swapping each byte (i.e. swapping each character pair). This allows for compatibility in migrations where Concept Mag Direct was used.
Mag Site	Reads mag cards in character mode. Like Wiegand Custom Sitecode allows user definable site code, except lengths and offsets are specified in characters instead of bits. Unlike IRMag, the cards are assumed to not be encrypted. Credentials are store as site code, not raw data.
Mag Hash 5	Reads the first 22 characters from a mag card and generates a 5 byte hash from this, using the same algorithm as the Concept "Credit Card" format.
IR Mag Swipe	Decrypts a Concept Secure Mag card and returns its site code, card number and issue number. Although site code parameters are user definable for this format, the decryption part will probably only work if it follows the IRMag Secure scheme.

IR Secure40	Decrypts an IR Secure 40 card and matches it on site code and card number. Only needs to be put in the card template of the user. If the reader is set to this format it will operate as a wiegand raw format. In the format the scheme in use must be chosen, whether Standard, Registered Site or Enterprise.
Mag Raw 88	Reads up to the first 22 characters of a mag card, until it gets an end or separator sentinel character. This usually reads financial cards as the number is written on them (no nibble swap) prepended with the number of bits read (4 per character) and 0's.
Mag Site (bits)	This format makes the reader return the binary data from the card instead of the characters. For most mag cards (i.e. financial cards) this is 4bits for the character and one bit of parity. This supports hypothetical cards where the site info is stored as binary data instead of characters
Wiegand 3K Raw	Reads the wiegand card data, removes the start bit and puts the data in a 5 byte field and left justifies that data. It then prepends the credential with "28000000000000" For instances, the 26bit wiegand card with binary data '11001111000001111010101000' (Wiegand Raw (26) = 1A00000000000000033C1EA8(hex)) would be read as per the next column. This helps migrations from concept direct entry wiegand systems where the start bit was not used (99% of all sites).

Table 3

Creating a new Card Format…

1. Open the 

panel from the 

tab.
2. Click the 

button to create a new Card Format.
3. Give the Card Format a new name and enter any necessary notes in the Notes field.
4. Expand-out Options and select the desired Card Type from the drop down list. Refer to Table 3 for details.
5. Expand-out Card Programming and select the bit length of the card in the Wiegand Card Type field. If the bit length is variable or unknown, 'N Bit' can be used.
6. Expand-out Site Code Parameters (Card Type dependant).
   a. Enter the bit length of the card format in the Total Bits field.
   b. Enter the offset from the first bit where the site code begins in the bit stream.
   c. Enter the total bit length of the site code in the Site Code Length field.
   d. Enter the offset from the first bit where the card number begins in the bit stream.

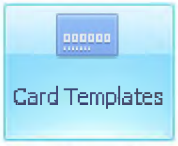
e. Enter the total bit length of the card number in the Card Number Length field.
f. Enter the offset from the first bit where the card issue number begins in the bit stream.
g. Enter the total bit length of the card issue number in the Issue Number Length field.
h. If the selected Card Type is Secure 40, there are three schemes to choose from:
   - Standard
   - Registered Site
   - Enterprise

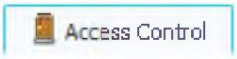
7. Save and close the editor window for the Communications Task.

7.2 Card Templates

Card Templates have been created to make life easier when adding new credentials to the Integriti system.

To create a new Card Template…

1. Open the 

panel from the 

tab.

2. Click the 

button to create a new Card Template.

3. Give the Card Format a new name and enter any necessary notes in the Notes field.

4. Expand-out Card Format and select the desired Card Format for this Card Template.

5. Expand-out Site Code and enter the Site Code for the credentials you will be adding to the system in either binary or decimal.

6. Save and close the editor window for the Communications Task.

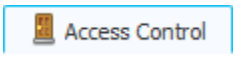
7.3 Cards

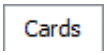
User credential (proximity card, swipe card, fob…) programming only requires a card template selection and data. The data field commonly refers to the card number (or issue number) of the credential that is to be issued to the user.

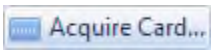
Card templates are created using a card format. Card formats contain detail explaining where data is situated on a card.

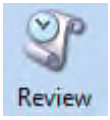
To add a new credential to a user:

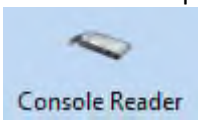
1. Open the 

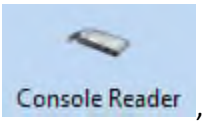
panel from the 

tab
2. Double-click a user for editing.
3. Click on the 

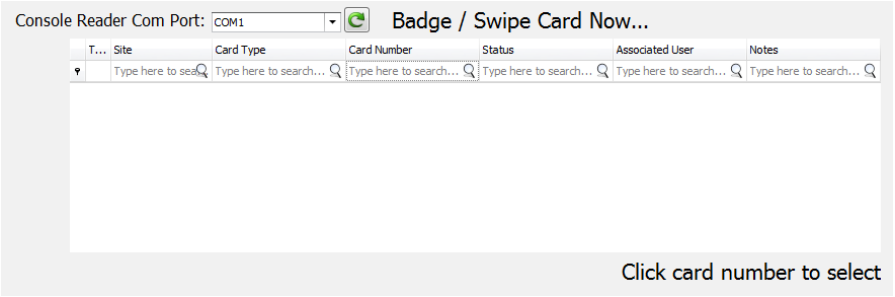
tab for swipe/proximity cards
   - Click 

to open the card acquire window.
     a. Click on 

or 

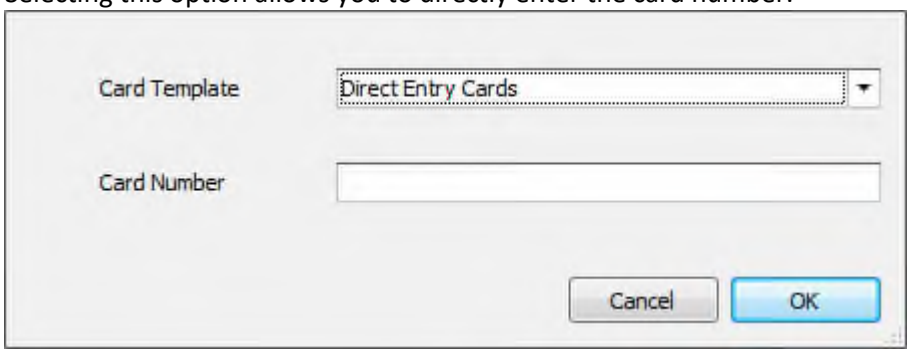
to select your card acquisition source.
        - If you selected 

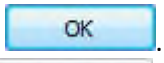
, You might need to change the serial communications port.



     b. Present the card to a reader attached to the controller (if you selected Review) or to the enrolment station.
     c. Double-click the card that appears in the list.
   - Click 

for manual card entry.
     a. Selecting this option allows you to directly enter the card number.



     b. Select the desired card template.
     c. Enter the card number.
     d. Click 

.
   - Click on 

to select an existing card in the system. A new card selection window will appear.

a. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.

b. Select a card from the list and click OK.

Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.

- Removing a credential from a user is as simple as double-clicking on the button to the right of the credential.

4. Click the button to commit these changes.

7.4 RF Remote Templates

RF Remote Templates map the various messages sent from the RF remote to actions, inputs and area control on the Integriti controller.

To map a button, you will need to observe the messages displayed in review for information on what button was pressed. RF expanders will need to have the option 'Log RF Remote Details' ticked.

To enable logging on the RF expander…

1. Open the Radio Expander panel from the Hardware tab.
2. Double-click the RF expander to open for editing.
3. Expand-out Misc.
4. Tick the option 'Log RF Remote Details'.
5. Save and close the editor window for the RF Expander.

Pressing buttons on the RF remote will result in review messages similar to the following:

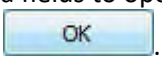
```
Unknown User Paradox REM2 Prg1 button Unlicensed…
Unknown User Paradox REM2 Arm1 button Unlicensed…
```

In the two example review lines above, you can see Prg1 and Arm1. These labels indicate the buttons being pressed. Review text containing 'Prg' indicate actions. e.g. Prg1 = Action1, Prg2 = Action2, etc…

Creating a new RF Remote Template…

1. Open the RF Remote Templates panel from the Access Control tab.

2. Click the 

button to create a new RF Remote Template.
3. Give the RF Remote Template a new name and enter any necessary notes in the Notes field.
4. Expand-out Button Definitions
   a. Drop-down actions 1-4 and select an action as required for each button available on the RF Remote.
   b. Click on the  to the right of the Area fields to open the Area selection window.
   c. Select the Area from the list and click 

.
   d. If the RF Remote reports input states, click on the  to the right of the Input fields to open the Input selection window.
      - Inputs mapped using RF Remote Templates should have the option 'Ignore Physical Input' set.
5. Paradox REM3 RF Remotes support PIN codes. There are three options available for these remotes. Expand-out Options.
   a. Ticking 'Needs 6 Digits' sets a requirement for all PIN codes used with a REM3 must be 6 digits.
   b. Ticking 'Needs PIB for Programming' sets a requirement for PIN entry to control Actions (Action 1-4).
   c. Ticking 'Needs PIN for Area On/Off' sets a requirement for PIN entry to control Areas (Area 1-2).
6. Save and close the editor window for the RF Remote Template.

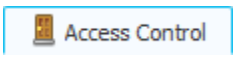
7.5 RF Remotes

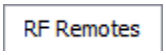
There are two methods available for creating RF remotes. The simplest method is to create a new RF remote by enrolling a remote to a user. The alternative method is manual entry.

RF Remotes need to have an RF Remote Template.

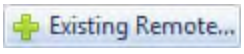
To create a new RF Remote (enrolling to a user)…

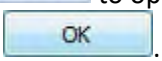
1. Open the 

panel from the 

tab
2. Double-click a user for editing (The user you want to enrol the RF Remote to).
3. Click on the 

tab for wireless devices.
4. Click on 

to open the find remote window.
5. Once the window is open, press a button on the remote. It should then appear in the list.
6. Double-click the remote in the list.
   - Alternatively you can use 

to open a list of enrolled RF Remotes.
   - Select a remote from the list and click 

.
7. Save and close the editor window for the User.

Selecting a remote that has already been allocated to a user will generate a synchronisation warning (users can not share the same remote).To resolve this issue, go to the other user record and remove the remote.

To create a new RF Remote (manual entry)…

1. Open the 

panel from the 

tab
2. Click the 

button to create a new RF Remote.
3. Give the RF Remote a new name and enter any necessary notes in the Notes field.
4. Expand-out Credential.
5. Enter the unique serial number of the remote in the Remote Data field.
6. Click on the 

to the right of Remote Template.
7. Select the appropriate RF Remote Template from the list and click 

.
8. Save and close the editor window for the RF Remote.

The unique ID of the RF Remote can be determined by looking at the end of a RF Remote review message. Pressing a button on the RF Remote will produce a review event similar to the following:

```
Unknown Paradox Door Alarm at C3K-RadioExp: 01 Sig=07
ID=00000B2B
```

You will need to ensure 'Log RF Remote Details' is enabled on the RF Expander. Details on how to set this option have been explained in the section titled 'RF Remote Templates'.

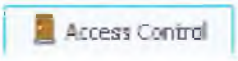
7.6 Cards

User credential (proximity card, swipe card, fob…) programming only requires a card template selection and data. The data field commonly refers to the card number (or issue number) of the credential that is to be issued to the user.

Card templates are created using a card format. Card formats contain detail explaining where data is situated on a card.

To add a new credential to a user:

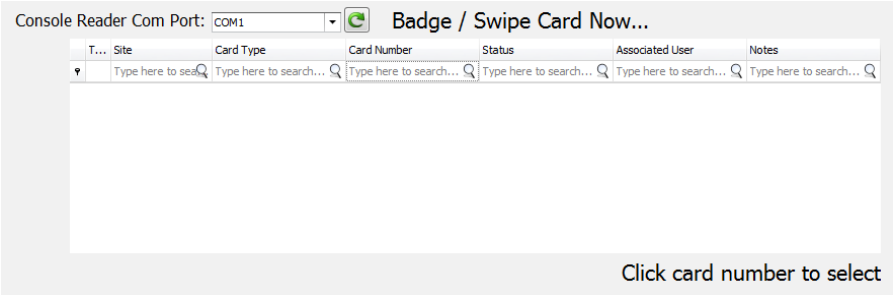
1. Open the 

panel from the 

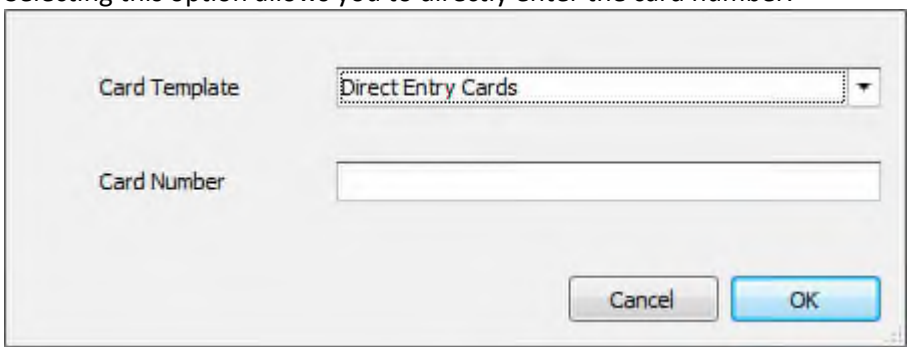
tab
2. Double-click a user for editing.

3. Click on the Cards tab for swipe/proximity cards

- Click Acquire Card... to open the card acquire window.
  - a. Click on Review or Console Reader to select your card acquisition source.
    - If you selected Console Reader, You might need to change the serial communications port.



  - b. Present the card to a reader attached to the controller (if you selected Review) or to the enrolment station.
  - c. Double-click the card that appears in the list.
- Click Enter Number ... for manual card entry.
  - e. Selecting this option allows you to directly enter the card number.



  - f. Select the desired card template.
  - g. Enter the card number.
  - h. Click OK.
- Click on Existing Card... to select an existing card in the system. A new card selection window will appear.
  - c. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.
  - d. Select a card from the list and click OK.

Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.

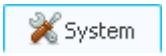
- Removing a credential from a user is as simple as double-clicking on the  button to the right of the credential.

4. Click the  button to commit these changes.

8 Scheduling

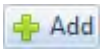
8.1 Time Periods

The time periods panel is accessible from the 

and 

tabs.

Time periods are most commonly used as the “when” in permissions, but can also be used in named actions.

Time periods are created by adding a schedule period by clicking the 

button directly below the schedule pane.

- Overlapping schedule periods do not impact one another.
- Only Holidays associated with the Time Period will have an effect on the validity of the Schedule Periods.
- Time Periods without the Holidays check box ticked will be invalidated when the Holidays associated with the Time Period are valid.

To create a new Time Period:

1. Open the time periods panel.
2. Click the Add New icon in the time periods Panel.
3. Give the Time Period a name and add any necessary details in the notes field.
4. Click the Add button and change the parameters of the newly created schedule period.
   - Ticking the Ignore Holidays option will cause any of the Holidays specified in the Holidays tab of this Time Period to be ignored.
5. Click on the Holidays tab followed by Add to add holidays to the Time Period.
6. Click the button and close the dialog.

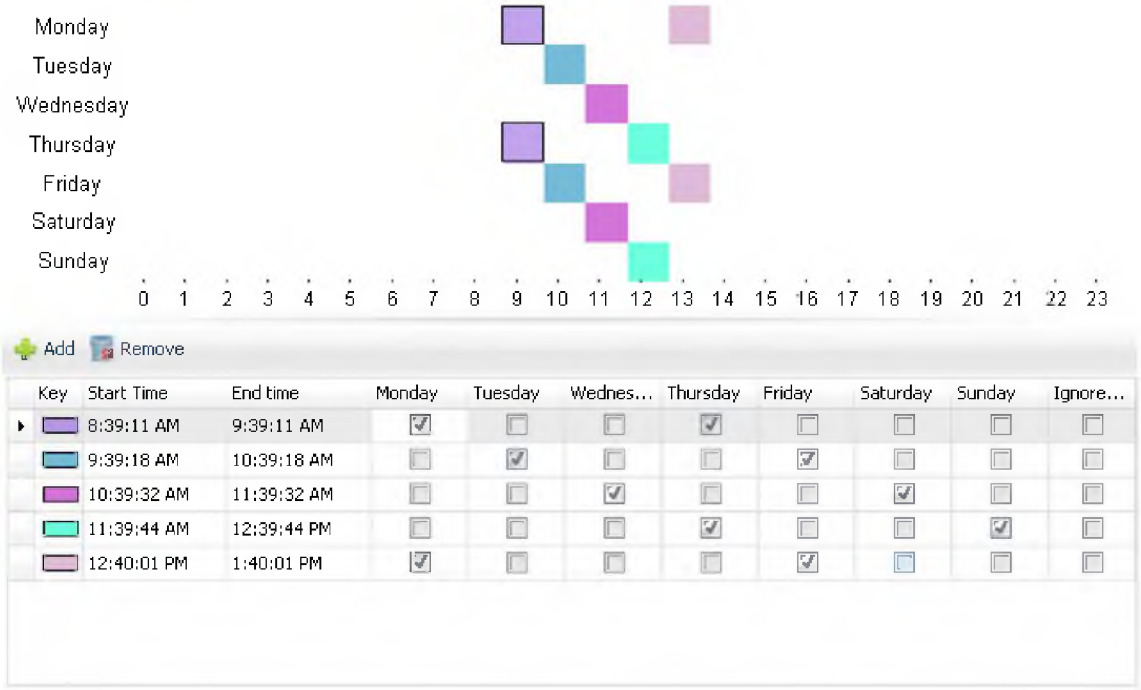


Figure 34

8.1.1 Schedule Overrides

Schedule Overrides are managed by the Integriti server. The addition of Schedule Overrides allows the operator to easily adjust Time Periods over specific date ranges during the year.

To create a new Time Period Override:

1. Clicking the Add button will open the Edit Time Peiod Override dialog.

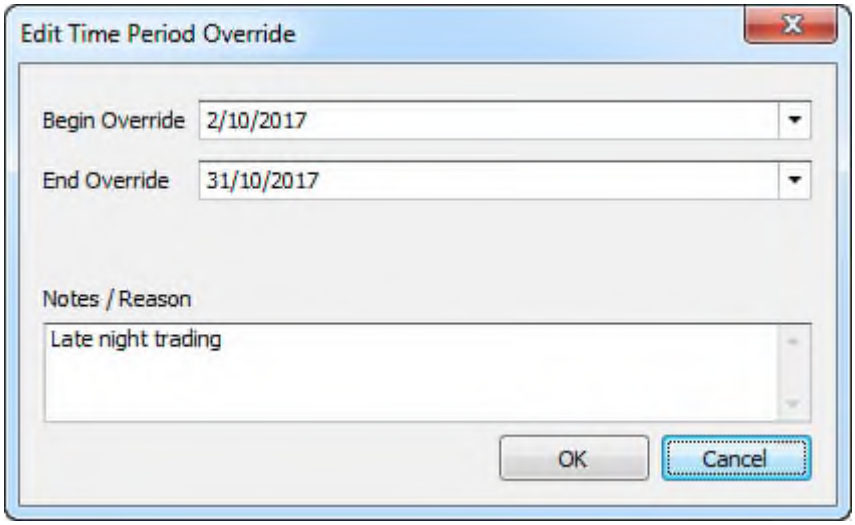


Figure 35

2. Change the Begin and End override dates accordingly.
3. Optionally enter notes in the Notes / Reason text box.
4. Click the OK button to add the Time Period Override to the list.

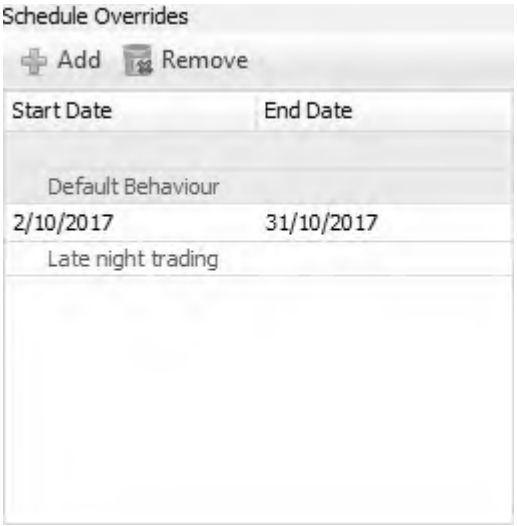
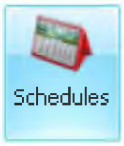
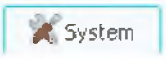


Figure 36

To remove a Time Period Override, click on the Time Period Override followed by the Remove button.

8.2 Schedules

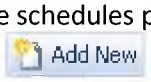


The schedules panel is accessible from the 

tab.

Schedules allow for reoccurring events. Schedules can be set to trigger hourly, daily, weekly, monthly, yearly or weekday of month.

To create a new Schedule:

1. Open the schedules panel.
2. Click the 

button in the schedules panel.
3. Give the Schedule a Name and add any necessary details in the Notes field.
4. If UTC time is used, tick the UTC check box.
5. Set the recurrence of the schedule as required.
6. Change the start date to that of the schedule.
7. Change the end date to that of the schedule.
8. Tick the days that the schedule is to be valid.
9. Click the  button and close the dialog.

8.3 Holidays

The holidays panel is accessible from the Home and System tabs.

To create a new Holiday:

1. Open the holidays panel.
2. Click the Add New button in the holidays Panel.
3. Give the Holiday a Name and add any necessary details in the Notes field.
4. Change the start time and date to that of the holiday.
5. Change the end time and date to that of the holiday.
   – or –
   Change the Duration (Days) to the appropriate number of days the holiday is to last for.
6. If the holiday is to recur annually, tick the Recur Annually check box.
7. If UTC time is used, tick the UTC check box.
8. Click the button and close the dialog.

8.4 Scheduled Tasks

Scheduled tasks contain one or many actions that can be executed sequentially, parallel or a combination of both on predefined triggers.

Scheduled Tasks are for automated actions in response to a trigger (which can be either time or review messages).

There are 15 action types to choose from:

- Backup Database
- Control Workstation
- Controller Action
- Escalate Alert
- Custom Enhancement
- Execute Report
- Invoke Integrated Device Command
- Log Review
- Parallel Task List
- Pause
- Run External Program
- Send Communication Message
- Send Integrated Device Event
- Sequential Task List
- Synchronise Controller Time

Detail on these actions can be found in the section titled “Action types” in the appendix.

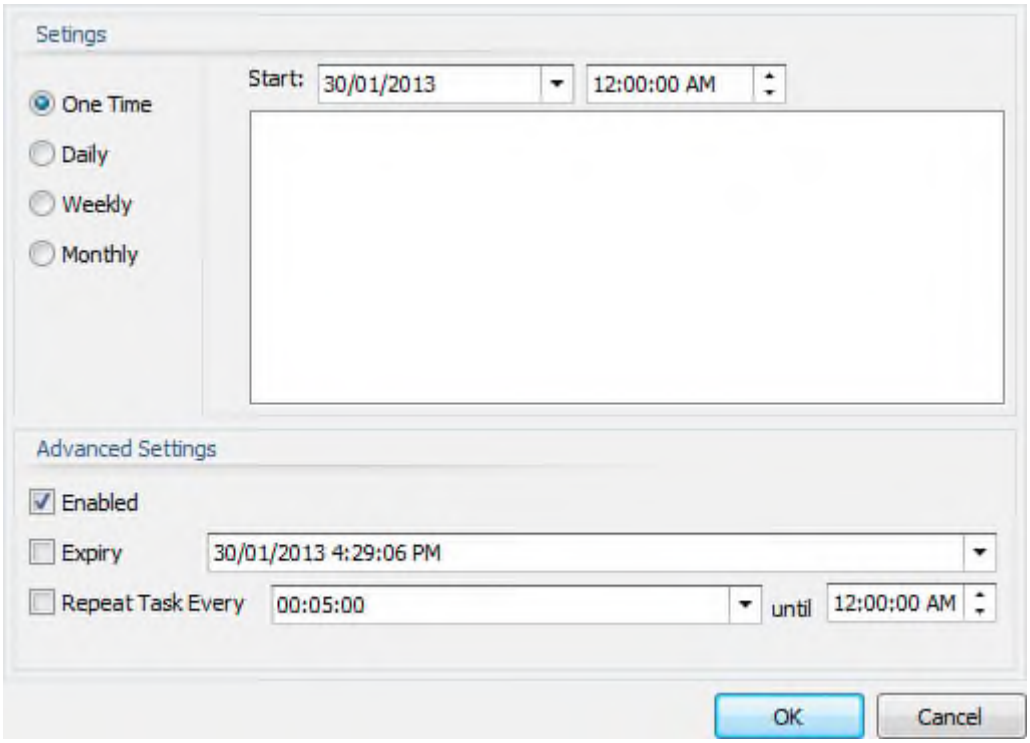
Triggers can be a combination of either Time or Review. Click 

under the 

tab to add a new trigger.

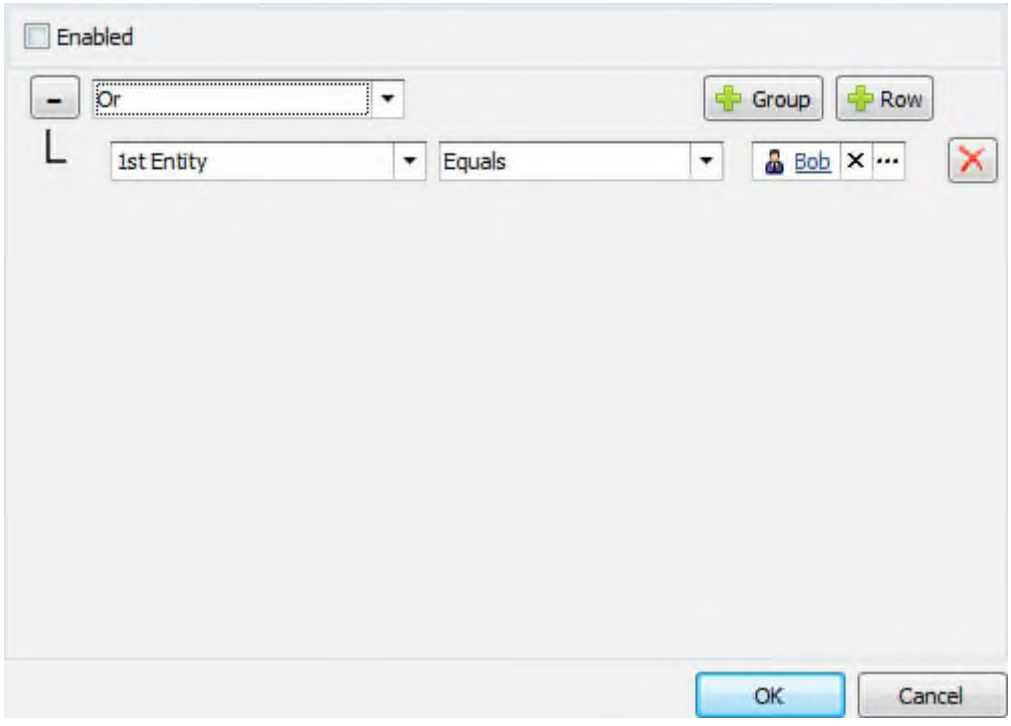
Time Trigger

Time based triggers can be configured to activate once, daily, weekly or monthly.
Time based triggers will only operate when the Enabled checkbox is ticked.
An optional configurable expiry can be set. The expiry can be adjusted to the minute.



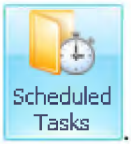
Review Trigger

To add a new criteria to the Review Trigger, click the Row button. The first drop down list specifies the review component to test against. The Second drop down list specifies the criteria operator. The last drop down list is the operand value.



Creating Scheduled Tasks…

1. Click on the 

tab followed by 

.
2. Click 

to create a new Scheduled Task.
3. Give the Scheduled Task a Name and add any necessary details in the Notes field.
4. Specify an action to take if the task is already running.
    - Do Nothing – The Scheduled Task will not execute.
    - Run After Completion – If the Scheduled Task was triggered while it was already running at the Scheduled Task will re-run immediately after completion.
    - Run In Parallel – The Scheduled Task will run immediately regardless of whether the task was already running or not.
5. If required, tick the Retry On Fail check box.
    a. Specify the Maximum Retry Attempts. Leaving this value set at 0 will cause the Scheduled Task to retry until it passes.
6. Add one or many Time or Review based triggers.
7. Add one or many Actions to the Scheduled Task.

9 Automation

9.1 Counting Input Types

There are four input types to allow for scenarios where counting is required.

Inputs with the 'Count up' or 'Count Down' type will have their own count value. Whenever the input transitions to the 'Alarm' state, the input will count up or down depending on the input type selected. Count inputs can be any value from 0 to 65535.

The 'Previous Count Up' and 'Previous Count Down' types will change the count value of the nearest 'Count Up' or 'Count Down' input type with a lower ID. 'Previous Count Up' and 'Previous Count Down' types must be on the same module as the 'Count Up' / 'Count Down' input.

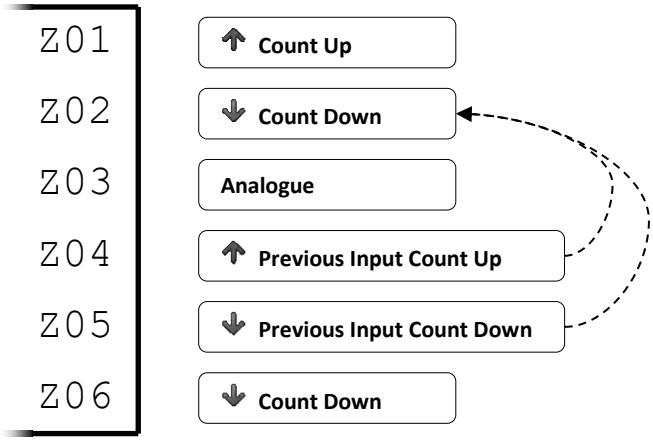


Figure 37

In the example above we can see that input 2 is affected by zones 4 and 5. Each time input 2 or 5 transitions to the alarm state, the count value of input 2 will decrease by 1. Each time input 4 transitions to the alarm state, input 2 will increase by 1.

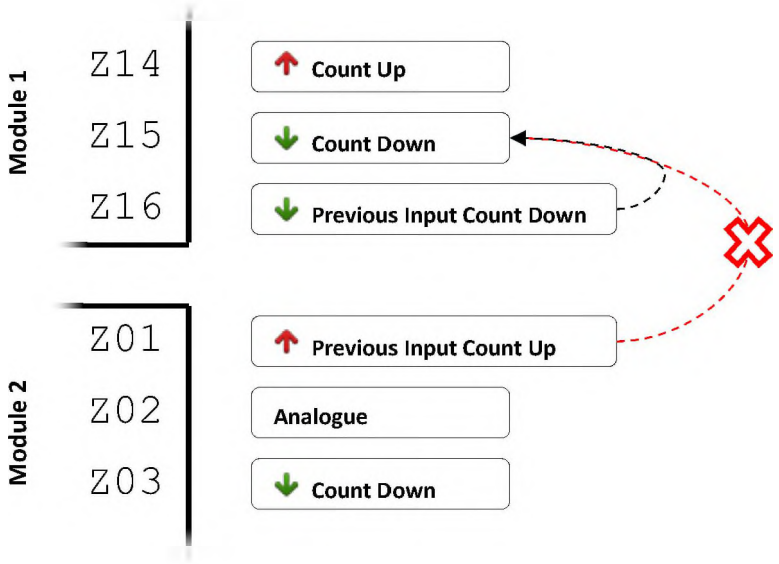


Figure 38

In the example above input 16 on module 1 will decrease the count of input 15 on module 1. However input 1 on module 2 will not increase the count of input 15 on module 2 because the inputs are not on the same module.

9.2 Auxiliaries

Auxiliaries are the digital outputs on the Integriti system. There are three different types of auxiliary that you can use.

Relay Output

Relay outputs are the most common and most practical of auxiliary output types. The relay output may provide an optional voltage out (jumper selection). The auxiliary relay ratings have different voltage and amperage ratings depending on the module used.

Open Collector

Open collector outputs are switched by a small semiconductor. . Open collector outputs are mainly found on Concept compatible LAN modules. As a result, the load can only be small. These types of outputs are good for LEDs and driving slave relays.

Phantom

Phantom auxiliaries are outputs that don't physically exist. They will still operate the same as a normal auxiliary. The Integriti controller has 30 phantom auxiliaries available unless expanded using UniBus relay expanders. LAN modules may also have auxiliaries available.

9.3 Auxiliary Lists

Auxiliary Lists can contain up to 16 auxiliaries. Auxiliary lists are particularly useful for applications where a number of auxiliaries may need to be controlled simultaneously.

9.4 Compound entities

Compound Entities represent the logical state of a collection of up to 8 entities. The state returned is a result of the logical relationship between them.

The logical relationship between entities is processed sequentially from lowest to highest.

Compound entities can be used to combine multiple controller entities for anything an entity is used as the source (e.g. as the “When” of a permission or permission group, the trigger for a named action, in an expression in a Macro).

Compound Entities can be used to combine multiple controller entities and trigger named actions (e.g. open a door, unsecure a floor, etc.).

Using Compound Entities to concatenate a time period and a schedule:

- Create a time period (e.g. “Opening Hours” 9:00 am to 5:00 pm Mon - Sat)
- Create a “never repeats” schedule that overlaps (e.g. “Extended Hours 1” 24/12/2013 4:50 p.m. to 10:00 p.m.).
    - Note: Don’t start the schedule at the same minute that the time period expires as a race condition may ensue and an open door condition could get there just before a close door condition (for example).
- Create a compound entity (e.g. “Modified Trading hours” that is the OR of these two entities)
- Create a named action that performs the action you want (e.g. Control a door)
- Use the compound entity you created as the “Optional Trigger” for this action.

Note that to find the compound entity in the “Search for Entity of Named Action” window you will currently need to look in “Unfiltered Controller Items” and filter on either Name or ID.

In this way you can program up a named action with modified hours in advance.

If you chose, you could have more than 1 “Extended Hours” feature that occurred in the future.

Because you have set it up never to repeat, there’s no need to clear these out after they’ve activated.

You can re-use them the next time you get a special event that you want to schedule.

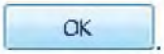
In a similar way, Compound Entities can be used to combine multiple time periods, or time periods with other state (e.g. the state of an Aux).

Creating Compound Entities…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new Compound Entity should appear.
3. Give the Compound Entity a name.
4. On the right-hand side under Properties.
5. Expand-out Misc.
   a. Click on the  to the right of Entity 1.
   b. Select the entity from the window that appears and click 

.
   c. If the state of the entity needs to be inverted, click the Invert Entity 1 checkbox.
   d. Click on the  to the right of Logical Relation 1.
   e. Select the relationship between entity 1 and entity 2 (none, AND, OR, XOR).
      - ‘none’ is only required if the entity is the last in the list.
   f. Repeat steps **a** - **f** for the remaining entities as required.
6. Save and close the editor window for the Compound Entity.

9.5 Named Actions

Named actions provide a means to perform an action on the controller. These actions can be controlled by the user or from a trigger (entity).

User access is controlled by Action Groups. Users with the appropriate Action Groups can view and control the Named Action.

Creating Named Actions…

1. Click on the 

tab followed by 

.
2. Click 

. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action and select an action to take from the drop-down list.
   More detail on Action types is available in the appendix.
6. If required, expand-out Optional Trigger.
7. Specify an optional trigger by clicking on the ellipsis to the right of Entity and select an entity from the list.
8. Optionally users can have direct control over Named Actions via the Terminal.
   a. Expand-out User Interface.
   b. Click on the drop-down list to the right of Interface Style and select the appropriate option based on the configured Action to Take.

c. If a Sense Entity is specified the state of the Named Action will reflect the state of the selected Sense Entity. If no entity is specified the state of the Named Action is determined by the entity controlled by the action.
d. Ticking the Invert Sense Entity will invert the reported state of the Named Action.
e. Allow Logged Off Access will allow terminal users to control the Named Action without logging in to the terminal.

9. Expand-out User Access followed by Action Groups.

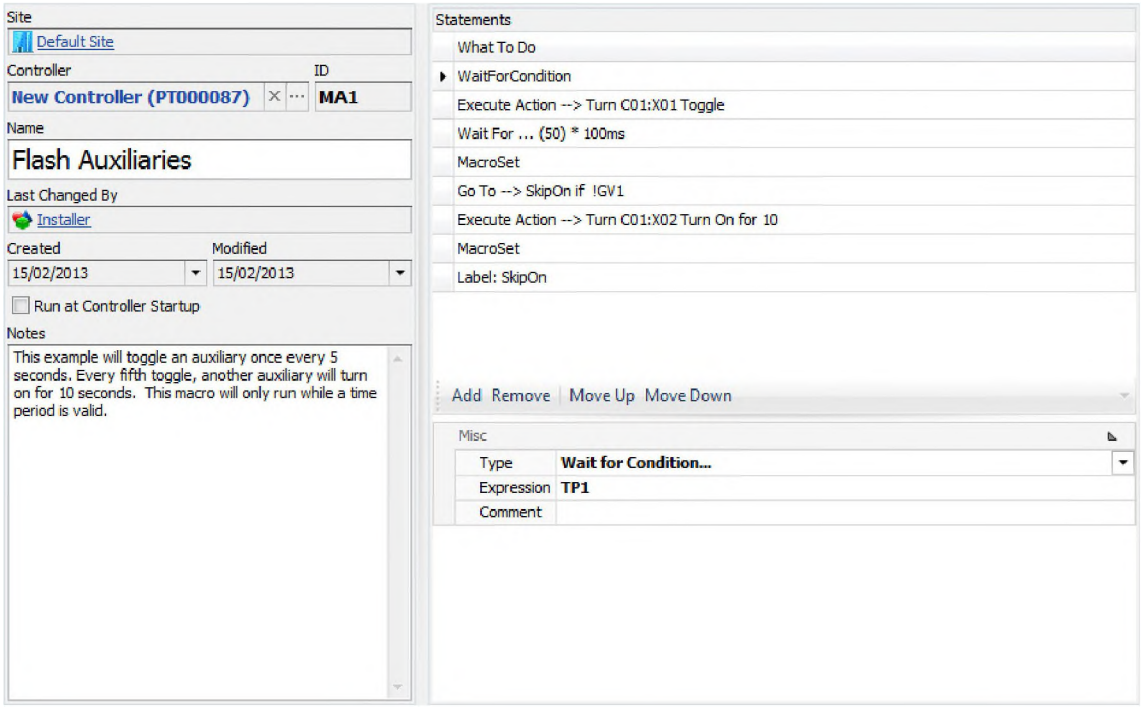
10. If no Action Groups are selected, any user can control the Named Action. If one or many Action Groups have been selected, users must have any one (or more) of the same Action Groups.

11. Save and close the editor window for the Named Action.

9.6 Macros

Macros within the Integriti controller provide an advanced level of flexibility where the use of actions is inadequate.

Programming of macros can only be created through the Integriti system management software.



9.6.1 Macro characteristics

All macros are implicitly looped –

Once a macro has started it will continue to run until stopped or the controller is restarted.

Macros can start automatically –

A macro can be configured to automatically start on controller start-up.

Actions are only asserted within macros –

'`Do an Action`' and '`Do an Action if…`' statement types will only assert the specified action.
The Dis-asserted option(s) are ignored.

Timing accuracy –

'Pause for Time…' statements are expressed in units of 100 milliseconds. Macro timings are accurate to roughly 100ms depending on the overall load on the Integriti controller.
Macro timing is affected by other higher priority processes taking place on the controller. Communications tasks and module communications are two examples of higher priority processes.

9.6.2 Controlling / Running macros

You can control macros from the Integriti management software or from the terminal (using 'Named Actions'). You can also configure macros to run on controller start-up or from an action.

Please refer to the section titled 'Named Actions' for more information on how to create a named action that will control a macro.

The section titled 'Actions' describes how to create an action with 'Run Macro' as the action.

9.6.2.1 Running macros from the Integriti management software

1. Open the macros panel.
2. Right-click the macro in the automation the macro panel and select 'Start'. (***Figure 39***)

Figure 39

9.6.2.2 *Running macros on controller start-up*

1. Open the macros panel.
2. Double-click the macro.
3. Tick 'Run at Controller Startup'.
4. Save ( ) the macro and close the dialog.

9.6.3 Creating a new macro

1. Open the macros panel.
2. Click Add New in the Macro panel.
3. The properties window will appear with the usual basic options on the left side.
4. Tick 'Run at Controller Startup' if you need the macro to run once the controller is online.

To add a new statements to macros

- Click the Add button.

To remove a statements from macros

- Click on the statement you want to remove followed by the Remove button.

To relocate statements within macros

- Click the statement you want moved followed by the Move Up or Move Down button.

5. Save ( ) the macro and close the dialog.

9.6.4 Statements

Each macro consists of one or many statements. At the very least an expression will have a type and a comment. Each statement must be one of the following types:

Statement type	Description
`Do an Action`	`Perform the defined action.`

Statement type	Description
Do an Action when the Expression Changes…	When this statement is evaluated for the first time it will perform the defined action. Every time the statement is evaluated after this, the defined action will only be performed if the result of the expression has changed.
Goto <label> if…	Go to a label defined elsewhere within the macro if an expression is true.
Pause for Time…	Suspend further execution of the macro for $n \times 100\text{ms}$.
Define a Label	A placeholder within a macro that execution can carry over to.
Set Entity To Expression…	Set an input to a specific count or analogue value.
Wait for Condition…	Further execution is suspended until the defined condition is met.
Execute Modified Action…	Perform the defined action using the values of entities to control the variables of the selected action.
End Current Macro	Terminates the macro.

9.6.5 Execute Modified Action…

This is a complex and powerful macro statement type. As described above, 'Execute Modified Action…' will perform the defined action using the values of entities to control the variables of the selected action.

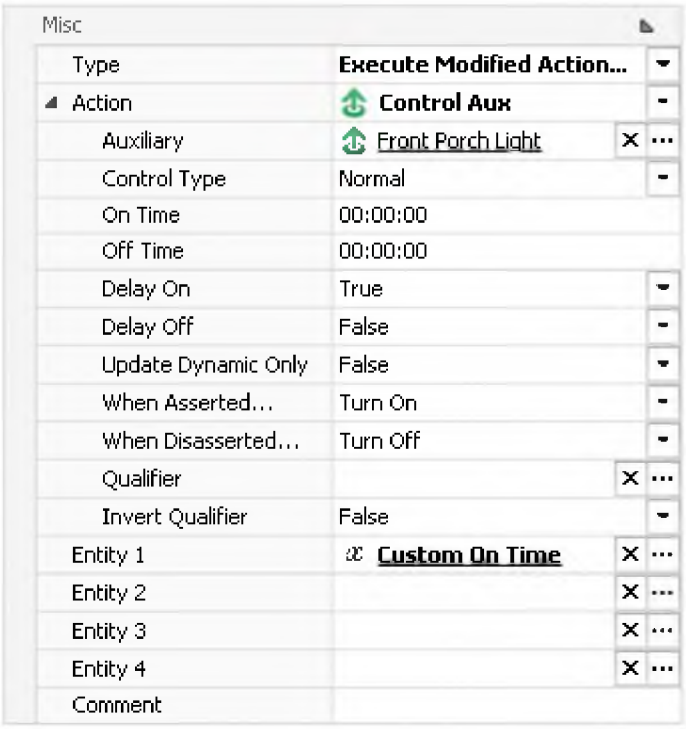


Figure 40

Entities are associated with the variables of the selected action. In *Figure 40* there are two variables for the selected action (Control Aux). On Time will be controlled by the value of the global variable 'Custom On Time'. Off Time could be controlled by the value of Entity 2 (If set).

Control Aux & Control Aux List

- Entity 1 will control the On Time
- Entity 2 will control the Off Time

Control Door & Control Door List

- Entity 1 will control the Door Unlock Time

Trigger Input

- Entity 1 will control the Desired Global State
  - 0 All states sealed
  - 1 Alarm
  - 2 Sensor Mask
  - 3 Sensor Orientation
  - 4 Sensor Fault
  - 5 Sensor Range
  - 6 Tamper Low (e.g. short circuit)
  - 7 Tamper High (e.g. open circuit)
  - 8 General Tamper (e.g. Cabinet tamper)
  - 9 Zone self test fail
  - 10 Low battery
  - 11 Encryption fail on encrypted link
  - 12 Poll fail
  - 14 Input is in "soaking test"
  - 15 Input has failed a soak test

16 Input is isolated

Set Input Counters

- Entity 1 will control the Count value

Control Siren

- Entity 1 will control the Siren Time (value is multiples of 100ms)
- Entity 2 will control the Tone

9.6.6 Macro Expressions

Macro Expressions are represented as infix notation strings and have support for bracketing and operator precedence. They can include numeric constants (entered as decimal numbers) and entity references (entered in standard Inner Range address notation)

As with all things in Integriti, when an entity is evaluated in an expression it can have either an analogue (numeric) or Boolean value. The type used by a particular expression is chosen automatically by the controller based on context.

A few examples of valid macro expressions:

`"D03 && D05"` = Both Door 3 and 5 are unlocked.

`"C01:X01 > 55"` = C01:X01 has an analogue value greater than 55.

`"C01:X01 > C01:X02"` = C01:X01 is greater than C01:X02.

Expressions are not sensitive to whitespace, so the expression `"((5+3)/7>C01:X01)&&D01"` is interpreted identically to `"( (5 + 3) / 7 > C01:X01) && D01"`.

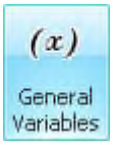
There are two special zone value modifiers. The 'hash' (**#**) modifier can be used to test the count value of an input entity. The 'at' (**@**) modifier can be used to test the analogue value of an input entity. To use the modifiers, place either one before the entity to be evaluated in the macro statement.

Example usage – Test the input count is above 5: `"#C01:Z01>5"`.

The following table is a list of all operators, in order of precedence.

Operator	Name	Arguments	Argument Type	Return Type
!	NOT	1	Boolean	Boolean
*	Multiply	2	Numeric	Numeric
/	Divide	2	Numeric	Numeric
+	Plus	2	Numeric	Numeric
-	Minus	2	Numeric	Numeric
<<	Shift Left	2	Numeric	Numeric
>>	Shift Right	2	Numeric	Numeric
<	Less Than	2	Numeric	Boolean
<=	Less Or Equal	2	Numeric	Boolean
>	Greater Than	2	Numeric	Boolean
>=	Greater Or Equal	2	Numeric	Boolean
==	Equal	2	Numeric or Boolean	Boolean
&	Bitwise AND	2	Numeric	Numeric
^	Bitwise XOR	2	Numeric	Numeric
|	Bitwise OR	2	Numeric	Numeric
&&	Logical AND	2	Boolean	Boolean
||	Logical OR	2	Boolean	Boolean

9.7 General Variables



The general variables panel is accessible from the 

tab.

General variables are used to store values for a number of applications. Values are assigned by other entities such as inputs, macros or named actions.

To create a General Variable:

1. Click the 

button in the General Variable panel.
2. The properties window will appear with the usual basic options on the left side.
3. The only property that can be set is the optional test value.

The test value is used to determine whether the general variable evaluates to true or false when tested in a logic statement.

For example:

The general variable has been assigned a test value of 50.

- If the general variable is equal to 50 or less, the general variable when tested will return false.
- If the general variable is equal to 51 or greater, the general variable when tested will return true.

9.8 General Timers

The general timers panel is accessible from the Automation tab.

General timers are used similarly to general variables. You can use another entity such as an input, macro or named action to set its value. The general timer will count back down to 0. The timer counts down every 100ms. When counting down, the general timer will be in an invalid state. When the general timer reaches 0 it will be in a valid state. General timers do not automatically restart.

To create a General Timer:

1. Click the Add New button in the General Variable panel.
2. The properties window will appear with the usual basic options on the left side.
3. Simply give the general timer a name, save the record and close.

10 Hardware and LAN management

Once Integriti hardware has been installed and is running, the next thing you will need to do is enrol controllers. Integriti controllers can be added (enrolled) either manually or automatically to the Integriti server.

If you are connecting a controller over the internet or between networks, you will need to ensure that TCP port 4711 is forwarded to the Integriti Controller Server.

10.1 Controller configuration

Before enrolling a controller, you will need to ensure it has been appropriately configured for the network it has been attached to.

Determining what IP address was given to an Integriti controller:

This procedure assumes the controller is connected to a LAN with a DHCP server and a terminal is attached to the device bus with its address set to 1.

If you can't determine if there is a DHCP server present on the network, follow this procedure through to step 7. If the displayed IP address is `0.0.0.0`, the controller was not issued with an IP address. Follow the procedure '*Manually assigning an IP address of the Integriti controller*' below.

1. After performing the pre-power up checks, turn the Integriti controller on.
2. Wait for the controller to start. When the controller is up and running, the Status 1 and Status 2 LEDs will flash in an alternating pattern (***Figure 41***).

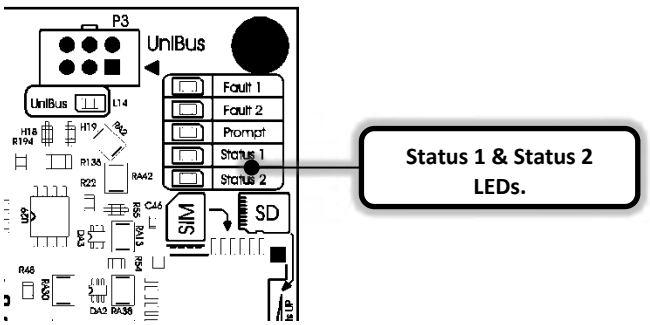


Figure 41

3. Log in to the terminal by pressing: **[0], [1], [Ok]**
4. Go in to controller information by pressing: **[Menu], [1], [9]**
5. Press **[▼]** once to display the controller serial number.
6. Press **[▼]** once more to display the controller MAC address.
7. Press **[▼]** two more times to reveal the controller IP address. (assuming the controller is connected to a network and a DHCP server has assigned an IP address to the controller)

Manually assigning an IP address of the Integriti controller:

This procedure assumes the controller is connected to a LAN without a DHCP server and a terminal is attached to the device bus with its address set to 1.

1. After performing the pre-power up checks, turn the Integriti controller on.
2. Wait for the controller to start. When the controller is up and running, the Status 1 and Status 2 LEDs will flash in an alternating pattern (*Figure 41 above*).
3. Log in to the terminal by pressing: **[0], [1], [Ok]**
4. Go in to controller NIC configuration by pressing: **[Menu], [7], [3], [4]**
5. Press **[Ok]** once to configure NIC01.
6. Enter in the desired IP address for the Integriti controller followed by **[Ok]**.
7. Enter in the subnet mask followed by **[Ok]**.
8. Enter in the gateway address (if required) followed by **[Ok]**.
9. Enter in the primary DNS address (if required) followed by **[Ok]**.
10. Enter in the secondary DNS address (if required) followed by **[Ok]**.
11. The controller is configured to use DHCP by default. Press **[5]** to disable DHCP.

10.2 Enrolling controllers

Integriti controllers can connect to Integriti Controller Servers via Ethernet, USB or Modem. Ethernet connectivity can be direct or with the aid of the Inner Range SkyTunnel service.

With the exception of USB, at some point during the enrolment procedure you will need to decide how the data synchronisation is handled. Selecting a data synchronisation method will determine whether the data on the server or the data on the controller will take precedence in the event of a clash. When an entity within the controller does not match the corresponding entity in the Integriti server, one of the three options will occur:

Merge Changes –

Differences between the Software and Controller databases are merged, such that both the controller and server have a consistent database containing all programmed records. If there is a conflict on a particular record, the record from the Software will overwrite the record in the Controller.

This mode is suitable for single controller installations or installations where keypad programming is desired.

Disallow Changes From Controller –

All global entities in the Controller database are overwritten with the records from the Software database. This mode will NOT allow changes to global entities to be made via the keypad.

This mode is suitable for multi-controller installations where the system is centrally managed using the Integriti Pro Management Software.

Prefer Controller Changes –

Differences between the Software and Controller databases are merged, however records from the Controller database will overwrite records in the Software database.

This mode is suitable for situations where the only copy of the system programming is currently held within the controller and you wish to retrieve it.

If you are unsure about what option you should select, leave the default (recommended) setting- ' Prefer Controller Changes'.

10.2.1 Automatic controller discovery (Method 1)

The simplest method of adding controllers to Integriti is by using the 'Auto Discover new Controllers…' feature. This feature will only work if the controller is on the same subnet.

Please note that Automatic controller discovery can only work across the local network. To connect to controllers over the internet, see Method 4.

To access this feature, click on the Home tab followed by the Connect New Controller button (*Figure 42*).

Figure 42

The 'Connect to Controller' window will appear.

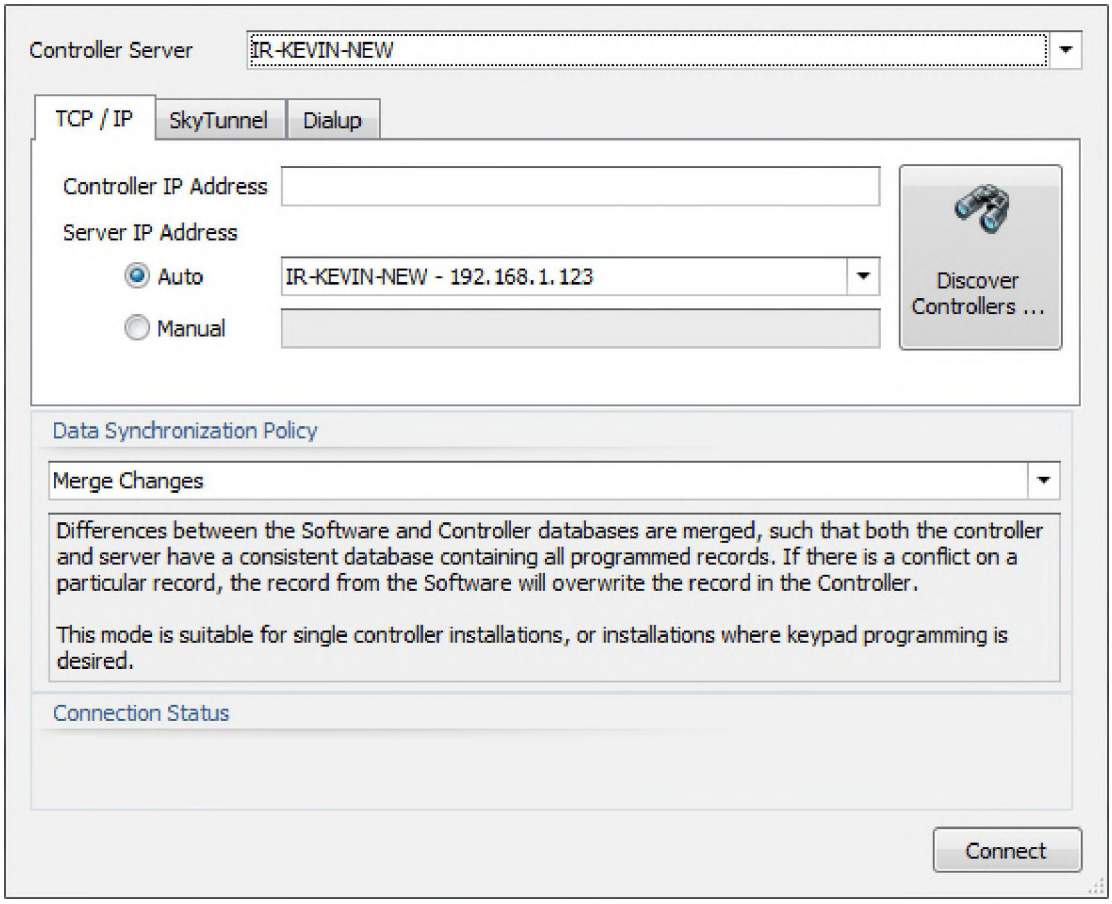


Figure 43

Click on the 

button and the 'Discover Controllers' window will appear. Automatic controller discovery will begin (*Figure 44*).

When the automatic controller discovery has completed the Integriti controllers will be listed in the upper section (Discovered Controllers) of the window (*Figure 44*).

The automatic controller discovery progress is displayed as a green progress bar to the right of the Integriti server under 'Scan Status'.

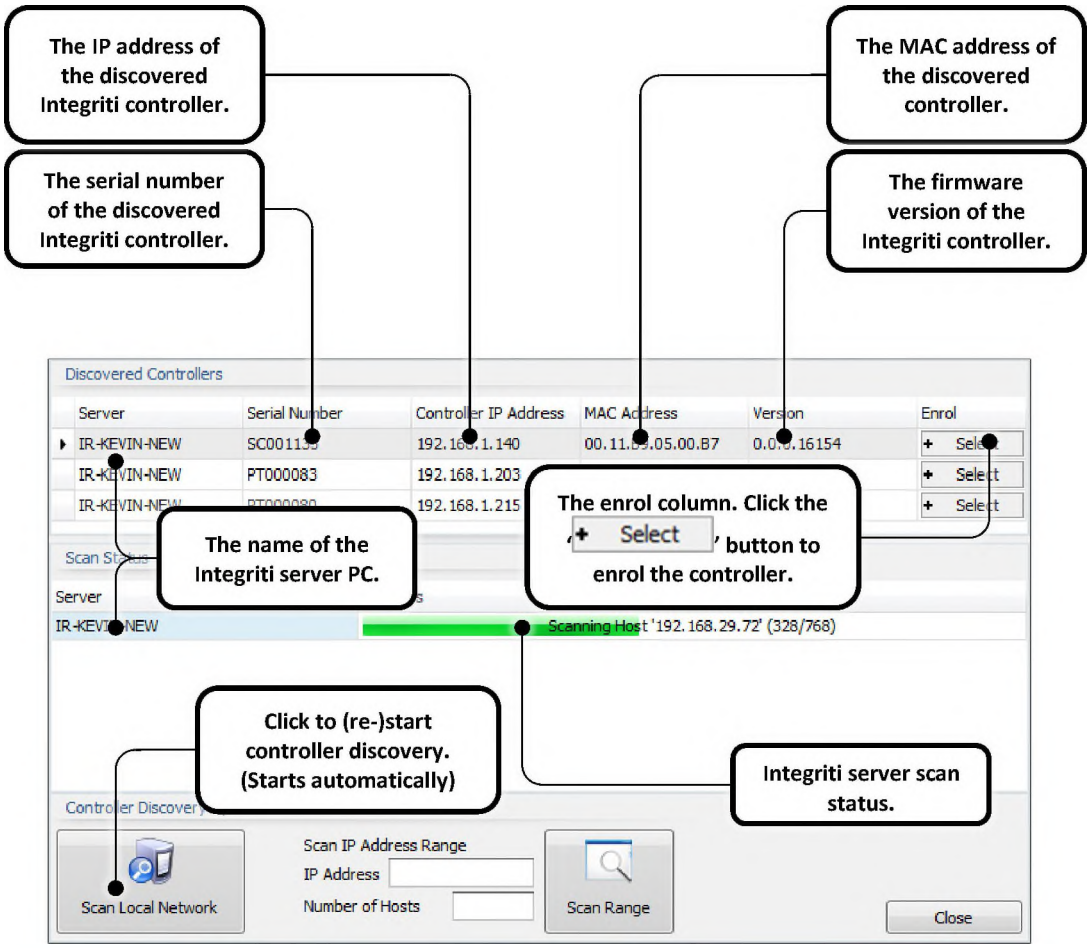


Figure 44

Each individual controller has its own unique serial number. The serial number and MAC address are printed on a label which is placed on the Integriti controller during production.

You can enrol controllers as soon as they appear in the 'Discovered Controllers' list. Simply click the Select button to go back to the 'Connect to Controller' window (*Figure 45*).

There is no limit on the number of controllers you can enrol simultaneously. As soon as the controller is visible, you can begin enrolment.

Discovered controllers with a greyed out enrol button (Select) are controllers that have already been enrolled.

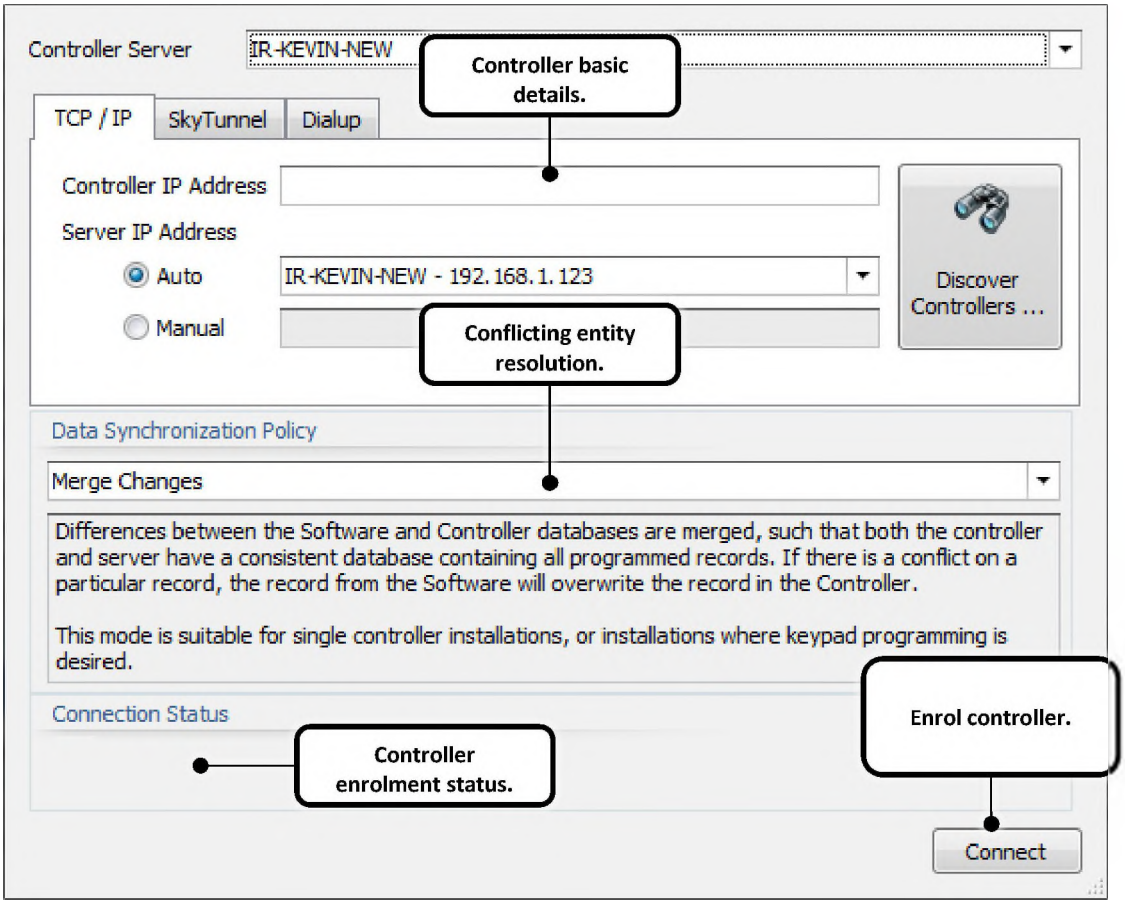
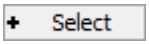


Figure 45

After clicking the 

button, there is only one item that requires your attention before starting the enrolment process. You will need to select one of the three Data Synchronisation Policy options. See 'Enrolling controllers' (***above***) for detail on the synchronisation options available.

When you are ready to enrol the controller, click the 

button.

10.2.2 Manual controller enrolment (Method 2)

Please note that there is no need for any port forwarding on the controller side.

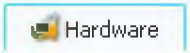
To manually enrol a controller, use the following procedure:

LCD Terminal specific instructions:

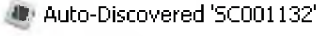
1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to controller communications task programming: **[Menu], [7], [3], [1]**
3. Configure communications task `CT01`: **[Ok], [9], [Ok]**
4. Select '`Integriti CT`' as the communications task type: **[▶], [▶], [Ok]**
5. Enter the exposed IP address of the server followed by **[Ok]**.
   - Values less than 3 digits should be entered with leading zeros.
6. Enter the Port used to connect to the server: **[0], [0], [4], [7], [1], [1], [Ok]**
7. Skip the DNS option: **[Ok]**
8. Set the encryption method to `AES128`: **[▶], [Ok]**
9. Enable `P` under the Gip options: **[▶], [▶], [▶], [▶], [▶], [▶], [▶], [9], [Ok]**
10. Leave the site fields blank: **[Ok], [Ok]**
11. Leave the GUID fields blank: **[Off], [Ok], [Off], [Ok]**
12. Leave the telephone number fields blank: **[Ok], [Ok]**
13. Select `Ethernet` for `Priority 1`: **[▶], [▶], [Ok]**
14. Skip the remaining priority options: **[Ok], [Ok], [Ok]**
15. Enable the `C` and `A` options: **[▶], [▶], [▶], [▶], [▶], [▶], [9], [9], [Ok]**
16. Skip the remaining `C` and `A` options: **[Ok], [Ok], [Ok]**
17. Skip the `Imodem` and `Emodem` options: **[Ok], [Ok], [Ok], [Ok]**
18. Enable the communications task and log out: **[9], [End]**

Software specific instructions:

1. Click on the 

button under the 

tab.
2. The Controller panel should appear.
3. In the controller panel, the configured controller should appear automatically in the list of controllers as 'Auto-Discovered'.



   - If the controller does not appear in the list, check the following:
     i. Double-check your NIC and Comms Task programming options.
     ii. Check / update your licenses.
     iii. Verify the 'IR Integriti Controller Server' service is running.
     iv. Check your network configuration, firewall, port forwarding…

4. Select the auto-discovered controller and click Edit.
5. Change the name of the controller to something more appropriate.

Module Details

6. Under module details, expand out the Inputs group.
7. Click on the ellipsis ... to the right of each EOL configuration option and select Concept3K

Connection Details

8. The connection configuration changes required have been highlighted below:

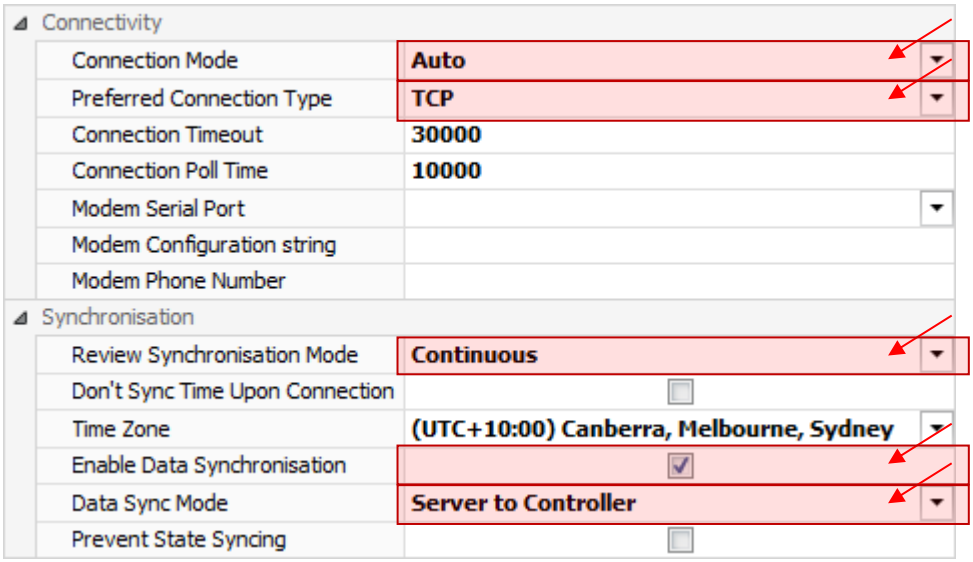


Figure 46

9. Click the button and close the window.
10. An icon ( ) should appear to the right of the controller in the Hardware panel indicating that the server is synchronising with the Integriti controller.

10.2.3 Controller enrolment using the SkyTunnel service (Method 3)

Inner Range has provided a service where controllers can be connected to the Integriti controller server provided there is internet connectivity at both ends.

To make use of this service, the controller must be configured to connect to the SkyTunnel service before the Integriti server can enrol it.

To connect a controller to the SkyTunnel service:

LCD Terminal specific instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to the SkyTunnel communications task quick start: **[Menu], [8], [0]**
3. Start the SkyTunnel communication task: **[On]**
4. Write down the 8 digit password provided.
5. Log off: **[End]**

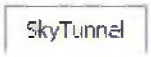
If you are using Integriti CS, you will need to change the Installer PIN code or create a new user with a PIN code other than 01. To do this, follow these instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to user programming: **[Menu], [2], [1]**
3. Edit the Installer user: **[Ok]**
4. Change the user PIN: **[Ok], [Ok],** *{enter a 2 to 8 digit PIN}*
5. Log off: **[End]**

To enrol a controller connected to the SkyTunnel service from the System Designer:

1. Click on the 

button under the 

tab.
2. The 'Connect to Controller' window should appear.
3. Click on the 

tab and enter the serial number of the controller in the 'Controller S/N' field provided.
4. Enter the randomly generated 8 digit password from the procedure above in the Sky Tunnel Password field.
5. Select the synchronisation method from the drop down list box. See 'Enrolling controllers' (***above***) for more detail.
6. Select either Server Authentication or User Login to connect to the controller.

10.2.4 Connecting directly to a controller using USB (Method 4)

Connecting to a controller using USB is very simple. After logging in to System Designer, connect your controller to an available USB port on the server. On the PC, you should notice the driver for the controller being installed automatically. Shortly after, the controller should appear under the 'Default' site as an 'Auto-Discovered' controller.

10.2.5 Connecting to a controller using a modem (Method 5)

In circumstances where any of the connection methods above cannot be achieved, controller connections using a dialler has been made available.

To configure the controller for a dialler connection:

LCD Terminal specific instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to controller module programming: **[Menu], [7], [2], [0], [1]**
3. Change the number of rings to answer: **[◄], [0], [0], [0], [0], [6], [Ok]**

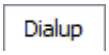
- If you are using 'User Login' to authenticate with the controller, follow the remainder of this procedure.

4. Go in to user programming: **[Menu], [2], [1]**
5. Edit the Installer user: **[Ok]**
6. Change the user PIN: **[Ok], [Ok]**, *{enter a 2 to 8 digit PIN}*
7. Log off: **[End]**

To enrol a controller connected via dialler from the System Designer:

1. Click on the 

button under the 

tab.
2. The Connect to Controller window should appear.
3. Click on the 

tab.
4. Select the communications port that the modem is connected to.
5. Enter the telephone number of the controller.
6. If required for your specific make/model of modem, enter an initialisation string.
7. Select the synchronisation method from the drop down list box. See 'Enrolling controllers' (***above***) for more detail.
8. Select either Server Authentication or User Login to connect to the controller.

10.3 Maintaining Firmware

Controller and module firmware can be managed easily via the Integriti firmware manager under the 

tab.

Click 

to open the update manager (***Figure 47***).

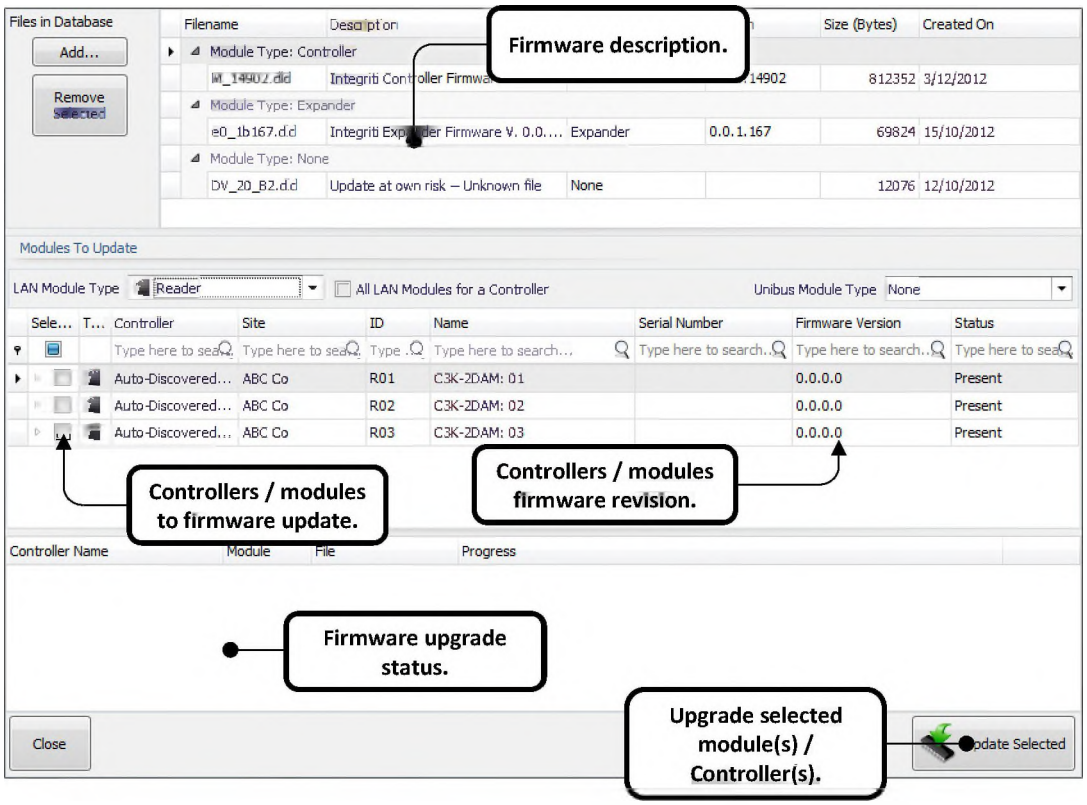
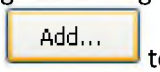


Figure 47

The available firmware list at the top of the window will display all of the firmware files you add to the update manager.
If you select a firmware file in the update manager you will see the list of modules to update change according to the type of firmware file selected.

Click 

to add new firmware revisions to the update manager.

Updated firmware files are made available to qualified installers from time to time via the Inner Range support website.

The firmware upgrade status will indicate the progress of each individual controller / module being upgraded. The process is completed when the controller / module has come back online.

10.3.1 Upgrading module & controller firmware

1. Select the firmware revision you want to upgrade to from the list at the top of the update manager.
2. Select one or many controllers/modules from the modules to update list by ticking the appropriate check box(es).
3. Click 

.

The time it takes to upgrade the firmware of a particular module or controller will vary depending on connectivity to the Integriti server. Please allow up to 30 minutes for the upgrade process to complete.

We recommend stopping, re-starting and testing communications tasks after controller firmware upgrades.

10.4 Module Programming

It is recommended that the Integriti controller LAN remains locked during normal operation. This will prevent the addition of new modules and the possibility of foreign modules interfering with the existing infrastructure.

To access the controller LAN settings, right-click the controller in the navigation panel:

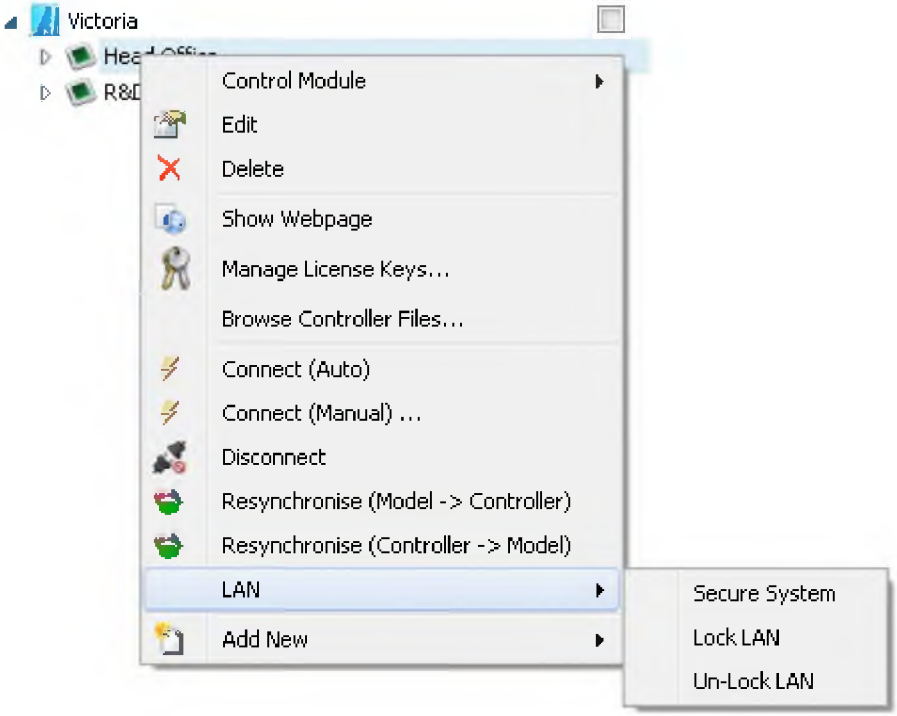


Figure 48

Secure System

Securing the LAN will send out a secure flag to all of the modules currently connected to the controller. The modules will remain secure until the next time the LAN is secured.

Modules that are not secured will have the status: "`Present (Unsecured)`". This usually occurs when a module has been attached to the LAN after secure system has been selected.

Lock LAN

Locking the LAN prevents any newly attached module from connecting to the Integriti controller. Modules that are not present at the time the LAN was locked will be ignored by the controller. The controller will log the presence of any foreign modules. This excludes new UniBus devices being attached to existing LAN modules.

Un-Lock LAN

Unlocking the LAN is required before adding new modules to the Integriti controller.

10.4.1 Adding New Modules

Once a module has been attached to the Integriti LAN, the controller will detect the presence of the module and it will appear under the controller in the site navigation panel.

10.4.2 Deleting Modules

To remove and delete a module from an Integriti controller simply right-click the module and select 

.

11 CCTV

Integriti integrates with a large number of video surveillance products. Support for products is provided as a plugin installer. The plugin must be installed separately on the Integriti server and any clients that will be used to view images provided by the integrated device.

11.1 Installing Insight DVR plugins

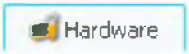
The Integriti software management suite can be used with Insight DVR plugins. Installing and using these plugins requires a slight change to the install procedure.

To install Insight Professional DVR plugins for use with Integriti:

- Stop all Integriti services.
- Run the Insight DVR plugin installer and continue through until you get to the "Select Destination Location" dialog.
- Change the destination folder from the default to your Integriti installation folder. Typically this path is "`C:\Program Files\Inner Range\Integriti Pro\`" on a Windows 7 64bit platform.
- Complete the installation.
- Start all Integriti services.

If you click the browse button to select the destination folder location when installing Insight Professional DVR plugins, '`\Insight`' will be appended to the destination folder. You will need to remove this to continue.

11.2 Enrolling video systems

1. Click on the 

tab followed by 

.
2. Select the DVR plugin from the list in the new dialog that appears and click 

.

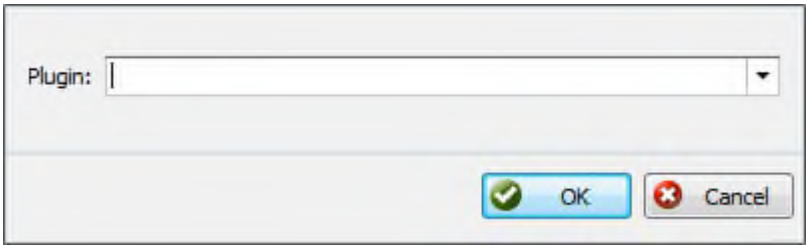


Figure 49

3. Enter the necessary connection settings for the plugin. These settings will vary from plugin to plugin but will mostly consist of an IP address, User name and Password.

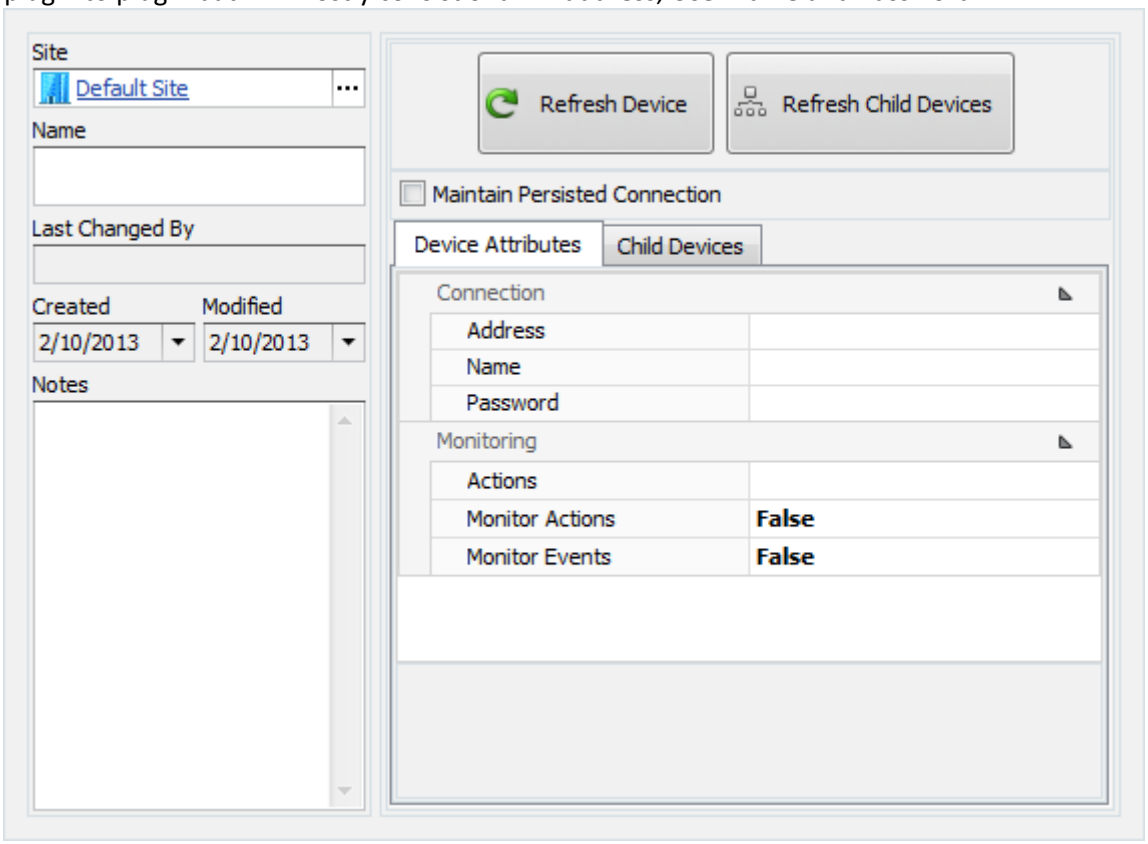
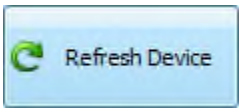


Figure 50

4. If available, click the 

and 

buttons to ensure the actions, cameras and/or any other devices are detected and enrolled accordingly.
5. The option Maintain Persisted Connection is only required for situations where messages are sent and/or received from the device.
6. Save and close the editor window for the CCTV Recorder.

11.3 CCTV camera configuration

Once a video system has been enrolled, not all of the cameras may be required. Enabled cameras take up camera licenses.

Disabling CCTV cameras...

1. Click on the 

tab followed by 

.
2. Double-click a CCTV Camera to disable. The Editor Window for the CCTV Camera should appear.
3. On the right-hand side, click on Disable Device.
4. Save and close the editor window for the CCTV Camera.

11.4 Associating cameras with entities

By associating cameras with entities, operators can play back archived video from CCTV Recorders when review events are generated for the entity.

Associating cameras with entities ...

1. Click on the 

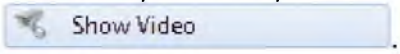
tab followed by 

.
2. Double-click a Camera to associate entities to. The Editor Window for the Camera should appear.
3. On the right-hand side under 

, click on the 

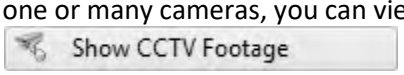
button.
4. From the window that appears, select the entity to associate with the Camera.
5. Save and close the window.

11.5 Viewing associated video from associated entities

If an entity has been associated with one or many cameras, you can view live video by right-clicking the entity and selecting 

.
Live feeds will appear for all cameras associated with the entity.

11.6 Viewing associated video with review

If an entity has been associated with one or many cameras, you can view archived video by right clicking the entity and selecting 

from review or filter windows.

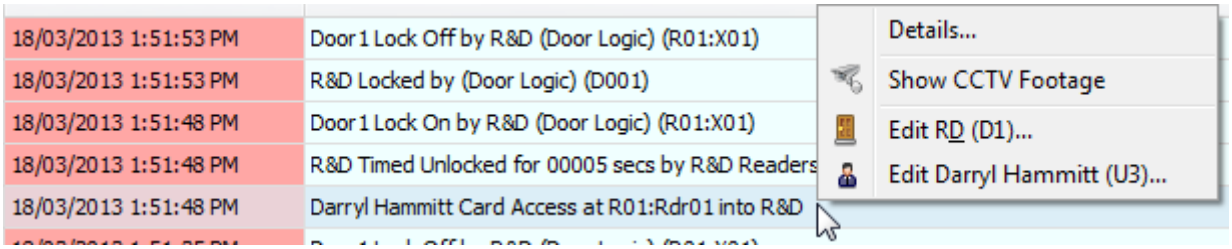


Figure 51

If more than one CCTV Camera has been associated with the one entity, clicking 

will open a panel with a camera matrix.

The video will begin playback from the time that the entity appeared in review.

11.7 Viewing video from schematics

You can view video from a schematic using one of two methods:

1. Right-click an icon used to represent a camera and click on Show Video

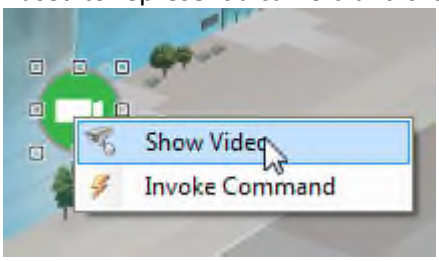


Figure 52

2. Click on an icon used to represent a camera then click on Show Video in the Commands toolbox.

Figure 53

12 Photo ID

Photo ID allows you to create Photo ID designs and print identification tags and badges for Users (employees, contractors, visitors, etc…)

The Photo ID designer features include rotation and flipping of images, creation of various arbitrary shapes, object alpha, support for double sided cards, barcodes, user photos and custom field images.

There is no restriction on the number of designs or design dimensions. Photo ID designs can be any one of a number of standard formats or user defined.

Printing ID cards is a two step process. First, you must create a Photo ID Design. Photo ID provides simple tools which allow you to customise the design by inserting the required graphics and fields into the card design and defining what fonts and colours will be used.

You can create and save as many different deigns as you like, each with a different layout. Designs may include images, simple graphics, text and user database information such as user names, company details and photos.

Once a design has been created, it can be used to print a batch of Users. To print designs, you first select the users who will be issued with the new Photo ID Design, then issue the print command from the context menu.

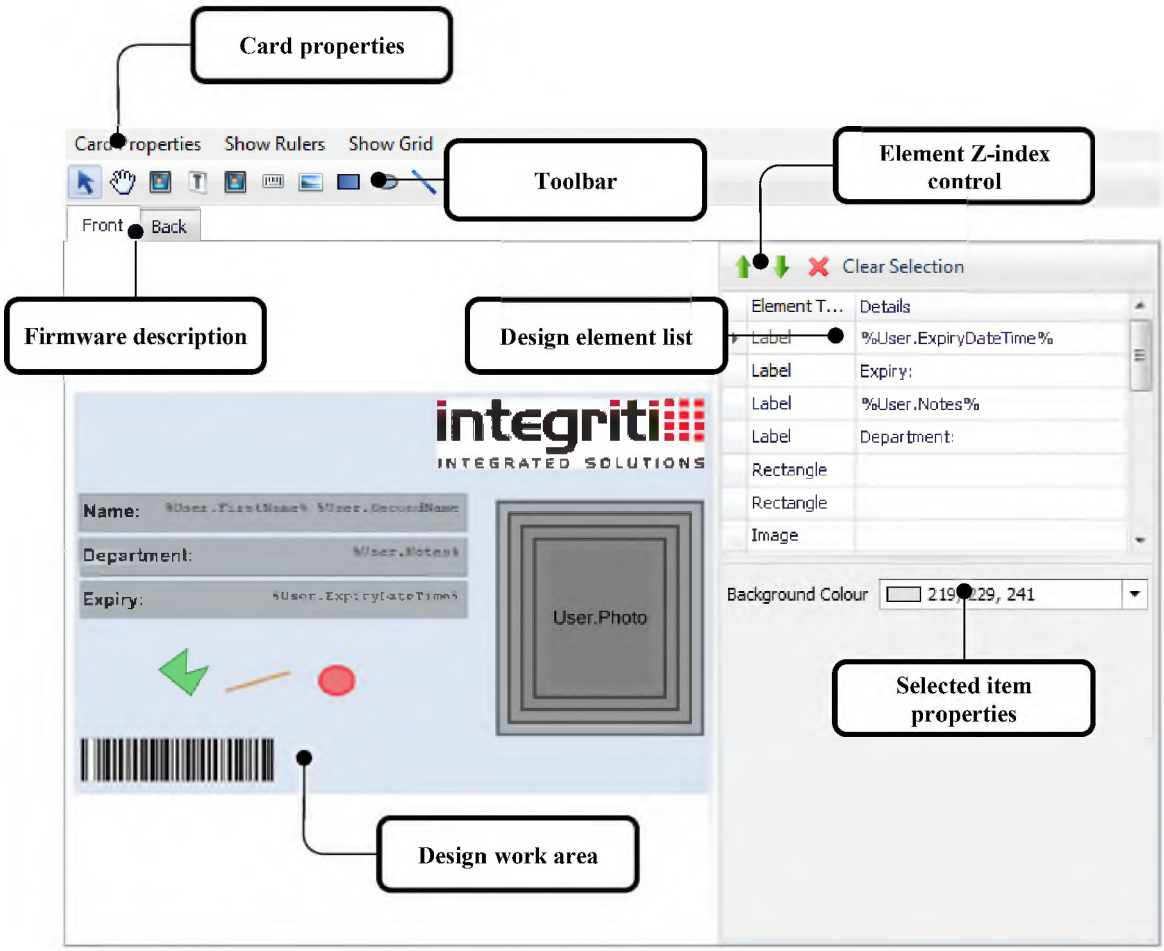
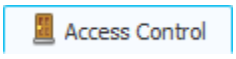


Figure 54

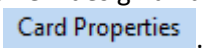
12.1 Creating a Photo ID Design

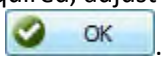
To create a Photo ID Design…

1. Open the 

panel from the 

tab.
2. Click the 

button to create a new Photo ID Design.
3. Give the new design a name and enter a description in the notes field.
4. Click on 

.
5. Specify whether the design will be single or double sided.
6. Select the card orientation.
7. Specify the card measurement units.
8. Select the physical dimension standard or custom from the Card Type drop-down list.
    a. If custom was selected, specify the Width and Height.
9. If required, adjust the DPI.
10. Click 

.
11. Place items on the design area.
12. Select an item from the toolbar.
    a. Click and drag in the design area to place a new design element.
    b. Adjust the placement of the newly placed design element by adjusting the element handles.
    c. Tweak the display element further by modifying the element properties to the right.
13. Continue creating items as required.
14. Save and close the editor window for the Photo ID design.

13 Schematics & Element Presenters

Schematic allows operators to monitor status and control entities via an intuitive interface based around graphical floor plans, site maps and mimic panels. Special items can be placed on each diagram that indicate the status of various entities such as inputs, areas and auxiliaries in real time.

Schematic can be used to:

- Import site plans
- Navigate between maps / diagrams
- Add entities to maps / diagrams
- Monitor site activity in real time
- View and acknowledge alarms
- Control items
- View video from associated CCTV sources.

Schematic maps, mimic panels and similar graphical interfaces are created using the Integriti System Designer. Schematic maps can then be viewed in either Gate Keeper or System Designer.

Items placed on the schematic are called map elements. Map elements are optionally linked to entities. These can either be icon based, or be drawn as shapes.

Map elements can be used to highlight items on the schematic or indicate the state of entities.

Map elements do not update when you are modifying or creating a schematic map.

Supported image formats used throughout Integriti:

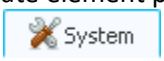
- BMP
- JPG
- GIF
- PNG

13.1 Element Presenters

A presenter is a collection of format settings and rules that govern how a map item will behave on the schematic. Presenters can only be assigned to a schematic map item if it is linked to an entity.

A significant number of element presenters with a common theme exist by default within the Integriti system, but there are occasions where the customer wants something a little more specific to their particular installation. Integriti includes the ability to create new presenters.

To create element presenters, click on the 

button in the Schematics group under the 

tab.

Click on the 

button to create a new element presenter.

Often, it is desirable to create a new element presenter, based on an existing one (we do not suggest editing default presenters as these may be over-written during software updates). To achieve this, right click on the presenter on which you wish to base a new presenter, select "Duplicate" and change the name, then edit the new presenter.

Double-click an existing element presenter to edit it.

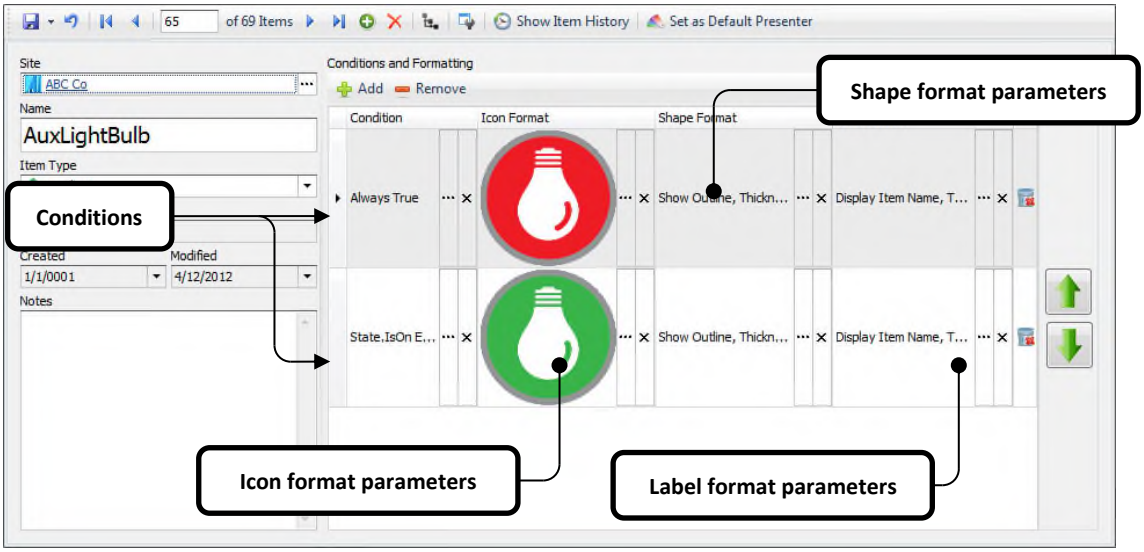


Figure 55

13.1.1 Condition

The condition under which the Icon, Shape or Label format will change to the values specified.

Clicking on the ... button will open the presenter rule/condition for editing.

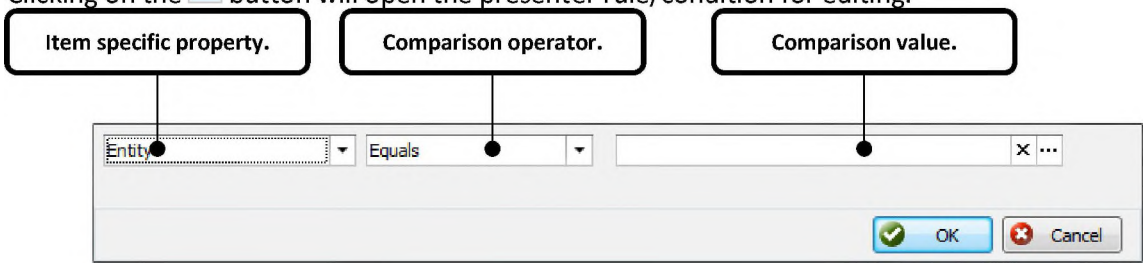


Figure 56

Depending on the selected item type of the presenter, options in the presenter rule editor will vary.

Examples of item specific properties for a door are:

- Is On
- Summary
- Last Updated
- Extended Status
- Entity

If a number of conditions are met, the icon shape or label format associated with the last (bottom-most) condition in the list is used. Because of this, it is often desirable to have, as the very topmost condition in the list, an “Always True” condition which will be displayed when none of the other conditions are met.

13.1.2 Icon Format

From here you can select an image for the specific condition.

Clicking on the ... button will open the icon format window.

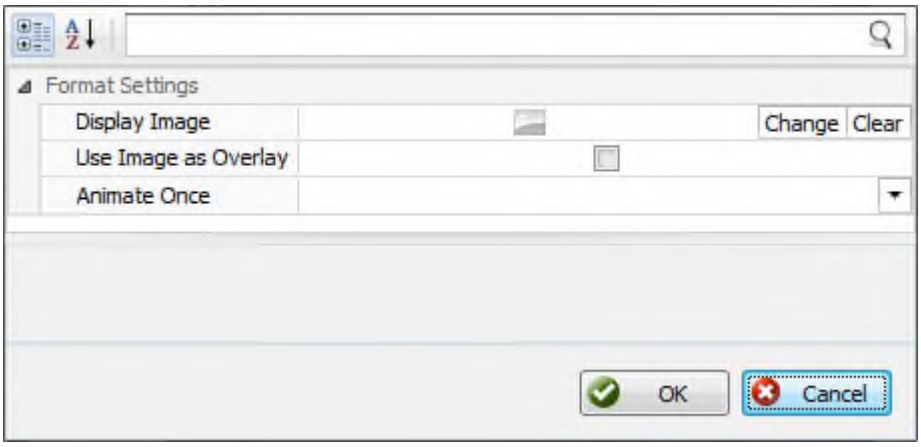


Figure 57

Click Change to select the desired image.

If the image is to be used to overlay other images of the element presenter, check the 'Use Image as Overlay' checkbox.

If the selected image is an animated GIF, you can change the 'Animate Once' to True to play the animation once or False to loop the animation.

13.1.3 Shape Format

Figure 58

13.1.3.1 Show outline

Default value: True

Setting this option to False will disable the outline of the item.

13.1.3.2 Outline Thickness

Default value: 5 pixels

The value specified here will determine the thickness of the border / outline. A value of 0 will leave a 1 pixel border.

13.1.3.3 Opacity 0-255

Default value: 128 (semi-transparent)

The opacity affects both the Interior and outline colour. Use a value of 255 for opaque and a value of 0 for transparent.

13.1.3.4 Interior colour:

Default value: Grey (128,128,128)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255`	Blue
`255,0,0`	Red
`0,255,0`	Green
`0,255,255`	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

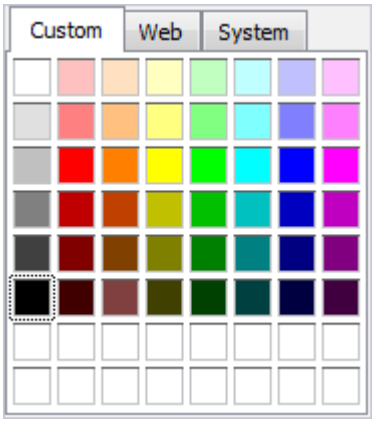


Figure 59

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

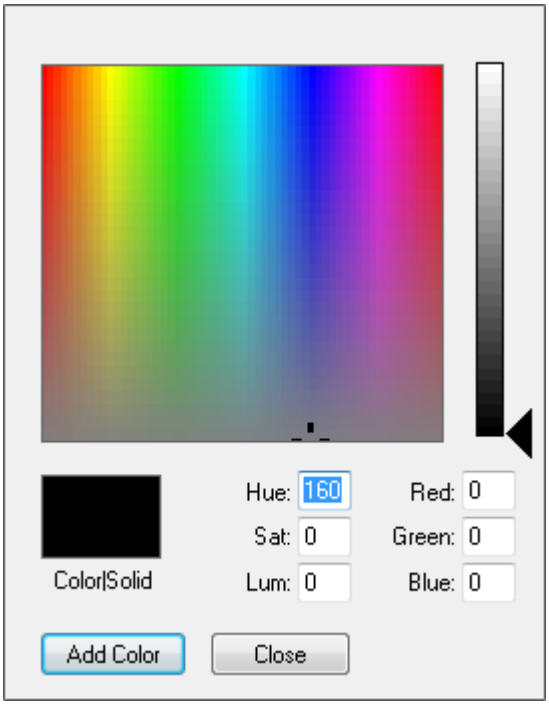


Figure 60

13.1.3.5 Outline color

Default value: Black (0,0,0)

The value specified here determines the colour of the outline/border surrounding the schematic map item.

If the border is transparent, only the opacity setting will affect the specified border width of the map item.

Example:

- Interior color – `Web -> Cyan`
- Opacity – `128`
- Outline color – `Web -> Transparent`
- Outline Thickness – `5`
- Show Outline – `True`

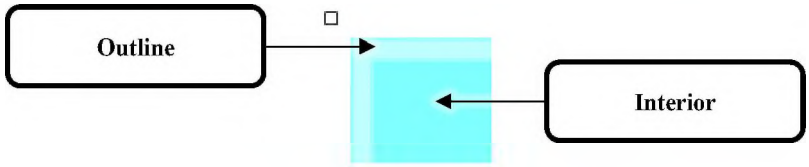


Figure 61

13.1.4 Label Format

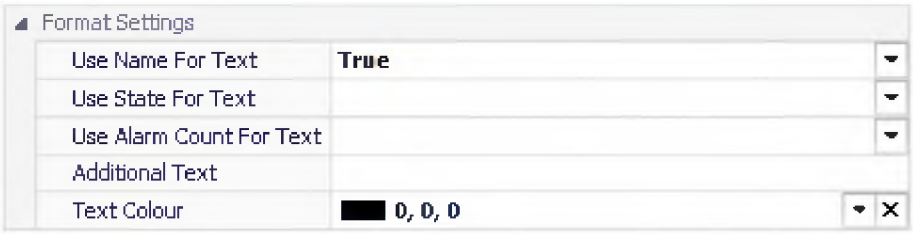


Figure 62

13.1.4.1 Use Name For Text

Default value: True

When set to True, the name of the item associated with the presenter will be displayed.

When set to False, the name of the item associated with the presenter will not be displayed.

13.1.4.2 Use State For Text

Default value: (Blank)

When set to True, the state of the item associated with the presenter will be displayed.
When set to False, the state of the item associated with the presenter will not be displayed.

13.1.4.3 Use Alarm Count For Text

Default value: (Blank)

When set to True, the alarm count of the item associated with the presenter will be displayed.
When set to False, the alarm count of the item associated with the presenter will not be displayed.
If the item associated with the presenter does not have an alarm count, setting this option has no effect.

13.1.4.4 Additional Text

Default value: (Blank)

Text entered in this field is appended to the end of the label for the associated map item. The text will be separated by a hyphen.

13.1.4.5 Text colour:

Default value: Black (0,0,0)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255` Blue 

255,0,0	Red
0,255,0	Green
0,255,255	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

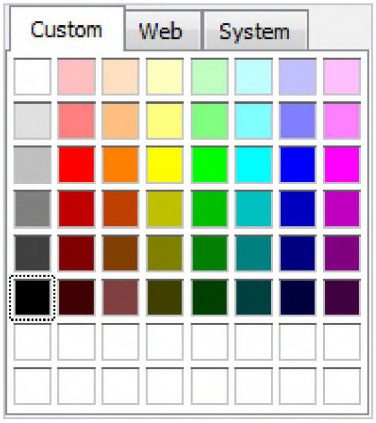


Figure 63

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

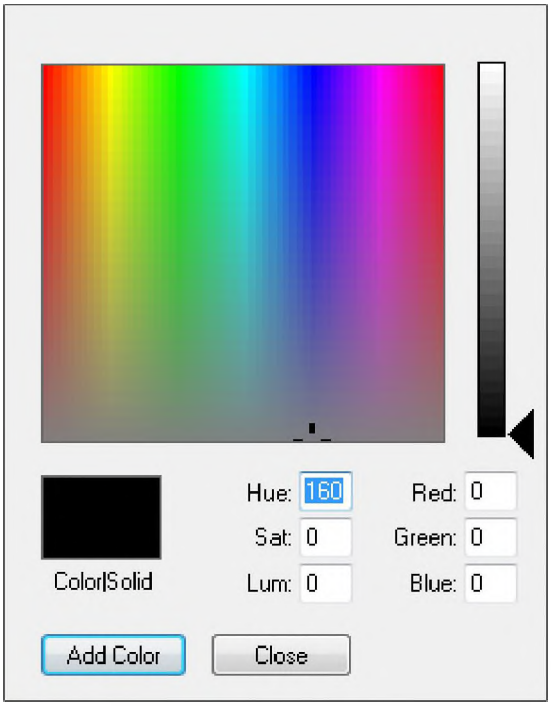


Figure 64

13.2 Configuration of Schematic Maps

Schematic maps are created, modified and removed through the Integriti System Designer. Schematic maps are found in the Schematics group under the System tab. Click the Schematic Maps button to open the schematic maps panel.

1. Click on Add New to open the schematic map designer.

To modify an existing schematic map:

1. Login to the Integriti System Designer.
2. Click on the System tab followed by Schematic Maps.
3. Double-click one of the existing the maps.

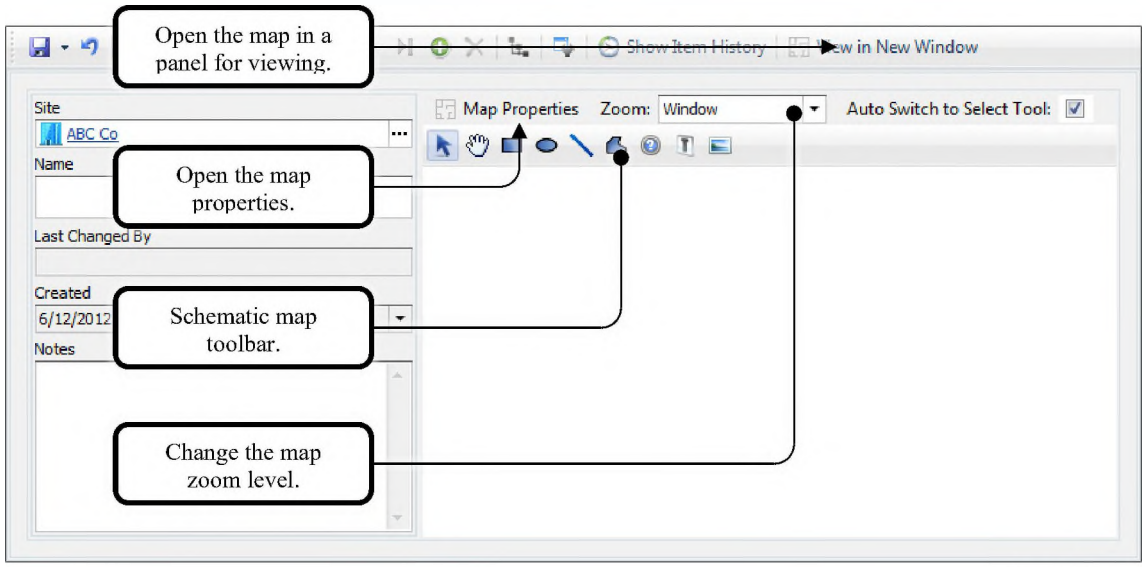


Figure 65

13.2.1 Map properties

Click the Map Properties button will open the schematic map properties.

13.2.1.1 Background

The map background width and height are determined automatically when loading a background image. You can adjust these values manually but this will stretch the background image (if one has been specified).

The background colour is white (255,255,255) by default. It is only visible if there is no background image or the image has transparent regions.

To load a background image, click on the Change button.

To remove the background image, click on the Clear button.

13.2.1.2 Grid Overlay

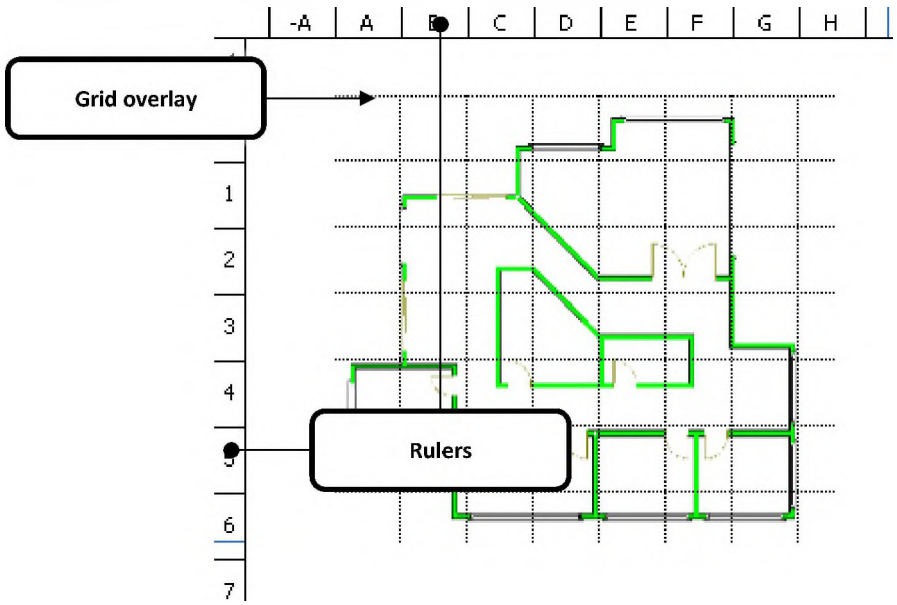


Figure 66

Enabling the grid overlay will place dotted grid lines over the schematic.

Enabling the rulers will place alphanumeric grid reference rulers to the top and left of the schematic map.

The grid block width and height are measured in pixels. The scale of the grid will vary with the schematic map zoom level.

13.2.1.3 Default Font

The default font used for schematic maps is Arial, 12pt. This can be adjusted by clicking on the ellipsis () and selecting your font preferences in the font selection window.

The default font will be used for all newly created schematic map items. Changing the default font will not override font settings for existing map items.

13.2.2 Schematic map toolbar

The schematic toolbar contains all of the controls necessary for creating the schematic.

 **Select tool**

The select tool allows you to select and modify properties of items on the schematic. Ticking Auto Switch to Select Tool will cause the select tool to become active after a new item has been successfully added to the schematic.

 **Pan tool**

If the schematic is at a zoom level larger than the screen, use this tool to move the schematic around the screen.

 **Rectangle tool**

To draw a rectangle on the schematic:

1. Select the rectangle tool.
2. Click and drag to draw a rectangle. Where you press and release your mouse button will define the shape of the rectangle.
    - Pressing and holding shift for this step will allow you to create a square.
3. The Map Element Properties window will appear immediately after the element has been drawn.

 **Ellipse tool**

To draw an eclipse on the schematic:

1. Select the eclipse tool.
2. Click and drag to draw an ellipse. Where you press and release your mouse button will define the shape of the ellipse.
    - Pressing and holding shift for this step will allow you to create a circle.
3. The Map Element Properties window will appear immediately after the element has been drawn.

Line tool

To draw a line on the schematic:

1. Select the line tool.
2. Click and drag to draw the line. Where you press and release your mouse button will define the position and length of the line.
3. The Map Element Properties window will appear immediately after the element has been drawn.

Freeform tool

To draw a freeform element on the schematic:

1. Select the freeform tool.
2. Click once at the starting point of where you want to create the freeform object.
3. Continue clicking on the schematic to place multiple points on the freeform element.
4. When you have finished, double-click.
5. The Map Element Properties window will appear immediately after the element has been drawn.

Once you have closed the Map Element Properties window, you can continue to fine tune the freeform element.
Click and drag your mouse along any freeform line to create a new node on the element.
Right-click any node on the freeform element to delete it.
You can click and drag any existing nodes on the freeform element.

Icon tool

Click where you would like to place the icon.

Label tool

Click where you would like to place a text label.

Image tool

Click where you would like to place the image.

13.2.3 Map Element Properties

Every item placed on the schematic map has its own set of properties.

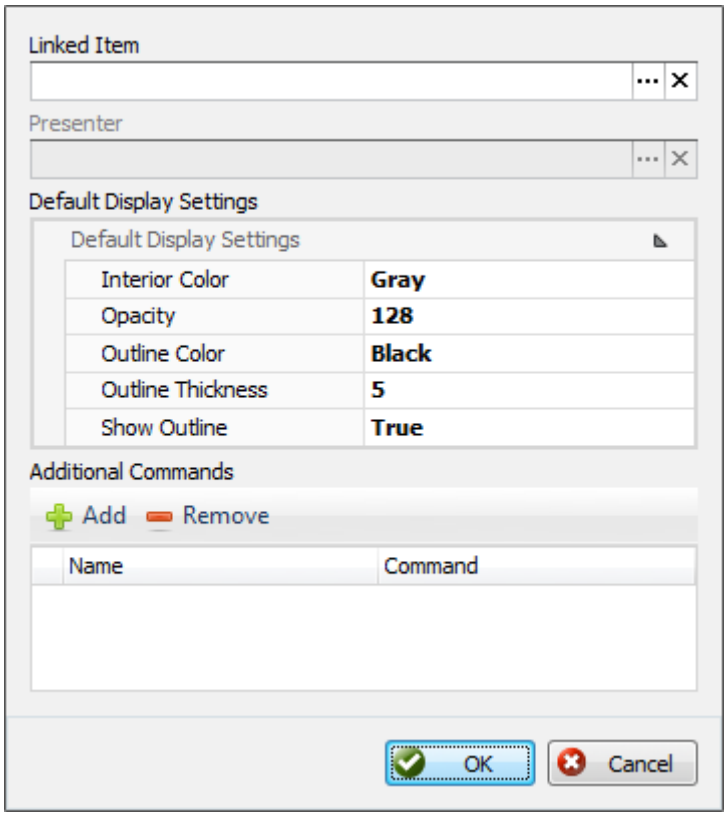


Figure 67

13.2.3.1 Linked Item

If a map element is linked to something, it will reflect the status of whatever it is linked to which is determined by the selected presenter.

To link the element to an item, click the ··· and select the item from the list that appears.

To remove the link, click on the ×.

13.2.3.2 Presenter

A presenter is a collection of format settings and rules that govern how a map item will behave on the schematic. Presenters can only be assigned to a schematic map item if it is linked to an entity.

When a linked item has been selected, an element presenter will automatically be associated with the schematic map item. If a default element presenter for the item type has not been designated, the element presenter that is automatically associated with the map item will be randomly selected.

Some presenters have been included with the Integriti software to cover common map item types. The included presenter item types are:

- Area
- Auxiliary
- Camera
- Controller
- Door
- Input
- LCD Terminal
- Macro
- Schematic Map

13.2.3.3 Default Display settings

13.2.3.3.1 Interior colour:

Default value: Grey (128,128,128)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255`	Blue
`255,0,0`	Red
`0,255,0`	Green
`0,255,255`	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

Figure 68

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

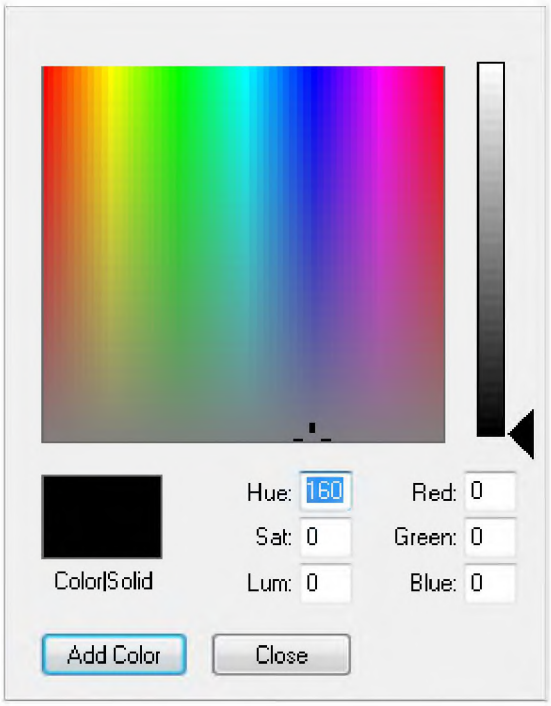


Figure 69

13.2.3.3.2 Opacity 0-255

Default value: 128 (semi-transparent)

The opacity affects both the Interior and outline colour. Use a value of 255 for opaque and a value of 0 for transparent.

13.2.3.3.3 Outline color

Default value: Black (0,0,0)

The value specified here determines the colour of the outline/border surrounding the schematic map item.

If the border is transparent, only the opacity setting will affect the specified border width of the map item.

Example:

- Interior color – `Web -> Cyan`
- Opacity – `128`
- Outline color – `Web -> Transparent`
- Outline Thickness – `5`
- Show Outline – `True`

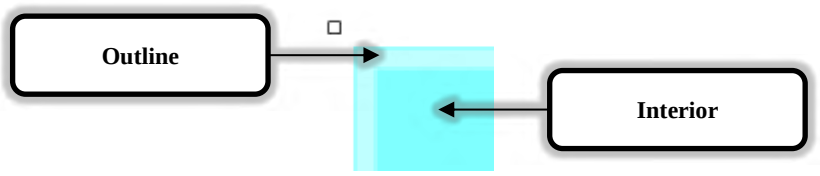


Figure 70

13.2.3.3.4 Outline Thickness

Default value: 5 pixels

The value specified here will determine the thickness of the border / outline. A value of 0 will leave a 1 pixel border.

13.2.3.3.5 Show outline

Default value: True

Setting this option to False will disable the outline of the item.

13.2.3.4 Additional Commands

Schematic map items can have custom commands assigned to them. When an operator clicks (or right-clicks) a schematic map item, a list of the available commands will be presented to them. Additional commands are appended to the end of the list.

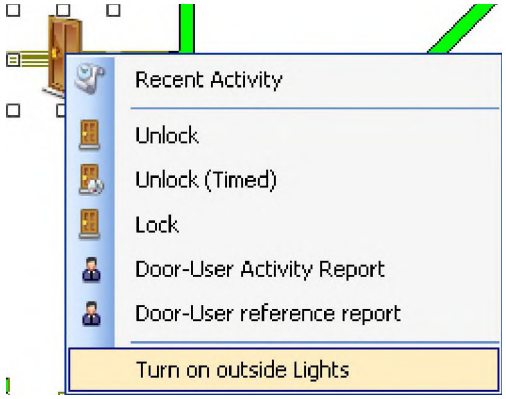


Figure 71

13.2.3.4.1 Creating additional commands

1. Click on 

to create an additional command in the additional commands list.
2. Click in the name field and give a name to the new command.
3. Click on the command field followed by  .
4. Select an option from the Action Type drop down list.
    - See the table below for more information.

None	Does not perform any action. Can be used as a place holder for future use or for entering notes.
ControllerAction	Can assert or dis-assert any action on the controller. Specify the action to send and the edge type.
DBBackup	Backup the entire database to a specified location. DB Backup has two options: • Include review data. • Append a date/time stamp the exported filename.
Delay	**Not used here.** This action type should only be used within a sequential list (below).
LogReview	Put a message in review. You can specify the review level and the message text.
ParallelList	Execute a list of commands in parallel. This will open a new Configure Task Action window where a list of actions can be executed in simultaneously.
SequentialList	Execute a list of commands in order. This will open a new Configure Task Action window where a list of actions can be executed in order.
SyncTime	Synchronise the time/date of one or many controllers. To update the time of all Integriti controllers, leave the controller field blank. To update a specific Integriti controller, open a controller for editing, copy its name and paste it in to this field.

14 Layouts & Editors

The layout of the entire management suite can be customised and stored. Stored layouts include:

- Positioning of each individual docking panel.
- Its own layout set. Which includes:
  - Positioning of each individual dialog window.
  - Content layout of each entity editor dialog window.

Layouts can be assigned to individual operators as required.

To customise an individual docking panel, open it and click the  button.

Additional layout configuration settings are found under the 

tab.

Pressing the 

button will restore the entire layout back to the factory default settings.

14.1 Layouts

Layouts contain information about the panel(s) that are displayed and their position. Client workstations can be configured to automatically load a layout on start-up. There are two types of layouts – Personal and System.

Personal layouts are tied to the individual operator. Where permitted, operators can create their own System Designer and Gatekeeper layout.

System layouts can be used as the 'default' or an 'enforced' layout by configuring operator type permissions.

Personal layouts are automatically associated with the operator who created them. They are intended to be used by "Power Users" who wish to define several layouts for their own personal use. System Layouts on the other hand can be associated with operators for whom it is desired that they have 1 fixed layout whenever they use the software. If you have already created a personal layout with your own operator, and need to change it into a System Layout, simply load the personal layout, then select the "Save Layout" button and press "System Layout". This can then be associated with another operator.

14.2 Creating and saving layouts

Click on the 

or 

buttons to open one of the layout managers.

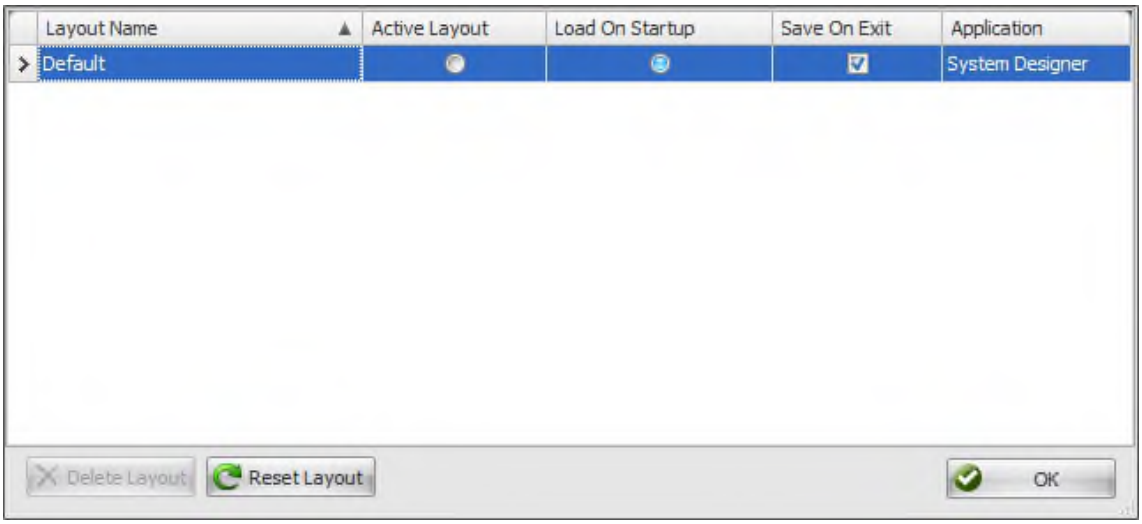
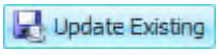


Figure 72

Each client can have its own layout that is loaded in start-up. To select the desired layout, click on the radio button in the 'Load On Startup' column to the right of the desired layout.

The active layout can be changed at any time by opening the layout manager and clicking on the radio button in the 'Active Layout' column to the right of the desired layout.

If the active layout has the 'Save On Exit' checkbox ticked, the layout will be saved when the Integriti software management suite is closed. Next time the layout is loaded, the layout will restore to the state it was in prior to Integriti closing.

Clicking the 

button will save the currently active layout over an existing layout.

Clicking 

will allow you to save the current layout as a new layout. A dialog window will appear prompting the user to enter a name for the new layout.

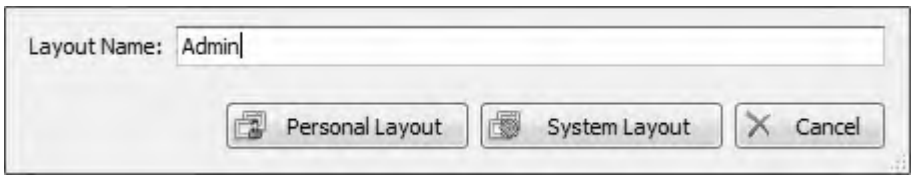
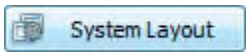


Figure 73

Enter the name of the layout then click on the 

or 

button to save.

Click on the 

button to load a specific layout.

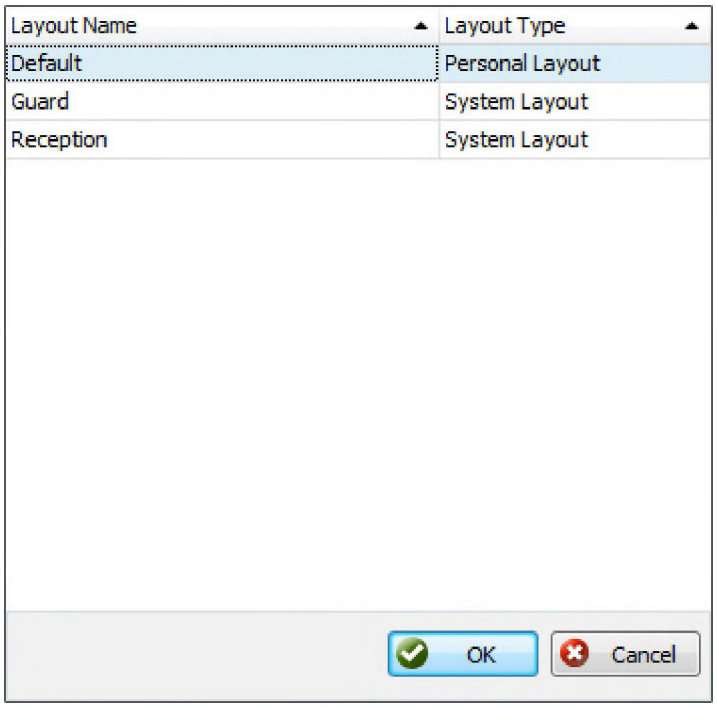
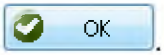


Figure 74

Click on the desired layout followed by 

.

14.3 Editor layout sets

Click on the 

button under the 

tab to open the editor layouts panel.

The 'Default' editor layout set is suitable for most applications. The ability to create custom editor layouts allows you to:

- Hide unused / unnecessary portions of the layout.
- Rearrange each individual layout.
- Add custom content to layouts.

Editor layouts may be customised to suit individual operators or operator groups.

Double-click an editor layout set to re-configure it or click 

to create a new one.

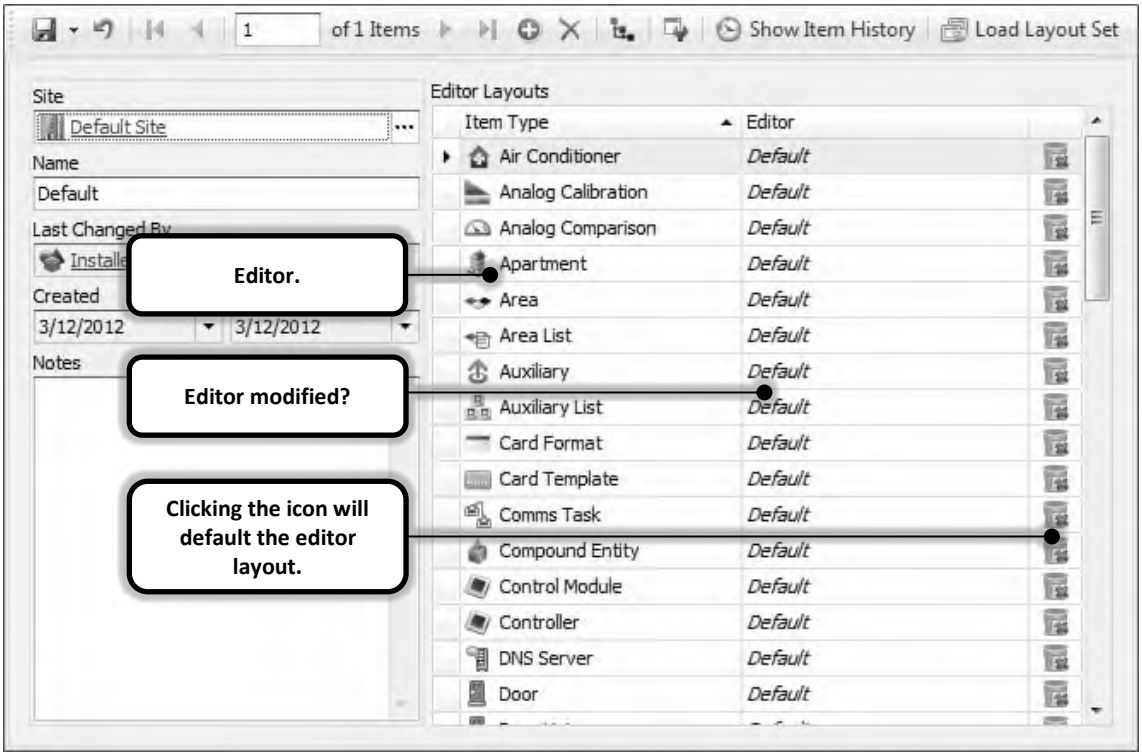


Figure 75

Individual editor layouts can be defaulted by clicking the icon.

To edit an editor layout, double-click it to open the editor dialog window in layout mode.

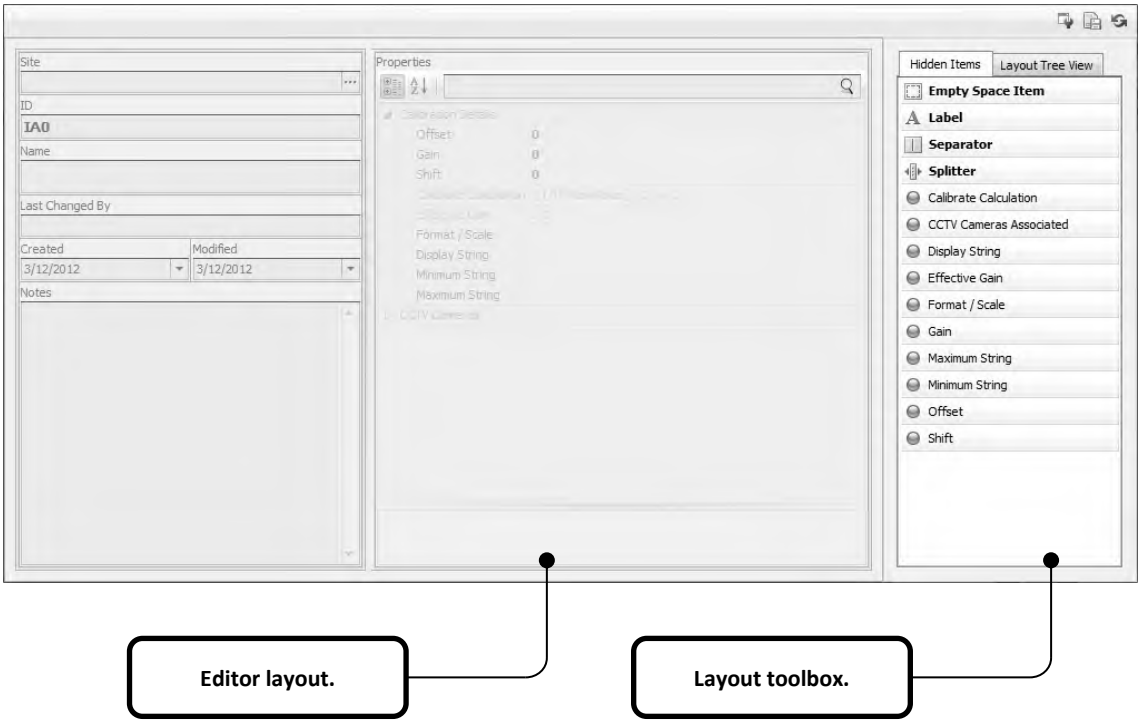


Figure 76

Please refer to the document titled 'Interface Elements for Integriti' for more information on how to use the layout manager.

	Toggle between the Editor and a preview of the
	Save the current layout.
	Restore the layout back to the factory default. (Click Save to commit changes)

Table 4

15 Communications Tasks

All external system communication is controlled by means of 'Comms Tasks'. As the name suggests a Comms Task is a communications task or job that you wish the system to carry out. Because there can be more than one Comms Task, it is also possible for more than one communications task to be operating at once.

e.g. To configure the system for a review printer you simply allocate one of the available Comms Tasks to perform the automation function. If you wish an alarms dialler to be operational as well, you simply assign another Comms Tasks the job of being a dialler format such as Contact ID.

The total number of available Comms Tasks available is ten (including the Integriti Comms Task). Comms Tasks can either be "active" or "idle". When the system is powered up, all programmed Comms Tasks are set to active so they can immediately start their intended function. If you wish to stop a Comms Task, for example abort a dialler format halfway through reporting, simply set that Comms Task to idle.

15.1 Serial Channel

Comms Tasks use communications ports to communicate with the outside world.

When a Comms Task is set to carry out a function, for example send data to a printer, it will be configured to use one of the available communications ports. For example a Comms Task programmed for automation may be configured to use "Unibus UART 1 (1)". This means that "Unibus UART 1 (1)" cannot be used for any other purpose unless the Comms Task is set to idle. Some Comms Tasks may share ports with other Comms Tasks. For example, Comms Tasks designed to be used with the modem can share the one communications port. Although these tasks may be configured to use the modem, when they are not reporting they are not using the port. If both tasks needed to use the modem for reporting at the same time, one Comms Task will use the port first and, when finished, the other Comms Task will use the port.

Comms Task types describe the job a particular Comms Task is to perform. For example, programming a Comms Task to Dialler will invoke a Contact ID, IR Fast, SIA or 4+2 dialler. The programming of options for the Dialler is unique to that Comms Task. If another Comms Task were also to be programmed to Dialler, the options for this Comms Task will be separate from those of the pre-existing one. This allows the commissioning of dual reporting with each Comms Task using its own Telephone Numbers and options. Listed below are the possible Comms Task types.

A maximum of 10 communication tasks can exist on the Integriti controller.

The number of serial channels available will depend upon the number of UniBus devices fitted to the Integriti controller.

Available Serial Channels:

- None
- Modem
- Onboard RS485 Reader Port
- UART 0
- Unibus UART 1 (1)
- Unibus UART 1 (2)
- Unibus UART 2 (1)
- Unibus UART 2 (2)
- Unibus UART 3 (1)
- Unibus UART 3 (2)
- Unibus UART 4 (1)
- Unibus UART 4 (2)
- USB Master
- USB Slave

15.2 Communications tasks:

15.2.1 Integriti

This communications task is usually present and active on an Integriti controller. The Integriti communications task is used to connect an Integriti controller its server. The Integriti communications task is usually the 1st communications task in the system.

15.2.2 Monitor

The Monitor communications task is reserved for use by Inner Range.

15.2.3 Dialler

This communications task uses the on board legacy modem to transmit messages back to the monitoring centre. Supported communications formats are:

- IRFast
- Contact ID
- SIA
- 4+2

15.2.4 GSM

The GSM Communications Task can interface with one of the many Inner Range FE3000 or Inner Range Multipath STU products. The Integriti Controller's GSM Communications Task is used to communicate reportable events to a Central Monitoring Station, to send reportable events via SMS message and/or to receive SMS control messages.

15.2.5 Automation

The automation communications task can be used for review printing and acknowledgement as well as control and interrogation of the controller. This communications task works over a serial UART or Ethernet.

Control and interrogation options require licensing.

15.2.6 EMS

Low and high level lift interfacing is available using this communications task. This is a licensed option.

15.2.7 Securitel

The Securitel network was a "direct-line" alarm transmission network that was supplied and maintained by Telstra. Alarm panels in the field were connected to a Subscriber Terminal Unit (a STU) and the STU would communicate events via the PSTN to Nodes that were hosted by Telstra. These events were then transmitted to a Central Monitoring Station for processing/actioning.

15.2.8 Intercom

The Integriti Controller has an Intercom Comms Task and an Apartment entity structure. The Integriti Controller's philosophy for an Intercom system is that there is an Apartment that can grant access to a Call Location. An Apartment can optionally have a Floor defined as well as having an Intercom System Floor and an Intercom System Unit. Up to 32 Call Locations can be defined in the Intercom Comms Task and each can optionally have a Door and/or up to 4 Lift Cars defined. When the Intercom Comms Task detects that an Apartment has granted access to a Call Location, the defined Door and Lift(s) are temporarily unlocked/unsecured to allow access.

16 Communications Handlers

Communications Handlers work as a conduit between the Integriti Application Server service (the Integriti server) and other 3rd party products.

16.1 Review Receiver

Integriti 3rd party review receiver allows review to be streamed from a third party TCP client to the Integriti server for review logging.

Please refer to the document titled 'Integriti Communications Handlers - Review Receiver' for more information.

16.2 Review Sender

Integriti review sender allows review to be streamed to a third party TCP client.

Please refer to the document titled 'Integriti Communications Handlers - Review Sender' for more information.

16.3 REST/XML Web Service

The Integriti application server hosts a REST/XML based Web Service allowing integration with a wide variety of programming languages and environments in a stateless, query based fashion.

Please refer to the document titled 'Integriti Communications Handlers - REST XML Web Service' for more information.

17 Alerts

Alerts bring to the attention of one or many operators the change of state of one or many events.

Alerts consist of Alert Definitions, Alert Groups, Alert Views and Response Plans. Alert Definitions contain all of the information necessary to define the source of the alert and the appearance of the alert. Alert definitions can optionally invoke actions at various stages of the alerts lifecycle.

Alerts are created and configured in the Integriti System Designer. Alerts are actioned within Integriti Gate Keeper.

Alerts should only be used in situations where human intervention is required.
i.e. “An Operator must acknowledge an alert”
For automated actions, a Scheduled Tasks should be configured.

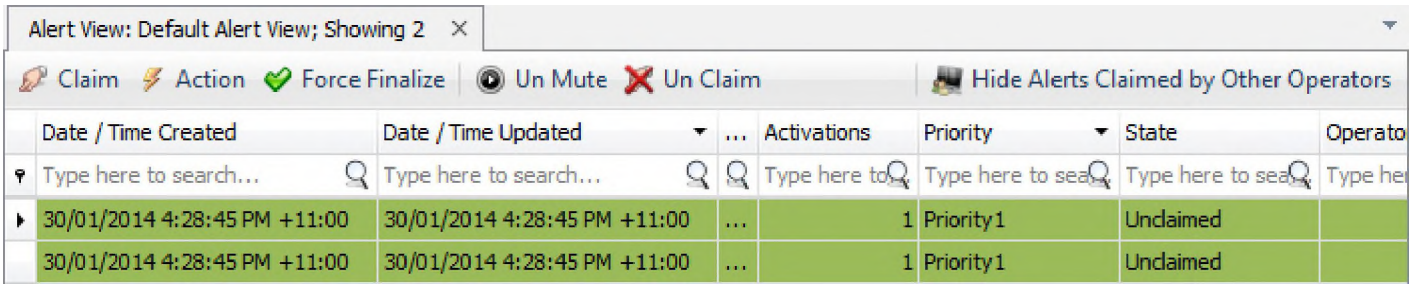


Figure 77

Alert Definitions

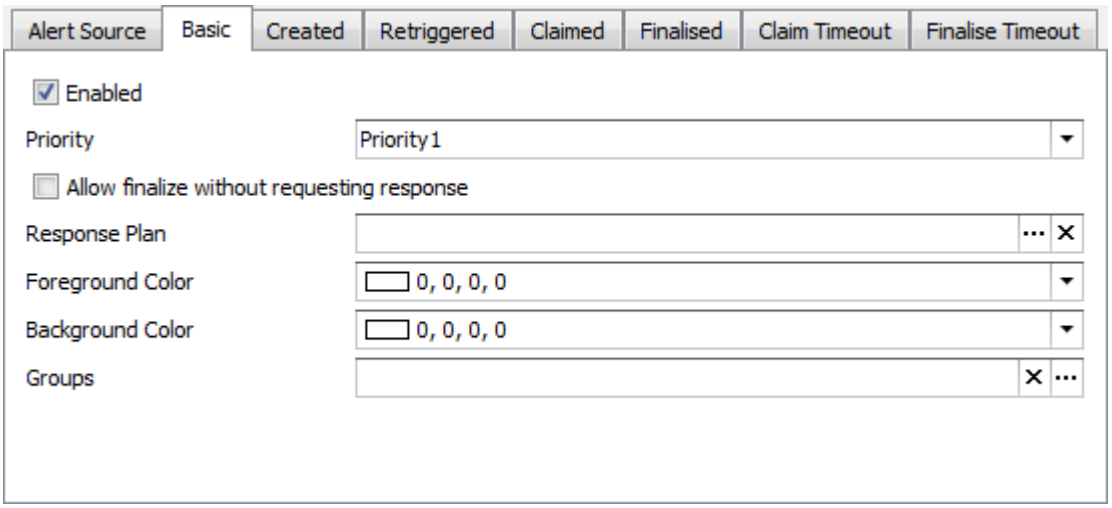


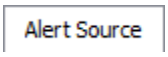
Figure 78

To create a new Alert Definition…

1. Open the 

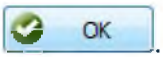
panel from the 

tab.
2. Click the 

button to create a new Alert Definition.
3. Give the new Alert Definition a name and enter a description in the notes field.
4. Click on the 

tab.
   a. Select an alert source from the drop down list.
      - Intruder Events
        i. Three filters are available for intruder events. If a field is left blank then it is considered as ‘all’. The three filters use OR logic.
        ii. Select one or many sites, areas or inputs by clicking the  to the right of the field to open a selection window.
        iii. Select one or many items from the list and click 

.
        iv. The two ‘Group Alerts by’ buttons will group alerts of the same type in the alert view based on Areas, Inputs or both.
      - Review Filter
        i. Information on how to create filter stacks is available in the appendix under the section titled ‘Filter Stacks’.
        ii. Tick ‘Group All Active Alerts for this Alert Definition’ to group alerts of the same type in the alert view.
      - Hardware Offline
        i. Two filters are available for hardware offline. If a field is left blank then it is considered as ‘all’. The filters use AND logic.
        ii. Select one or many sites and/or modules by clicking the  to the right of the field to open a selection window.

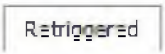
iii. Select one or many items from the list and click 

.

iv. Tick the group alerts by bodules checkbox to group alerts of the same type in the alert view.

- The remaining tabs have their own action list that will execute at various stages of the alert.
  a. To execute all of the items in the list simultaneously, click on the 

button.
  b. To add actions to a list, click on the 

button.
    - For more information on the various actions available, see the section titled 'Actions'.
  c. If 'Supress if muted' is ticked under the 

tab, actions in that list will not be executed.
- The 

and 

tabs each have their own time out in hours, minutes and seconds. Setting these values will cause the actions in the list to be executed once the time specified has expired.

5. Click  and close the Alert Definition.

17.1 Alert Groups

An Alert Group is a logical place holder for Alert Definitions. An Alert Group has no properties of its own. It is used for organising alerts only (such as in Alert Views).

To create a new Alert Group…

1. Open the 

panel from the 

tab.
2. Click the 

button to create a new Alert Group.
3. Give the new Alert Group a name and enter a description in the notes field.
4. Click  and close the Alert Group.

17.2 Alert Views

Alert Views are lists containing Alerts belonging to the groups specified within the Alert View.

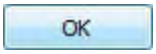
To create a new Alert View…

1. Open the 

panel from the 

tab.
2. Click the 

button to create a new Alert View.
3. Give the new Alert View a name and enter a description in the notes field.
4. Expand-out Settings and click on the  to the right of groups.
5. In the window that appears, click on the 

button and select one or many Alert Groups from the list that appears.
6. Click 

to confirm your selection. Click 

once more to go back to the Alert View editor window.
7. Click  and close the Alert View.

17.3 Response Plans

Response Plans can be used as an alternative to the default Finalize Response window. Response Plan windows can contain custom text in the form of instructions, checklists, buttons, alert details, response history and operator response items.

For more information on the Response Plan layout manager, please refer to the document titled 'Interface Elements for Integriti'.

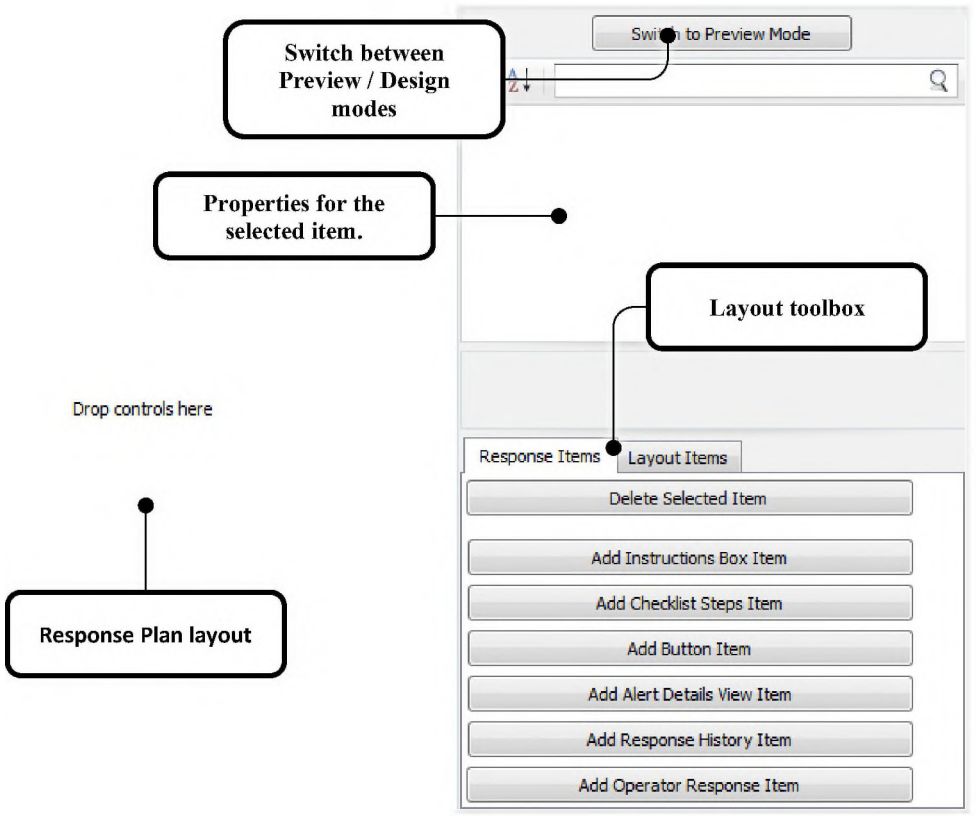


Figure 79

17.3.1 Delete Selected Item

Clicking this button will delete the selected item from the response plan layout.

17.3.2 Information Box Item

Selecting this and dragging it over to the Response Plan Layout designer on the left adds a text box containing configurable text.

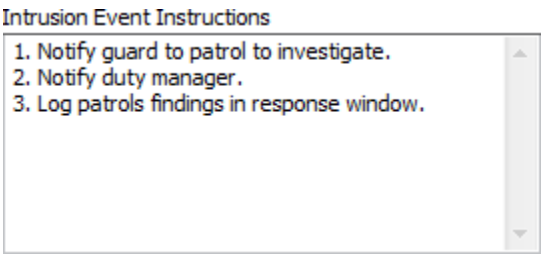
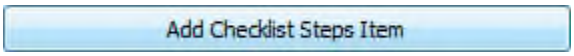


Figure 80

There are three configurable options available:
Information Text – Contains plain text. Format strings can be used here by clicking the ellipsis button.
Caption Text – This is an optional text label for the Instruction Box item.
Font – Set the type of font used.

17.3.3 Information Display Item



Selecting this and dragging it over to the Response Plan Layout designer on the left adds a box containing configurable important text. This text can be horizontally and vertically aligned, as well as have different sizes and formatting options.

Figure 81

There are five configurable options available:
Information Text –This can contain formatting tags and Format String Keywords alongside text. The Configure Format Strings form can be opened by clicking the ellipsis button.
Vertical Alignment – Allows setting of vertical alignment to Default, Top, Center, or Bottom.
Horizontal Alignment – Allows setting of horizontal alignment to Default, Top, Center, or Bottom.
Caption Text – This is an optional text label for the Checklist Step item.
Font – Set the type of font used.

17.3.4 Alert Custom Field

Selecting this and dragging it over to the Response Plan Layout designer on the left adds a field that is linked to a selectable Alerts Custom Field. This allows the operator experiencing the Response plan to add customisable input, which appears in Gatekeeper beside the alert.

17.3.5 Action Button

Clicking this button adds a Button Item to the Response Plan. Response plan buttons can invoke any action in the section 'Action types'.

Figure 82

Button Action – Set the action for this button to invoke when clicked.
Button Text – Text for this button to display.
Button Image – Optional button image. Click the ... to open a .bmp, .gif, .jpg, .png or .ico.
Button Text – Optional text displayed on the button
Image Width – The width of the image in pixels
Image Height – The Height of the image in pixels

17.3.6 Alert Details

The Alert Details View Item displays review history that is directly related to the alert.

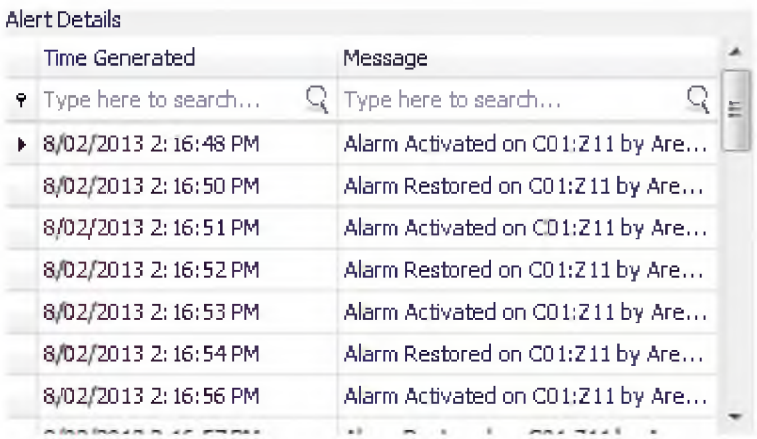


Figure 83

17.3.7 Response History Item

The Response History Item displays information regarding the alert such as the creation time, who claimed it, what checklist items have been given values and what response text operators have added to the alert.

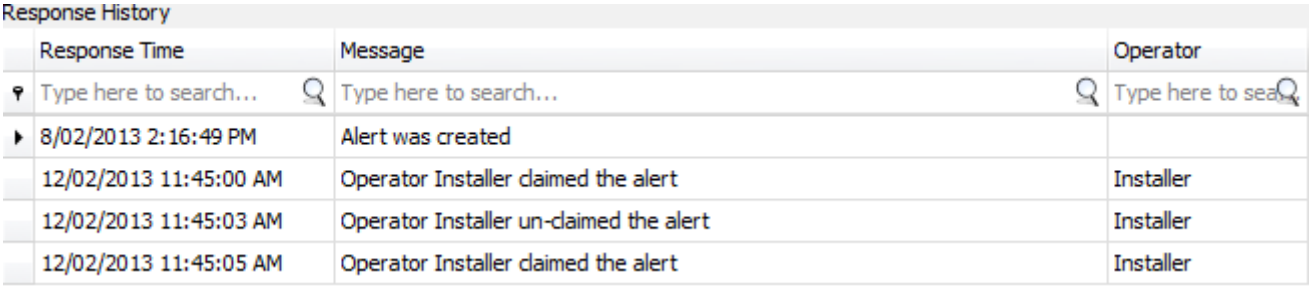


Figure 84

17.3.8 Add Operator Response Item

Clicking this button adds an Operator Response Item to the Response Plan. Operators can add their own text to the alert. Clicking the  will add the text to the Response History.

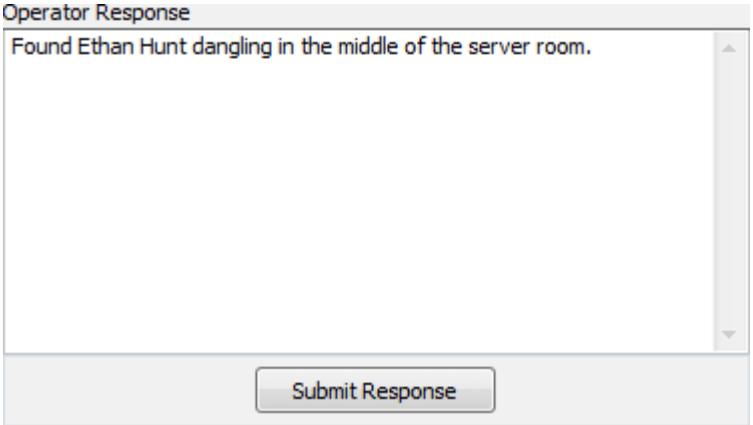


Figure 85

There are two options available:
Caption Text – Text to display above the stream.
Text Font – Which font to use.

17.3.9 CCTV Stream

Selecting this and dragging it over to the Layout Designer will create an area which displays a CCTV camera feed when the response plan is shown. This will automatically show feed from the CCTV Camera which has been associated with one or more of the entities which functioned as the trigger for the Alert.

There are two options available:
Caption Text – Text to display above the stream.
Text Font – Which font to use for the caption.

17.3.10 Browser Item

Selecting this and dragging it over to the Layout Designer will create a section which functions as a web browser displaying a single page when the response plan is shown. The URL can be configured via the 'Browser Url' setting of the item.

There are three options available:
Browser Url – The URL to open when the Plan is shown.
Caption Text – The text to display above the Browser Item.
Text Font – Which font to use for the caption.

17.3.11 Creating a new Response Plan

To create a new Response Plan…

1. Open the 

panel from the 

tab.
2. Click the 

button to create a new Response Plan.
3. Give the new Response Plan a name and enter a description in the notes field.
4. Using the information provided above, create your response plan layout. For information on layout editor usage, please read the document titled 'Interface Elements for Integriti'.
5. Click  and close the Response Plan.

18 Importing Data

Operators with access to the Import data button (accessible from the administration tab) can sort data from a CSV file in to the Integriti database. This feature gives the operator the ability to create, modify or remove a number of records with ease.

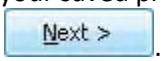
The import tool caters for CSV files with varying layouts and column placement. CSV exports from Insight or files provided by end users can be imported directly in to Integriti.

There are two methods used to import a CSV file. Users can manually import CSV files on a case by case basis or they can create CSV import settings if a known CSV format is going to be used regularly.

18.1 Importing CSV files - manually

1. Start by clicking on the 

button under the 

tab.
2. An open file dialog window will appear. Find and open your CSV file.
3. The following dialog will ask you to select your saved pre-set, from the list of options (if any), select 'Define settings as you go' and click 

.

Figure 86

4. The CSV settings dialog window will appear (*Figure 86*). Click 

to see if the CSV file will be imported correctly.

If it does not look correct you have a few options:

- You can attempt to open the CSV file yourself with a text editing program and see how the file is structured.
- You can play with the CSV settings and use the 

button to see if you can use a few educated guesses to determine the CSV layout.

- You can consult whoever issued you with this CSV file and see if they can provide details on the file structure.

Bad test import examples:

	Column0	Column1	Column2
▸	###	secondname	pin
	Installer		01
	Richie	Florencio	02
	Trenton	Buckalew	03
	Hugh	Sankowski	04
	Luci	Flesher	05

	Column0
▸	###,secon...
	Installer,,0...
	Richie,Flore...
	Trenton,Bu...
	Hugh,Sank...
	Luci,Flesher...
	Bertram...

Figure 87

A good example of what a test import should look like:

	###	secondname	pin
▸	Installer		01
	Richie	Florencio	02
	Trenton	Buckalew	03
	Hugh	Sankowski	04
	Luci	Flesher	05
	Bertram	Scargall	06

Figure 88

If you are importing from Insight, the settings required are Comma delimiter, Double quoted and Has column headers.

5. As of Version 17, the software does not allow duplicate credentials in the database. For example, 2 users each with an active card that has the exact same card data. This feature also extends to PIN's and RF Remotes.

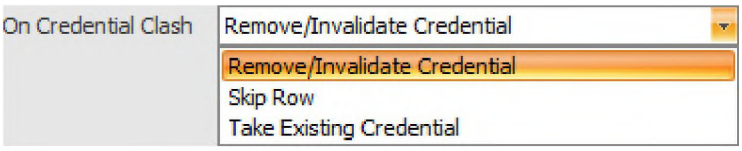


Figure 89

This option allows the user to choose how to resolve imported data that would otherwise cause a clash:

- **Remove / Invalidate Credential**

Still import all of the other user data / but without the problematic Credential

For Cards, this will leave the imported user with the card, but it will be marked as “Inactive – Duplicated”

For PIN’s, the imported users PIN will be blank (no PIN)

- **Skip Row**

  Only relevant for imports that contain more than one user. Keep importing, but don’t import this user at all.

- **Take Existing Credential**

  This option removes the Credential from the other (not being imported) user so the import can proceed.

  Caution: This could result in an existing user no longer having the access rights they should.

  Use this option if you are certain the imported data has the correct card assignments.

6. Click Next > to proceed to field mappings.

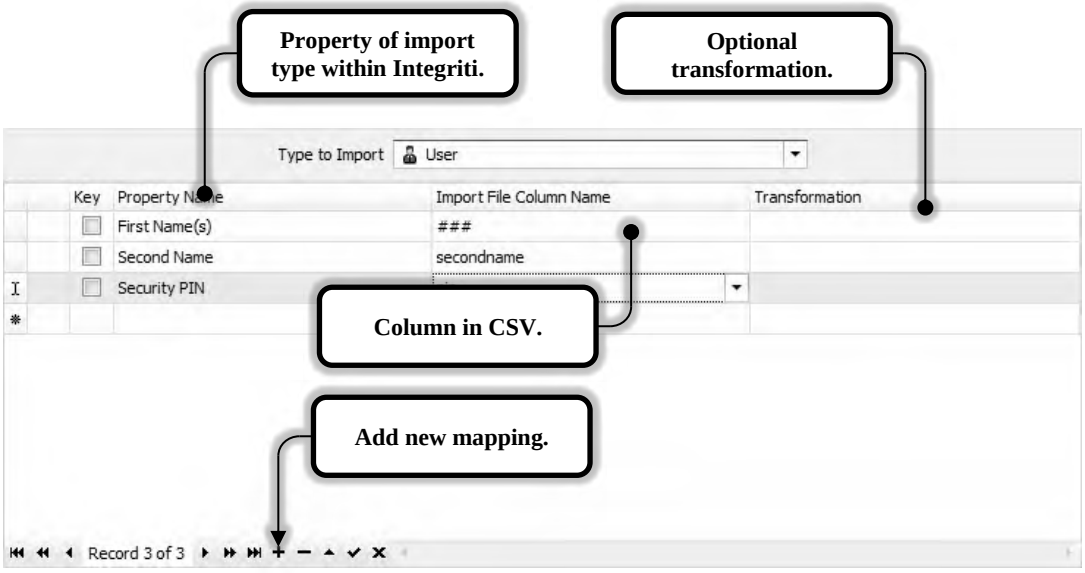


Figure 90

The field mappings dialog allows you to create a lookup table for as many fields in your CSV file as you require.

6.1. Select the type of data you will be importing from the CSV file.

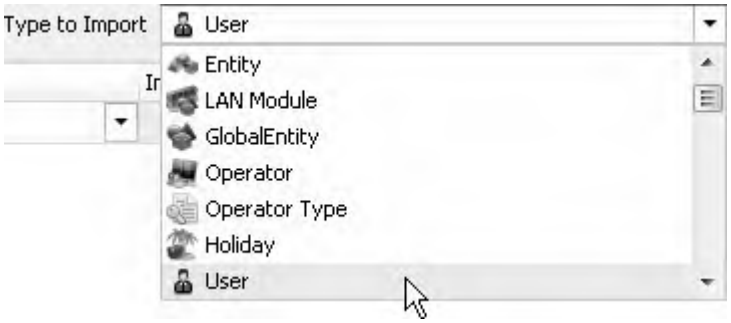


Figure 91

6.2. Begin filling in the lookup table by entering the 1st Property name of the import type.
6.3. Select the Import column to map to the CSV file.
6.4. Transformation is a powerful option that gives you the ability to govern how the data within the CSV field will be interpreted. In most cases you can leave this field blank.
6.5. Repeat steps **5.2** – **5.3** until the necessary mappings have been created.

7. When you are ready to proceed with the import, click Next > and the import process will begin.

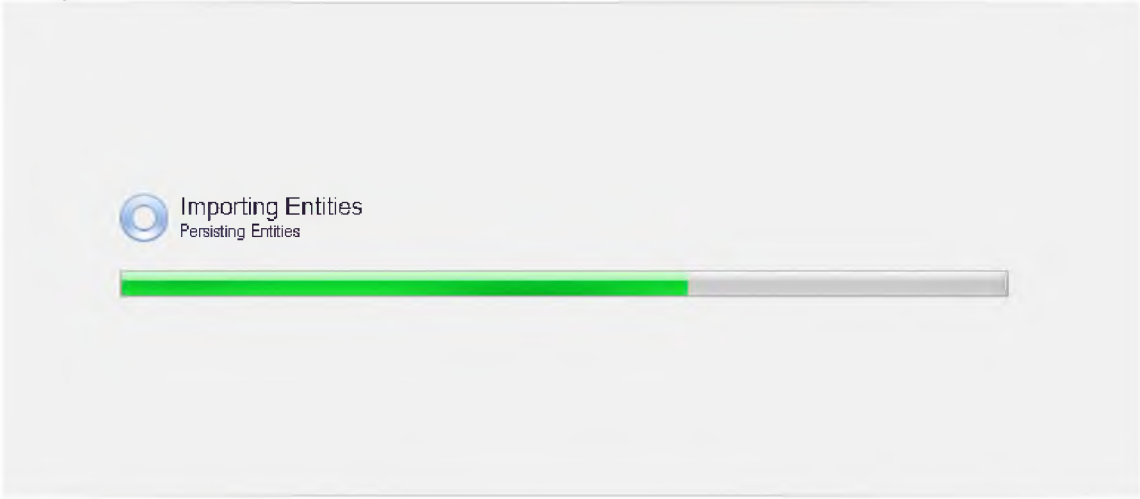


Figure 92

8. Click Finish.

18.2 Importing CSV files – Import Configuration

Import configuration allows you to save the import settings for use every time you need to import a file of the same type.

1. Start by clicking on the Import Configuration button under the Administration tab.
2. Click the Add New button in the Import Configuration panel.
3. Give the new Import Configuration a name and enter a description in the notes field.
4. Click the ... button and select the file that is to be opened and imported.
5. Just as in the manual import procedure above click the appropriate CSV settings.
6. Select the Type to Import.
7. Fill in the lookup table with the appropriate fields to match the imported file.
8. Click and close the Import Configuration.

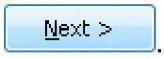
18.2.1 To use the newly created Import Configuration:

1. Start by clicking on the 

button under the 

tab.
2. An open file dialog window will appear. Find and open your CSV file.
3. The following dialog will ask you to select your saved pre-set, from the list of options. Drop the list box down and select the pre-set (Import Configuration) you created earlier and click 

.
4. Click 

.
5. Click 

.
6. Click 

.

19 Integriti Server Management

19.1 License Management

Use the license manager to view, add and update licenses.

License key management is found under the Administration tab. Click on the License Manager button to open the license manager.

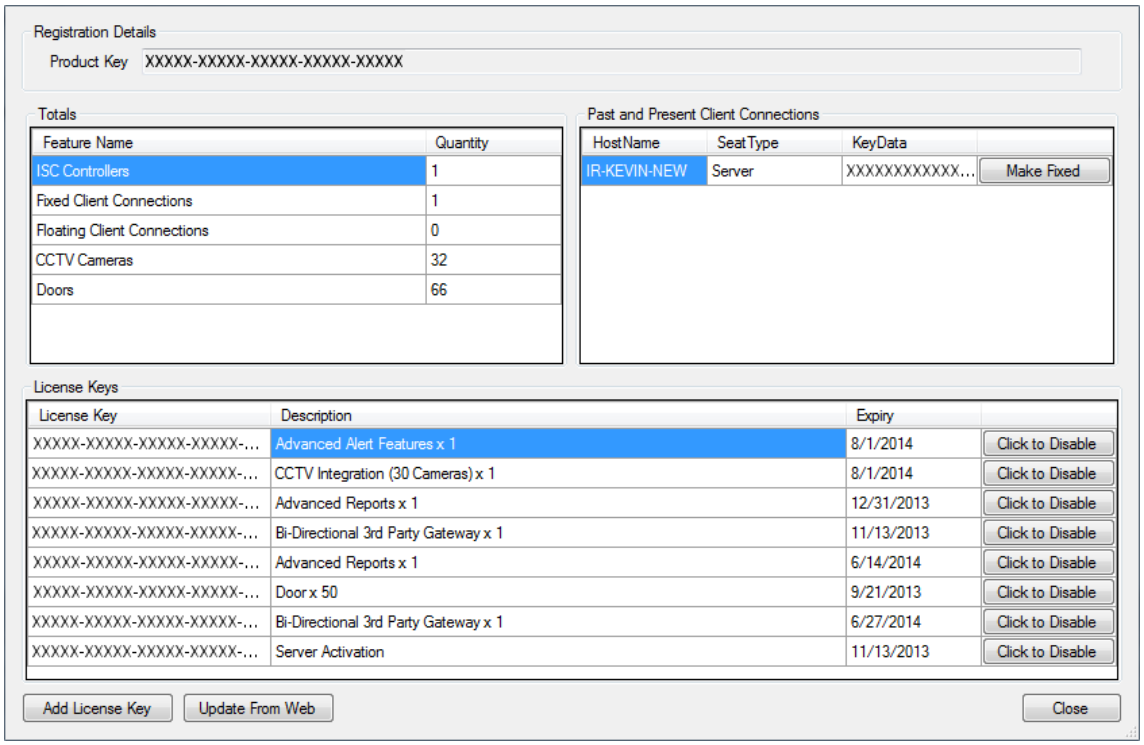


Figure 93

A summary of your license keys is displayed in the 'totals table' on the left side of the license manager.

Each individual license key is displayed in a list at the bottom of the license manager.

'Fixed Client Seats' are licenses allocated to client machines that are going to connect to the Integriti server.

Click Click to Disable to disable a license key. Once you have clicked the Click to Disable button, it will change to Click to Enable. To re-enable the license click Click to Enable.

Click Add License Key to open a new dialog and manually enter in your license key.

Click Update From Web to automatically update your license keys from the Integriti software license server.

19.2 Operators and Operator Types

Operators are used to access the Integriti software management suite. The Operator Types are groups of settings that define what content can be viewed, modified, removed, etc...

Each Operator is given an Operator Type that defines how much (or how little) they can access within the System Designer and Gate Keeper.

19.3 Operator Type

The Operator Types panel is accessible from the 

tab.

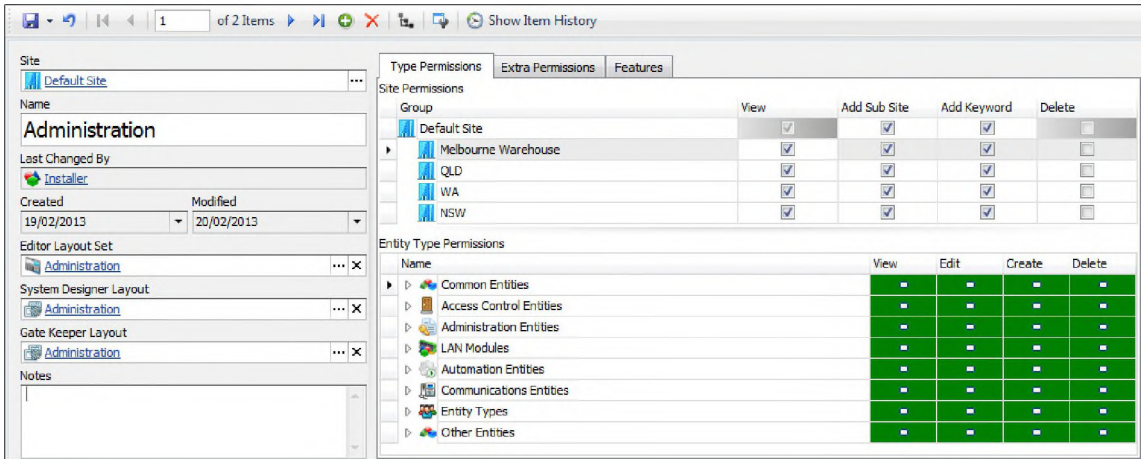
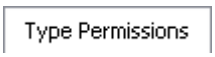


Figure 94

Each Operator Type can have an Editor Layout Set assigned to it. This gives the installer the opportunity to add, remove and re-arrange programming items on each individual editor page.

Custom System Designer and Gate Keeper layouts can also be assigned to the Operator Type.

19.3.1 Type Permissions



Under the Type Permissions tab there are two sections - Site Permissions and Entity Type Permissions.

Site Permissions contains a list of all of the sites within the database and the option to set View, Add sub site, Add Keyword and Delete permissions.

19.3.1.1 Site Permissions

Site permissions are used to grant access to view, add entities, add to site, add keyword and delete from the navigation panel.

Clicking on the View, Add Entities, Add Sub Site, Add Keyword or Delete check boxes will allow/deny access to all of the entity type permissions that fall under the selected site.

Permission	Description
View	Operators with this permission can see the site.
Edit	Operators with this permission can modify entities belonging to this site.
Add sub site	Operators with this permission can create sub sites.
Add keyword	Operators can add keywords.
Delete	Operators with this permission can delete this site and / or items under it.

19.3.1.2 Entity Type Permissions

The Entity Type Permission tree defines four levels of access to entities within the Integriti system. These are:

Permission	Description
View	Operators can see the entity.
Edit	Operators can modify the entity.
Create	Operators can create new entities of this type.
Delete	Operators can delete entities of this type.

Table 5

Values set at the top level of the tree cascade through to every branch entity.

Name	Description	
	Use the inherited permission.	**Deny**
	Deny.	
	One or many of the deny permissions are inherited.	
	Use the inherited permission.	**Allow**
	Allow.	
	One or many of the allow permissions are inherited.	

Table 6

A blank / empty box indicates that the entities for the group are a mixture of allow and deny permissions.

19.3.1.2.1 Entity Type examples

The following illustration indicates that the Operator Type has allow permissions for all Entity Types excluding Communication Entities. Edit permissions have been revoked from one or many of the Communication Entity Types. This is indicated by the blank edit permission box.

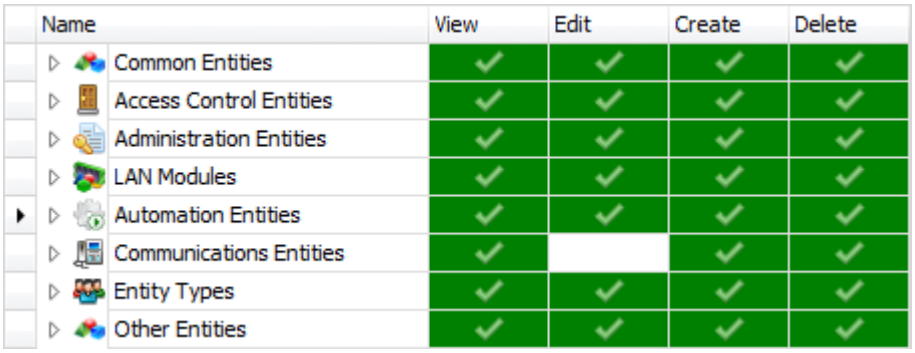


Figure 95

If we expand out the Communication Entities we can see that edit permissions have been removed from Comms Task entities.

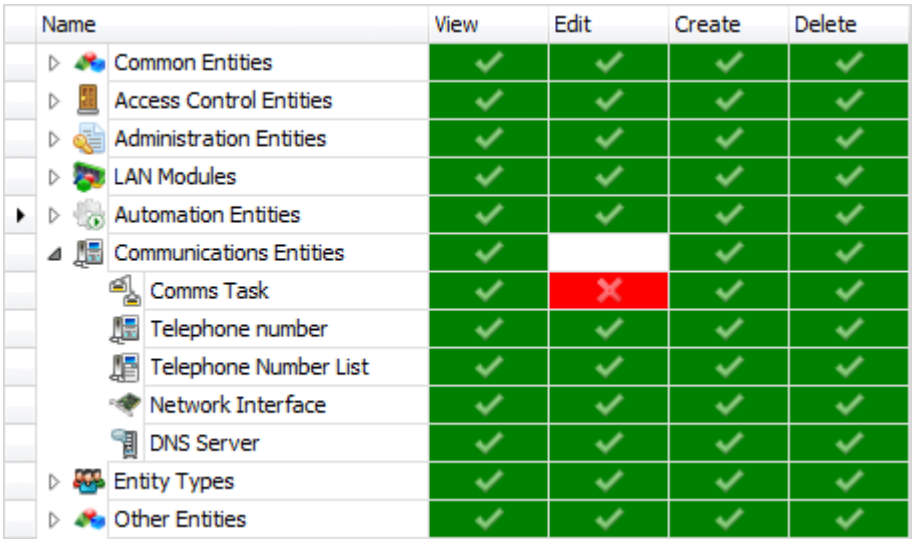


Figure 96

If at this point we were to add a new sub site, we would see the inherited permissions for the sub site appear like so.

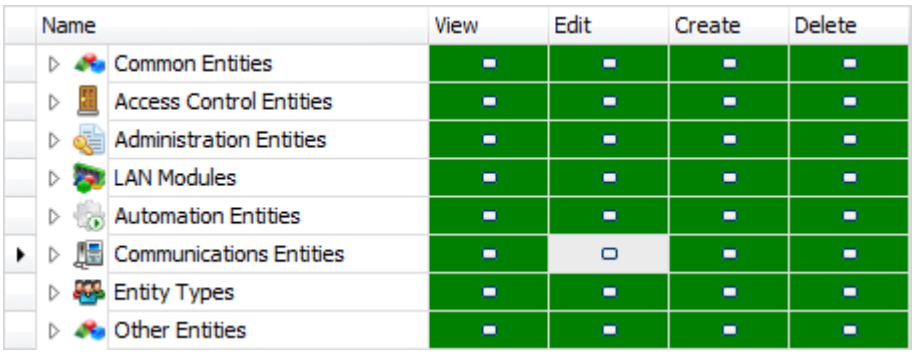


Figure 97

If we were to expand out Communication Entities, we would see that edit permissions have been revoked from Comms Task Entities. These permissions were all inherited from the parent site.

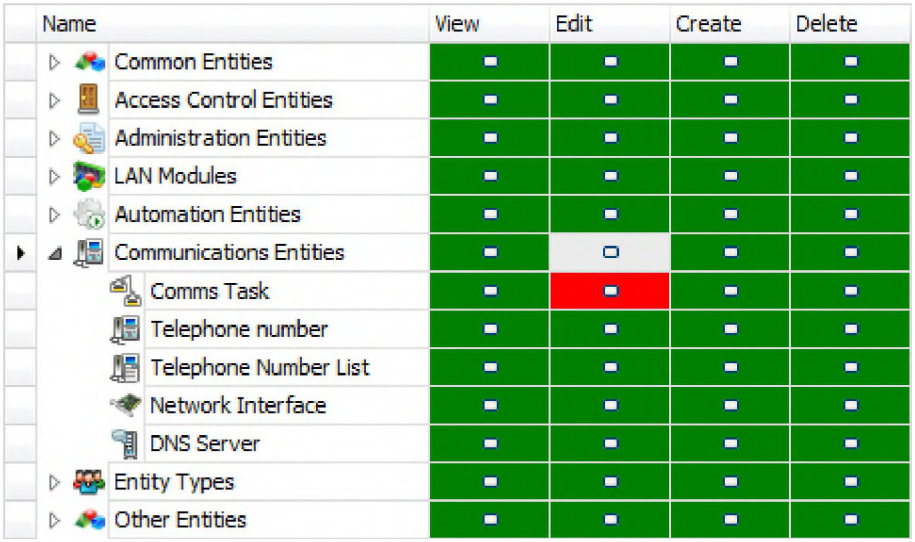


Figure 98

To override this inherited permission, click on the box to change it from deny to allow. You will notice that the Edit permission for Communication Entities will change to a , indicating that the group contains a mixture of allow permissions.

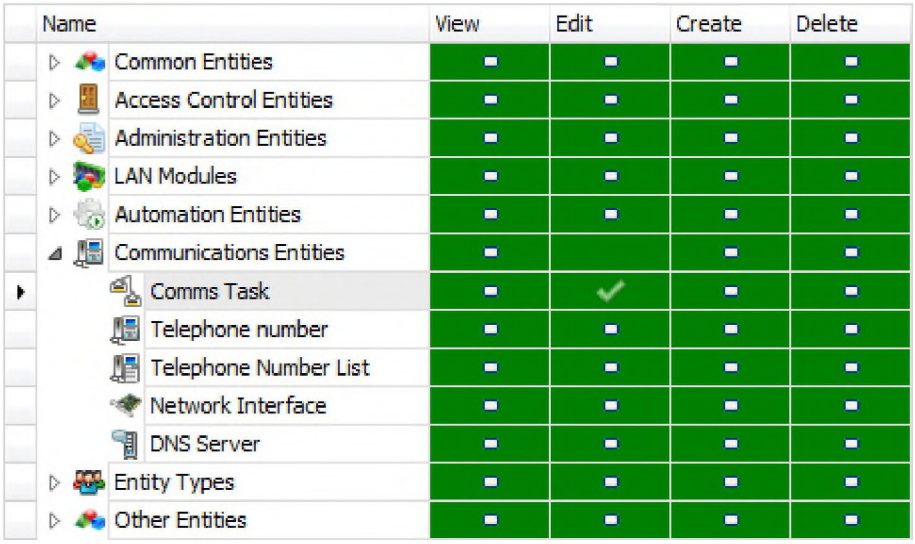


Figure 99

19.3.2 Extra Permissions

This allows you to give an Operator specific access to an individual item, in any entity across the entire Integriti System. The interface is extremely granular and should not be used to create the majority of the Operator programming. Use this tab to fine tune access to specific entity items.

The checkboxes in the Deny, View, Edit, Delete and Change Permissions columns are there to help you filter your extra permissions. The Entity column can be filtered / sorted by text entered.

The Extra Permissions dialog has four states for each item added to the list:

Permission	Description
View	Operators can see the item.
Edit	Operators can edit the item.
Delete	Operators can delete the item.
Change Permissions	Operators can change the access other operators have to this item.

19.3.3 Features

Features

19.3.3.1 Administration

- Ticking the Import Data checkbox allows the operator to import records.

19.3.3.2 Review

- Operators with View Review ticked will be able to view review.
- Highest Review Level sets the detail / view level of the review data the operator can see

19.3.3.3 Controllers

- Ticking Send Actions allows the operator access to control controller items.
- Ticking Enrol Controllers gives the operator permission to enrol additional controllers.
- Ticking Upgrade Controller Firmware gives the operator permission to upgrade controller firmware.
- Ticking View Controller Data gives the operator permission to access version / hardware information.
- Ticking Lock/Unlock the LAN
- Ticking Remote Hard Reset Controller allows the operator to remotely restart the controller.
- Ticking Disable/Enable LAN modules allows the operator to enable or disable LAN modules.
- Ticking See Blank Entities allows the operator view records that have been 'blanked'.

19.3.3.4 Licensing

- Tick Can Manage Licenses to allow the operator to view, add and update license keys.

19.3.3.5 Layout

- Tick Change Dock Layouts to give operators permission to change dock layouts.
- Tick Can Switch Dock Layouts to give operators permission to use different dock layouts.
- Tick Can Use Personal Layouts to give operators permission to use their own layout.
    - The operator must have Can Switch Dock Layouts ticked to be able to use personal layouts.

- The operator must have Change Dock Layouts ticked to be able to customise personal layouts.

19.3.3.6 CCTV

- Tick Enrol CCTV Device to give operators permission to enrol new DVRs.

19.4 Operator

The Operators panel is accessible from the Administration tab.

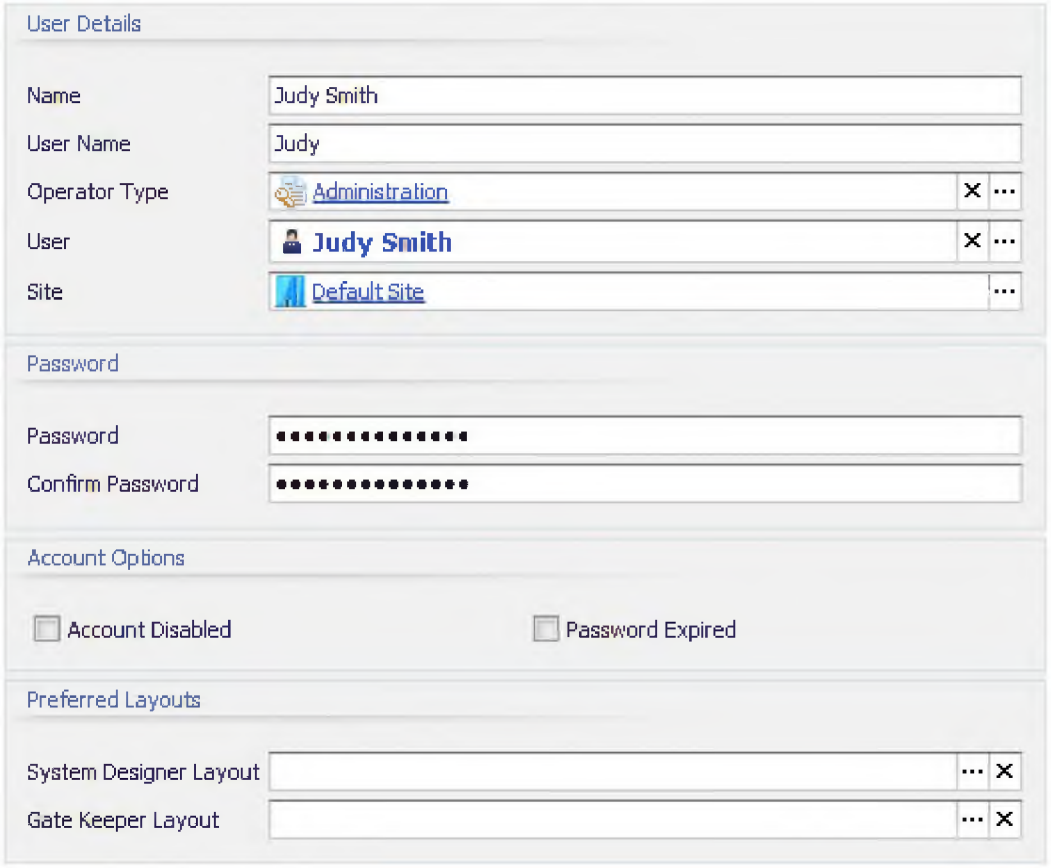


Figure 100

Operators consist of a few basic details:

Field	Description
Name	The actual name of the operator.
User Name	The name the operator enters when logging in to the Integriti client.
Operator Type	Configuration settings and permissions given to the operator.
User	Optionally, the operator can be associated with an Integriti controller user.
Site	
Password	The password the operator uses to log in to the Integriti client.
Account Disabled	Ticking this option will disable the operator account.
Password Expired	Ticking this option will force the operator to change his/her password next time they login to the Integriti client.
System Designer Layout	The default layout for the operator when using System Designer.
Gate Keeper Layout	The default layout for the operator when using System Designer.
Notes	Optional space for placing notes on the operator.

19.5 Custom Fields

Custom Fields provide a means through which the installer can add custom content to entity programming dialog windows.

Usage examples include but are not limited to:

- Users – Employee Payroll Number. (*Figure 102*)
- Users – Credit for goods and services available at a facility. (*Figure 102*)
- Powered modules – Date & Time the last service / battery change. (*Figure 101*)
- All modules – Photo / map of physical location of modules. (*Figure 101*)
- Air conditioner – A drop down editable list of the last mechanic to service the air conditioning.

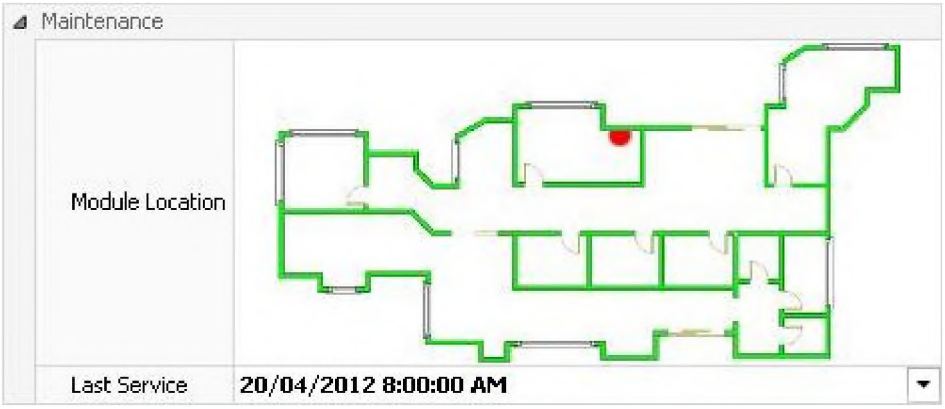


Figure 101

Custom fields can be configured by clicking on 

under the 

tab.

To create a new custom field:

1. Click 

to open a new custom field dialog.
2. Enter a Name to describe the custom field.
3. Select the item type.
4. Enter a category name.
5. Enter a description describing the purpose of the custom field.
6. Select the field type.
    a. If one of the drop-down box options was selected, click 

to add items to the custom field.

Once created, you cannot change the item type or the field type of custom fields.

Custom field descriptions appear at the bottom of the property grid.
If you create a custom field with the same category name as another property or custom field, the custom field will be grouped with it.

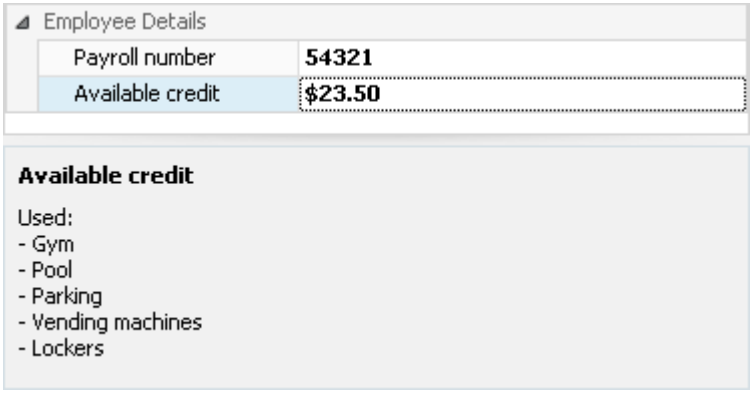


Figure 102

If the custom field type is an “editable drop down box” or “drop down box”, the values can be modified at any time. If an existing item with a custom field has a value that is modified at a later date, the item will retain the old value.

Field Type	Description
Text	A simple text field with up to 8000 characters.
Notes	A multiline text box with up to 8000 characters.
Integer	A number ranging from -2,147,483,648 to 2,147,483,647.
Decimal	A number with 15-16 decimal places ranging from -1.79769313486232E+308 to 1.79769313486232E+308.
Currency	A monetary value.
Date and Time	A combination of the following two field types.
Date	A date selector. From 01/01/0001 to 31/12/9999.
Time	A time selector. Hours, minutes, seconds, AM/PM.
Image	A BMP, GIF, JPG, JPEG, ICO or PNG image.
Check Box	Ticked or not.
Editable Drop Down Box	A drop-down list of selectable items. Custom text can be entered.
Drop Down Box	A drop-down list of selectable items.
Email address	An email address.
Telephone number	A Telephone number.

Large image sizes are supported but not recommended as they will impact Integriti client performance.

The checkbox will initially appear as  *because it is in an unknown state.*

19.6 Synchronization warnings

Synchronization warnings usually occur when there is a conflict between one or many controllers and the Integriti server.

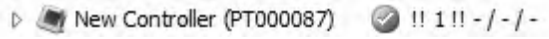
Clicking on the 

button under the 

tab will display the synchronisation warnings panel.

Example:

Two users have been given the same security PIN. When both records are saved, the server will attempt to download these records to the appropriate controllers. The controllers will reject the last one of the two users that were sent. The server will report a synchronization warning.

- The affected controllers will appear with an exclamation mark next to them in the hardware navigation panel to indicate that something needs attention.
  

- The user that was not sent to the controller(s) will be highlighted in the Users panel.

	Default Site	U7	Julianne Wetherell	14/01/2013 10:25:44 AM

- A warning message will appear at the bottom of the users programming window (*Figure 103*).
- The synchronisation warning will also appear as an entry in the system warnings panel.

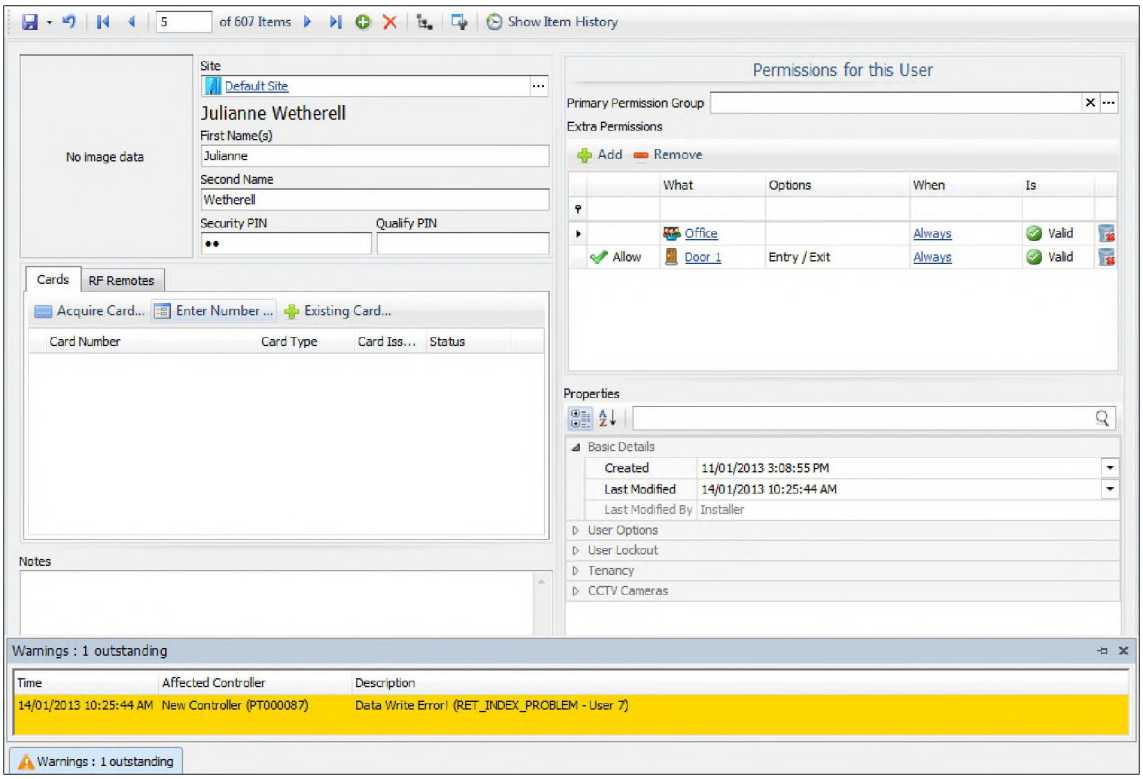

5
of 607 Items
Show Item History
No image data
Site
Default Site
Julianne Wetherell
First Name(s)
Julianne
Second Name
Wetherell
Security PIN
Qualify PIN
Cards
RF Remotes
Acquire Card...
Enter Number ...
Existing Card...
Card Number
Card Type
Card Iss...
Status
Notes
Permissions for this User
Primary Permission Group
Extra Permissions
Add
Remove
What
Options
When
Is
Office
Always
Valid
Allow
Door 1
Entry / Exit
Always
Valid
Properties
Basic Details
Created
11/01/2013 3:08:55 PM
Last Modified
14/01/2013 10:25:44 AM
Last Modified By
Installer
User Options
User Lockout
Tenancy
CCTV Cameras
Warnings : 1 outstanding
Time
Affected Controller
Description
14/01/2013 10:25:44 AM
New Controller (PT000087)
Data Write Error! (RET_INDEX_PROBLEM - User 7)
Warnings : 1 outstanding

Figure 103

19.7 Cross references

Cross references can be used to quickly discover what entities the current entity is referenced to or referenced from. Click the  button to display the cross references for the entity.

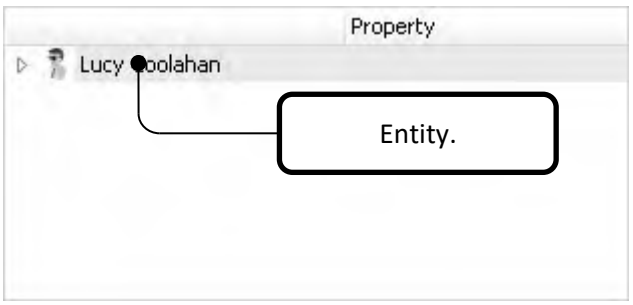


Figure 104

Clicking the triangle to the left of the entity displayed will expand-out said entity, displaying other entities referenced to/from.

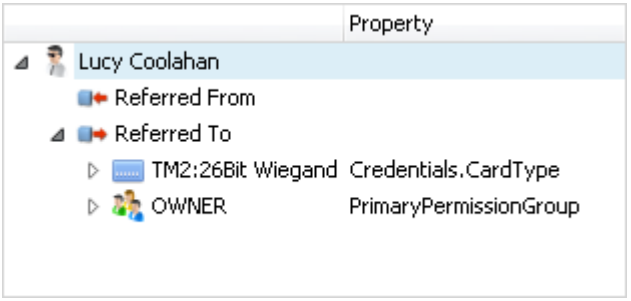


Figure 105

In ***Figure 105*** we can see that the user 'Lucy Coolahan' has been expanded out. There are two other entities that this entity refers to – a credential and permission group.

19.8 Audit Trail

The Audit panel contains a list of all changes made. Each individual change is logged within the Integriti database.

Take advantage of the audit feature. If you've made a programming error, use audit to help review the changes you made.

You can view the audit trail of an individual item by going in to that item's programming screen and clicking the Show Item History button.

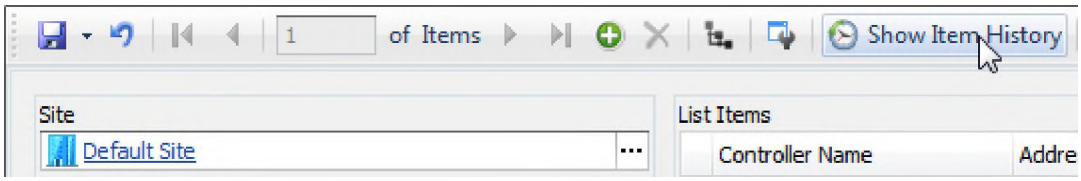


Figure 106

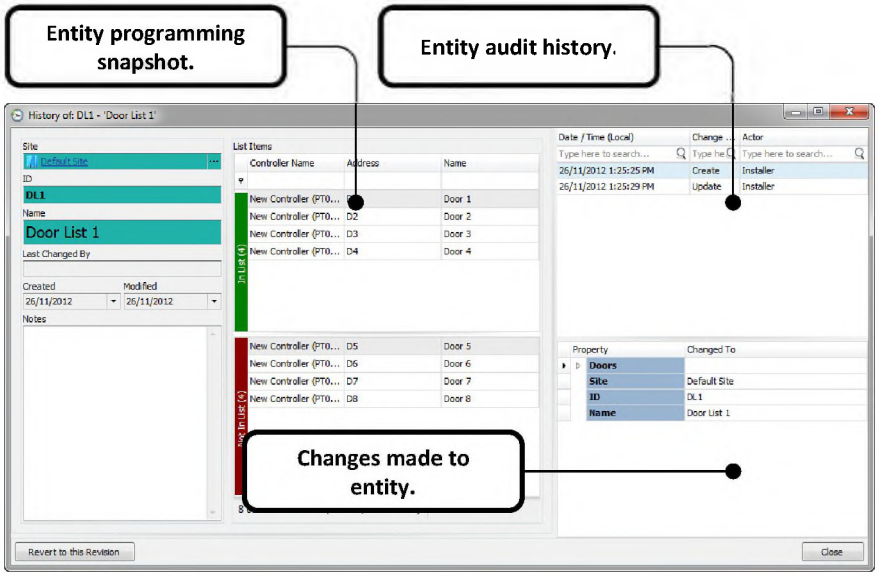


Figure 107

The entity audit history list will display the date / time, change type and actor for each event. Clicking on an item in this list will display a programming 'snapshot' of the entity at the selected time. A summary of the changes is easily viewed in the bottom right-hand corner of the screen.

Appendices

A. Integriti log viewer

It's important to understand how to use the Integriti log viewer in the event of an error. In most cases it is worthwhile for the administrator to read the most recent events in the log to diagnose errors.

GUI layout

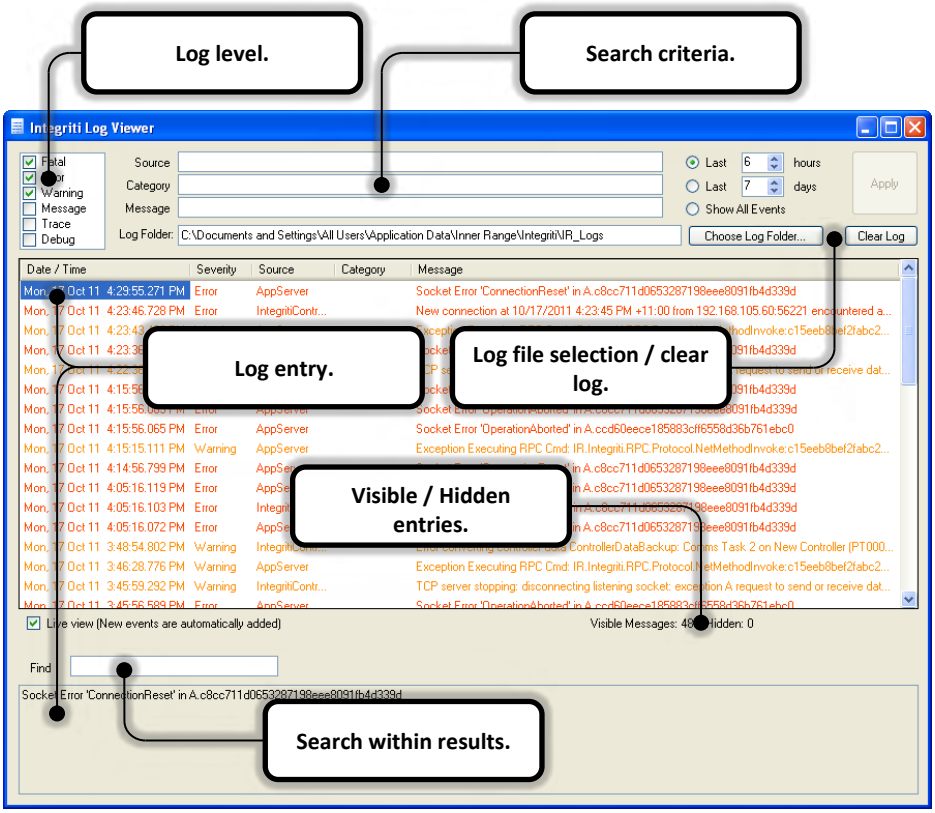


Figure 108

Log level

There are 6 log levels available – Fatal, Error, Warning, Message, Trace and Debug. By default only the first three items are ticked. Usually these items are all that is required to diagnose an error.

Search criteria

There are three search boxes available – Source, Category and Message. When applying your search criteria the returned results will match all three search boxes. The search boxes match the source, category and message columns in the list below.

Log file selection / clear log

Logs are simply groups of text files created with particular time & date stamps for organisation.

Log entry

Clicking on an individual log entry will reveal more detail in the box below.

Visible / Hidden entries

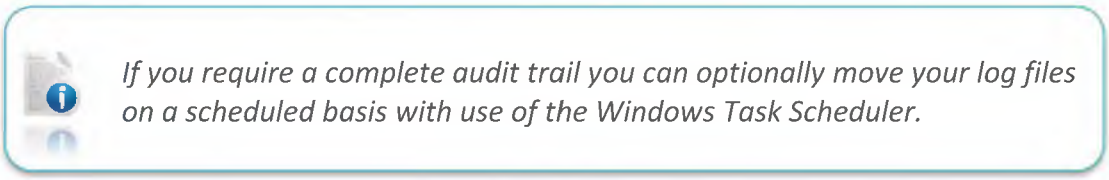
The total visible and hidden entries are filtered by the search criteria and the time frame selected.

Using the log viewer

Log file management

Clicking the 

button will delete the log files in the currently selected directory. It is recommended that you clear your logs regularly. This will make searching your log files easier if an error occurs.



Clicking the 

button allows you to select another folder that contains log files.

Using filters in the log viewer

The log viewer search boxes (Source, Category, Message and Find) support the following delimiters:

; A semicolon can be used to separate search terms (logic OR).

- A dash (minus) can be used to exclude search terms (logic NOT).

Searches performed are not case sensitive.

Examples

- "`Initializing database`" will search for log entries containing "`Initializing database`" whereas "`Initializing;database`" will search for results with "`Initializing`" or "`database`".
- "`Initializing;-database`" will search for entries containing "`Initializing`" that do not include "`database`".

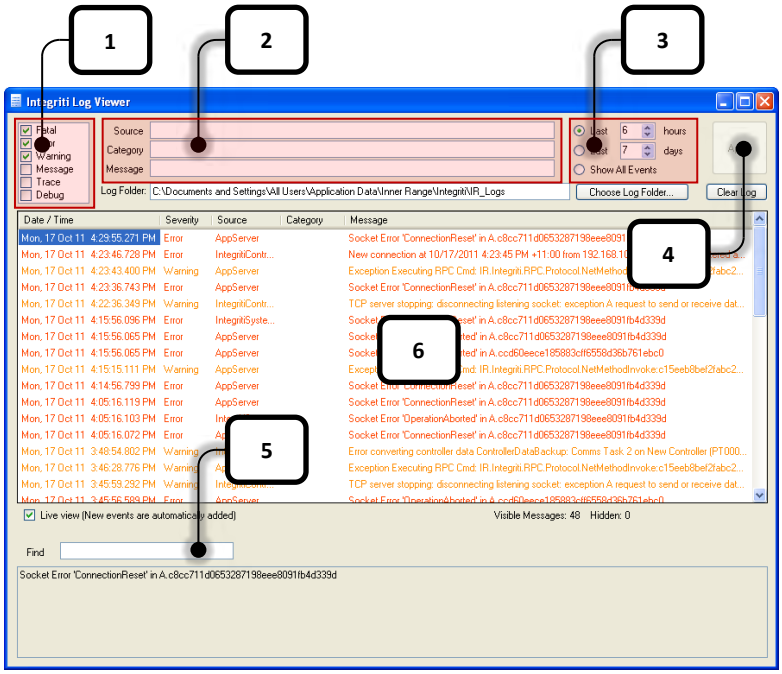


Figure 109

1. Select the desired log level.
2. Enter your search criteria.
3. Select the time period to search through.
4. Apply your search terms.
5. Optionally, use the "Find" box to narrow your search results.

Example usage

Search for errors where there was an issue initializing the database because the required services were not running in the last hour.

1. Ensure the Error checkbox is ticked. Un-tick the other checkboxes. (*Figure 109*)
2. Type "`AppServer`" in the Source search box.
    a. Type "`Initializing database`" in the message search box.
3. Select the Last Radio button. Type "`1`" in to the hours box to the right of the Last radio button.
4. Click Apply and wait for the results to be filtered.
5. If many results are returned you might want to search through the displayed results using the Find search box below the displayed results.
6. Click on a log entry to see more detail in the box at the bottom of the window.

B. Glossary of terms

ACCESS CONTROLLER (AC)	One type Integriti control module. (See also "CONTROL MODULE" and "SECURITY CONTROLLER")
ADDRESS	A number allocated to every module in the system that is connected to a Control Module via the LAN. Allows the Control Module to identify each module.
ALARM	The condition of a zone or system input when it is in an abnormal condition and the system has been set to respond to that condition. i.e. Area/s turned ON.
ALPHA-SEARCH	Many items in the system are identified with text names (as well as ID number). The Alpha-search option allows the User to quickly locate items by using the digit keys of the LCD Terminal to jump to names beginning with a specific letter.
ANTI-PASSBACK	A system to monitor/prevent a user passing through a door into the same area as the system records them as being already in. e.g. Prevents a user from passing their card back under a door for another person to use.
AREA	Dividing a system into areas allows different parts of the system to be protected differently. i.e. Turned ON or OFF at different times, Reported separately, etc. Areas are named for easy identification. e.g. WORKSHOP, OFFICE, STORE, etc. See TWENTY-FOUR HOUR.
AUXILIARY	A device used to control an external device or indicate that a particular condition or conditions exist in the system. An auxiliary may be a physical output (Lock auxiliary, Entry warning device, Strobe, etc.), or a "phantom" auxiliary used in the programming to link two or more functions together.
CREDENTIAL	General term for Magnetic Stripe, Proximity, Wiegand cards & other devices such as Insert keys, Barcodes, etc. that can be utilized to operate the system.
CONTROL MODULE	The Control module stores all data, communicates with all modules connected to the system LAN, and reports alarms & system activity to the central station and/or computer.
DE-BOUNCE	See "Zone De-bounce"

DEFER AREA	Option to define specific Area/s that when turned Off by specific User Type/s, will start a timer running. When the timer expires, the Area will automatically turn On again, unless the User enters their code to "Defer" the Area On function and re- start the timer.
DOOR	An access point in a system that can be programmed to provide and restrict access to users as required, and monitored for abnormal conditions.
DOOR FORCED	A System Input for each Door to indicate when a Door is Locked and has been opened without a valid unlock command. i.e. Without valid User Access, REN / REX button, Auto unlock via Time Period, etc.
DOOR OPEN TOO LONG (DOTL) (or DOOR HELD)	A System Input for each Door to indicate when a Door is held open for too long when opened with a valid unlock command. The "Maximum Door Open Time" is programmable for each door.
DUAL USER	Requirement for two Users to present their Cards / PIN codes at specified Door/s before access is granted.
DURESS	PIN code/s can be programmed that will activate a System input on the Terminal where the code was used, to report a Duress condition to the Central Station. i.e. When a user is being forced to turn OFF the system by an intruder, they would do so using their "Duress" PIN code.
DVR	Digital Video Recorder.
EMS	Elevator Management System.
ENTRY DELAY	The maximum time that a user has to turn OFF an area, after entering the area and activating any detection devices nominated as "Primary Entry" types.
EXIT DELAY	The maximum time that a user has to exit the area after turning the area ON. Detection devices nominated as "Exit" types, will not generate alarms during this time.
HLI	High-level Lift Interface. Serial data protocol that allows communications between an Elevator Management System and an Access Control System.

HOLIDAY	Specific dates or periods may be programmed as "Holidays". Holidays may then be utilized in the "Time Periods" to specify whether the Time Period will be valid OR in-valid on the holiday date/s specified.
INPUT	An input may be a physical Zone Input on a Module, or a System input activated when specific conditions occur on a Module. (e.g. Low Battery, Line fault, Cabinet Tamper, Door Open Too Long, Illegal Card, etc.) Programming of Inputs and Areas will determine how (and if) the system will respond (generate an alarm, activate an auxiliary, etc.) when any input changes state. (See also "ZONE" and "SYSTEM INPUT")
INTERLOCK GROUP	A programming option allowing a List of Doors to be interlocked together. i.e. A Door will not un-lock unless all the other Doors in the List are locked and closed. Interlock Groups can also be programmed to check the status of a specific Area, Auxiliary or Zone before allowing access if required.
ISOLATE / DE-ISOLATE	Isolating enables faulty devices wired to Zone inputs, or System inputs that cannot be immediately restored, to be temporarily taken out of service in order to prevent them causing alarms when the area is turned ON. Once the problem is rectified, the device is De-isolated to restore normal operation.
LAN	(Local Area Network) Data communications network used in the system to connect modules (LCD terminals, Expander Modules, Reader Modules, etc.) into the system.
LCD	(Liquid Crystal Display) A display that allows information to be viewed in plain English text. The LCD used in the LCD Terminals is backlit to allow viewing in any lighting conditions.
LED	(Light Emitting Diode) A semiconductor light source used as an indicator lamp with the advantages of lower power, longer life and higher speed over conventional filament lamps. Used on module PCBs to indicate status and diagnose problems. Also used on Elite LCD Terminals to indicate Area status and/or other sys- tem conditions.

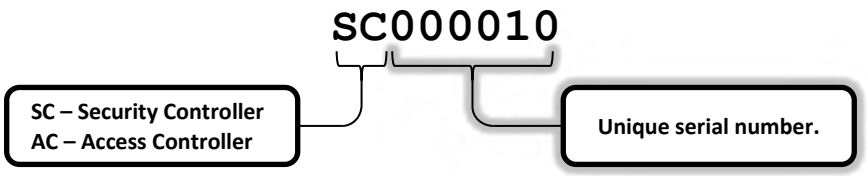
LIFT	A special access point in a system that can be programmed to provide and restrict user access to Lift Cars and Floors. This is achieved by enabling specific Floor selection buttons via a Reader in a Lift Car.
LISTS	Lists are used to simplify system programming. Once a List is created it can then be assigned in other programming options such as User Types, Time Periods, Calculated Auxiliaries and Named Actions, to define the items that are allowed to be controlled / accessed. There are 6 different types of Lists; Area, Siren, Door, Lift Car, Floor and Auxiliary Lists.
MCP	Main Control Panel. (See also "ACCESS CONTROLLER" and "SECURITY CONTROLLER")
MENU GROUP	Menu Groups are programmed to define system operations & menu options allowed, and are then allocated to User Types and/or LCD Terminals to determine the control and menu access available.
MODULE	Module is the general term used for any device that connects to the system LAN to form part of the system, and includes LCD Terminals, Several types of Expander Modules, Reader (Door) Modules and Analogue Input Modules.
PANIC	A Panic alarm can be activated by a User by pressing the **[Help]** key 3 times in quick succession.
PIN CODE	A unique numerical code of 1 to 8 digits, allocated to any user in the system required to perform functions at an LCD Terminal or Keypad.
PRIMARY ENTRY ZONE	A type of Input (defined in the Process Group) that will start an Entry delay timer running when a User first enters an Area. (See "Entry Delay")
PROCESS GROUP	Process Groups are programmed to define how Inputs (zones & system inputs) will be processed. Every Input in an Area is assigned a Process Group to deter- mine what processing (if any) will take place when the input changes state in that Area. (States include: Seal, Alarm, Tamper and Isolate)

PULSE COUNT	An option in Process Group programming that requires an Input to register a specified number of Seal to Alarm transitions within a specified time before it will be regarded as being in alarm. The number of pulses, and time are defined in Area programming if required.
READER	General term for a variety of card, insert key, biometric readers, etc. which may be utilized on the system to access Doors, access Lifts, Login, Logout, etc. Includes Magnetic swipe or insert, Proximity, Wiegand, Barcode, Hand geometry, Fingerprint, or scrambling Wiegand Keypads.
REED (or REED SWITCH)	(Also known as "Door Contact") Switch Contact activated with the presence of a magnetic field. Used to indicate the status of a Door/Window etc.
REN	(Request to Enter) Typically a button provided to unlock a door from the outside, bypassing the need to use a reader during low security periods.
REX	(Request to Exit) Typically a button provided to unlock a door from the inside either bypassing the need to use a reader during low security periods, or because an internal (exit) reader is not required. The "REX" device can also be a PIR or Photo-Electric beam to detect the User approaching the door.
REVIEW	Log of alarms and events that can be viewed at an LCD Terminal or PC. Each event is time/date stamped and programming options allow the installer to define which events are not logged.
SECURITY CONTROLLER (SC)	(Integriti Security Controller) See Control module.
SITE CODE	Used in conjunction with certain types of access control cards to identify a particular batch of cards when using the Site Code method. The system allows multiple Site Codes to be programmed.
SYSTEM INPUT	System inputs are activated when specific conditions occur on a Module. They are used to indicate situations such as Cabinet tamper, Siren tamper, AC fail, Low Battery, Fuse tamper, Communications problems, LAN problems, Panic, Duress, Door Open Too Long, etc. etc. Programming of Inputs and Areas will deter- mine how the system will respond (generate an alarm, activate an auxiliary, etc.) when any system input changes state.

TAMPER	An abnormal condition on a zone input or other device connected to the Integriti controller that indicates that interference or damage has occurred to the device or it's cabling. e.g. Open circuit or Short circuit condition. The system can be programmed to provide 24Hr monitoring for the tamper condition.
TERMINAL	Device connected to the system via the LAN to allow user interface via keypad entry and alphanumeric display. e.g. Elite LCD Terminal.
TIME PERIOD	A time period specified in terms of START time, END time, and valid DAY/S of the week. Four such periods can be specified in each Time Period. Time Periods are utilized in many functions such as specifying the valid period of user access, groups and lists, and turning areas and auxiliaries on and/or off automatically.
TWENTY-FOUR HOUR	
USER	Any person allocated a PIN code and/or card who is able to perform operations on the system.
WIEGAND	Data protocol originally developed for sending Wiegand access card data from the Reader head to the host controller and now adopted as an industry standard for access credential Readers including Proximity and Smart Card Readers.
ZONE (or ZONE INPUT)	A physical Input on any Module in an Integriti system. Zone inputs are used for connecting detection devices (PIRs, Door/Window Reeds, Photoelectric beams, etc.), Keyswitches, "Request to Exit" buttons, Smoke detectors, Seismic detectors, etc., etc. Programming of Inputs and Areas will determine how the system will respond (generate an alarm, activate an auxiliary, etc.) when any zone input changes state.
GUI	(Graphical User Interface) A user interface based on graphics (icons and pictures and menus) instead of text; uses a mouse as well as a keyboard as an input device.

C. Identifying the Integriti controller serial number

Each individual controller has its own unique serial number located on the CPU near the centre of the Integriti PCB. Controller serial numbers have the following format:



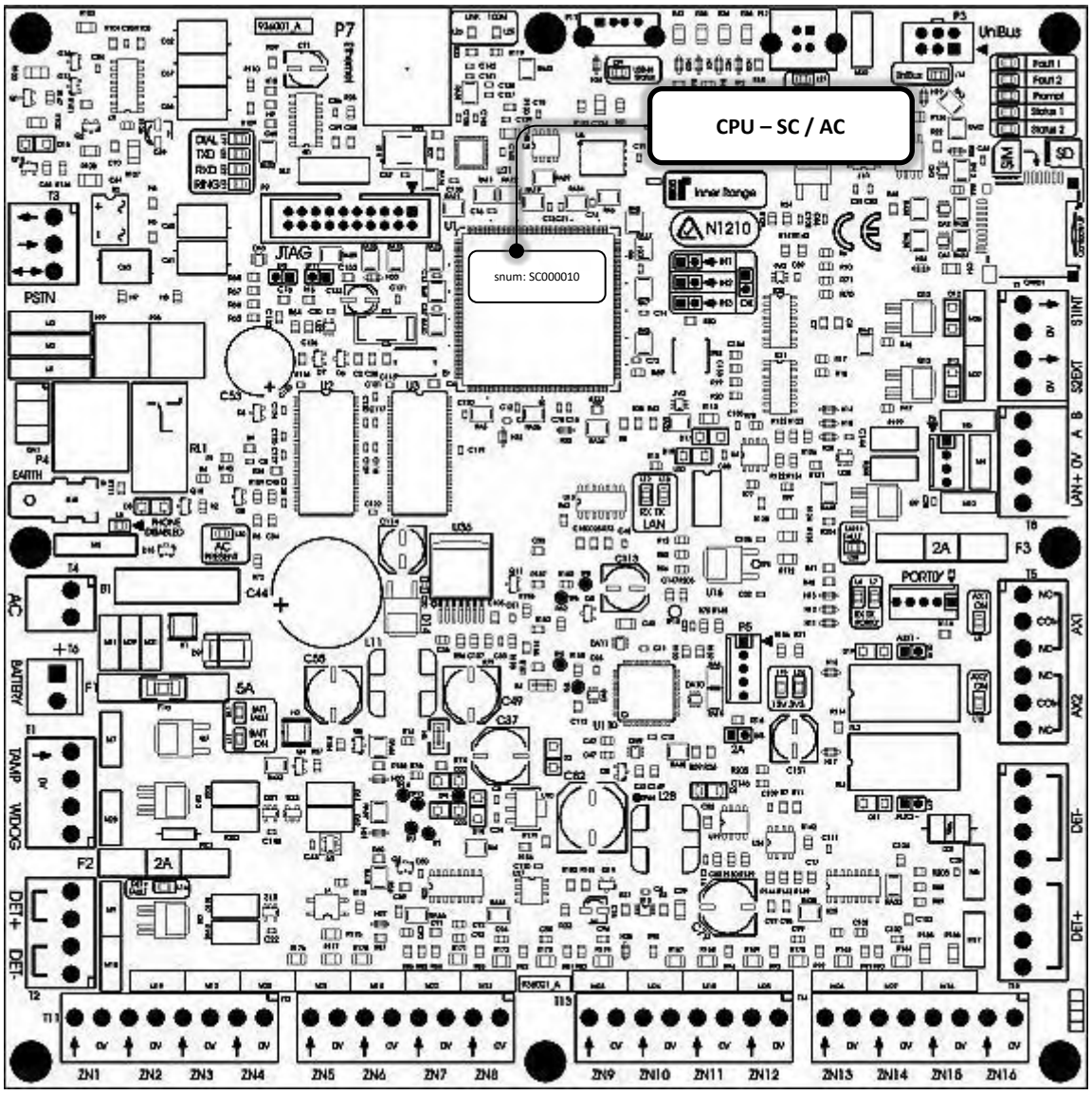


Figure 110

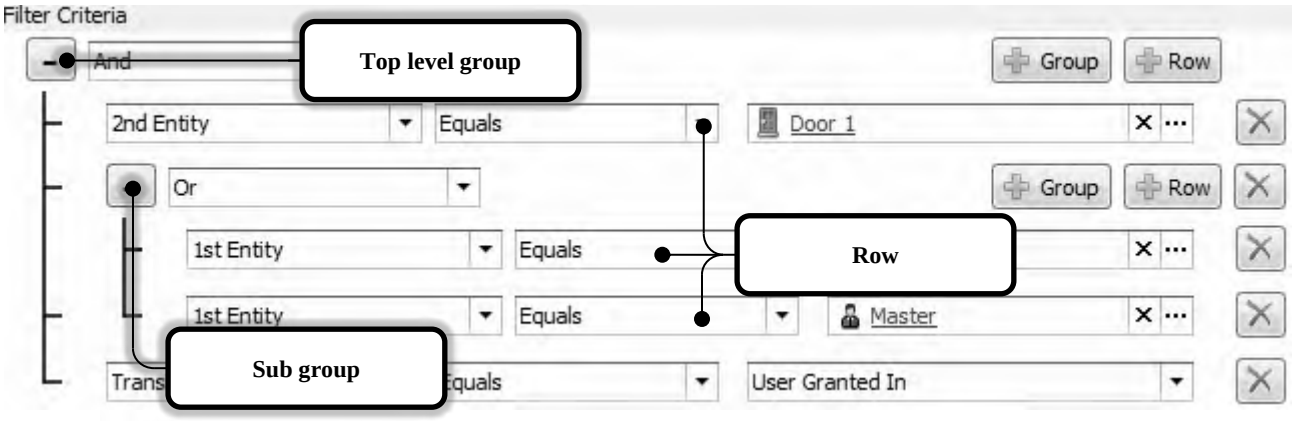
D. Random Number

The Integriti controller has the ability to generate a random number between 1 and 8388607.

To generate a random number, you will need to use a macro to 'Set Entity To Expression...'. If the expression value used is 8388607, the actual value of the entity that is being set will be a random number between 1 and 8388607.

E. Filter Stacks

Filter stacks can be found in a number of locations throughout the Integriti management software. This section describes how to use them.



Use the [-] and [+] buttons to expand and collapse groups.
Click [Group] to add a new sub group to the group.
Click [Row] to add a new row to the group.
Click [X] to remove the row / group.

A group is a set of conditions combined by the same logical operator. The filter criterion above contains two groups.

Each group has its own operator that defines the logical relationship between the sub rows and groups. Group sub items can use a logical AND or OR.

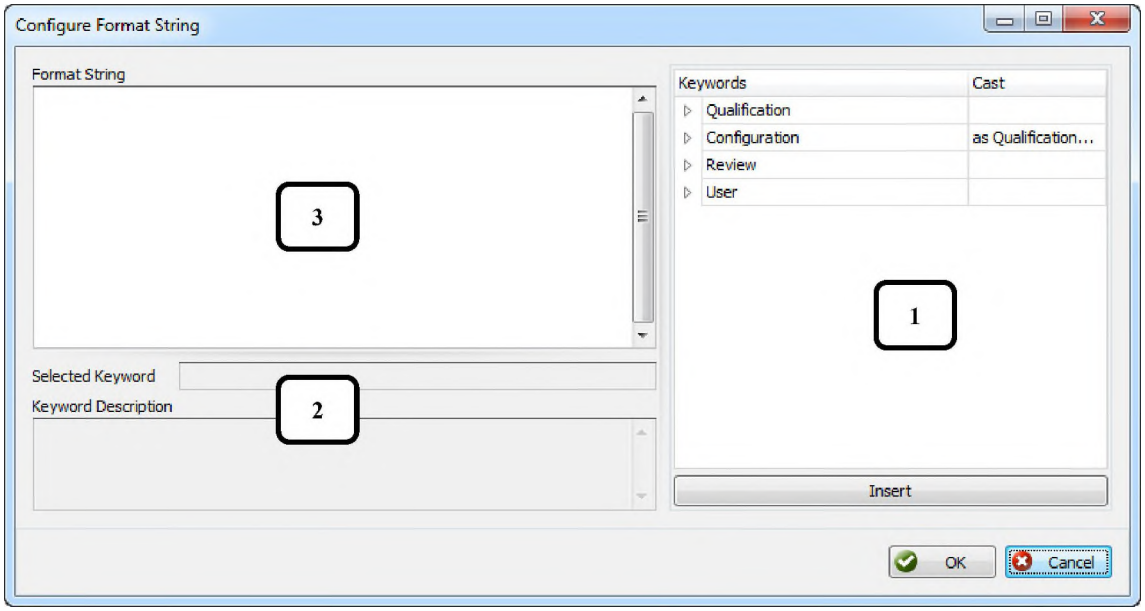
Each row has three properties – criteria, criteria operator and operand value.

F. Action types

Configure Format String

The Configure Format String editor will appear when editing customisable messages that can be sent as part of an action.

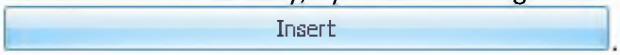
Actions such as Log Review or Run External Program have flexible text fields that can contain keywords relevant to the action it is being created for. Click on the ellipsis ... to open the Configure Format String editor.



The keywords **(1)** shown in the Configure Format String editor will differ depending on where the editor was opened from. E.g. 'Log Review' or 'Run External Program'

If a keyword has been selected from the list **(1)** a basic description may appear **(2)**.

The format string field **(3)** allows direct entry of custom text including keywords. Keywords can be entered manually, by double clicking or selecting the item and clicking Insert



Backup Database

This action type will save the database as a .bak file in the specified folder. The default location is 'C:\Program Files\Inner Range\Integriti Pro\Backups'.

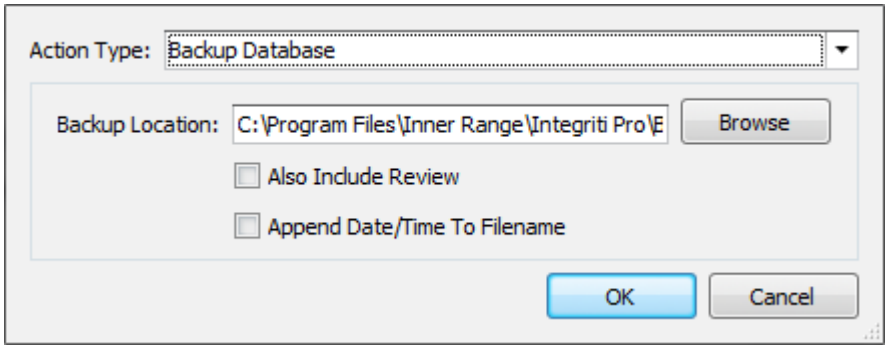


Figure 111

Backup Location

Click the Browse to select a save folder location or you can manually enter a location in the text box provided.

Also Include Review

Ticking this checkbox will cause all review events in the database to be saved in the database backup.

Append Date/Time To Filename

If this option is ticked, databases backed up by this action will have the date and time appended to the filename. Ticking this option is recommended.

An example of a database backup with this option ticked:

```
Integriti Backup 20130130 170613.bak
```

Control Workstation

Control workstation allows remote control of a workstation running the Gate Keeper client application.

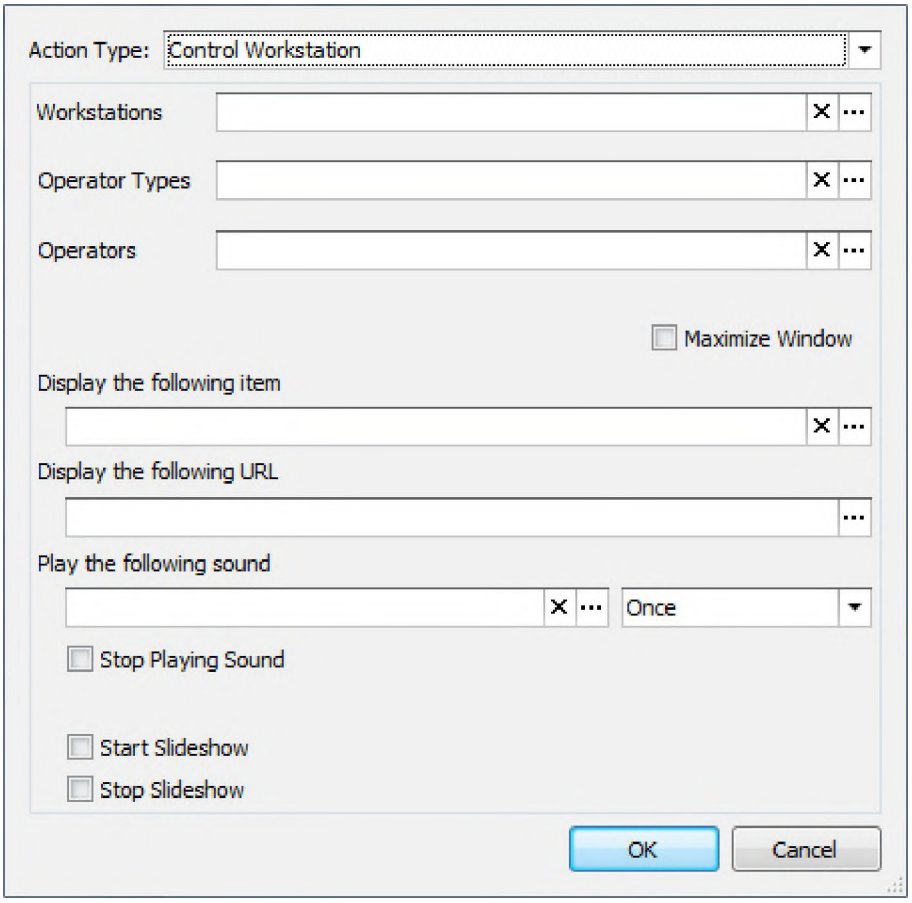


Figure 112

Workstations, Operator Types and Operators are all optional fields. At least one of the three fields must be filled in in order for the action to work. Each of the three fields are bound by AND logic. So for example, if the Workstations and Operators fields were populated, only the specified workstations with the specified operators logged in to them would be controlled by the action.

Ticking the Maximize Window checkbox will cause the Gate Keeper application to maximise from a minimised or floating state. If the Gate Keeper application was not already maximised, the application will be given focus.

Play the following g sound will play the selected .wav audio file on the Gate Keeper client application. The frequency can be set to Once, Twice, Thrice or Continuously.
When playback has been set to 'continuously', the sound can be stopped by another Control workstation action. Use the 'Play the following sound' once option, select 'Stop Playing Sound' or the operator can close the Gate Keeper client.

Select Start or Stop Slideshow to start/stop the pre-configured slideshow. These options have no effect on clients where the slideshow has not been configured.

Please refer to the Gate Keeper documentation for information on configuring slideshows.

Controller Action Types

This section covers items specific to the individual action types within the Integriti controller. For more information on actions please refer to the section titled Named Actions.

The following is a list of all of the available action types:

Control Area & Control Area List

These action types can be used to control an area, set an area defer, control a 24 hour area or cancel an area exit delay.

Control Type	**Normal**	- Controls the selected area.
	Defer	- Set/Reset the area defer.
	Twenty-four Hour	- Controls the 24 hour area.
	Cancel Exit Delay	- Stops the exit delay and arms the area.
When Asserted…	**Nothing**	- Don't do anything.
	Arm	- Arm the area / 24 hour area, Set/Reset the area defer or stop the exit delay.
	Disarm	- Disarm the area / 24 hour area.
	Toggle	- Toggle the arm/disarm state of the area / 24 hour area.
When Disasserted…	Can be used to arm, disarm or toggle the selected area or its associated 24 hour area.	

Control Aux & Control Aux List

These action types will control an auxiliary / auxiliary list.

Control Type	**Normal**	- Normal auxiliary control
	Timed Only	-
	Leave Timer	-
When Asserted/ When Disasserted…	Can be used to turn on, off or toggle the selected auxiliary.	
Delay On/		

Delay Off. Ticking these options will change the On/Off Time to a Delay On/Off Time.

Update Dynamic Only

Control Door & Control Door List

These action types will control a door / door list.

Unlock time Time to unlock the door for (up to 18 hours, 12 minutes and 15 seconds.

When Asserted/ When Disasserted… Can be used to turn on, off or toggle the selected auxiliary.

Secure/Unsecure a floor on a lift car, Secure/Unsecure a floor on a lift car list, Secure/Unsecure a floor list on a lift car & Secure/Unsecure a floor list on a lift car list

These action types will secure / unsecure a floor on a lift car / lift car list.

Floor The floor to secure / unsecure.

Lift Car/ Lift Car List The lift car / lift car list to secure / unsecure.

Cancel Button Timer

Floor Time Up to 4 minutes and 15 seconds.

When Asserted/ When Disasserted… Can be used to turn secure, unsecure or toggle the selected lift car / lift car list.

Trigger Input

This action type will control the state of the selected input.

Input State One of the 16 possible input states.

Update State If selected, it will make state change persistent (rather than momentary). The input state can be changed by another action or by the physical input.

When Asserted/ When Disasserted... Can trigger, restore or toggle the state of the selected input.

Set Area User is in

This action type can be used to relocate a user to a specific area.

User The user to .

Area One of the 16 possible input states.

Don't update area user counts One of the 16 possible input states.

When Asserted/ When Disasserted... Can trigger, restore or toggle the state of the selected input.

Set Area User Count

This action type can be used to adjust the user count of the specified area.

Input State One of the 16 possible input states.

Set Input Counters

This action type can adjust the count on the specified input.

Input State One of the 16 possible input states.

Control Siren

This action type will control the state of the selected siren.

Input State One of the 16 possible input states.

Set Timer Variable

This action type can be used to set a timer variable.

Input State One of the 16 possible input states.

Set Variable

This action type can be used to set the value of the specified variable.

Input State One of the 16 possible input states.

Control Airconditioning

This action type will control the specified air-conditioning unit.

Input State One of the 16 possible input states.

Macro Control

This action type will control the specified macro.

Input State One of the 16 possible input states.

Isolate

This action type will control the state of the selected input.

Input State One of the 16 possible input states.

Comms Task Control

This action type will control the specified communications task.

Input State	One of the 16 possible input states.

Grant Amnesty

This action type will grant controller wide amnesty for one transaction per user.

Controller	The controller to grant/deny amnesty.
When Asserted/ When Disasserted...	Can Grant, Deny or toggle controller wide amnesty.

Set Air-Conditioner Temperature

This action type will set the temperature of the specified air conditioning unit.

Air conditioner	The air conditioning unit to control.
Unit	The number of the unit to control.
Zone	The number of the zone to control.
Temperature	The temperature in degrees Celsius to set the air conditioning to.
When Asserted/ When Disasserted...	Can Turn On, Turn Off or toggle the air conditioning unit.

Call Floor

This action type will call a floor on a lift car.
Only the `Floor` and `Lift Car` fields are required. The remaining 'Action To Take` options have no effect.

Floor	The Floor to send the lift car to.
Lift Car	The Lift Car to control. The lift car must be a `Home Floor Caller`.

Escalate Alert

This action will escalate alerts within the specified alert groups. The priority, colour and alert definition can be modified.

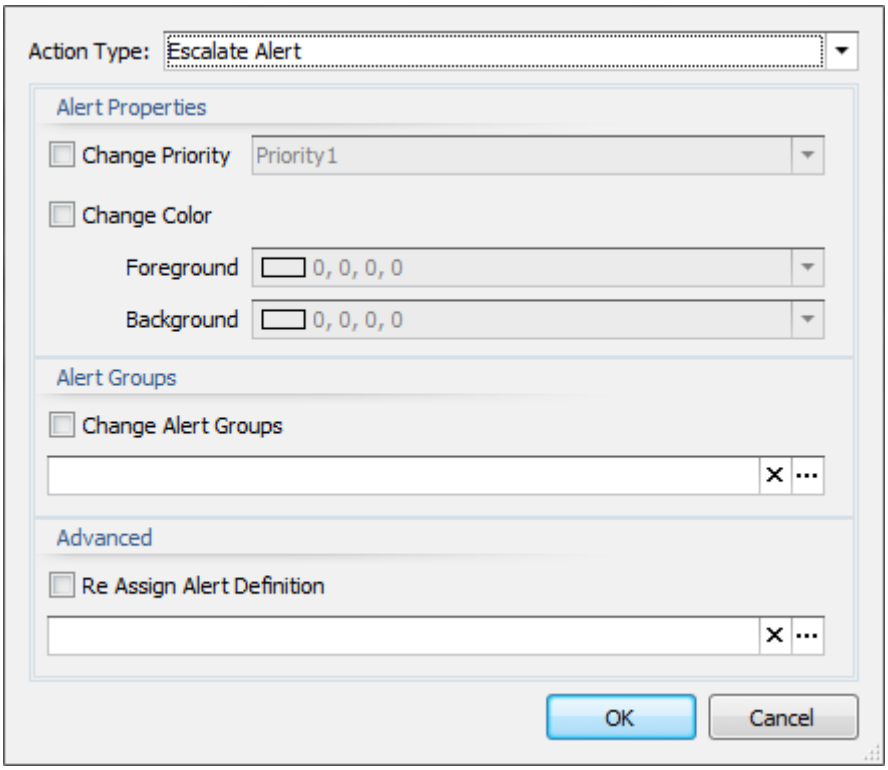


Figure 113

Change Alert Groups

The alert groups that the alerts belong to that are to be modified.

Re Assign Alert Definition

The Alert Definition of the alerts can be changed to the definition selected here.

Change Priority

Changes the priority of the Alert.

Change colour

Changes the foreground and background colours of the alert text seen in the alert viewer.

Log Review

Use Log Review to send custom text to review.

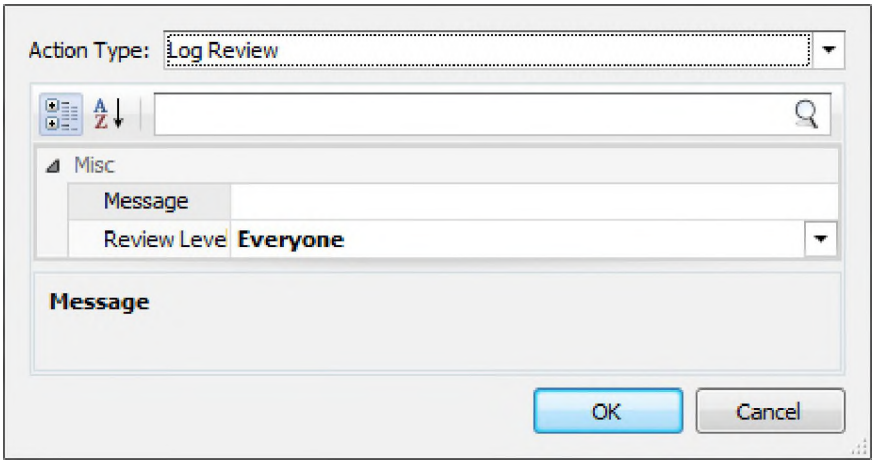


Figure 114

Message

The text to log to review.

Review Level

The review level for the message text.

Parallel Task List

Parallel Task List creates a new task list. All tasks added to this task list will be executed simultaneously.

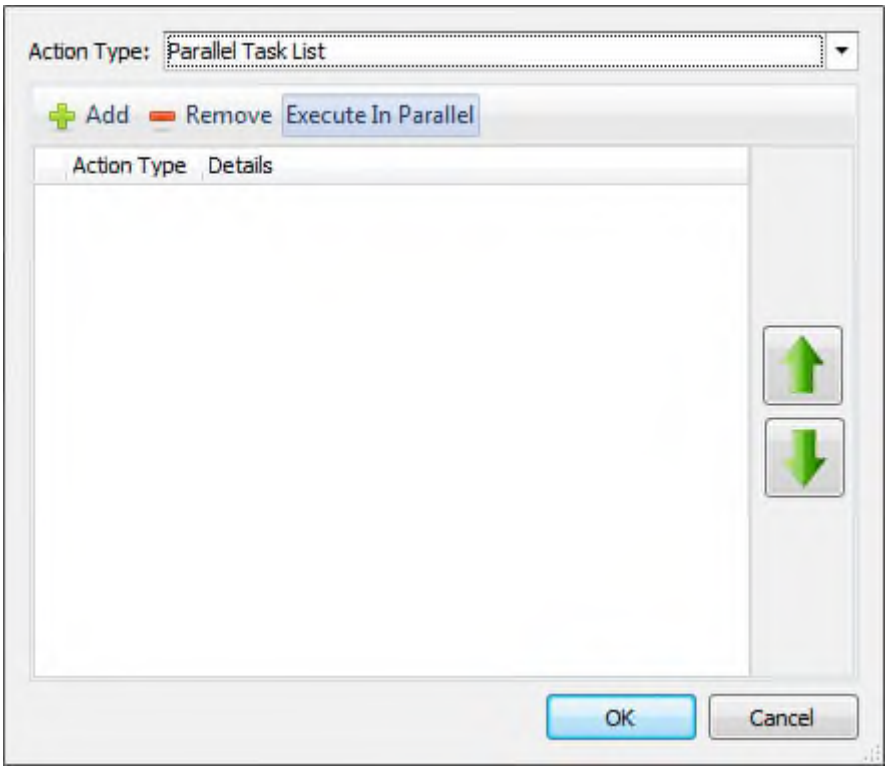


Figure 115

Pause

Pause will suspend execution of the action list for the duration set. This action has no effect in a Parallel Task List.

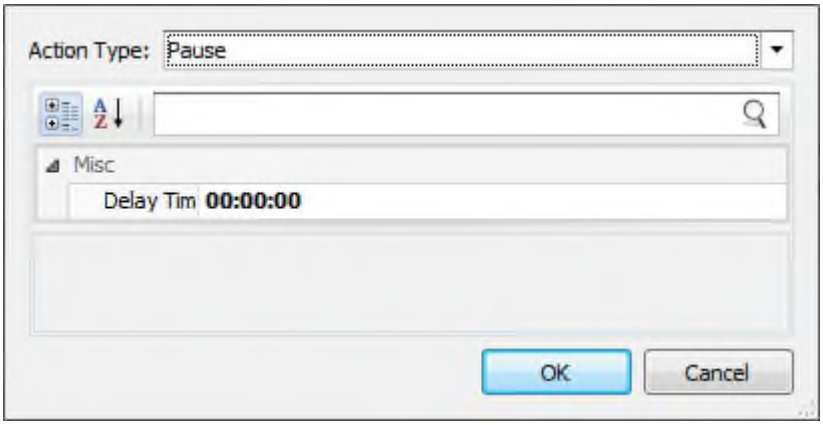


Figure 116

Run External Program

This action can be used to run a 3rd party program.

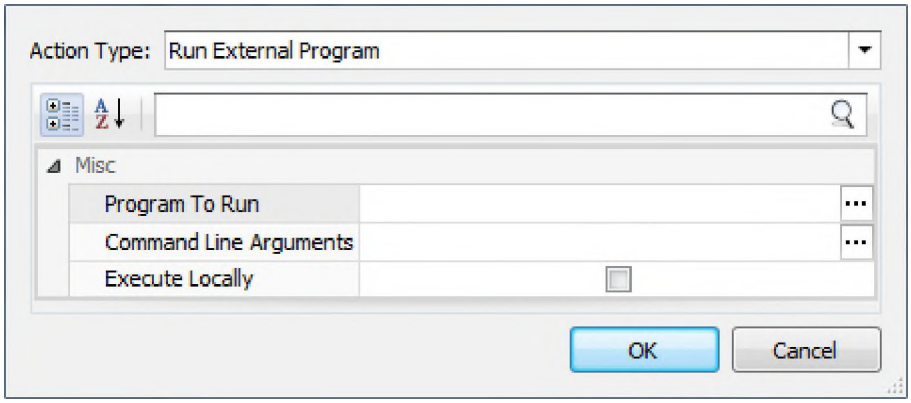


Figure 117

Program To Run

Click on the ellipsis to the right of 'Program To Run' to select the 3rd party application that will be launched.

Command Line Arguments

Optional command Line Arguments can be sent if required. Clicking on the ellipsis for this option will open the Configure Format String editor.

Execute Locally

Ticking the Execute Locally option will result in the application being launched on the client workstation instead of the Integriti server.

Send Communication Message

Use Send Communication Message to send an email or SMS to one or many recipients.

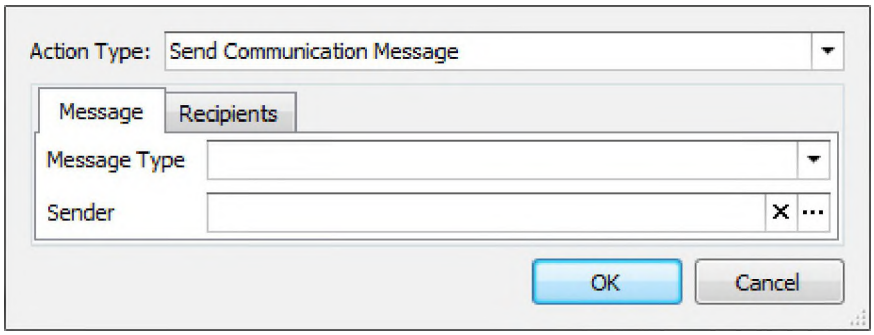


Figure 118

Message

Message Type

Set to SMS or Email. Use None to disable.

Sender

A communications handler must be created for sending of the SMS or Email.

Recipients

Click Add User under the Recipients tab to add users to the list of recipients.

Clicking Add Custom allows entry of a custom number/email/… for the message type selected.

Cleanup Database

This action type will purge review messages, audit history or alerts.

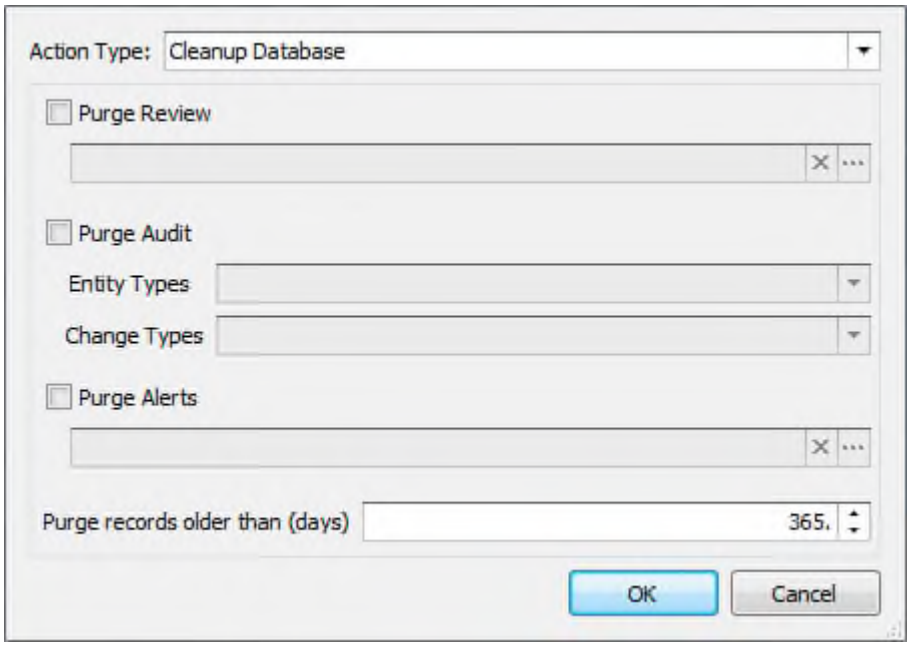


Figure 119

This action cannot be undone. Before using any of the three options, make sure the database has been backed up.

Custom Enhancement

Custom Enhancements are arranged by Inner Range Professional Services.

Sequential Task List

Sequential Task List creates a new task list. All tasks added to this task list will be executed in the order that they appear in the list.

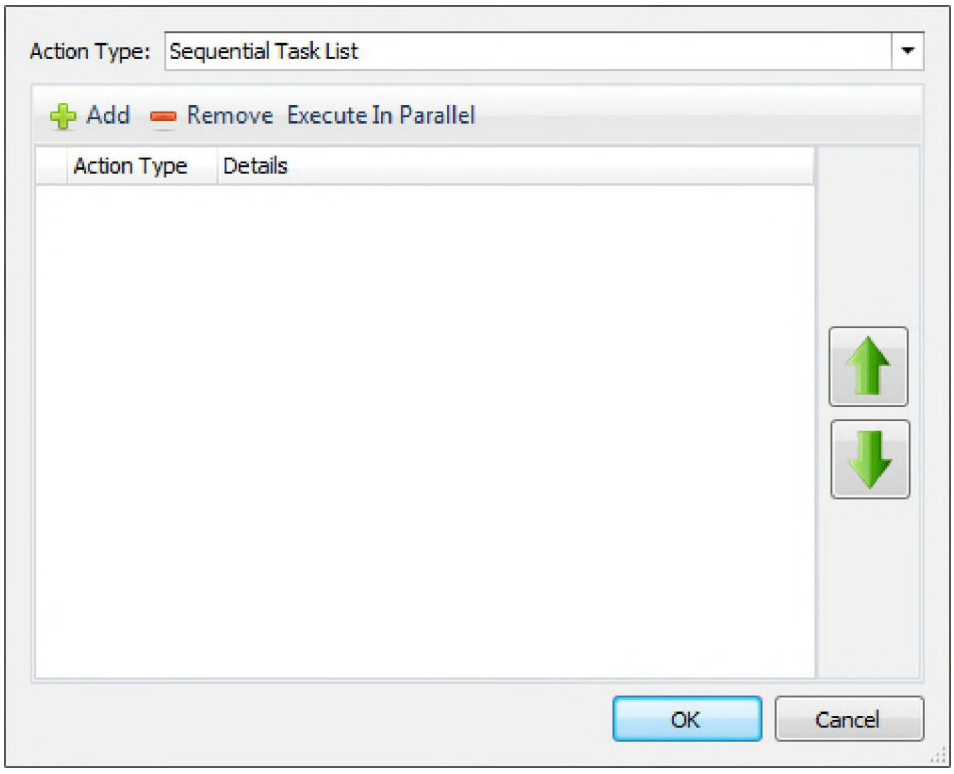


Figure 120

Synchronize Controller Time

Synchronise the time on one or many controllers.

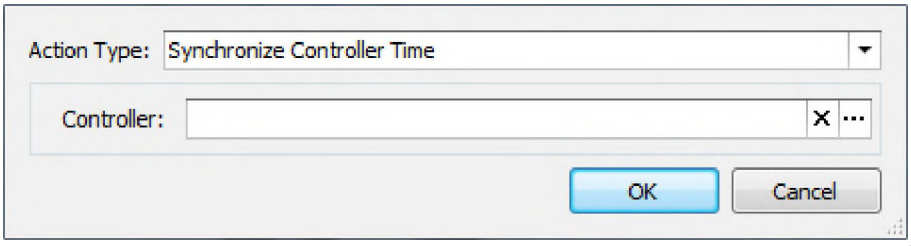


Figure 121

Execute Report

Using Execute Report will run the selected report and send the result to file, a printer or as an email attachment.

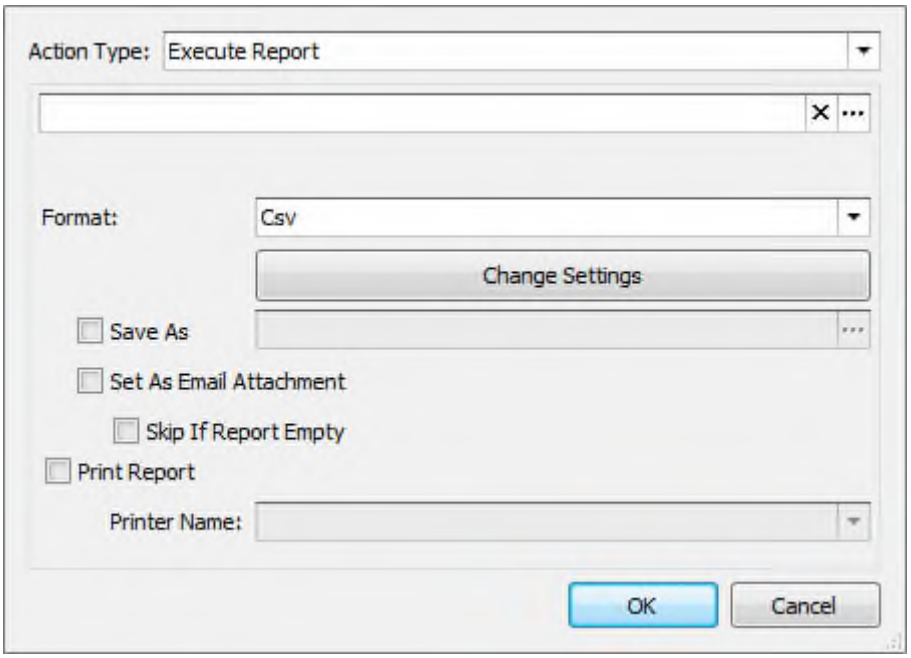
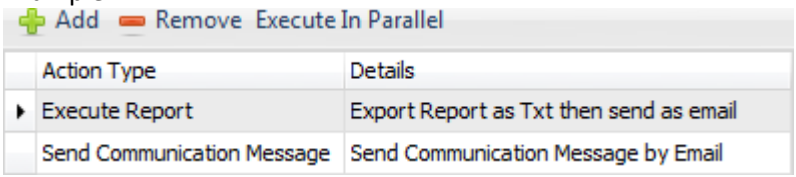


Figure 122

To send the report generated by this action as an email attachment, add the Send Communication Message after this action in a sequential list.

Example…



G. Entity states

Various entities have different valid and invalid states to make more sense of their application. For instance, instead of a door being valid / invalid it is represented as locked / unlocked.

Entity Name	Valid state	Invalid state
24 bit constant	Not zero	Zero
Air conditioning Unit	*n/a*	Always
Area	Area is on	Area is off
Area List	All areas on	One or many areas off
Area Timer eg exit timer	Timer is running	Timer is not running
Aux List	All auxiliaries on	At least one aux off
Auxiliary	Output on	Output off
Button	*n/a*	Always
Card Format	*n/a*	Always
Card Template	*n/a*	Always
Communications Task	Communications task is running	Communications task is not running
Compare	Value is >= threshold1 and <= threshold2	Value is < threshold1 or Value is > threshold2
Compound Entity	If evaluates to TRUE	If evaluates to FALSE
DNS names	*n/a*	Always
Door	Locked, reed & tongue (if present) sealed.	Unlocked or tongue or reed unsealed
Door List	All doors are valid.	One or many doors are invalid
Door Type	*n/a*	Always
EOL	*n/a*	Always

Entity Name	Valid state	Invalid state
FAT file-system file	*n/a*	Always
file/item combination	*n/a*	Always
Floor	Floor secured	One or many floors not secured
Floor List	All floors secure	At least one floor unsecure
Foreign Entities	*n/a*	Always
General Timer (100ms)	Expiry time has elapsed	Expiry time has not yet elapsed
General Variable	Current Value => The Test Value	Current Value < The Test Value
Generic	*n/a*	Always
Holidays	Valid	Invalid
Input	No State Asserted	Any state asserted
Input analogue value	Value is not 0	Value equals 0
Input Counter	Count is not 0	Count is 0
Interlock	Interlocked	Not interlocked
LAN Module	Present on the LAN	Not present on the LAN
LCD message	*n/a*	Always
Lift	Button timer running	Button timer not running
Lift Group	*n/a*	Always
Lift List	*n/a*	Always
Lift Type	*n/a*	Always
Macro procedure	Macro Procedure is running	Macro Procedure is not running
Menu Group	*n/a*	Always
None	Always	*n/a*

Entity Name	Valid state	Invalid state
Named Actions	*n/a*	Always
Pre-set text types	*n/a*	Always
Process Group	*n/a*	Always
Process ID	*n/a*	Always
Permission Group	*n/a*	Always
Qualify Door Type	*n/a*	Always
Qualify Lift Type	*n/a*	Always
Reader	*n/a*	Always
RF Remote Template	*n/a*	Always
Schedule	Valid	Not Valid
Siren module	Internal or external siren(s) are sounding with any tone	Siren(s) are not sounding
Telephone number	*n/a*	Always
Telephone number list	*n/a*	Always
Time Period	Valid	Not Valid
User	User Exists	User does not exist

Table 7

Note that for area lists, door lists, floor lists, compound entities and interlocks if the reverse flag is set then:

Entity Name	Valid state	Invalid state
Area List	All areas off	One or many areas on
Compound Entity	Expression == TRUE	Expression == FALSE
Door List	All doors are invalid	One or many doors are valid
Floor List	All floors unsecure	One or many floors are secure
Interlock	Not interlocked	Interlocked
Auxiliary List	All auxiliaries off	One or many auxiliaries on

Table 8

H. Entity types

All of various entity types are listed in this section.

Modules can have inputs and / or outputs attached to them. The following notation is used to refer to an individual input or output on the module:

C - Module Designator
01 - Module Address
: - Separator
X - Input / Output Designator
02 - Input / Output Address

Module Designator	Description
C	Control Module
T	LCD Terminal
K	Touch Terminal
P	LAN Power Supply
G	Graphic Terminal
E	Expander
R	Two Door Reader
I	Four Door Reader
F	Radio Expander
V	Virtual Module

Entity Type	Name
AC*x*	Air Conditioner
AL*x*	Area List
A*xx*	Area
CE*x*	Compound Entity
CF*x*	Card Format
CP*x*	Analog Comparison
CT*x*	Communications Task
C*xx*	Control Module
DL*x*	Door List
DT*x*	Door Type
D*xx*	Door
EL*x*	EOL configuration
E*xx*	Expander Module
FL*x*	Lift Floor List
FT*x*	RF Remote Template
F*xx*	Radio Expander
GT*x*	General Timer
GV*x*	General Variable
G*xx*	Graphic Terminal
HY*x*	Holiday
IA*x*	Analog Calibration
IL*x*	Interlock
LC*x*	Lift Car
LF*x*	Lift Floor

Entity Type	Name
LG*x*	Lift Group
LL*x*	Lift Car List
LT*x*	Lift Type
MA*x*	Macro
MG*x*	Menu Group
NIC*x*	Network Interface
PA*x*	Named Action
PG*x*	Process Group
P*xx*	Power Supply Module
QD*x*	Qualified Door Type
QG*x*	Permission Group
QL*x*	Qualified Lift Type
R*xx*	Reader Module
TL*x*	Telephone Number List
TM*x*	Card Template
TN*x*	Telephone Number
TP*x*	Time Period
T*xx*	Terminal
U*xx*	User
XL*x*	Auxiliary List

Table 9

I. Calibrations

There are two types of calibrated values - scaled and unscaled.
The unscaled value is always an integer and it is determined using the following formula:

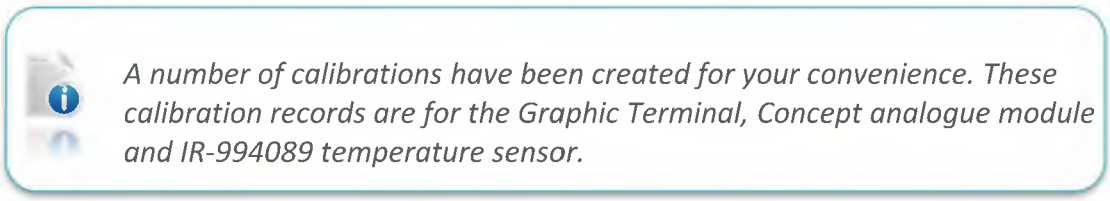
$$\frac{Gain \times RawValue}{2^{shift}} + Offset$$

To know what $RawValue$ is you must know something about the underlying hardware of that input.

Examples:

- The $RawValue$ of a standard voltage input on a C3K analog module will be a number between $0\text{-}254$ directly proportional to 0-5V on the input.
- The temperature sensor on a graphic terminal is an integer which is the decikelvins of the temperature measured.

These inputs can be arranged in a straightforward manner to display what is actually being measured at the input using a calibration.



A number of calibrations have been created for your convenience. These calibration records are for the Graphic Terminal, Concept analogue module and IR-994089 temperature sensor.

Offset

Offset allows us to have values that can go into the negative region have minima above 0, i.e. Degrees Celsius. It is expected that $RawValue$ is an unsigned number.

Gain

Gain is simply an integer that multiplies the $RawValue$.

Shift

Shift is the exponent to the power of 2, so a shift of 3 will divide the $Gain \times RawValue$ product by 8 ($2^3 = 8$).

Let's say we have a module with an analogue input that is measuring 0-10V and it has a 10bit resolution (so its $RawValue$ is 0-1023). We will choose our unscaled calibrated value to be millivolts as we won't gain any more accuracy by going to a smaller integral unit as there are 10000mV in 10V which is much greater than the 1024 possible values we can have. So we

will choose a gain of 10000 as this is our base unit. If we leave shift as 0 we would have a value between 0-10,240,000. We typically make the shift the same number of bits as our ADC so this will become 0-10,000 which is what we want. (Actually this isn't true, we will get:0 − $\left(10000 \times \left(\frac{1023}{1024}\right)\right)$), this inaccuracy can be compensated for in the gain, If you are interested, view the calibration example for an example of how to make a sensor correctly display its full range using a calibration).

It is important to note that for Macros and Compare structures you will need to use the unscaled analogue value for any comparison.

Format / Scale

This way we end up with an integer which is an unscaled calibrated value, which will be representative of the quantity measured, e.g. microvolts, millibar, decikelvin, etc. We need to scale and format it to make it more human readable, using the Format/Scale string. This takes the form of:

```
Kx {S|F}y.x
```

Where `x` and `y` are a value from 0 to 9.

The number after K is the number of places to move the decimal point to the left (up to 9), which allows us to display a fractional number. The S or F determines whether we display a sign in front of the displayed value, with S displaying the sign. Note that if the value becomes negative and the format uses 'F' then the negative sign won't be displayed. Also, if the 'S' option is used then positive values will always display a '+' sign in front.

The number before the dot is the number of digits before the decimal place to display. This has to be large enough to display the full number, and will always display leading zeroes on smaller numbers, as the formats are always fixed width currently. The same is true for the number after the dot, which is the number of digits shown after the decimal place. This also is fixed width and will always show trailing zeroes if empty. It is expected that usually the number after the decimal place will equal the number after 'K'.

As an example, if we want to display millivolts as 0-10 volts with no sign we would use the following string: K3 F2.3. To display decikelvin as -99.0 to +99.0 Celcius (assuming offset of -2730 to make 0 the melting point of water) we would use: K1 S2.1.

Display String

The Display String is merely a string that follows the formatted value with a whitespace in between. If the Display String is "C" then the displayed value for our temperature example would be "+22.3 C". If we use "Volts" with the volts example we might get "09.812 Volts".

Minimum & Maximum String

The minimum string and maximum string state what we expect the minimum and maximum values that are di splayed would be. This has no effect on the text of the displayed analogue value but it does affect graphical displays. On the iPhone app if a meter icon is used to display an analogue value. The minimum and maximum deflections on the scale will correspond to the minimum and maximum string values. In future this will also happen on some of the Graphic Terminal icons and some of the presenter elements in Integriti Schematics. The minimum and maximum strings should be the same format as the Format/Scale string, i.e. same sign and number of digits and decimal places, so 0 volts should be "00.000" and 10 volts should be "10.000".

Calibration Example

This example describes how to make a calibration record for a sensor that has linear output of 4-20mA into Concept 3/4K Analog module (with current mode inputs):

Let us say a sensor measures some value over range $MINvalue$ to $MAXvalue$:

$$MINvalue\ (4mA)\ \rightarrow MAXvalue(20mA)$$

Let us say it measure percentage of relative humidity (RH) from 000.0% to 100.0% as four significant figures, we define $MINinteger$ and $MAXinteger$ as:

$$MINinteger = MINvalue\ \times 10^{n}$$
$$MAXinteger\ = MAXvalue\ \times 10^{n}$$

n = number of significant figures required in the output display – max digits in the integer part of $MAXvalue$.

So here $n = 4 - 3 = 1$, so $MINinteger = 0000$ and $MAXinteger = 1000$.

$Range = MAXinteger - MININteger$, in this case $MAXinteger = 1000$.

$$GAINfloat = \frac{256}{204} \times Range = 1254.902$$

$$OFFSETfloat = MINinteger - \frac{51}{255} \times GAINfloat = -250.98039215686274509803921568627$$

Now we can get the real calibration values:

$Offset = \lceil OFFSETfloat \rceil$ (Rounded up = -250)

$Gain = \lceil GAINfloat \rceil$(Rounded up = 1255)

$Shift = 8$ (Always in this example)

$\frac{Format}{Scale} = Kn\ Sx.n$ where n = n, x = max digits in the integer part of MAX_{value}, y = n

Display String: Anything, perhaps "%RH" for relative humidity.

Minimum String = MIN_{value}

Maximum String = MAX_{value}

J. Default entities

This section contains lists of all of the entities found within a defaulted Integriti database. These entities have been created for your convenience.

Process Groups

ID	Name	Action 1 (Assert)	Action 2 (Assert)	Contact ID Message Type	EN Pin	Entry Zone	Exit Zone	External Siren States	Internal Siren States	Message Category	Message Enable States	No 24 Hour if Armed	Primary Zone	Process 24 Hour	Report Entry	Reporting States	Siren Lockout	Siren Tone	States for this PG
PG1	Intruder/Burglary	A	Tl, Th, T	130	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG2	Entry-Exit/Delayed Burg	A	Tl, Th, T	130	Intruder	✓	✓	A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG3	Primary Intruder/Burg	A	Tl, Th, T	130	Intruder	✓	✓	A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I		✓			A, Tl, Th, T, I	✓	Sweep	A, T
PG4	Silent Alarm	A	Tl, Th, T	150						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG5	Local Alarm	A	Tl, Th, T	0				A	A	1	A, Tl, Th, T, I						✓	Sweep	A, T
PG6	Local Silent	A	Tl, Th, T	0						1	A, Tl, Th, T, I								A, T
PG7	Fire		Tl, Th, T	110	Fire			A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓	Evacuation	A, T
PG8	Duress			121	Panic											A, Tl, Th, T, I			
PG9	Panic			123	Panic			A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I		Bell	A, T
PG10	Emergency			100				A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I		Evacuation	A, T
PG11	Automation			0															A, T
PG12	Log/Report Only			300										✓		A, Tl, Th, T, I			A, T
PG13	Log Only			0										✓					A, T
PG14	Tamper	A	Tl, Th, T	145	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, I	✓			✓	A, Tl, Th, T, I	✓	Sweep	A, T
PG15	LAN Fault	A		333	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG16	AC Fail	A	Tl, Th, T	301	Power					1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG17	Battery Problem	A	Tl, Th, T	302	Power					1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG18	Pwr Supply Fault	A	Tl, Th, T	312						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG19	Comms Problem	A	Tl, Th, T	350						1	A, Tl, Th, T								A, T
PG20	RF Tx Fault	A	Tl, Th, T	381						1	A, I					A, I			A, I
PG21	RF Tx Jam	A	Tl, Th, T	344	Primary ATS					1	A, I					A, I			A, I
PG22	Access Alarm			423				A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓		A, T
PG23	Access Silent			426						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG24	Access Local			0						1	A, Tl, Th, T, I								A, T
PG25	Time Report			602							A								A

A - Alarm, Tl - Tamper Low, Th - Tamper High, T - Tamper, I - Isolate, Z - ZST Fail

Analogue Calibrations

ID	Name	Calibrate Calculation	Display String	Effective Gain	Format / Scale	Gain	Maximum String	Minimum String	Offset	Shift
IA1	Raw Value	((1 X RawValue) / 1) + 0	Raw Units	1	K0 F5.0	1	65535	0	0	0
IA2	IR 994089 Temp Sensor	((10 X RawValue) / 2) + 0	C	5	K1 S2.1	10	40	0	0	1
IA3	C3K Alog 0-5 Volts	((5020 X RawValue) / 256) + 0	Volts	19.60938	K3 F1.2	5020	5	0	0	8
IA4	C3K Alog 4-20mA as ma	((20079 X RawValue) / 256) + 0	mA	78.43359	K3 F2.1	20079	20	4	0	8
IA5	C3K Alog 4-20mA as %	((12550 X RawValue) / 256) + -2500	%	49.02344	K2 S3.1	12550	100	0	-2500	8
IA6	GT Light %	((1004 X RawValue) / 256) + 0	%	3.92188	K1 F3.1	1004	100	0	0	8
IA7	GT Temp DegC	((1 X RawValue) / 1) + -2732	C	1	K1 S2.1	1	50	-10	-2732	0
IA8	Unibus Alog 0-10 Volts	((20480 X RawValue) / 8192) + 0	Volts	2.5	K3 F2.2	20480	10.00 Volts	00.00 Volts	0	13
IA9	Unibus Alog 4-20mA as ma	((20480 X RawValue) / 2048) + 0	mA	10	K3 F2.2	20480	20	4	0	11

Card Formats

Card Type	Encoding Method	Issue Number Length	Issue Number Offset	Secure 40 Scheme Type	Site Code Length	Site Code Offset	Total Bits	Wiegand Card Type
Wiegand Raw Data	Standard	0	0	Standard	0	0	0	N Bit
Wiegand Site Code	Standard	0	0	Standard	8	1	26	N Bit
Wiegand Site Code	Standard	0	0	Standard	13	0	27	N Bit
Wiegand Site Code	Standard	0	0	Standard	12	1	30	N Bit
Wiegand Site Code	Standard	0	0	Standard	8	7	32	N Bit
Wiegand Site Code	Standard	0	0	Standard	12	1	32	N Bit
Wiegand Site Code	Standard	0	0	Standard	8	7	32	N Bit
Wiegand Site Code	Standard	0	0	Standard	16	1	34	N Bit
Wiegand Site Code	Standard	0	0	Standard	11	22	34	N Bit
Wiegand Site Code	Standard	0	0	Standard	12	2	35	N Bit
Wiegand Site Code	Standard	0	0	Standard	8	2	35	N Bit
Wiegand Site Code	Standard	0	0	Standard	18	1	36	N Bit
Wiegand Site Code	Standard	0	0	Standard	18	1	36	N Bit
Wiegand Site Code	Standard	4	17	Standard	12	21	36	N Bit
Wiegand Site Code	Standard	0	0	Standard	0	0	37	N Bit
Wiegand Site Code	Standard	0	0	Standard	16	1	37	N Bit
Wiegand Site Code	Standard	0	0	Standard	19	1	37	N Bit
Wiegand Site Code	Standard	0	0	Standard	13	24	38	N Bit
Wiegand Site Code	Standard	0	0	Standard	12	4	40	N Bit
IR Secure40	Standard	0	0	Standard	0	0	0	N Bit
IR Mag Swipe	Standard	2	22	Standard	10	6	24	N Bit
Hashed Credit Card	Standard	0	0	Standard	0	0	0	N Bit
Mag Swipe Raw Data	Standard	0	0	Standard	0	0	0	N Bit

ID	Name	Card Number Length	Card Number Offset
CF1	Direct Entry Wiegand	0	0
CF2	26Bit Wiegand (H10301)	16	9
CF3	Indala 27 Bit - Wiegand	14	13
CF4	Keri 30 Bit Wiegand	16	13
CF5	Ind/Kant KSF 32Bit Wiegand	16	15
CF6	HID 32 Bit Wiegand	18	13
CF7	KASTLE 32Bit Wiegand	16	15
CF8	HID 34Bit Wiegand (H10306)	16	17
CF9	Indala 34Bit Wiegand	16	1
CF10	HIDCorp1000 35Bit (H50360)	20	14
CF11	HID 35 Bit Wiegand	20	10
CF12	Indala 36 Bit Wiegand	16	19
CF13	HID 36Bit Wiegand (Std)	16	19
CF14	HID 36Bit Wieg (S906133A)	16	1
CF15	HID 37Bit No SC (H10302)	35	1
CF16	HID 37Bit SC (H10304)	19	17
CF17	HID iClass 37Bit Wiegand	16	20
CF18	BQT 38Bit Wiegand	19	1
CF19	HID 40Bit Wiegand	16	16
CF20	IR Secure40 Wiegand	0	0
CF21	IRMag Secure	6	16
CF22	C3K Mag Direct	0	0
CF23	Integrity Mag Direct	0	0

K. System Input Process Group Defaults

The table below describes what System Input should be assigned to a system Area with what Process Group.

Process Group	System Input Name
AC Fail	AC fail Ext AC fail Low Volts
Access Alarm	Door DOTL Door*x* DOTL
Access Silent	Door Forced Door*x* Forced
Battery Problem	Batt Test Ext Low Batt Ext Batt Test Low Batt
Comms Problem	Phone Line
Duress	Duress Deadman Rdr*x* Duress
LAN Fault	LAN Comms Unibus
Local Alarm	DET Fuse Ext DET Fuse Ext LAN Fuse Ext Low Volts Invalid Card LAN Fuse Light Level Low Volts Pin Attempts Reset Temperature
Local Silent	DBase Changed Rdr*x* Fault Rdr*x* Invalid
Panic	Panic

Process Group	System Input Name
Pwr Supply Fault	Ext PS Fail PS Fail
RF Tx Fault	Xmit LowBatt XmitPollFail
RF Tx Jam	Xmitter Jam
Tamper	Cab Tamper Door Reed Door Tamper Door Tongue Doorx Fault Ext Sir Tamp Int Sir Tamp Pin Attempts Rdr Tamper
Time Report	Time Report

Table 10

L. Integriti Programming Examples

This portion of the document contains programming examples to help get a better understanding of how to fully utilise the Integriti controller.

Example 1 - Flashing auxiliaries during a time period

This example demonstrates the use of macros in conjunction with a few entities. This example will toggle an auxiliary once every 5 seconds. Every fifth toggle, another auxiliary will turn on for 10 seconds. This macro will only run while a time period is valid.

Entities used:

- 1x General variable
- 1x Macro
- 1x Time period
- 2x Auxiliaries

Entity configuration:

In this example we have created a time period called '`Working Hours`'. This time period has been configured for 09:00 to 17:30 Monday to Friday.

The general variable used has been called 'Example Counter'. The test value for the general variable has been set to 4.

The two auxiliaries (C01:X01 and C01:X02) have been labelled 'Flasher 1' and 'Flasher 2'.

Macro statements:

A total of eight statements are required to achieve this goal:

Macro: **Example 1**

#	Statement	Configuration	
1	Wait for Condition…	**Expression:**	TP1
2	Do an Action	**Action:**	Control Aux
		Auxiliary:	C01:X01
		When Asserted:	Toggle
3	Pause for Time…	**Expression:**	50
4	Set Entity To Expression…	**Expression:**	GV1+1
		Entity to Set:	GV1
5	Goto <label> if…	**Expression:**	!GV1
		Label:	SkipOn
6	Do an Action	**Action:**	Control Aux
		Auxiliary:	C01:X02
		On Time:	00:00:10
7	Set Entity To Expression…	**Expression:**	0
		Entity to Set:	GV1
8	Define a Label	**Label:**	SkipOn

Statement summary for macro: **Example 1**

1. Prevent further execution of the macro until the time period (TP1) is valid.
   - TP1 (Work Hours) has been configured for 09:00 to 17:30 hours Monday to Friday. If the panel time and day fall within these values then the test of time period TP1 will return true and remainder of the macro will be executed.
2. This statement toggles the first auxiliary (Flasher 1).
   - C01:X01 (Flasher 1) has been to toggle on assert. Every time this statement is executed the state of the auxiliary will be inverted.
3. Pause for 50 x 100ms (5 seconds).
   - The macro will pause for a period of 5 seconds.
4. Add 1 to the general variable (GV1).
   - The general variable GV1 is set to a value that is itself plus one.
5. If the test of general variable (GV1) does not return true, go to the label 'SkipOn'.
   - When the general variable (GV1) was configured, its test value was set to four. If the general variable is greater than this value, it will return true.
   - The expression '!GV1' is a test to see if GV1 is not returning true (If the value is equal to four or less).
   - If the expression returns true, the following two statements will be skipped.
6. Turn on the second auxiliary (Flasher 2) for 10 seconds.

- If an on time other than zero is specified for an auxiliary action, the target auxiliary will turn off after the time expires.

7. Reset the general variable (GV1) back to `0`.
   - The general variable GV1 is set to zero.
8. This is the label (`SkipOn`) that the macro moves execution to if the general variable (`GV1`) does not return true (GV1 is greater than 4).
9. Return to step 1.

Example 2 - Random bag inspections

During work hours random bag inspections are carried out. Users going through door x will be denied access at random. An input or users with special access can be used to reset the random bag inspection and allow the user to pass through.

Entities used:

- 1x Door
- 1x General variable
- 1x Input
- 1x Named Action
- 1x Reader module
- 1x Time period
- 2x Macros
- 2x Permission Groups
- 2x Users

Entity configuration:

In this example we have configured a door (Door x) as a normal entry door associated with a reader module (Reader x).

We have two users - User '`Employee`' is subject to random bag inspections. The '`Supervisor`' user is not. We will name the two permission groups '`Employees`' and '`Supervisors`' respectively. Each user has its own credential.

We have called the time period '`Working Hours`'. This time period has been configured for 09:00 to 17:30 Monday to Friday.

The general variable '`Random inspection`' is used to determine user access. It is assigned a random number using the first macro 'Random bag' and reset to zero by the other macro 'Reset random bag'.

The named action 'Start random bag' is triggered by 'Door x' but only when working hours are valid. 'Start random bag' will start the macro 'Random bag' every time 'Door x' is opened.

The Input 'Reset bag' is used by the supervisor on duty. Pressing the button attached to the input 'Reset bag' will start the macro 'Reset random bag'.

Macro statements:

Both macros are small (only containing two statements each):

Macro: **`Random bag`**

#	Statement	Configuration	
1	`Set Entity To Expression…`	**Expression:**	`8388607`
		Entity to Set:	`GV2`

2	End Current Macro	

Macro: **Reset random bag**

#	Statement	Configuration
1	Set Entity To Expression…	**Expression:** 0 **Entity to Set:** GV2
2	End Current Macro	

Statement summary for macro: **Random bag**

1. The entity GV2 'Random inspection' is assigned a value of 8388607.
    - The number 8388607 is a magic number. Entities assigned this number are actually given a random number between 1 and 8388067. For more information, please refer to the appendices.
2. Stop the macro.
    - This statement will cause the macro to stop.

Statement summary for macro: **Reset random bag**

1. The entity GV2 'Random inspection' is assigned a value of 0.
2. Stop the macro.
    - This statement will cause the macro to stop.

M.Licenses

Software and hardware licenses are used to enable specific features within the controller or software management suite.

Integriti licenses are managed online by KeyPoint.

Licenses can be managed from https://license.innerrange.com/

Software licenses

Below is a list of all of the available Integriti licenses.

#	Name	Description
996905UPG	Integriti Express to Pro Upgrade	Users running Integriti Express can upgrade to Integriti Pro using this license key.
996909	Allow RDP Remote Connections	This license allows remote desktop connections.
996910	Software Client License (Fixed)	This license is reserved for a specific client machine. (Can be changed to another computer if needed) Ideal for situations where specific client machines must / should be connected to the Integriti server at all times.
996911	Software Client License (Floating)	This client license adds to a pool of available client connections. Ideal for situations where many machines may connect to the Integriti server for a session but not all simultaneously.
996912	Extra Controller Connection License for Integriti Pro	Licenses the connection of an additional Integriti controller.
996920	CCTV – First 32 Cameras	Permits the connection of up to 32 cameras.
996921	CCTV – Extra 8 Cameras	Permits the connection of additional cameras. The 'CCTV – First 32 Cameras' license (996920) is required.
996922	Integriti Photo ID	Enables printing of Photo IDs.
996923	Integriti Advanced Reports	Enables Integriti advanced reporting.

#	Name	Description
996925	Integriti Advanced Alert - Alarm event & Escalation Manager	Enables more functionality in the Integriti alert handler.
996930	Integriti Communications Module SMS & EMAIL	Enables the SMS and eMail communication handlers.
996940	Integriti Pro – Additional Door License	
996950	XML READ – 3rd Party Interface	Enables 3rd party read functionality. 3rd party software can interrogate the Integriti database.
996951	XML Write – 3rd Party Interface	Enables 3rd party write functionality. 3rd party software can write to the Integriti database.
996952	XML Control – 3rd Party Interface	Enables 3rd party control of Integriti entities.
996955	Integriti DUIM	Enables the dynamic user import module. Automatically imports users for creation, modification or deletion from a 3rd party product.

Table 11

Hardware licenses (Smart card)

There are 5 license levels the Integriti controller can have. The following table describes the controller limitations for each level. Integriti controllers without a smart card will have a license level of '*none*'.

License	Review	Users	Zones	Doors
none	10,000	200	100	16
Level 1	20,000	2,000	200	40
Level 2	30,000	10,000	600	80
Level 3	60,000	65,000	2,000	160
Level 4	100,000	100,000	3,000	240

Table 12

Below is a list of all of the available Integriti controller licenses.

#	Name	Description
996020U01	ISC Smart Card Upgrade BLANK to Level 1	Level 1 license: 20,000 Review events, 2,000 Users, 200 Zones and 40 Doors
996020U12	ISC Smart Card Upgrade Level 1 to Level 2	Level 2 license: 30,000 Review events, 10,000 Users, 600 Zones and 80 Doors
996020U13	ISC Smart Card Upgrade Level 1 to Level 3	Level 3 license: 60,000 Review events, 65,000 Users, 2,000 Zones and 160 Doors
996020U14	ISC Smart Card Upgrade Level 1 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996020U23	ISC Smart Card Upgrade Level 2 to Level 3	Level 3 license: 60,000 Review events, 65,000 Users, 2,000 Zones and 160 Doors
996020U24	ISC Smart Card Upgrade Level 2 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996020U34	ISC Smart Card Upgrade Level 3 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996021	ISC Smart Card 5 User Web Interface License	Enables remote web access to the Integriti controller. Designed to be used in conjunction with the Android or Iphone Integriti app.
996022	ISC Smart Card Automation Interface License	Enables 3rd party interface communication tasks.
996023	ISC Smart Card EMS License (Lift Integration)	Enables high-level lift integration.
996024	ISC Smart Card Global Salto	Enables Salto integration.
996020L1	ISC Smart Card – Level 1	

#	Name	Description
996020L1T	ISC Smart Card Blank Card Version 1	

Table 13

Global anti-passback

Document created with reference to Controller firmware V3.2.x.xxxxx and Software version Vx.x.x.xxxx

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Introduction

Anti-passback on the Integriti controller is managed using Locations and/or Areas. Locations are specific to global (multi-controller) anti-passback. Areas are local to the controller.

Doors can have an inside and outside location and an inside and outside area. Location is a global entity used for access and global anti-passback. Area is a local entity used both for access control and security. A users location can either be a global location or a local area, not both at the same time. If a door has both, the user is put in the location when they enter.

Global Anti-passback not flagged in controller

The following occurs when the 'Enable Global Antipassback' option is not set in the Integriti controller.

Users can get access through a door if they have the inside area (or area list containing inside area) as a permission and that permission has the access area flag set in the permission, even if they don't have the door as a permission (but not if they have a deny on that door).

Users can get access through the door if they have the door as a permission (or it is in their door list permission) unless they have a deny permission with the enter area flag set which includes the inside area.

Area counting and automatic area arming when user count is 0 can be used wherever area based access control is used.

When doors are setup for anti-passback, the controller will only look at the user's area when deciding whether to allow or deny. If the user is currently located in a location it will appear as if they are in no area for the purpose of anti-passback processing.

Global Anti-passback flagged in controller

The following occurs when the 'Enable Global Antipassback' option has been set in the Integriti controller.

A user can enter a door if they have the inside location as a permission, even if they do not have the door as a permission (but not if they have a deny permission on the door).

Note that at the time of writing there is currently no location list. Locations would have to be aggregated in permission groups if users start to run out of permissions when using location based access.

Users with the location permission inherit access, as the permission serves no other purpose (area permissions are also for arming/disarming).

If a user has a door as a permission, they will be denied if they have a deny permission on the inside location.

Area counting is disabled when global anti-passback is enabled. If doors have inside and outside areas, no area counting will be done.

When doors are set up for anti-passback, they will only look at the users location. If the user is currently in an area they are considered to be in no location for the purpose of anti-passback.

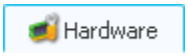
Not affected by Global Anti-passback

Doors can still allow or deny if the entry/exit area is armed based on Menu Group (allowed disarm on entry), user area off list, Door Type (disarm entry area, deadlock).

Users can arm/disarm areas on access at a door (eg: pushbutton arm, disarm entry/exit area on egress/ingress, 3 swipe arm, etc) depending on programming and user permissions.

Configuring global anti-passback

To enable global anti-passback in the controller…

1. Click on the 

tab followed by 

.
2. Double-click a controller to open the editor window.
3. Under Module Details, expand-out General Behaviour.
4. Tick the Enable Global Antipassback option.
5. Save and close the Editor Window for the controller.
6. Repeat steps 1-5 for the remaining controllers that are to be used for global anti-passback.

INTEGRITI Hardware and Software Prerequisites

V25.1.0

INNERRANGE.COM

CONTENTS

PREREQUISITES

The Integriti suite consists of Server and Client software. Integriti software installation files contain all of the client and server software in one package for easy deployment. The entire software suite can be installed on a single machine for typical installations or as one server and *n* clients.

We recommend the use of a dedicated computer for the purpose of running the Integriti server.

Controller/Panel Requirements

- Inner Range Integriti controllers (Integriti Security Controllers or Integriti Access Controllers).

Supported platforms

- Microsoft Windows 11 Pro Version 21H2 or higher
- Microsoft Windows 10 Pro Version 21H2 or higher
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

NOTE: 64-bit (x64) operating systems are required for all Integriti server installations.
64-bit (x64) operating systems are preferred (but not required) for Integriti client installations.
All operating systems should be maintained with the latest service packs.
Operating systems that have reached end of support or retirement are not supported.

Supported MS SQL versions

- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

NOTE: SQL Server Standard edition or higher may be required depending on system size.
Not all versions of SQL Server listed above are supported by the operating systems that we support.
Please refer to Microsoft's SQL Server documentation to find out if your preferred SQL Server version is supported.

MS SQL Configuration

It is recommended to explicitly restrict the SQL Server Memory usage in the SQL configuration. This prevents SQL from using all memory in the system.
The recommended maximum memory allocation for SQL is the amount of memory installed – 12GB. E.g. for a system with 32GB of RAM installed, the maximum SQL Server Memory usage should be set to 20GB or less. This value should be further reduced if the system regularly gets close to 100% memory usage.

Dot Net Version Requirements

The Integriti software suite requires a minimum Dot Net version of v4.8.
The Dot Net version installed should be consistent across all Server and Client installations.

SERVER HARDWARE REQUIREMENTS

Installations of the Inner Range Integriti system range from small, low traffic single controller/single computer installations to enterprise-wide systems that need to cope with millions of events every week.

To determine your hardware requirements, choose your “Installation type”

Type	To be classified as a “Small” or “Medium” installation, you must be able to answer YES to ALL of the questions for that type.
Small	• Number of controllers: 1 – 3 • Average review rate (including all controllers): Less than 5,000 per day • Highest Burst review rate: 100 per minute • Number of concurrent Integriti Clients: 1 – 3
Medium	• Number of controllers: 1 – 8 • Average review rate (including all controllers): Less than 25,000 per day • Highest Burst review rate: 200 per minute • Number of concurrent Integriti Clients: 1 – 6
Large	• Number of controllers: 1 – 50 • Average review rate (including all controllers): Less than 200,000 per day • Highest Burst review rate: 500 per minute • Number of concurrent Integriti Clients: 1 – 20
Enterprise	Please contact Inner Range to further discuss your requirements.

CLIENT WORKSTATION SPECIFICATIONS

At the time of writing, almost any PC purchased today should easily run the Integriti client software. These specifications are also suitable for installations where there is one PC and one Controller in use.

- Any of the operating systems listed in the Supported Platform section and are still under Microsoft support.
- 2GHz or higher quad core processor.
- 8GB DDR II memory or higher.
- 500GB SATA HDD or higher.
- Gigabit Ethernet adaptor.

SERVER WORKSTATION SPECIFICATIONS

Please refer to the table in Server Hardware Requirements to determine the "installation type".

Small sites

The following specifications are suitable for a PC used as a dedicated Integriti server. Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

Processor	A core i5 family or higher processor
Memory Capacity	16GB Minimum Recommended
Hard Drives	1TB SATA HDD or higher
Network Adapter	Gigabit Ethernet Adapter
Operating System	Microsoft Windows 10 or greater
SQL	Microsoft SQL Server Express 2019 or greater

Medium sites

The following specifications are suitable for a PC used as a dedicated Integriti server. Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

Processor	A core i7 family or higher processor
Memory Capacity	32GB Minimum Recommended
RAID Controller	Hardware RAID Controller
Hard Drives - Raid 1	2x 1TB SATA HDD or higher
Network Adapter	Gigabit Ethernet Adapter
Power Supply	Dual, Hot-plug, Redundant Power Supply (1+1)
Operating System	Microsoft Windows Server 2019 or greater
SQL	Microsoft SQL Server Standard 2019 or greater

Large sites

The following specifications are suitable for a PC used as a dedicated Integriti server. Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

Processor	Intel® Xeon® Processor – Minimum of 6 Cores
Memory Capacity	64GB Minimum Recommended
RAID Controller	Hardware RAID Controller
Hard Drives - Raid 1 (OS)	2x 10K RPM SAS 6Gbps Hot-plug Hard Drive
Hard Drives - Raid 5 (Integriti)	3x 10K RPM SAS 6Gbps Hot-plug Hard Drive
Network Adapter	Intel Ethernet Server Grade Adapter
Power Supply	Dual, Hot-plug, Redundant Power Supply (1+1)
Operating System	Microsoft Windows Server 2019 or greater
SQL	Microsoft SQL Server Standard 2019 or greater

INTEGRITI SPECIFICATIONS

Approximate disk usage:

- ~100MB - Integriti software management suite
- 550MB – 10GB - SQL Express 2017[1]

Running processes:

- ~120MB - IntegritiSystemDesigner.exe
- ~42MB - IntegritiControllerServer.exe
- ~35MB - IntegritiApplicationServer.exe

There will also be additional SQL processes running. Memory usage and process names will vary depending on the SQL instance name, database size and version of SQL server. For more information, please refer to the Microsoft SQL documentation.

Ports used:

- 44000 - TCP Client ↔ Application server communications
- 4711 - TCP Controller ↔ Controller server communications

By default, Integriti uses the Microsoft SQL Server 2017 Express database engine, which limits the database to 10 GB of data.

Whilst the installation itself only takes approximately 600MB of hard disk space, the SQL Express database can grow to 10GB over time with the storage of your controllers' historic review data. If up to 4 or 5 million review events are expected over a 12 month period and SQL Express is required to host the Integriti database, then 5GB of free hard disk space is recommended. The average review event takes up approximately 1.5KB/review event, so the 10GB database will allow room for more than 6 million review events, but note that a moderate to busy site could easily generate that number

[1] Database size can vary dramatically due to a number of factors such as the version of MS SQL or number of Integriti controllers and Integriti controller activity.

of events every year. For large / busy sites, (more than 6 million review events per year) it is strongly recommended to purchase the full version of Microsoft SQL Server Standard.

Contact the manufacturer for hardware specifications when the recommended number of review events will be exceeded.

To ensure any sized site continues to operate smoothly, Scheduled Tasks should be setup to purge / archive old review.

Global Headquarters

Inner Range Australia
+61 3 9780 4300
sales.au@innerrange.com

Inner Range United States
+1 (844) 588-0874
sales.usa@innerrange.com

Inner Range United Kingdom
+44 (0) 845 470 5000
sales.uk@innerrange.com

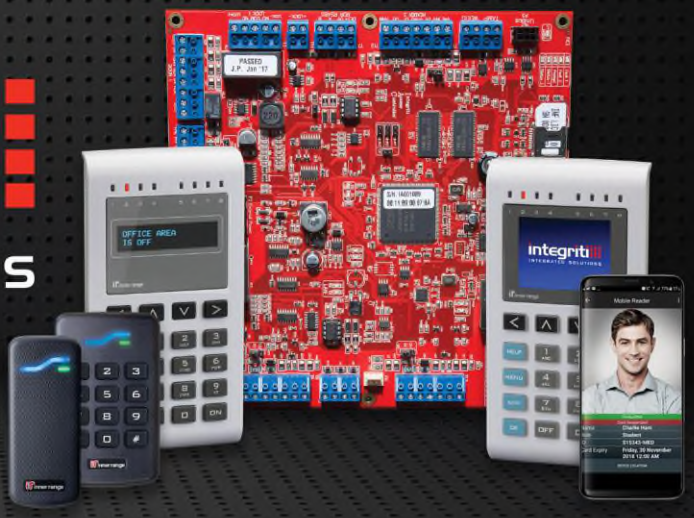
Inner Range Canada
+1 (844) 588-0874
sales.canada@innerrange.com

Inner Range Middle East
+971 4 8067100
sales.me@innerrange.com

Inner Range India
+91 80 4070 3333
sales.india@innerrange.com

INNERRANGE.COM

integriti
INTEGRATED SOLUTIONS



V20 Licensing Change Release Notes

Overview

A major part of the Integriti V20.0 release involved assessing and evaluating the full Integriti hardware and software licensing model. The primary focus was to simplify the story.

The result is a condensed and lean license model that should be much easier to understand and explain, should remove many pitfalls from the old model and significantly reduce the time and effort it takes to produce a system quote.

All of the changes mentioned in this document will be included with V20.0 of Integriti Software and Hardware. This document will highlight many of the changes that come with this licensing restructure and includes a detailed breakdown of all changes at the end.

New Product Editions

A major new change with Integriti is the introduction of two new Integriti product editions. Instead of having individual feature licenses for features such as Advanced Alerts or Photo ID, there are now software editions that include sets of features.

The editions are designed so that it should be obvious which edition of the software is required for a job. However, upgrade options (like the existing Express to Professional Upgrade license) are available.

Express

Basic administration of single controller sites

Professional

Extends management abilities to multiple controllers and multiple sites

3rd-party integration starting point

Business

For businesses who use Integriti in their daily routines

CCTV integration starting point

Corporate

Fully featured enterprise-grade software that unlocks Integriti's full potential

Ideal for onsite guards

A breakdown of the editions and their included features can be seen in the following table.

	EXPRESS	PROFESSIONAL	BUSINESS	CORPORATE
Controllers	1	Unlimited	Unlimited	Unlimited
Included Doors	16	16*	16*	16*
Included Clients	0	2	5	30**
Allows Integrations	No	Yes	Yes	Yes
Integriti Mobile		Unlimited	Unlimited	Unlimited
Communicator		Yes	Yes	Yes
DUIM		Yes	Yes	Yes
Photo ID		Yes	Yes	Yes
CCTV (w. LPR)			First 32, expandable	Unlimited
Advanced Reports			Yes	Yes
Web Server			Yes	Yes
Active Directory (Operators)			Yes	Yes
Active Directory (Users)			Yes	Yes
Advanced Alerts				Yes
Operator Challenge				Yes
User Qualifications				Yes
Guard Tour				Yes
SNMP Health Monitor				Yes

*Additional doors can be licensed **Contact Inner Range Sales if more clients required

Some highlights include:

- Controller connections are no longer licensed in Professional, Business, or Corporate editions of the software. Controllers can be freely connected to these product editions.
- All client seats are now floating and the number of seats is part of the editions
- Integriti Professional now includes Communicator, the Dynamic User Import Module and Photo ID as built-in features.

Controller + Smart Card Changes

Multiple changes are also being made around Controllers and their smart cards. Almost all licenses are being removed, but some will remain. With this in mind, as with the Integriti Access Controller, smart cards will now be included with Integriti Security Controllers.

Smart Card Level Licenses Removed

The major change with Controllers is that Controller Level licenses are being removed. From V20.0 firmware onwards, controllers will all support maximum expansion capacity of 250 doors, 100,000 users, 3,000 inputs and 100,000 events.

Smart Card Included Features

Several features are no longer licenses and will be included with V20.0 firmware. Specifically:

- Integriti Mobile App Connections
- Virtual Modules
- C-Bus Lighting
- Wireless Doors
- Locker Banks

Specialist Smart Card Licenses

High-Security Fence Integration and Honeywell Fire Integration licenses remain, however they have been improved to no longer be quantity-based per virtual module. Instead, a once-off price unlocks the integration and as many virtual modules can be created as necessary.

New Parts List

The following table illustrates the remaining parts list after the Integriti 20.0 release. It condenses down over 75 licenses to only 37 licenses. With the introduction of the product editions, most of those remaining licenses are used only for specialised expansion of the system.

Ideally, choosing the base edition and how many extra doors or cameras to include should make up most of the license quoting process.

License Number	License
Software Products	
996905	Integriti Express
996901	Integriti Professional
996901B	Integriti Business
996901C	Integriti Corporate
996905UPG	Integriti Express to Professional Upgrade
996901UPGB	Integriti Professional to Business Upgrade
996901UPGC	Integriti Business to Corporate Upgrade
996940	Integriti Door
996921	CCTV - Extra 8 Cameras (Business Only)
Specialist Software Integrations	
996928	Real-Time Location System (RTLS) Integration
996932	Intercom Integration
996933	Elevator Management Integration (Lift HLI)
996934	KeyLocker Integration
996935	Visitor Management Integration
996936	Integriti Biometric Export Licence for Morpho Manager Software
996937	VingCard Integration
996939	Milestone XProtect Access Integration
996941	3rd Party Door
996931	Event Review I/O Communications
996950	XML READ
996951	XML WRITE
996952	XML CONTROL
996962	RightCrowd Enterprise Integration
996964	Mobile Credential Management Integration
996968	Modbus Slave Integration
996969	Biometric Management Integration
Specialist Expansion	
996915	Partition License
996965	Additional Server Node (High Availability)
996906	Integriti Mimic Viewer
996907	Inner Range Mobile Reader
996956	Active User Rotation Module
Specialist Controller Licenses	
996022	ASCII Automation Interface
996023	Elevator Management System HLI (Lift EMS)
996025	High-Security Fence Integration
996030	Advanced Peer-to-Peer
996228M	Modbus BMS Interface
996239	Honeywell Fire Integration

SMAs + Upgrades

All of the changes described require version 20.0 or later of Integriti software and hardware. Like currently, upgrade fees are required to upgrade the system, however, this process has been overhauled too.

After the included upgrade period has expired, an upgrade fee must be paid to upgrade the system. The fee is calculated based on the system's total software license value.

New Software – Up to 24 Months of Upgrades

New software systems come with up to 24 months of upgrades from the date of purchase, covering releases in the calendar year it was purchased in and the following calendar year. So, a system purchased in 2020 is automatically entitled to all V20.X and V21.X releases. This applies to existing systems too, so all systems purchased in 2019 are eligible for V20.X software and firmware updates.

Software Upgrades

To upgrade an older site, one option is a simple Software Upgrade.

- No backdating is involved, it is the same fee whether the system is 3 or 5 years old
- No contracts or agreements are required. It is just a simple upgrade license
- Once purchased, it allows upgrades for the calendar year it was purchased in. If purchased any time during 2025, then the system can be upgraded up to and including all 25.X releases.

Software Maintenance Agreement (SMA) *Australian and New Zealand Markets Only

Another option is to purchase an SMA. An SMA includes:

- No backdating when starting an SMA
- Software upgrades for the years that it is active
- Access to a priority manufacturer support line (Victorian business hours)
- Direct end-user support
- Options for 1, 2, 3 or 5-year SMAs
- Optional 24/7 Support addon

Upgrades and SMAs Now Sold via Distributors

Previously, software upgrade or SMA fees were paid directly to Inner Range which required up-front payments. With Integriti V20.0 onwards, these are now sold from distributors, allowing them to be placed onto distributor accounts with standard payment terms.

Contact your distributor for more information about these options and on pricing.

Existing Sites

Once these changes are live, the old licensing model will be retired and the new model will take effect. This means that any licenses that have been removed in the model, replaced by another license or are now bundled with Integriti product editions can no longer be purchased separately.

Many licenses remain unchanged or have just been remaned though and can still be added to existing sites, like additional doors for basic expansion.

See the detailed table on the following pages for the full breakdown.

Automatic Level 4 Controller Upgrade

As mentioned, with Integriti V20.0, Controller Level Licenses are being removed. Version 20.0 Integriti firmware will no longer look at the level license on a smart card, but that does not help the existing controllers out there.

To assist this, when these changes go live, Level 4 licenses will be automatically issued to all smart cards. This will allow existing sites to expand with additional users, doors and inputs without worrying about running into a level limit.

Automatic Edition Upgrades

For sites that already have additional licensed features, upgrading to V20 of Integriti will automatically upgrade their software edition to the one that contains those features.

For example, an existing Integriti Professional system with Advanced Reports would automatically be upgraded to Business with V20. In addition to gaining Communicator, Photo ID and DUIM functionality from V20 Professional, they would also gain CCTV integration, the web interface, and Active Directory (Operators) functionality.

Having existing client connections does not qualify a system for an automatic edition upgrade. Instead, the existing clients are added to the clients that come with the edition. So, a system with 3 client connections that is being promoted to Business, will now have 8 client connections.

In short, existing Professional systems will be upgraded to Business if they have:

- CCTV – Initial 32 Cameras, or
- Advanced Reports, or
- At least one Web Client Interface, or
- Active Directory (Operators), or
- Active Directory (Users)

Similarly, existing Professional systems will be upgraded to Corporate if they have:

- Advanced Alerts, or
- User Qualifications, or
- Guard Tour, or
- SNMP Health Monitor

Detailed Part Changes

The following is a full breakdown of the Integriti licenses, including which licenses have been removed, replaced, modified, renamed, or unchanged.

Part Number	License / Part	Change Type	Change Summary
Controller Licenses			
996020L0	ISC/IAC Blank Feature License (Level 0)	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020L1	ISC/IAC Smart Card - Level 1	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020L4	ISC/IAC Smart Card - Level 4	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U01	ISC/IAC Smart Card Upgrade BLANK (L0) to Level 1	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U12	ISC/IAC Smart Card Upgrade Level 1 to Level 2	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U13	ISC/IAC Smart Card Upgrade Level 1 to Level 3	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U14	ISC/IAC Smart Card Upgrade Level 1 to Level 4	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U23	ISC/IAC Smart Card Upgrade Level 2 to Level 3	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U24	ISC/IAC Smart Card Upgrade Level 2 to Level 4	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996020U34	ISC/IAC Smart Card Upgrade Level 3 to Level 4	**Removed**	Controller level licenses are being removed. From 20.0, all controllers support maximum expansion capacity.
996021	Smartphone-Controller Interface	**Removed**	Removed. No limits anymore when connecting the Integriti Mobile App to Controllers
996022	Automation - BMS Interface (Std & Adv)	**Renamed**	Renamed License: ASCII Automation Interface.
996023	Elevator Management System HLI (Lift EMS)	**Unchanged**	
996024	Salto SALLIS Door Integration (Per Door)	**Removed**	Smartcard Wireless Door licenses have been removed. To add wireless doors to a controller, smart card level licenses or smart card wireless door licenses are no longer needed, however a software Additional Door License is still required.
996025	High Security Fence Integration (32zn/32aux)	**Modified**	Changed to be a once-off purchase instead of quantity-based. Enables the High Security Fence integration on a controller. Virtual Modules can be freely created for fence segments.
996026	Virtual Module (32zn/32aux)	**Removed**	Removed. No limits to Virtual Module creation anymore

Part Number	License / Part	Change Type	Change Summary
996027	C-Bus Lighting Integration	**Removed**	Removed. C-Bus Lighting is an included feature from 20.0 onwards
996028	BACnet/IP, Modbus, KNX Integration HLI	**Removed**	Removed. Modbus interface is natively supported with license 996228M. Other protocols (BACnet, KNX, etc) require additional 3rd party hardware that convert from Modbus to those protocols. Contact Inner Range Sales for more information.
996029	ISC/IAC Allow CS Remote Connection (Subscription)	**Removed**	Already removed with Integriti CS 19.0.1 release.
996030	Advanced Peer-to-Peer	**Unchanged**	
996032	Aperio Door Integration (Per Door)	**Removed**	Smartcard Wireless Door licenses have been removed. To add wireless doors to a controller, smart card level licenses or smart card wireless door licenses are no longer needed, however a software Additional Door License is still required.
996032NC	Aperio Door Integration (Per Door)	**Removed**	Smartcard Wireless Door licenses have been removed. To add wireless doors to a controller, smart card level licenses or smart card wireless door licenses are no longer needed, however a software Additional Door License is still required.
996033	SimonsVoss Door Integration (Per Door)	**Removed**	Smartcard Wireless Door licenses have been removed. To add wireless doors to a controller, smart card level licenses or smart card wireless door licenses are no longer needed, however a software Additional Door License is still required.
996034	IAC Infiniti Expanded Mode	**Removed**	Removed. From 20.0, Infiniti IAC no longer has module count restrictions.
996228M	Modbus BMS Interface	**Unchanged**	Note: Other protocols (Bacnet, KNX, etc) use this interface and require additional 3rd party hardware that convert from Modbus to those protocols. Contact Inner Range Sales for more information.
996235	Locker Bank Feature (Block of 10)	**Removed**	Removed. No limits to the Locker Bank feature
996239	Honeywell Fire Integration - 32 Points (Standard)	**Modified**	Changed to be a once-off purchase instead of quantity-based. Enables the Honeywell Fire integration on a controller. Virtual Modules can be freely created for fire points.
Software Products			
996901	Integriti Professional	**Modified**	Now includes unlimited controller connections, an additional Client license, unlimited Integriti Mobile App connections, Communicator feature, DUIM feature and Photo ID feature
996901B	Integriti Business	**New Product**	
996901C	Integriti Corporate	**New Product**	
996905	Integriti Express	**Unchanged**	

Part Number	License / Part	Change Type	Change Summary
996905UPG	Integriti Express to Professional Upgrade	**Unchanged**	
996901UPGB	Integriti Professional to Business Upgrade	**New License**	Allows upgrading of Integriti Professional to Integriti Business
996901UPGC	Integriti Business to Corporate Upgrade	**New License**	Allows upgrading of Integriti Business to Integriti Corporate
996906	Integriti Mimic Viewer	**Unchanged**	
Software Feature Expansion			
996907	Inner Range Mobile Reader	**Unchanged**	
996908	Web Client Interface (Floating Session)	**Bundled Component**	No longer purchased separately. Business edition provides Web Interface now. Web client logins use standard client seats now.
996909	Allow Remote RDP Connections	**Removed**	Removed. No longer a restriction in Integriti
996910	Client Connection (Fixed)	**Bundled Component**	No longer purchased separately. Additional seats require Integriti edition updates. Sites with existing Client Connection licenses will keep them in addition to those included in their product edition. "Fixed" client seat logic is now a built-in feature to Integriti. See the V20 Integriti software release notes for more information.
996911	Client Connection (Floating)	**Bundled Component**	No longer purchased separately. Additional seats require Integriti edition updates. Sites with existing Client Connection licenses will keep them in addition to those included in their product edition.
996912	Extra IAC/ISC Controller Connection	**Removed**	Removed. From 20.0, controllers can be freely connected to Integriti Professional and above
996912IAC	Enable Unlimited IAC Connections	**Removed**	Removed. From 20.0, controllers can be freely connected to Integriti Professional and above
996915	Integriti Partition License	**Unchanged**	
996922	PhotoID Card Design	**Bundled Component**	No longer purchased separately. Included with Integriti Professional
996923	Advanced Reports	**Bundled Component**	No longer purchased separately. Included with Integriti Business
996924	User Qualification Manager	**Bundled Component**	No longer purchased separately. Included with Integriti Corporate
996925	Advanced Alert - Alarm Escalation, Response Plans & Operator Challenge	**Bundled Component**	No longer purchased separately. Included with Integriti Corporate
996926	Smartphone-Server Interface	**Bundled Component**	No longer purchased separately. Included with Integriti Professional
996927	Guard Tour Module	**Bundled Component**	No longer purchased separately. Included with Integriti Corporate

Part Number	License / Part	Change Type	Change Summary
996930	Communicator - Email, SMS & Pager	**Bundled Component**	No longer purchased separately. Included with Integriti Professional
996940	Additional Door Key	**Unchanged**	
996956	AURM Active User Rotation Module	**Unchanged**	
996957	Active Directory USERS	**Bundled Component**	No longer purchased separately. Included with Integriti Business
996958	Active Directory OPERATORS	**Bundled Component**	No longer purchased separately. Included with Integriti Business
996965	High Availability Multi-Activation	**Modified**	Renamed License: Additional Server Node (High Availability / Load Spreading). No longer requires two for the first purchase.
Software Integrations			
996920	CCTV - Initial 32 Cameras	**Bundled Component**	No longer purchased separately. Included with Integriti Business
996921	CCTV - Extra 8 Cameras	**Renamed**	Renamed License: CCTV - Extra 8 Cameras (Business Only). Can add 8 extra cameras to Integriti Business. Corporate includes unlimited cameras
996928	EkoTek User Location System Integration (Receiver)	**Renamed**	Renamed License: Real-Time Location System (RTLS) Integration. Generalized license that will support Ekotek, Stanley, Bosch Security Escort, and future RTLS integrations
996931	Event Review I/O Communications	**Unchanged**	
996932	Intercom Integration	**Unchanged**	
996932CG	CellGuard Intercom Integration	**Replaced**	Removed. CellGuard Intercom integration now requires 996932 Intercom Integration license from Integriti V20 onwards
996933	Schindler PORT Lift Integration HLI	**Renamed**	Renamed License: Elevator Management Integration (Lift HLI). Generalized license that supports Schindler PORT, Kone Access and future elevator integrations
996934	KeyLocker Integration	**Renamed**	Renamed License: Keylocker / Locker Integration
996935	Visitor Management Integration	**Unchanged**	
996936	Biometric Reader Integration	**Renamed**	Renamed License: Morpho Biometric Reader Integration.
996937	VingCard Integration - VingCard as Master	**Modified**	Renamed License: VingCard Integration. Changed to be a once-off purchase instead of quantity-based.
996939	Milestone Access Control Manager (ACM) Integration	**Renamed**	Renamed License: Milestone XProtect Access Integration

Part Number	License / Part	Change Type	Change Summary
996941	Salto XS4 Integration (SHIP Interface)	**Renamed**	Renamed License: 3rd Party Door. Quantity-based license per-door. Generalized license for integrating and controlling 3rd party door systems via the Integriti software that does not connect via Inner Range hardware.
996950	XML READ	**Unchanged**	
996951	XML WRITE	**Unchanged**	
996952	XML CONTROL	**Unchanged**	
996955	DUIM Dynamic User Import Module	**Bundled Component**	No longer purchased separately. Included with Integriti Professional
996960	SNMP & Health Monitor	**Bundled Component**	No longer purchased separately. Included with Integriti Corporate
996961	Stanley Real Time Location System (RTLS) Integration	**Replaced**	Removed. Requires 996928 Real-Time Location System (RTLS) Integration from Integriti V20 onwards
996962	RightCrowd Enterprise Integration	**Unchanged**	
996963	Bosch Security Escort Integration	**Replaced**	Removed. Requires 996928 Real-Time Location System (RTLS) Integration from Integriti V20 onwards
996966	License Plate Recognition Integration	**Bundled Component**	No longer purchased separately. Included with Integriti Business
996967	HID Mobile Credential - Allow 1000 Credentials	**Replaced**	Removed. Requires 996964 Mobile Credential Management Integration from Integriti V20 onwards
996967UL	HID Mobile Credential - Allow Unlimited Credentials	**Replaced**	Removed. Requires 996964 Mobile Credential Management Integration from Integriti V20 onwards
996964	Mobile Credential Management Integration	**New License**	Replaces the 996967 licenses. Generalized license that will support HID Origo and future Mobile Credential Management integrations
996968	Integriti ModBus TCP Slave Service	**Renamed**	Renamed License: Modbus Slave Integration.
996969	Integriti TBS Biometric Reader Integration	**Renamed**	Renamed License: Biometric Management Integration. Generalized license that will support TBS and future biometric management integrations

Integriti Operator Tenancies

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Operator Tenancies

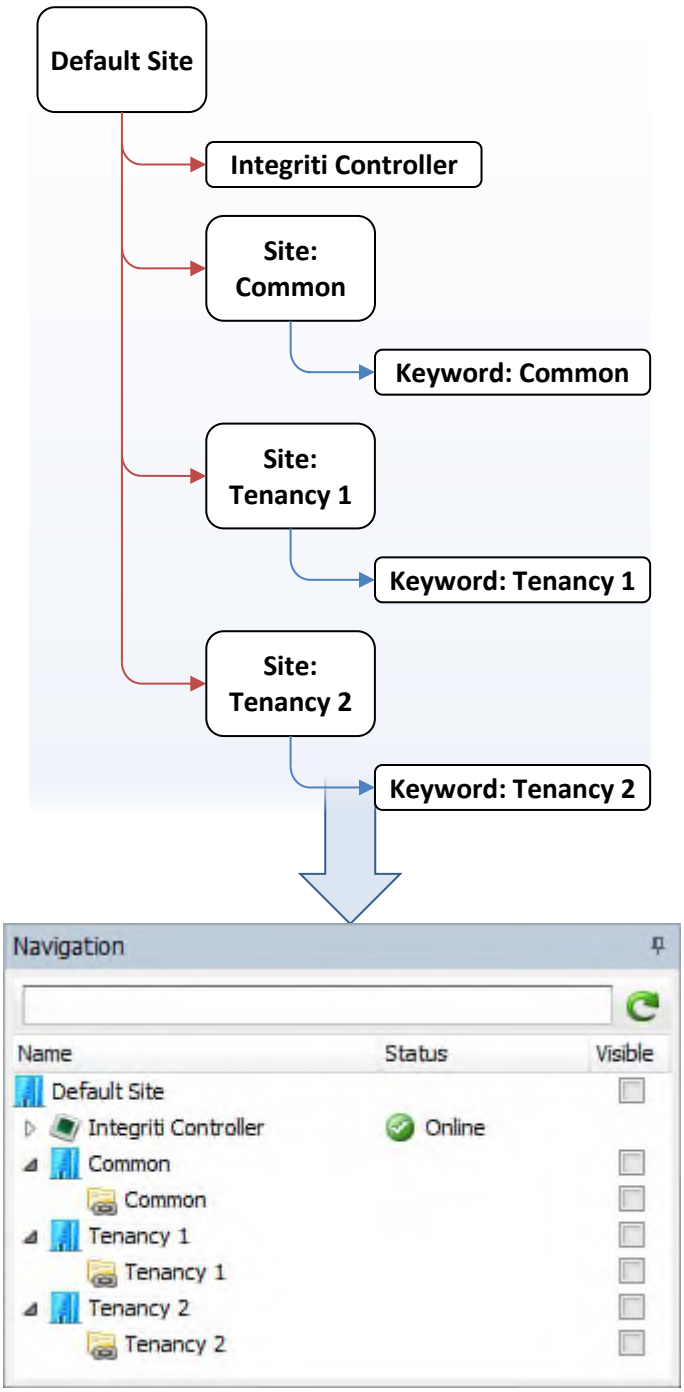
Operator Tenancies are programmed in Integriti using a combination of Sites and Keywords. These Sites and Keywords allow for easy assigning of operator permissions through the Operator Type window.

The following Programming steps are for a tenancy in a single panel site where the installer operator retains all access and two tenants are restricted to their respective permissions.

1. The Integriti panel is to remain under the default site.

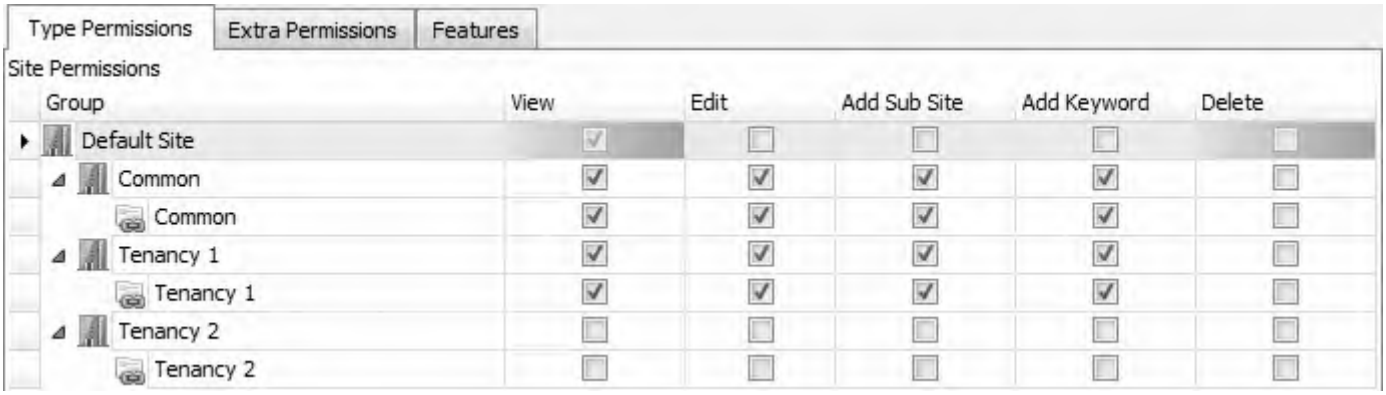
2. Create three additional sites:
    a. Common: this will be used to provide permissions to entities that all tenants will have access to. e.g. primary entry door, entry area
    b. Tenancy 1
    c. Tenancy 2

3. In each of these sites a Keyword is to be created. The site is to resemble the following layout.



4. Create two new Operators and Operator Types. E.g. Tenant 1 & 2

5. In the Operator types the Tenant 1 Site Permissions will be limited to Common and Tenancy 1 sites. The ability for the tenant to add Subsite, Keyword or Delete a site can be changed here.

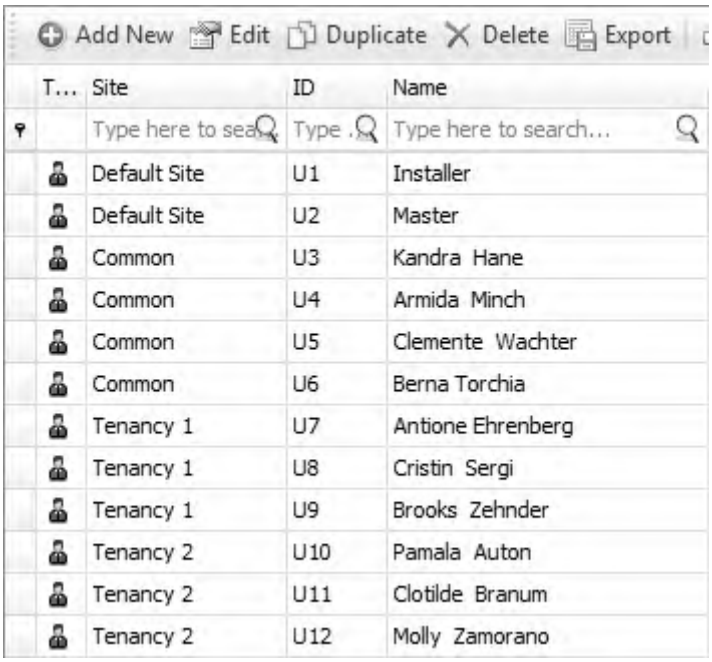


6. In the Entity Type Permissions while each site is individually selected the permissions must be set to Allow for the Common site and the Tenant site.

Make sure that the Default site and the other Tenancy sites are set to deny.

This will be the division in the entities for the use of tenancy.

Many entities in the system can relate to a specific site. This occurs when a new item is created while a specific site is highlighted. Alternatively the Installer can just drag and drop entities onto the specific site if they wish to change the site.
Below are users under Tenant 1 and others under Tenant 2 sites.



T...	Site	ID	Name
	Type here to sea	Type	Type here to search...
	Default Site	U1	Installer
	Default Site	U2	Master
	Common	U3	Kandra Hane
	Common	U4	Armida Minch
	Common	U5	Clemente Wachter
	Common	U6	Berna Torchia
	Tenancy 1	U7	Antione Ehrenberg
	Tenancy 1	U8	Cristin Sergi
	Tenancy 1	U9	Brooks Zehnder
	Tenancy 2	U10	Pamala Auton
	Tenancy 2	U11	Clotilde Branum
	Tenancy 2	U12	Molly Zamorano

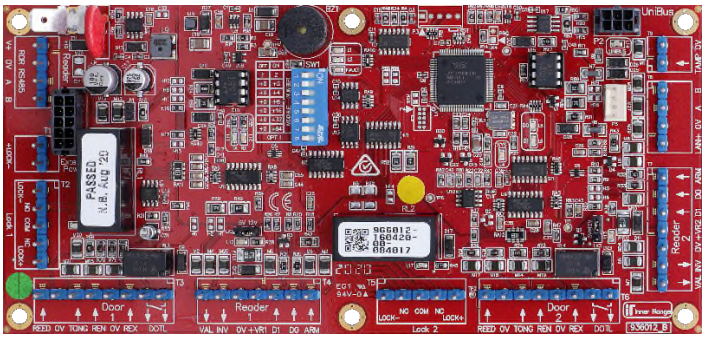
As the tenants only have access to the common site and their own, any users they create will automatically be assigned to one of the two.

Entities that are not site specific but panel specific will need to be added to the keywords. The Installer can just drag and drop entities onto a specific Keyword to grant a certain operator access to that entity. Since the keywords are under the sites they inherit the 'allow' given in the operator types.

7. Once all the operator types permissions are set and the entities are in their Sites/Keywords logging in as either tenant only their specified items will be visible.

Intelligent LAN Access Module (ILAM) Offline Operation

The Inner Range Intelligent LAN Access Module (ILAM) is a 2-door access control module, which is expandable up to 8 doors with 2-door UniBus expanders. Up to 8 Wiegand readers, or 16 SIFER or OSDP readers can be connected to the module. Lock outputs, door reed and tongue inputs, door REX and REN inputs, valid and invalid outputs and Door Open Too Long (DOTL) outputs are all on-board for wired doors. Additionally, the ILAM can be used with various wireless door locks such as Aperio, Salto, Intego and Allegion.



In normal operation, the ILAM connects to an Integriti Controller via the RS-485 LAN, or IP LAN if using an Ethernet Bridge or CLOE module. When a credential is presented to an ILAM's reader, the ILAM sends a message to the Controller to notify it of the access attempt. The Controller determines if access should be granted and responds to the ILAM. The ILAM then provides feedback via its outputs, the reader LEDs & beeper, and activates lock relays if access is granted.

In the rare event of the ILAM losing connection to the controller, the ILAM will detect that it is offline and will switch to its offline operation mode. In offline operation, the ILAM processes all access requests locally using its onboard database. The ILAM will also store up to 100,000 access granted and door event review events in its onboard database and will send these to the controller once a connection is re-established.

ILAM Onboard Database

The Integriti Controller maintains a database with all programming for the controller and its connected modules. A subset of this database is synchronised with the ILAM's onboard database over the RS-485 LAN, so the same programming applies to online and offline operations. The ILAM's database is stored permanently in non-volatile memory. In the event of a power cycle, the ILAM's database and its operation will be intact, without the need to connect to a controller, allowing user access through the ILAM's doors.

Whenever an ILAM module connection is detected by a controller or programming changes are made that are relevant to an ILAM's offline operation, the controller initiates a priority database synchronisation and logs 'ILAM database downloading now Started' in the controller review.

Local Time	Source	Text	Category
15/06/2023 12:42:59 PM	Head Office	ILAM database downloading now Started	LAN FR DLoad

The time taken to complete a database synchronisation depends on a range of factors, including the number of users in the database, how many credentials, PINs, time periods and holidays. The number of other modules on the LAN, the amount of LAN traffic and the use of Ethernet Bridge and CLOE modules also affect the synchronisation time. Large and complex User databases with the maximum of 100,000 credentials can take up to 20 hours to download to the ILAMs, with smaller databases of 100 Users downloading in less than 15 minutes.

Once the priority database synchronisation is completed, the controller will log 'ILAM database downloading now Synchronised' in the controller review.

Local Time	Source	Text	Category
15/06/2023 2:29:02 PM	Head Office	ILAM database downloading now Synchronised	LAN FR DLoad

The database synchronisation process is continual. Once a priority download is complete, a lower priority synchronisation is initiated in the background, to ensure the ILAM onboard database is current and complete.

Changes to the ILAM's module programming are communicated outside of the database synchronisation process and are typically completed within seconds.

ILAM Firmware V4.0.0 Onwards

ILAM firmware V4.0.0 and later expand the ILAMs onboard database and offline operation capabilities. The offline behaviour of ILAMS now more closely follows that of an Integriti Controller.

To enable the offline functionality of ILAM firmware V4.0.0 or later, it is necessary to have the Integriti controller's firmware version V22.2.0 or later. If an ILAM with firmware V4.0.0 or later is used alongside an Integriti controller running firmware version V22.1.0 or earlier the ILAM will be limited to the offline functionality available in V3.3.0 and lower.

Offline Operation

Features supported when offline by ILAM firmware V4.0.0 or later include:

Credential Types

Card, Face Biometric, Hand Biometric, Eye Biometric and License plate Credential Types are supported.
A maximum of 100,000 credentials in total are supported, if users have multiple credentials, this will decrease the number of offline users supported. e.g. If each User has 2 different credential types, there can be a total of 50,000 offline Users.

User PIN Codes

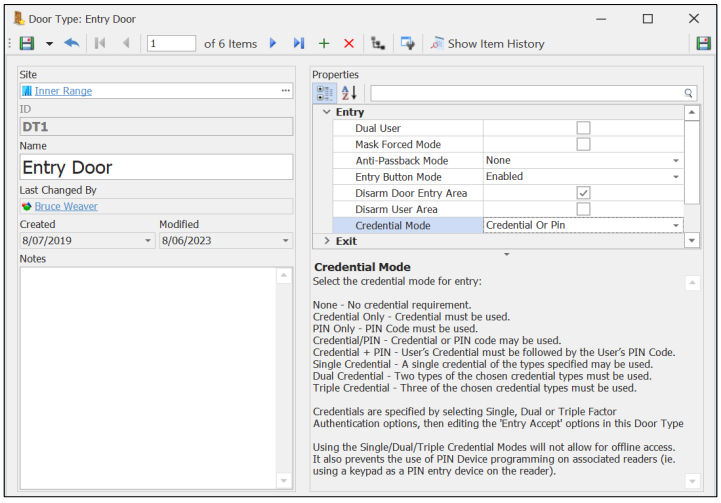
A maximum of 100,000 Users' security and qualified PINs are stored in the ILAM onboard database for use when the ILAM is offline.

Credential Mode

The following Door Type Credential Modes are supported offline:

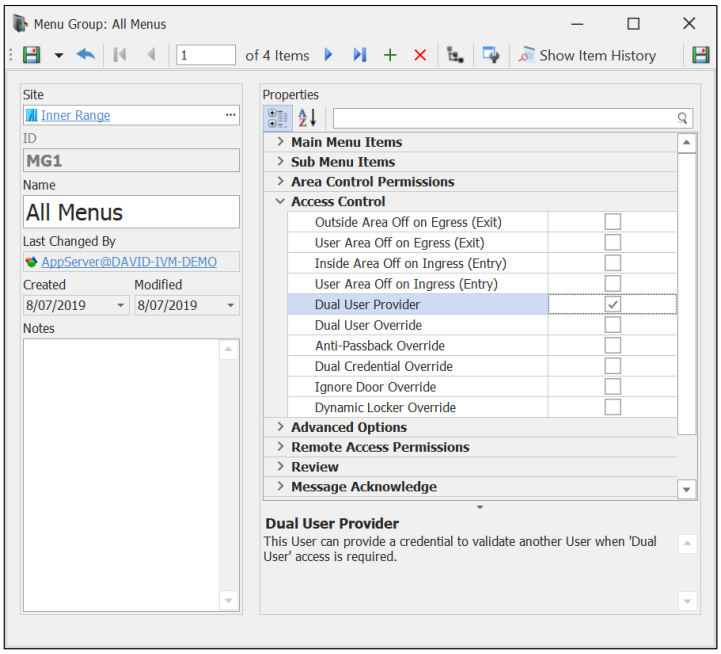
- None
- Credential Only
- PIN Only
- Credential or PIN
- Credential and PIN
- Single Credential
- Dual Credential
- Triple Credential

The Door Type's Credential mode is individually selectable for both door Entry and door Exit paths in *Door Type > Entry > Credential Mode* and *Door Type > Exit > Credential Mode.*



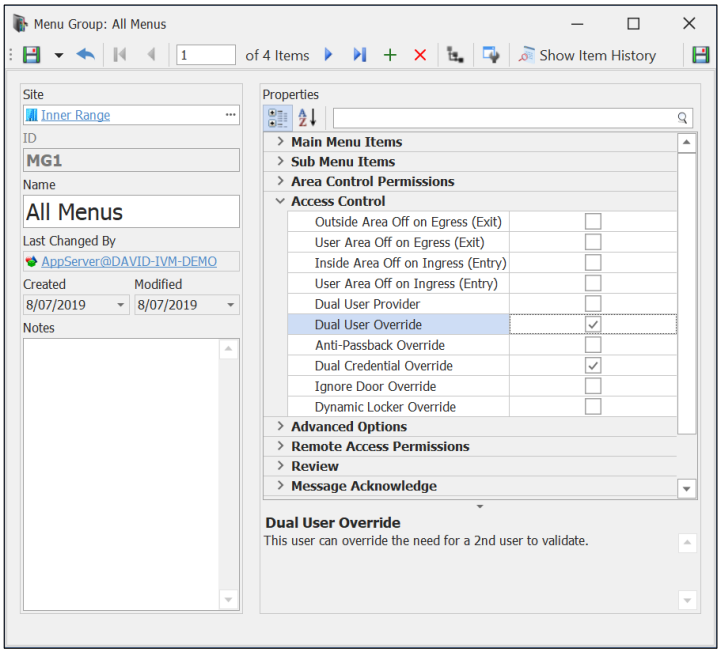
Dual User Access

The Door Type Dual User feature requires access authentication of two users and is configurable for both Entry and Exit paths in the Door Types. This operates in conjunction with the Credential Mode setting, where a user is required to present the selected number of credentials. To qualify for Dual User authentication, a user must be set as Dual User Provider in their *Menu Group > Access Control* Options.



Overrides

User permissions of “Dual Credential Override” and “Dual User Override” are supported offline. Users with override permissions do not need to provide multiple credentials or have a second user authenticate to access the door. A user must be given override permissions in their *Menu Group > Access Control* Options.



REX and REN Functionality

ILAM REX and REN inputs can be configured to work in offline mode. Settings for Door Offline REX and REN functionality are configured in both the ILAM modules *Offline Operation* settings and the Door Type or first door in a Qualified Door Type.

The ILAMs REX and REN function the same whether the ILAM is online or offline based on the configuration, or they can have explicitly different functionality depending on the ILAM's connectivity.
See the Offline REX and REN Programming example below for more details.

Time Zones and Holidays

Users' door access permissions can be qualified by Time Zones and Holidays. Time Zones and Holiday periods are applied in the user's permissions.

NOTE: The ILAM does not retain time across a reset, so it must remain powered and not reset while offline to accurately determine the validity of Time Zones and Holidays. In the event of a power loss to the ILAM, the time periods and holidays will become out of sync with real-time.

For example, if an ILAM loses power for one hour, and then regains power but does not connect to a controller, the onboard time will be one hour behind real time. Time zones and Holidays will begin one hour behind real time. Events logged by the ILAM will be recorded one hour behind real time, and reported as such when connection to a controller is restored.

Wireless Locks

Aperio, Salto Sallis, Intego and Allegion wireless locks operate as normal when an ILAM is offline.

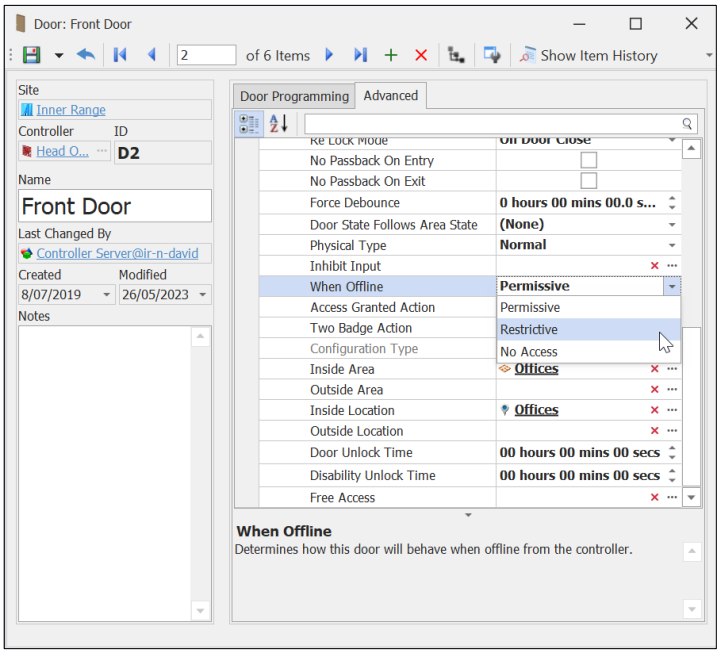
Offline Door Operation

The offline behaviour of individual doors on the ILAM can be configured in the *Door > Advanced > When Offline* setting. Three settings are available:

Permissive Normal access based on Door permissions, Time Zones and Holidays. If entities from other modules are used as door access qualifiers such as areas, inputs, or auxiliaries, these will be assumed invalid, and door access will be denied.

Restrictive Access to doors with Time Zone, Holiday or other qualifiers will be denied. Access to unqualified doors will still be allowed.

No Access All Users are denied access at this Door when ILAM is Offline.



Offline Operation Limitations

When an ILAM is offline from a controller, it cannot communicate with other parts of the system, and entities existing in those other parts cannot be controlled from the ILAM.

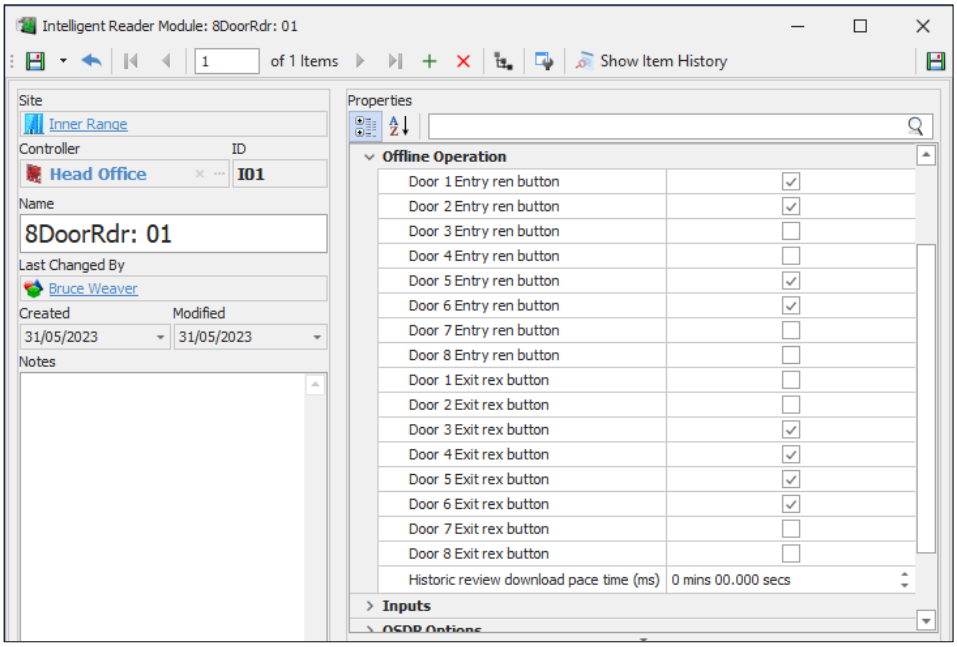
Due to this, the following functions are not supported in ILAM Offline operation:

- Reader Purpose: Control a Lift, Log On, Area control or Access Locker / Locker Bank.
- Reader LED control based on Area or Locker states.
- User Cancel on Card.
- Cancel on PIN.
- Duress Code.
- Disabled User unlock time extension.
- Card Format / Direct Entry Ignore Mask.
- Area-related operations including:
    - Area Control.
    - User Counting.
    - Tenancy Control.
    - Defer Arming.
    - Input Isolation.
- Door-related features including.
    - Interlocking (including when the interlocked doors are on the same ILAM).
    - Anti-passback.
- Door access qualifiers from other entities such as areas, inputs, or auxiliaries.
- Lift operation.
- Qualified Door Types, the first door type in a qualified door type will be used offline.
- Door Relock modes, *On Door Close* will always be used offline.

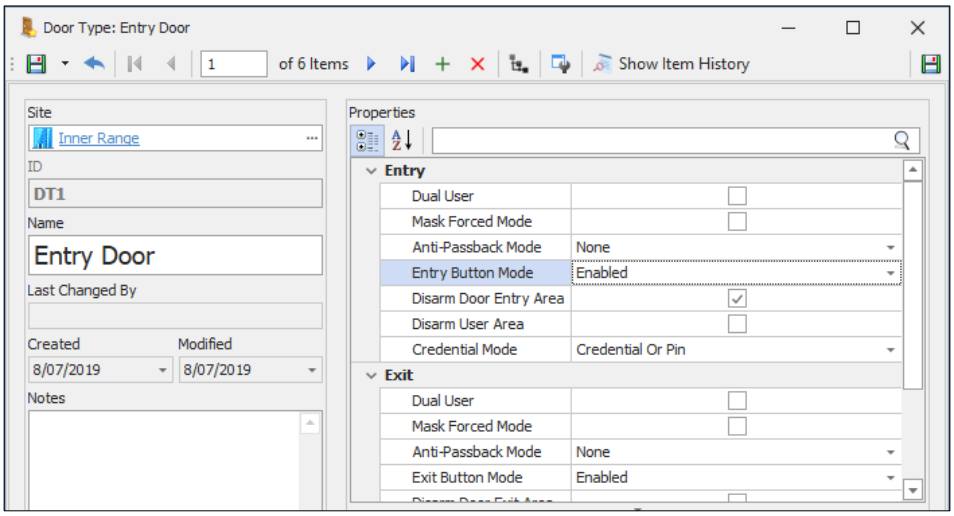
Offline REX and REN Programming

REX and REN offline operation is controlled both individually per door in the ILAM module programming and also in the Door Type programming. Offline REX and REN functionality requires ILAM firmware V4.0.0 or later and Controller firmware V22.2.0 or later.

In the ILAM *Offline Operation* settings, REX and REN offline functionality can be enabled for each door on the module when the ILAM is in offline mode.



If those options are not flagged, the REX and REN operation is determined by the door type. In *Door Type > Entry> Entry Button Mode* and *Door Type > Exit > Exit Button Mode*



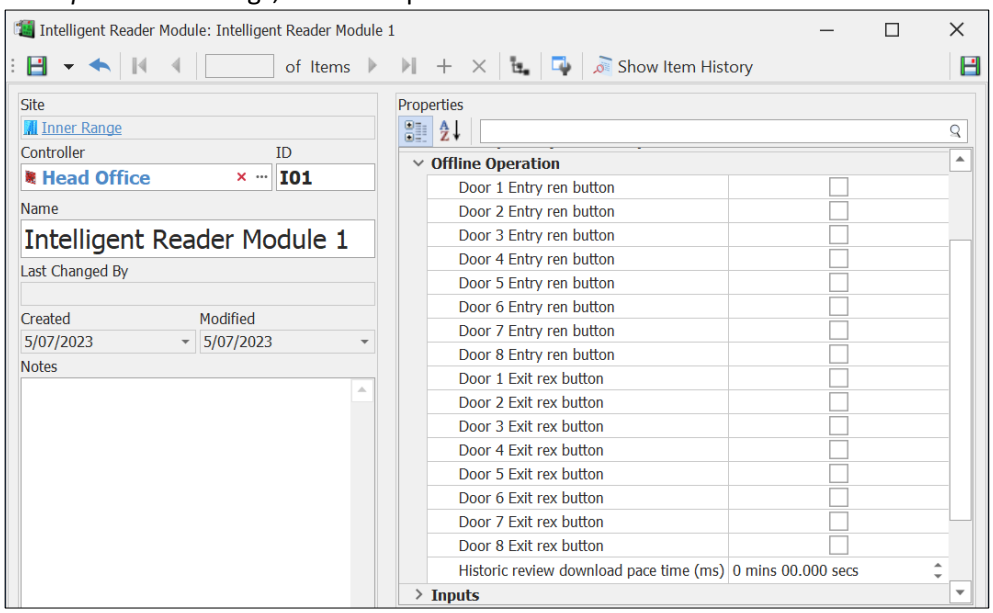
If set to *Enabled,* the buttons will be enabled regardless of if the ILAM is online or offline.

If set to *None,* the buttons will be disabled. This can be overridden in the individual door programming as shown in the Offline Operation settings above.

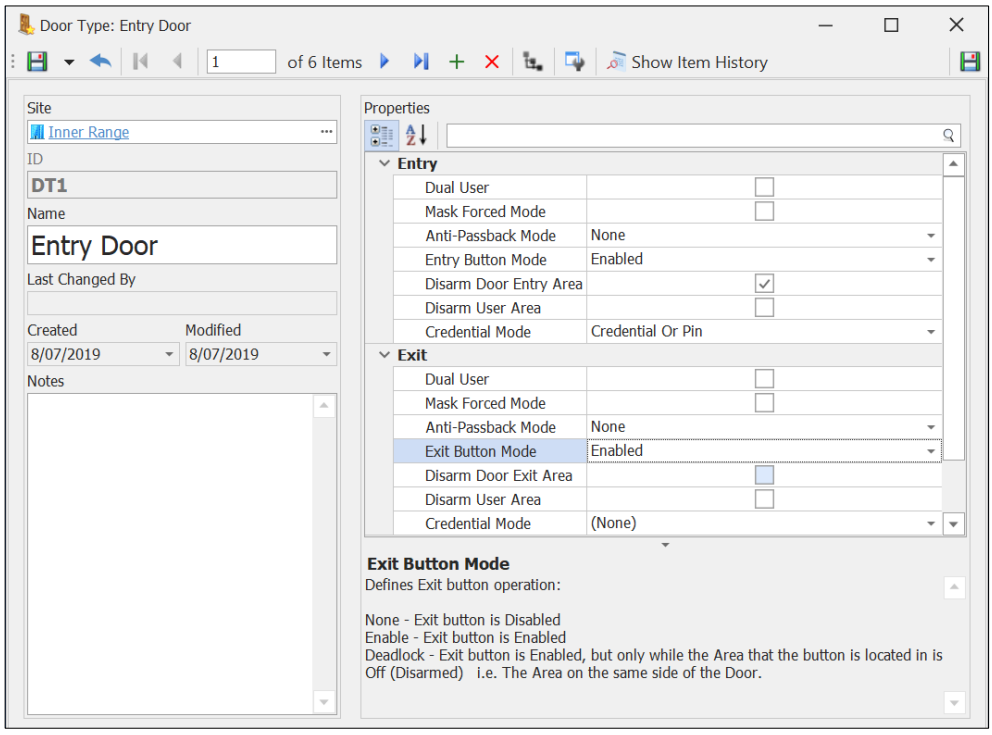
If set to *Deadlock*, the buttons are enabled if the ILAM is online and the area containing the buttons is disarmed. If the ILAM is offline, the buttons will be disabled, as the ILAM cannot verify area state.

Scenario 1 – REX and REN Enabled for Online and Offline Operation

In the ILAM *Offline Operation* settings, leave all options unticked.

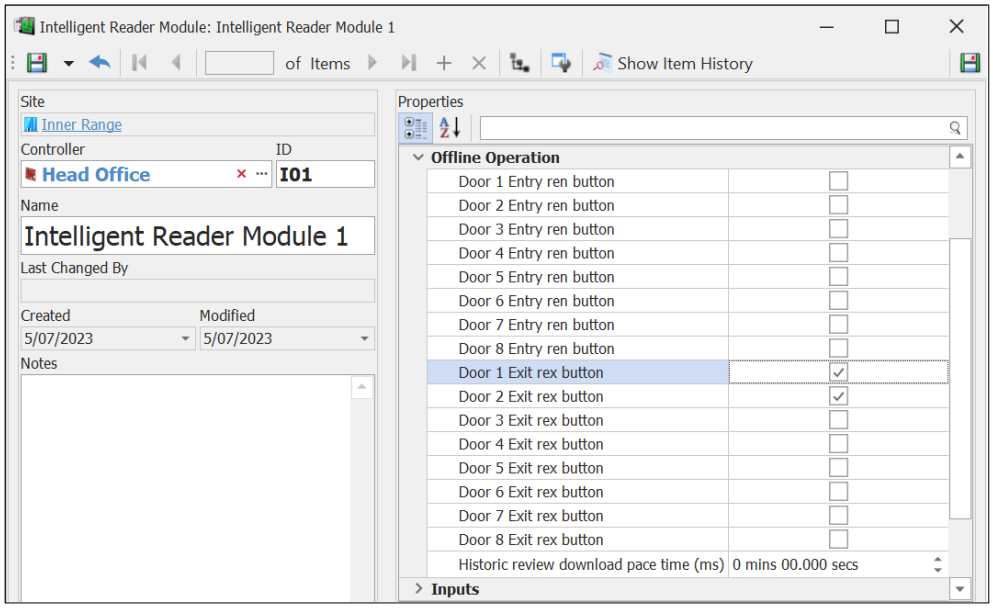


In *Door Type > Entry > Entry Button Mode* and *Door Type > Exit > Exit Button Mode,* set the mode to *Enabled*.

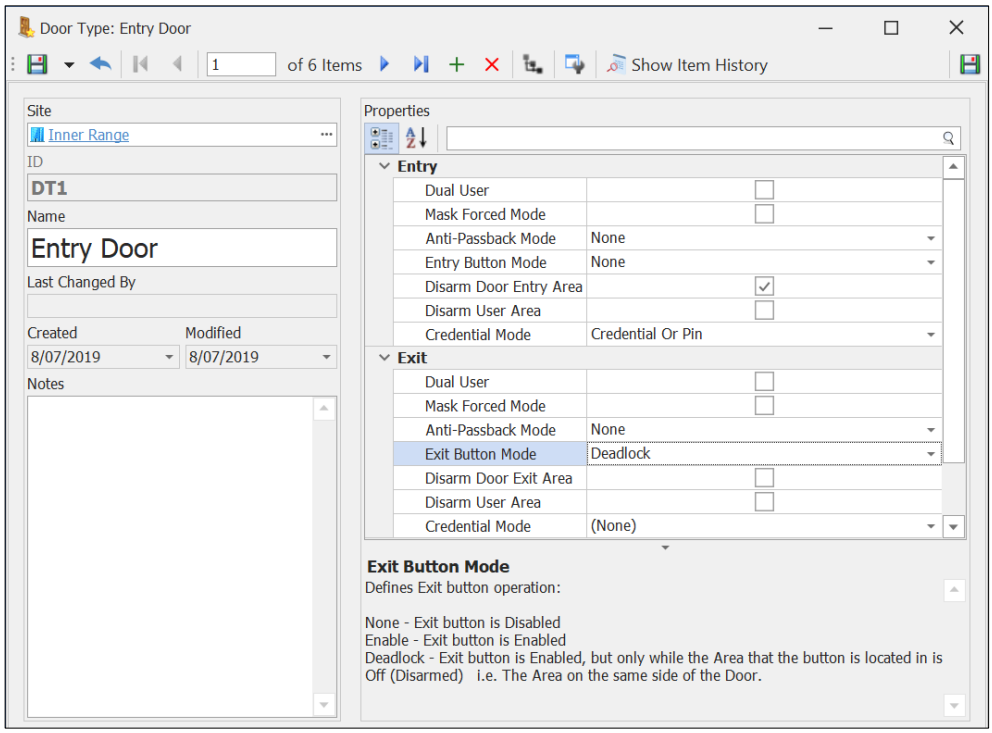


Scenario 2 – Deadlock REX Enabled for Online Operation, REX Enabled for Offline Operation. REN Disabled for Online and Offline Operation

In the ILAM *Offline Operation* settings, tick the REX option for the doors that must have offline REX operations enabled.

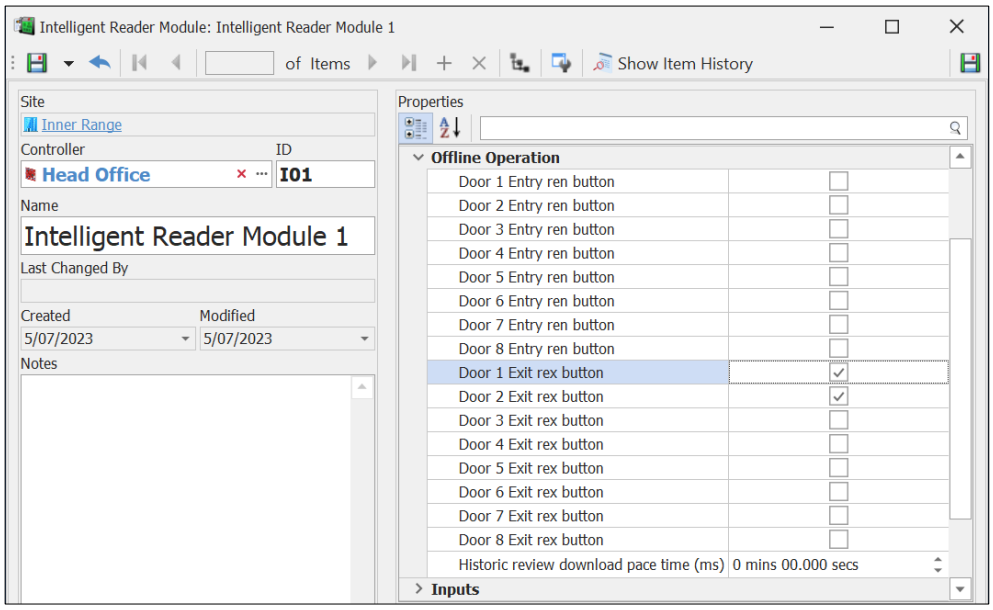


In *Door Type > Exit > Exit Button Mode,* set the mode to *Deadlock*. In *Door Type > Entry > Entry Button Mode,* set the mode to *None.*

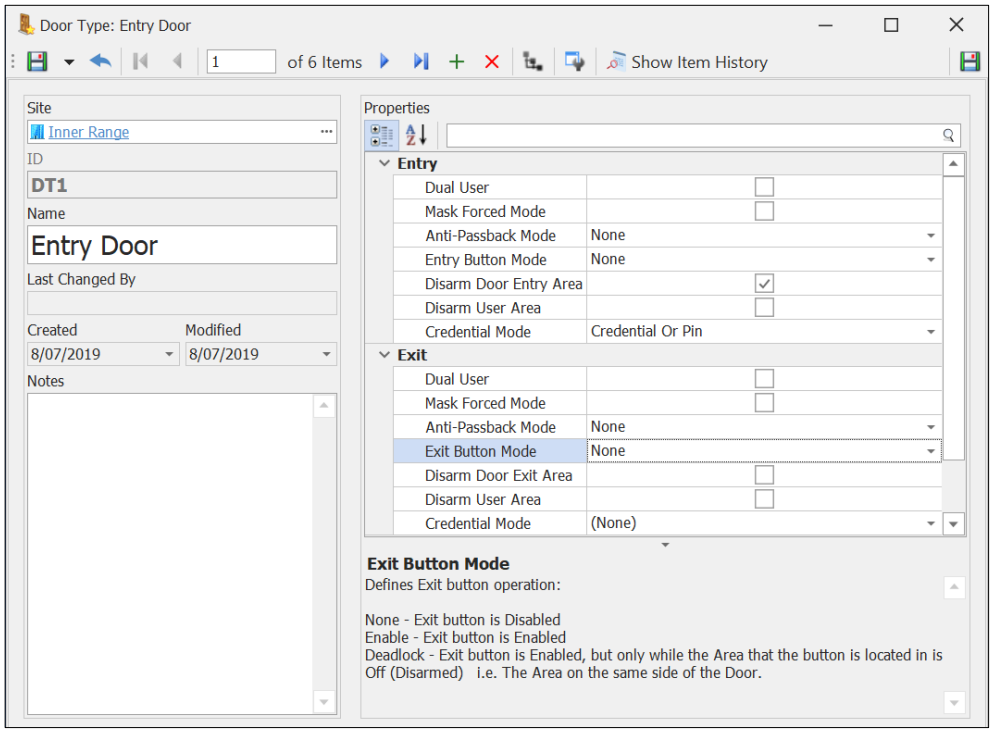


Scenario 3 – REX Enabled for Offline Operation Only. REN Disabled for Online and Offline Operation

In the ILAM *Offline Operation* settings, tick the REX option for the doors that must have offline REX operations enabled.



In *Door Type > Entry > Entry Button Mode* and *Door Type > Exit > Exit Button Mode,* set the mode to *None*.



ILAM Firmware V3.3 and Lower

Offline Operation

Features supported when offline by ILAM firmware V3.3 or earlier are listed below.

If an ILAM with firmware V4.0.0 or later is used alongside an Integriti controller running firmware version V22.1.0 or earlier, the ILAM offline functionality will be limited to these same features.

100,000 User Cards

A maximum of 100,000 Card type credentials are supported.

Time Zones and Holidays

Users' door access permissions can be qualified by Time Zones and Holidays. Time Zones and Holiday periods are applied in the user's permissions.

NOTE: The ILAM does not retain time across a reset, so it must remain powered and not reset while offline to accurately determine the validity of Time Zones and Holidays. In the event of a power loss to the ILAM, the time periods and holidays will become out of sync with real-time.

For example, if an ILAM loses power for one hour, and then regains power but does not connect to a controller, the onboard time will be one hour behind real time. Time zones and Holidays will begin one hour behind real time. Events logged by the ILAM will be recorded one hour behind real time and reported as such when connection to a controller is restored.

Wireless Locks

Aperio, Salto Sallis, Intego and Allegion wireless locks operate as normal when an ILAM is offline. Support for these locks was added in the following firmware versions:

Wireless Lock	ILAM Firmware
Aperio	V2.1.0
Salto Sallis	V3.2.1
Intego	V3.2.1
Allegion	V3.4.0

Offline Operation Limitations

In addition to all limitations in firmware V4.0 and higher, earlier ILAM firmware also has these additional limitations:

- No User PINs
- No Biometric or License Plate credentials
- No Door Credential Types, only Card Only access is supported.
- No Door Dual User or Dual User override
- No Door REX/REN

May 2025

Information Security and Cybersecurity Overview

Inner Range is a manufacturer of unified Video, Access Control and Security solutions. Founded in Melbourne, Australia, Inner Range has over 35 years of innovation and has more than 150,000 systems deployed globally. With a strong foundation in cybersecurity, Inner Range offers advanced, reliable, and secure solutions tailored for critical infrastructure and high-security environments. This document outlines the cybersecurity and information security capabilities of the Inner Range "**Integriti**" platform, highlighting our encryption protocols, governance practices, certifications, and alignment with international standards. It's important to note that this document must be read in conjunction with Inner Range's general cyber security statement, which can be found on our homepage here: www.innerrange.com

1. Data Ownership and Privacy

Integriti is designed as an on-premises or privately hosted solution. Inner Range does not operate Integriti as a SaaS. All data entered into the system is customer-owned and resides within the domain of the customer. Optionally, Inner Range only holds basic contact information during support interactions, and this is handled securely and confidentially.

2. Information Security Governance

Inner Range maintains a comprehensive and robust information security program. This program is underpinned by internal policies aligned with industry-recognised standards such as ISO 27001 and NIST SP 800-53. Security measures include:

- Mandatory use of Inner Range-managed devices with endpoint protection for accessing corporate resources.
- Enforced multi-factor authentication (2FA) for access to services such as email, VPN, and internal systems.
- Full-disk encryption (BitLocker) on all PCs and laptops.
- Enterprise-grade malware and ransomware protection incorporating intrusion detection and prevention systems (IDS/IPS).
- A principle of least privilege enforced through a tightly controlled and regularly audited permission structure.
- VPN access with 2FA, secure backups, and data encryption both at rest and in transit.

Internal awareness training programs help staff understand and implement secure computing practices. These programs are reinforced with regular independent audits, such as a recent security governance audit conducted by IBM.

3. Certifications and Cybersecurity Compliance

- ISO 27001: Inner Range's parent company, Wesco, holds ISO 27001 certification. Inner Range is actively pursuing ISO 27001 certification, targeted for completion in 2025-2026.
- Essential Eight Maturity Model: Integriti aligns with the Australian Cyber Security Centre's Essential Eight Maturity Level 3. Key alignment features include:
    - User authentication enforcement with no unauthenticated access.

- Granular, role-based permission structures for all operator accounts.
- Integration with Active Directory and OAuth for central account management.
- Full support for multi-factor authentication.
- Regular patching, OS hardening, and secure software update procedures.

4. Encryption and Secure Communication

Integriti implements layered encryption to secure all communication and data:

- AES-128:
  - Between card reader and door module (using OSDP).
  - Between controller and field modules (via Ethernet Bridge or CLOE).
  - Between peer controllers (peer-to-peer multicast).
  - Between controller and server software.
- AES-256:
  - Between client software and server software.
  - Within MS SQL Server using Transparent Data Encryption (TDE).
- SSL/TLS:
  - For web client sessions.
  - Between controllers and SkyTunnel cloud service.
  - Between SkyCommand/Mobile apps and SkyTunnel.
  - For third-party integrations, depending on the external system.
- SkyTunnel and SkyCommand: Support TLS 1.2 and 1.3.
- Cipher Suites: Governed by Windows OS configuration. Integriti field devices use proprietary protocols layered on AES128 (CBC mode), with additional authentication layers applied.

5. Product Security and Penetration Testing

Inner Range engages third-party experts to conduct regular penetration tests. Independent assessments have been carried out by:

- Sense of Security.
- Wipro.
- Protiviti.
- IBM (focused on infrastructure and governance).

Testing includes:

- Static and dynamic application security testing (SAST/DAST).
- Secret scanning and dependency analysis.

- Hardware, firmware, and network security reviews.

Inner Range follows secure coding best practices inspired by OWASP. This includes:

- Input validation.
- Zero warning policies in code builds.
- Principle of least privilege.

Penetration test results are confidential and not publicly distributed.

6. Vulnerability and Patch Management

Inner Range issues regular updates that often contain cybersecurity enhancements. If a critical vulnerability is discovered, patches are released for both the current and previous major versions. Release Notes always include details of resolved bugs and security fixes.

7. Integriti Application Access Control and Audit Logging

- Supports detailed operator role configuration with granular permissions (create, view, edit, delete per site or entity).
- Authentication through local accounts, Entra ID, Active Directory, or Okta.
- All activity is logged in internal Review and Audit tables.
- Data can be exported or viewed via Advanced Reports.
- SIEM integration is achievable via:
    - REST XML API
    - Review Sender tool
    - Scheduled Advanced Reports

8. Infrastructure and Networking

- DMZ: Deployments behind a DMZ are fully supported when the network and proxies are correctly configured.
- VPN: TCP/IP communication works reliably over VPN connections.
- Cloud/Virtualisation: Integriti can be hosted on AWS, Azure, or other virtual environments under customer control.

9. Standards and Integrations

- Supported Standards: OSDP, DC09, CSV IP Alarm standards.
- ODBC: Supported for interoperability but native SQL client preferred for performance and T-SQL compatibility.
- SQL Server: Integriti uses advanced TSQL features like triggers, stored procedures, and user-defined types.
- Database Compatibility: While ODBC provides basic access, high-performance features are optimised for Microsoft SQL Server.

Inner Range remains committed to continuous improvement in cybersecurity. By aligning with global standards and incorporating rigorous testing, encryption, and governance measures, we ensure the ongoing security and reliability of our solutions. This dedication supports customers in achieving and maintaining compliance in even the most demanding security environments.

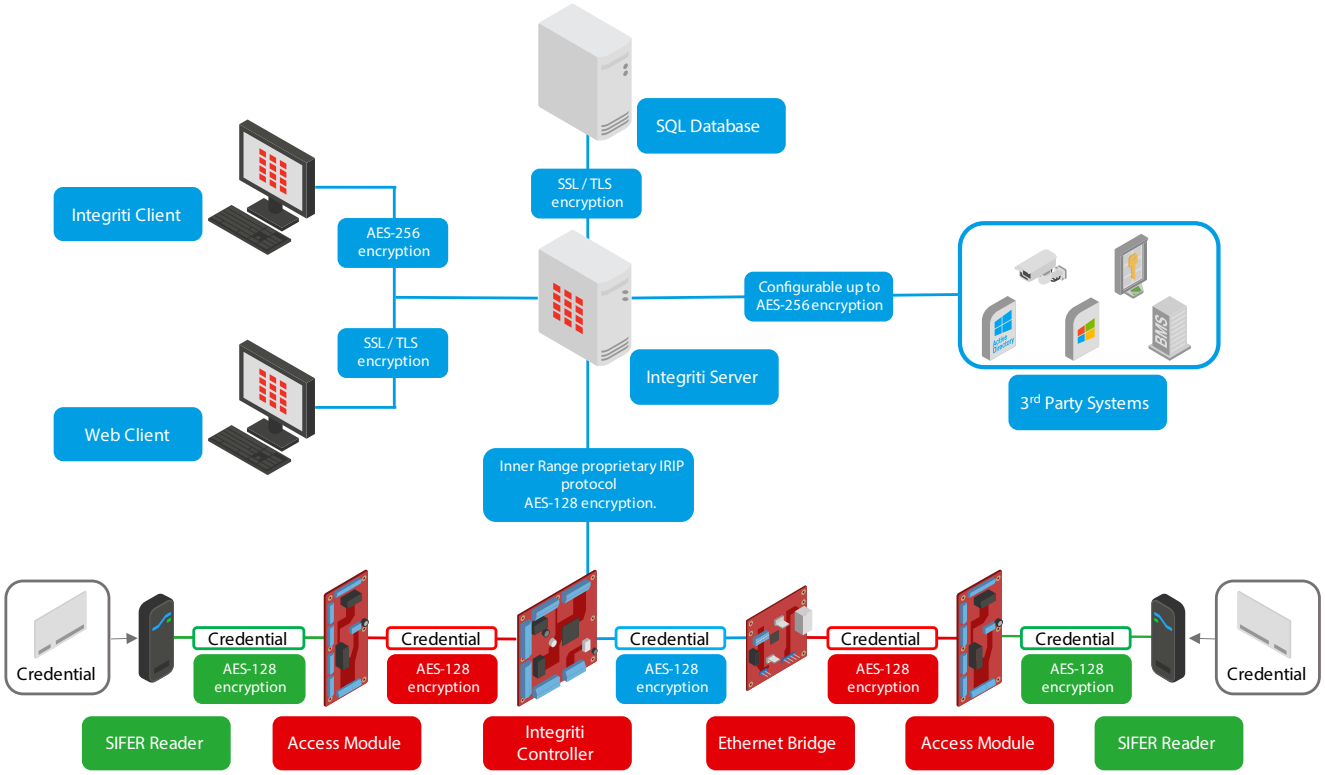
Phone: +61 3 9780 4300
enquiries@innerrange.com
www.innerrange.com
Inner Range Pty Ltd
PO Box 9292, Scoresby, VIC 3179
1 Millennium Court, Knoxfield, VIC 3180

integriti
INTEGRATED SOLUTIONS

Integriti Encryption

The Inner Range Integriti system secures not only buildings and personnel but also user data. All user credentials such as card data and PIN and user details such as usernames, passwords and other personal information are secured as they move through the Integriti system.

IP connections between the Integriti Server and user interfaces are encrypted using SSL/TLS or AES-256 encryptions. All connections between the Integriti Server and field controllers, whether by direct IP or via SkyTunnel, are also encrypted. Credential data and PIN entries from readers and keypads are all encrypted as they are transmitted over the Integriti LAN.



Inner Range is committed to ensuring all our systems' security, as seen in our Cyber Security Statement. As well as relying on the inbuilt security of Integriti we recommend following the best practices laid out in the Integriti Cyber Security Hardening guide.

Operator Challenge

Document created with reference to

Controller firmware V3.0.2 and Integriti software V3.1.0.6951

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Introduction

Operator Challenge displays information to the operator about a card access request.

Operator Challenge can be set up to randomly select users, allowing random bag searches or drug tests for example to be administered.

Users who do not have access permissions to particular doors can be granted access by using Operator Challenge.

In Integriti, the Challenge dialog is completely customizable allowing User Photos, CCTV streams, Allow/Deny buttons, Challenge History, Information display with changeable font/colours and several other items to be arranged and sized as desired.

The Operator Challenge can be used to passively view or interactively grant/deny access to users as they pass through one or many doors.

Operator Challenge dialogs can optionally display:

- CCTV footage
- The User's photo
- Custom text
- Challenge history
- Allow button
- Deny button
- A web page

A list of Task Actions can be executed automatically on any challenge, random selection, allow or deny. These Task Actions are the same as used throughout the system, allowing control of controller items, sending of messages, etc...

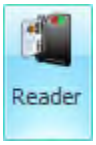
Configuring Integriti hardware

The Integriti hardware needs to be configured to use the Operator Challenge feature. If configured for Operator Challenge, the controller will attempt to contact the Integriti server. The door, user and other details are sent to the Integriti server for processing access control.

There are four entity types that need to be configured for Operator Challenge:

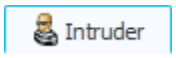
- Integriti controller records
- Integriti communications task records
- Reader modules
- User records

1. Click on the 

tab followed by 

or 

.
2. Double click on a reader module that will be used for Operator Challenge.

3. Expand out Readers followed by Reader *n*.
    - *n* = The number of the reader to be used for Operator Challenge.
4. Tick the Ask PC option.
5. Save and close the editor window for the Reader Module.
6. Repeat steps **7** – **11** for any additional reader modules.
7. Click on the 

tab followed by 

.
    - For one user…
        - **a.** Double click on a user that will be used to trigger Operator Challenge.
        - **b.** Expand out User Options.
        - **c.** Tick the Ask PC option.
        - **d.** Save and close the editor window for the User.
    - For many users…
        - **a.** Select a group of users.
        - **b.** Right-click one of the selected users and select edit.
        - **c.** Expand out User Options.
        - **d.** Tick the Ask PC option.
        - **e.** Save and close the editor window for the selected Users.

20. Repeat step **13** for any additional users.

Creating an Challenge Definition

A Challenge Definition consists of three sections:

- What To Challenge.
- Challenge Response Layout.
- Automatic Actions.

To create a new Challenge Definition…

1. Click on the Access Control tab followed by Operator Challenge.
2. Click Add New. The Editor Window for a new Operator Definition should appear.
3. Give the Operator Definition a name.
4. Click on the Doors to Challenge tab.
   - You can use a combination of Doors, Sites/Keywords and Filters to specify what doors you want to monitor using this Challenge Definition.

   > *You should specify at least one Door, Sites/Keyword or Filter. Otherwise the Operator Challenge will not work.*

   a. You can add individual doors by clicking on the Doors tab followed by the Add button.
   b. You can add an entire site or keyword by clicking on the Sites / Keywords tab followed by the Add button.
   c. You can add doors by creating a filter.
5. Click on the Users To Challenge tab.
   - You can use a combination of Users, Sites/Keywords and Filters to specify what users you want to monitor using this Challenge Definition.

   > *You should specify at least one User, Sites/Keyword or Filter. Otherwise the Operator Challenge will not work.*

   a. You can add individual users by clicking on the Users tab followed by the Add button.
   b. You can add an entire site or keyword by clicking on the Sites / Keywords tab followed by the Add button.
   c. You can add users by creating a filter.
6. Click on the Settings tab.

7. The Show Challenge To Operator settings determine when the Challenge dialog will appear.
    - Setting this option to Never will mean that the Operator Challenge will never display. If users, readers, etc… are configured for Operator Challenge and there is no corresponding Operator Challenge, the controller will send a challenge request, time out after 20 seconds, then process the user based on their permissions.
    - Setting this option to Always will result in the Operator Challenge appearing on every access event.
    - Only on Random Selection will result in the Operator Challenge appearing on a random access event based on X occurrences out of Y challenges.
8. Settings for Requires Operator Input behave the same way as Show Challenge To Operator. When an Operator is not required to Input anything, the controller will continue to process the user based on their permissions.
9. Select X Occurrences and Out of Y Challenges is used to represent the random percentage of access events that will trigger the Operator Challenge.
    - E.g. Select 1 Occurrences Out of 3 Challenges will give you a 33% chance that the user will be picked for Operator Challenge.
10. Random Selection Message is a simple text string used to display a message to the Operator when an Operator Challenge event occurs.
11. Click on the Challenge Response Layout tab.
12. The Challenge response layout is configured the same way as an Alert Response Plan.
    a. Information Boxes display custom text. '%' tags and multiple lines are supported.
    b. Information Displays support basic HTML tags. The supported tags are listed below.
    c. Challenge Pass Button is required for situations where Operator response is required.
    d. Challenge Deny Button is required for situations where Operator response is required.
    e. User Image can display either the user image or a custom image field of the user that triggered the Operator Challenge.
    f. CCTV stream will display live CCTV video from the camera or cameras associated with the door(s) associated with the Operator Challenge.
    g. Challenge history displays a live stream of past and present Operator Challenges.
    h. Browser Item will display the web page specified. Keywords associated with the user can be used in the browser URL.

13. Click on the Automatic Actions tab.
14. Under the On Challenge, On Random Selection, On Allow and On Deny you can add one or many actions to perform on each of the four events.
    - On challenge occurs on every occurrence of the Operator Challenge based on the What To Challenge criteria.
    - On Random Selection occurs on a random Operator Challenge event based on the What To Challenge Settings.

- On Allow and On Deny occur when an Operator selects these options via the Operator Challenge dialog.

Information Display supported HTML

Tag	End Tag	Description
** **		Inserts a single line break.
<color=value>	</color>	Specifies the text color.
Examples:		
<color=red>		
<color=0,255,0>		
<color=#0000FF>		
<backcolor=value>	</backcolor>	Specifies the background color.
Examples:		
<backcolor=red>		
<backcolor=0,255,0>		
<backcolor=#0000FF>		
<size=*value*>	</size>	Specifies the font size.
Examples:		
<size=10>		
<size=+4>		
<size=-4>		
****		Defines bold text.
****		Defines italic text.
<u>	</u>	Defines underlined text.

Note that if you need to use angle brackets ('<' and '>') in the text of the controls that support HTML text formatting, you need to use an additional '<' bracket as a prefix. For example, to get "<some text>" you should assign "<<some text>" to the corresponding property.

Testing Challenge Definitions

Challenge Definitions should be tested by observing messages sent to the review log.

The following is an example of a typical Operator Challenge:

```
Locker 9B Actuator Off by Locker 9B (Door Logic) (R01:X01)  Single Aux Change
Locker 9B Locked by (Door Logic) (D002)  Door Event
Locker 9B Actuator On by Locker 9B (Door Logic) (R01:X01)   Single Aux Change
Locker 9B Timed Unlocked for 00005 secs by Storage (Door Logic) (D002) Door Event
John Card Access at R01:Rdr01 into Locker 9B User Access
John Card Access at R01:Rdr01 into Locker 9B - Software Auth. Response User Access
John Card Access at R01:Rdr01 into Locker 9B - Software Auth. Request  User Access
Wiegand Raw (26) = 1A00000000000000004E00F7(hex) at R01:Rdr01   Card Info
```

You will be able to determine if the challenge request is coming through to the Integriti server to be processed by observing the following messages...

The following messages are appended to review data (as seen in the above example).

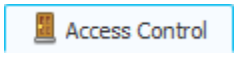
Review message	Description
Software Auth. Overflow	A card has been presented to a reader that is configured for operator response. The controller is waiting for an operator response and… • Another card has been presented to the same reader. • A card has been presented to a different reader which is a part of the same Challenge Definition.
Software Auth. Denied	An Operator denied access to the user.
Software Auth. Timeout	An Operator did not action the Challenge request.
Software Auth. Request	A card has been presented to a reader configured for Operator Challenge.
Software Auth. Response	An Operator has allowed access to the user.

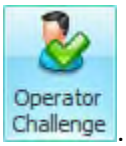
If a Challenge Definition does not exist for a reader that has been configured for Operator Challenge then users with the Ask PC option will be granted access. This includes users without access permissions to the associated door record(s).

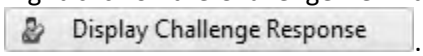
Viewing Challenge Definitions

Once created, Challenge Definitions need to be manually opened by the operator.

Viewing a Challenge Definition in System Designer…

1. Click on the 

tab followed by 

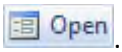
.
2. Right-click on the Challenge Definition and select 

.

Viewing a Challenge Definition in GateKeeper…

1. Click on the 

tab followed by 

.
2. Double-click on the Challenge Definition.
–or–
2. Select the Challenge Definition and click 

.

DATA SHEET

SIFER Credentials

A wide variety of credentials are available to suit Inner Range SIFER card readers. SIFER credentials are available in various form factors for use with physical and logical access control systems. All SIFER credentials use the highly secure MIFARE® DESFire© EV3 card format.

Form factor types for SIFER credentials include:

ISO Cards, Key Fobs, self-adhesive Tags/Coils and Wristbands.
Three ordering options are available for each form factor type.

SIFER-P: Pre-programmed 'Stock' Credentials.

SIFER-P credentials are pre-programmed with the Inner Range Global Encryption Key and can be used with standard SIFER Readers without any need for card or reader configuration. SIFER-P credentials are supplied with a pre-programmed site code and a card number that is guaranteed to be unique and are 'locked' to disallow re-programming in the field. SIFER-P credentials are supplied with the SIFER-P mark and are printed with the unique card number.

SIFER-U: User-programmable Credentials.

SIFER-U credentials have an identical set of specifications to that of SIFER-P with the major difference being that they can be reprogrammed in the field. By default SIFER-U credentials are shipped pre-programmed with the Inner Range SIFER Global Encryption Key and can be used with standard SIFER Readers without any need for card or reader configuration. Although SIFER-U credentials are supplied pre-programmed, the site code and encryption key can be re-programmed in the field using a SIFER card programming station. (It is not recommended to re-program SIFER-U card numbers as they are already unique)

When SIFER-U credentials have been re-programmed, the SIFER readers must also be re-configured to use the same encryption key. To perform the Reader configuration, a "Reader Configuration Card" must be produced using the SIFER card programming station. SIFER-U customisation is a process that is carried out by the installer and as such the unique encryption key must be stored and managed for safekeeping by the installer, this facilitates additional card batches at a future date. Where a unique SIFER-U encryption key has been lost it cannot be recovered.

SIFER-U: Gold Card Service.

As an alternative to the installer specifying their own custom encryption key, Inner Range offers a 'Gold Card' service, providing the installer with a unique Gold Key Configuration Card ('Gold Card'). The Gold Card delivers a guaranteed unique custom encryption key for use with the SIFER programming station and SIFER-U credentials. Inner Range assigns a unique encryption key from the reserved 'Gold Card' range. The encryption key is then associated with the customer's site to facilitate future card orders. The encryption key is securely stored within Inner Range where it cannot be viewed or shared. Being a reserved key, the key can never be manually entered using a SIFER programmer.

SIFER-C: Custom Programmed Credentials & Reader Configuration Cards.

The SIFER-C option allows installers to order reader configuration cards and user credentials from the factory with specific custom programming. SIFER-C allows the card number range, site code and encryption key to be programmed to order. SIFER-C card numbers are guaranteed to be unique and are 'locked' to disallow credential re-programming in the field. SIFER-C credentials are supplied with the SIFER-C mark and are printed with the unique card number. Where SIFER-C credentials are to be deployed the SIFER readers/keypads on the site must also be re-configured to use the matching encryption key. To accommodate this a Reader Configuration Card (994614CNF) is also required.

ECOLITE: Budget-friendly, Less Secure..

ECOLITE is a budget range of credentials that is compatible with Inner Range SIFER Readers, Integriti & Inception systems. These credentials are based on the MIFARE Ultralight EV1 technology which is a lower priced - lower security option compared to the standard DESFire EV3 technology used in our SIFER-P, SIFER-U & SIFER-C range of credentials.

Ordering Options

Standard SIFER Credentials. All credentials are MIFARE® DESFire© EV3 4K - ECOLITE Cards are MIFARE Ultralight EV1 technology

ISO Cards
SIFER-P ISO Card **994610**
SIFER-U ISO Card **994612**
SIFER-C ISO Card **994614**
ECOLITE ISO Card **994580**

Silicon Wrist Bands
SIFER-P Wristband **994625P**
SIFER-U Wristband **994625U**
SIFER-C Wristband **994625C**

Special Order Multi Application Cards & Fobs*
994614A Dual Application ISO card SIFER/Aperio
994614H Dual Application ISO card SIFER/HID
994614AH Tri Application ISO card SIFER/Aperio/HID

Key Fobs
SIFER-P Key Fob **994616**
SIFER-U Key Fob **994618**
SIFER-C Key Fob **994620**

SIFER-U Gold Card
994612G for use with SIFER-U credentials

994620A Dual Application Key Fob SIFER/Aperio
994620H Dual Application Key Fob SIFER/HID
994620AH Tri Application Key Fob SIFER/Aperio/HID
*All multi-application credentials must be based on MIFARE® DESFire©® EV1/EV2 media (56 bit)

Self Adhesive 20mm Coils
SIFER-P Tag/Coil **994621P**
SIFER-U Tag/Coil **994621U**
SIFER-C Tag/Coil **994621C**

SIFER Reader Configuration Card
994614CNF for use with SIFER-C credentials
& SIFER readers and Keypad Readers

July 2025

Inner Range Sifer ISO Cards

Inner Range confirms the following in relation to our Sifer ISO cards.

1. The cards support the ISO 14443A standard or equivalent.
2. The temperature range of the cards is -25ºC to +40ºC.
3. The ISO card is white.
4. The card frequency is 13.56 Mhz.

For clarification please do not hesitate to contact the undersigned.

Yours on behalf of Inner Range

Tim Northwood

Digitally signed by Tim Northwood
Date: 2025.07.14 13:52:49 +01'00'

Tim Northwood
Sales Director EMEA

Phone: +44 (0) 845 470 5000
enquiries.uk@innerrange.com
www.innerrange.com
Inner Range
Inspired, Easthampstead Road, Bracknell,
Berks RG121YQ, UK

Back

SIFER ISO Card

994610 / 994612 / 994614

The SIFER ISO Card is a MIFARE DESFire EV3 credential. There are three ordering options available which are mentioned below. These cards are printable and punchable. This form of credential is commonly used for sites where the credential itself can be used as an ID badge or where a custom printing is required. Designated hole punchouts can be used to connect lanyards.

Related products | Ordering Options | Documents

	Global
SIFER-P ISO Card	994610
SIFER-U ISO Card	994612
SIFER-C ISO Card	994614

SIFER Keypad Card Reader

994725

The SIFER Keypad is a combined IP67 rated Keypad and Smart Card reader that allows dual credential Card & PIN high security access control. (PIN only or Card only is also supported)

The SIFER Keypad is a multi-drop RS-485 device that employs 128 bit AES encryption from the card/keypad through to the door module, providing a far superior level of security than that of traditional Wiegand based keypads & card readers.

SIFER Keypads utilise the Mifare DESFire© EV1/EV2/EV3 card format. As SIFER Keypads utilise a superset of the OSDP protocol, the keypads may also be deployed on any system capable of using OSDP. SIFER Keypads are connected to the RS-485 reader port for full Reader-In and Reader-Out operation of various Inner Range products as below.

- Integriti Access Controller (IAC) - Up to 16 on-board
- Intelligent LAN Access Module (ILAM) - Up to 16 Keypads/Readers
- Standard LAN Access Module (SLAM) - Up to 4 Keypads/Readers
- Inception Controller - Up to 8 on-board

SIFER Keypads are IP67 rated and available with site-specific encryption keys.

Multi-Format Version
A SIFER Multi-Format Keypad/Card reader is also available and offers an identical set of features to the Standard SIFER Keypad with additional support for reading the CSN of third party 13.56 Mhz credentials.

Features | Related products | Ordering Options | Documents | Software & Firmware

Reader Features

- Secure 128bit AES Encryption
- Encrypted from Keypad/Card through to Access Module
- Supports Card & PIN, Card only or PIN only modes
- Auto-dimming backlit Silicon rubber keypad
- Mifare DESFire© EV1/EV2/EV3 Card Format
- Water & Dust Resistant to IP67
- Vandal Resistant (fully potted)
- Flexible LED colour & function Assignment
- Audible Buzzer (can use as DOTL)
- Multi-drop RS-485 Reader LAN
- Individual Reader Heartbeat Monitoring
- Auto Reader Discovery on Inner Range systems
- OSDP Compatible
- Read Card Serial Number (CSN) From 3rd Party Cards (Multi-Format Version Only)
- Support for Custom Site Codes and Site Specific Encryption
- User Programmable Cards Offer Great Flexibility for Installers
- Global Configuration from Inner Range Systems (including firmware updates)
- Small Footprint (Dimensions: 64 (W) x 106(H) x 18 (D) mm)

Australia / NZ | Asia | Canada | Middle East | UK / Europe | USA

Address
1 Millennium Court Knoxfield. Victoria, 3180, Australia

Call Us
+61 3 9780 4300

Mail Us
sales.au@innerrange.com

Back

SIFER Reader

994720

The SIFER card reader is a Smart Card reader designed and manufactured by Inner Range. It is a multi-drop RS-485 based reader that employs 128 bit AES encryption from the card through to the door module, providing a far superior level of security than that of traditional Wiegand based card readers. SIFER readers utilise the Mifare DESFire© EV1/EV2/EV3 card format.

As SIFER readers utilise a superset of the OSDP protocol, the readers may also be deployed on any system capable of using OSDP. SIFER readers are connected to the RS-485 reader port for full Reader-In and Reader-Out operation of various Inner Range products as below.

- Integriti Access Controller (IAC) - Up to 16 Readers on-board
- Intelligent LAN Access Module (ILAM) - Up to 16 Readers
- Standard LAN Access Module (SLAM) - Up to 4 Readers
- Inception Controller - Up to 8 Readers on-board

SIFER readers are IP67 rated and available with site-specific encryption keys.

Multi-Format Version
The SIFER Multi Format Card reader offers an identical set of features to the Standard SIFER Reader with additional support for reading the CSN of third party 13.56Mhz credentials.

Features | Related products | Ordering Options | Documents | Software & Firmware

Reader Features

- Secure 128bit AES Encryption
- Encrypted from Reader/Card through to Access Module
- Mifare DESFire© EV1/EV2/EV3 Card Format
- Water & Dust Resistant to IP67
- Vandal Resistant (fully potted)
- Flexible LED colour & function Assignment
- Audible Buzzer (can use as DOTL)
- Multi-drop RS-485 Reader LAN
- Individual Reader Heartbeat Monitoring
- Auto Reader Discovery on Inner Range systems
- OSDP Compatible
- Read Card Serial Number (CSN) From 3rd Party Cards (Multi-Format Version Only)
- Support for Custom Site Codes and Site Specific Encryption
- User Programmable Cards Offer Great Flexibility for Installers
- Global Configuration From Inner Range Systems (including firmware updates)
- Small Footprint (Dimensions: 39(W) x 95(H) x 15(D) mm)

3 priedas

[NAUDOJAMA, KAI PREKĖS TIEKIAMOS, NEATLIEKANT UŽSAKYMŲ]

PREKIŲ PERDAVIMO - PRIĖMIMO AKTO FORMA

PREKIŲ PERDAVIMO - PRIĖMIMO AKTAS NR. ----------

(data)

Tiekėjas:	
Sutarties Nr.:	
Sutarties pavadinimas:	

Visos tiekiamos prekės, nurodytos prekių sąraše, buvo pristatytos, pateikti visi reikalingi dokumentai (sertifikatai, naudojimo ir priežiūros instrukcijos ir panašiai).

Visos su prekių viešojo pirkimo-pardavimo sutarties vykdymu susijusios paslaugos buvo suteiktos (jei numatyta sutartyje): [įrašyti suteiktas paslaugas].

Pirkėjas pristatytas prekes priėmė ir patvirtina, kad pristatytos prekės atitinka sutarties sąlygas ir yra tinkamos naudoti.

Prekių sąrašas:

							Valiuta:	**Eur**
Eil. Nr.	**Pristatymo data**	**Vietos adresas**	**Garantinis terminas**	**Prekės pavadinimas (įvardinant tikslius prekių gamintojų ir prekių modelių pavadinimus)**	**Mato vnt.**	**Kiekis**	**Vieneto kaina be PVM**	**Suma be PVM**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9=7×8**
							Iš viso be PVM:	
							PVM [tarifas]*:	
							Iš viso su PVM:	

Perdavė Tiekėjas		**Priėmė Pirkėjas**	
Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:	
Parašas:		Parašas:	
Data:		Data:	
A.V.		A.V.	

* - *tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, atitinkamos skiltys nepildomos ir nurodomos priežastis, dėl kurių tiekėjas PVM nemoka.*

T33238

[NAUDOJAMA, KAI PREKĖS TIEKIAMOS, ATLIEKANT UŽSAKYMUS]

PREKIŲ PERDAVIMO - PRIĖMIMO AKTO FORMA

PREKIŲ PERDAVIMO - PRIĖMIMO AKTAS NR. ----------

(data)

Tiekėjas:	
Sutarties Nr.:	
Sutarties pavadinimas:	

Visos tiekiamos prekės, nurodytos prekių sąraše, buvo pristatytos, pateikti visi reikalingi dokumentai (sertifikatai, naudojimo ir priežiūros instrukcijos ir panašiai).

Visos su prekių viešojo pirkimo-pardavimo sutarties vykdymu susijusios paslaugos buvo suteiktos (jei numatyta sutartyje): [įrašyti suteiktas paslaugas].

Pirkėjas pristatytas prekes priėmė ir patvirtina, kad pristatytos prekės atitinka sutarties sąlygas ir yra tinkamos naudoti.

Prekių sąrašas:

								Valiuta:	**Eur**
Eil. Nr.	**Užsakymo data**	**Pristatymo data**	**Vietos adresas**	**Garantinis terminas**	**Prekės pavadinimas (įvardinant tikslius prekių gamintojų ir prekių modelių pavadinimus)**	**Mato vnt.**	**Kiekis**	**Vieneto kaina be PVM**	**Suma be PVM**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10=8×9**
								Iš viso be PVM:	
								PVM [tarifas]*:	
								Iš viso su PVM:	

Perdavė Tiekėjas		**Priėmė Pirkėjas**	
Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:	
Parašas:		Parašas:	
Data:		Data:	

A.V. A.V.

** - tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, atitinkamos skiltys nepildomos ir nurodomos priežastis, dėl kurių tiekėjas PVM nemoka.*

T33238

GARANTINIŲ ĮSIPAREIGOJIMŲ ĮVYKDYMO AKTO FORMA

GARANTINIŲ ĮSIPAREIGOJIMŲ ĮVYKDYMO AKTAS NR. ----------

(data)

Tiekėjas:	
Sutarties Nr.:	
Sutarties pavadinimas:	

(metai, mėnuo, diena) buvo pasirašytas Prekių perdavimo - priėmimo aktas.

Šiuo aktu Pirkėjas patvirtina, kad Tiekėjas ---
(metai, mėnuo, diena) įvykdė Sutartyje numatytus garantinius įsipareigojimus.

Tiekėjas		**Pirkėjas**	
Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:	
Parašas:		Parašas:	
Data:		Data:	

A.V. A.V.

5 priedas

Trišalės atsiskaitymo sutarties forma

TRIŠALĖ ATSISKAITYMO SUTARTIS

20___ m._____ __ d. Nr. _____

Vilnius

Perkančiosios organizacijos pavadinimas:

Įmonės kodas:

PVM mokėtojo kodas:

Adresas:

Atsiskaitomosios sąskaitos numeris:

toliau – Pirkėjas,

Tiekėjo pavadinimas:

Įmonės kodas:

PVM mokėtojo kodas:

Adresas:

Atsiskaitomosios (-ųjų) sąskaitos (-ų) numeris (-iai) mokėjimams vykdyti:

toliau – Tiekėjas,

(Jeigu tai jungtinės sutarties veiklos pagrindu veikianti tiekėjų grupė, nurodyti, iš kokių ūkio subjektų sudaryta, visų šių subjektų pavadinimus, įmonės ir PVM kodus, adresus, atsakingojo partnerio pavadinimą bei šį partnerį atstovaujančio asmens pareigas, vardą ir pavardę)

ir

Subtiekėjo pavadinimas:

Įmonės kodas:

PVM mokėtojo kodas:

T33238

Adresas:

Atsiskaitomosios (-ųjų) sąskaitos (-ų) numeris (-iai) mokėjimams vykdyti:

toliau – Subtiekėjas,

toliau kiekviena atskirai vadinama Šalimi, o visos kartu vadinamos Šalimis, atsižvelgdamos į tai, kad [*Pirkėjas ir Tiekėjas*] [*įrašyti datą*] sudarė viešojo pirkimo-pardavimo sutartį Nr. [*įrašyti numerį*] (toliau – Pirkimo sutartis), siekdamos nustatyti tiesioginio atsiskaitymo tvarką pagal Pirkimo sutarties specialiųjų sąlygų *[įrašyti punkto numerį*] punktą, sudarė šią trišalę atsiskaitymo sutartį (toliau – Trišalė sutartis).

1. straipsnis. Sutarties dalykas

1.1. Šios Trišalės sutarties dalykas yra tiesioginio atsiskaitymo su Subtiekėju tvarka ir sąlygos.

1.2. Šiuo Susitarimu yra įgyvendinamos Pirkimo sutarties sąlygos. Jokios šios Trišalės sutarties nuostatos neturi būti aiškinamos kaip prieštaraujančios ar panaikinančios Pirkimo sutarties sąlygas.

1.3. straipsnis. Atsiskaitymo tvarka

1.4. Avansinis mokėjimas nemokamas. Pirkėjo pareiga sumokėti Subtiekėjui pagal šią Trišalę sutartį atsiranda tuo pačiu momentu, kaip ir Pirkėjo pareiga sumokėti Tiekėjui pagal Pirkimo sutartį.

1.5. Kiekvieno mokėjimo suma nustatoma pagal faktiškai [*suteiktų paslaugų kiekį bei jų vertę ir/arba [pristatytų prekių kiekį bei jų vertę*].

1.6. Subtiekėjas prieš teikdamas mokėjimo dokumentus Pirkėjui pateikia Tiekėjo pasirašymui ir patvirtinimui tinkamai įformintus Pirkimo sutarties vykdymo dokumentus (po 3 (tris) egzempliorius): Trišalės atsiskaitymo sutarties perdavimo-priėmimo aktą ir Pirkimo sutarties įgyvendinimo ataskaitą (jeigu taikoma).

1.7. Sutarties Šalys susitaria, jog Subtiekėjo pateikti Pirkimo sutarties vykdymo dokumentai laikomi tinkamai įformintais ir pateiktais, jeigu nurodytuose dokumentuose pateikta informacija apie Subtiekėjo [*suteiktas paslaugas*] [*pristatytas prekes*] yra teisinga, [*suteiktos paslaugos*] [*pristatytos prekės*] bei dokumentų įforminimas atitinka Pirkimo sutarties sąlygas;

1.8. Tiekėjas gavęs iš Subtiekėjo Pirkimo sutarties vykdymo dokumentus patikrina juos ir nustatęs, kad dokumentuose pateikta informacija apie Subtiekėjo [suteiktas paslaugas] [pristatytas prekes] yra teisinga, [suteiktos paslaugos] [pristatytos prekės] atitinka Pirkimo sutarties sąlygas, pateikti dokumentai įforminti tinkamai, ne vėliau kaip per 3 (tris) darbo dienas nuo tokių dokumentų gavimo dienos:

1.8.1. pasirašo ir patvirtina Trišalės atsiskaitymo sutarties perdavimo-priėmimo aktą;

1.8.2. Pasirašo ir patvirtina Pirkimo sutarties įgyvendinimo ataskaitą (jeigu taikoma);

1.8.3. pateikia Pirkimo sutarties vykdymo dokumentus Pirkėjui.

1.9. Jeigu Tiekėjas nustato, kad Subtiekėjo pateikti Pirkimo sutarties vykdymo dokumentai yra netinkamai įforminti, pateikti ne visi Pirkimo sutarties vykdymo išlaidas pagrindžiantys dokumentai, dokumentuose pateikta informacija apie [*suteiktas paslaugas*] [*pristatytas prekes*] yra neteisinga, [*suteiktos paslaugos*] [*pristatytos prekės*] neatitinka Pirkimo sutarties sąlygų ar esant kitiems neatitikimams Tiekėjas turi ne vėliau kaip per 5 (penkias) darbo dienas nuo tokio sprendimo priėmimo dienos, raštu informuoti apie tai Subtiekėją, nurodydamas trūkumus ir nustatydamas protingą terminą trūkumams pašalinti.

1.10. Per Tiekėjo nustatytą terminą Subtiekėjui pašalinus trūkumus, Tiekėjas nustatyta tvarka pakartotinai patikrina dokumentus ir pateikia pasirašytus ir patvirtintus dokumentus Pirkėjui.

1.11. Pirkėjas ne vėliau kaip per [*nurodyti terminą ne trumpesnį kaip 5 darbo dienos*] nuo Pirkimo sutarties vykdymo dokumentų gavimo dienos, patikrina pateiktus dokumentus ir, jeigu pateikti dokumentai yra tinkamai įforminti, dokumentuose pateikta informacija apie [*suteiktas paslaugas*] [*pristatytas prekes*] yra teisinga, [*suteiktos paslaugos*] [*pristatytos prekės*] atitinka Pirkimo sutarties sąlygas, pasirašo Trišalės atsiskaitymo sutarties perdavimo-priėmimo aktą ir kitus dokumentus, jei taikoma, bei pateikia pasirašytus dokumentus (po 1 (vieną) egzempliorių) Tiekėjui ir Subtiekėjui.

1.12. Jeigu Pirkėjas nustato, kad Tiekėjo pateikti dokumentai yra netinkamai įforminti arba pateikti ne visi Pirkimo sutarties vykdymo išlaidas pagrindžiantys dokumentai arba dokumentuose pateikta informacija apie [*suteiktas paslaugas*] [*pristatytas prekes*] yra neteisinga, [*suteiktos paslaugos*] [*pristatytos prekės*] neatitinka Pirkimo sutarties sąlygų ar esant kitiems neatitikimams, ne vėliau kaip per 5 (penkias) darbo dienas nuo tokio sprendimo priėmimo dienos, raštu informuoja Tiekėją, nurodydamas trūkumus ir nustatydamas protingą terminą trūkumams pašalinti.

1.13. Per Pirkėjo nustatytą terminą Tiekėjui pašalinus trūkumus ir pakoregavus dokumentus, Pirkėjas ne vėliau kaip per 3 (tris) darbo dienas nuo visų tinkamai įformintų dokumentų gavimo dienos, pasirašo Trišalės atsiskaitymo sutarties perdavimo-priėmimo aktą ir kitus dokumentus, jei taikoma, ir pateikia pasirašytus dokumentus Tiekėjui ir Subtiekėjui.

1.14. Subtiekėjas tik gavęs be išlygų visų Šalių suderintą ir pasirašytą Trišalės atsiskaitymo sutarties perdavimo-priėmimo aktą, suformuoja elektroninę sąskaitą-faktūrą/PVM sąskaitą-faktūrą (toliau – Elektroninė sąskaita) ir per sąskaitų administravimo bendrąją informacinę sistemą SABIS adresu https://sabis.nbfc.lt/ pateikia ją Pirkėjui.

1.15. Jei Subtiekėjas pateikia sąskaitą kitomis priemonėmis, Pirkėjas turi teisę tokios sąskaitos neapmokėti.

1.16. Pirkėjas ne vėliau kaip per [*nurodyti terminą, kuris turi būti ne ilgesnis, už Pirkimo sutartyje nurodytą atsiskaitymo terminą*] nuo Elektroninės sąskaitos gavimo dienos, patikrina Elektroninę sąskaitą ir, jeigu pateikta Elektroninė sąskaita yra tinkamai įforminta perveda lėšas į Subtiekėjo nurodytą banko sąskaitą.

1.17. Ne vėliau kaip per 5 (penkias) darbo dienas po kiekvieno kalendorinio mėnesio pabaigos Pirkėjas raštu teikia informaciją Tiekėjui apie per ataskaitinį mėnesį atliktus mokėjimus Subtiekėjui..

2. straipsnis. Pakeitimo ir nutraukimo sąlygos

2.1. Visi Trišalės sutarties pakeitimai galioja tik tada, kai jie sudaryti raštu ir pasirašyti Šalių įgaliotų atstovų. Tokie Trišalės sutarties pakeitimai yra neatskiriama Trišalės sutarties dalis.

2.2. Sutarties sąlygų keitimą gali inicijuoti kiekviena Sutarties Šalis, pateikdama kitai Šaliai atitinkamą prašymą bei jį pagrindžiančius dokumentus. Šalis, gavusi tokį prašymą, privalo jį išnagrinėti per 10 (dešimt) darbo dienų ir kitai Šaliai pateikti motyvuotą raštišką atsakymą. Šalių nesutarimo atveju sprendimo teisė priklauso Pirkėjui.

2.3. Trišalė sutartis keičiama šiais atvejais:

2.3.1. kai keičiamos Pirkimo sutarties sąlygos, turinčios įtakos Trišalės sutarties įgyvendinimui;

2.3.2. kai keičiamos Subtiekimo sutarties sąlygos, turinčios įtakos Trišalės sutarties įgyvendinimui;

2.3.3. kitais atvejais.

2.4. Trišalė sutartis gali būti nutraukiama raštišku visų Šalių susitarimu šiais atvejais:

2.4.1. kai atsisakoma tiesioginio atsiskaitymo būdo;

2.4.2. kai nutraukiama Subtiekimo sutartis;

2.4.3. kai nutraukiama Pirkimo sutartis.

3. straipsnis. Šalių atsakomybė

3.1. Šalių atsakomybė yra nustatoma pagal galiojančius Lietuvos Respublikos teisės aktus, šią Trišalę sutartį ir kitus su šios sutarties vykdymu susijusius dokumentus. Šalys įsipareigoja tinkamai vykdyti savo įsipareigojimus, prisiimtus šia sutartimi, ir susilaikyti nuo bet kokių veiksmų, kuriais galėtų padaryti žalos viena kitai ar apsunkintų kitos Šalies prisiimtų įsipareigojimų įvykdymą.

3.2. Tiekėjas atsako Pirkėjui už Subtiekėjo prievolių neįvykdymą ar netinkamą įvykdymą, o Subtiekėjui – už Pirkėjo prievolių neįvykdymą ar netinkamą įvykdymą.

3.3. Pirkėjas ir Subtiekėjas neturi teisės reikšti vienas kitam piniginių reikalavimų, susijusių su sutarčių, kiekvieno iš jų sudarytų su Tiekėju, pažeidimu.

4. Straipsnis. Baigiamosios nuostatos

4.1. Nė viena Šalis neturi teisės perleisti visų arba dalies teisių ir pareigų pagal šią Trišalę sutartį.

4.2. Bet kokios nuostatos negaliojimas ar prieštaravimas Lietuvos Respublikos įstatymams ar kitiems norminiams teisės aktams šioje Sutartyje neatleidžia Šalių nuo prisiimtų įsipareigojimų vykdymo, taip pat neturi įtakos kitų Sutarties nuostatų galiojimui. Šiuo atveju tokia nuostata turi būti pakeista atitinkančia teisės aktų reikalavimus kiek įmanoma artimesne Trišalės sutarties tikslui bei kitoms jos nuostatoms.

4.3. Trišalės sutarties Šalys susirašinėja lietuvių kalba. Visi pranešimai, sutikimai ir kitas susižinojimas, kuriuos Šalis gali pateikti pagal šią sutartį, bus laikomi galiojančiais ir įteiktais tinkamai, jeigu yra asmeniškai pateikti kitai Šaliai arba išsiųsti registruotu ar elektroniniu paštu preambulėje nurodytais adresais, kitais adresais, kuriuos nurodė viena Šalis, pateikdama pranešimą.

4.4. Sutarties įsigaliojimo data laikoma sutarties pasirašymo diena, jei Šalys pasirašo skirtingu metu, Sutarties įsigaliojimo data laikoma paskutiniosios Šalies parašo data.

4.5. Susitarimas pasirašomas Šalių kvalifikuotais elektroniniais parašais.

4.6. Šiuo Šalys patvirtina, kad Sutartį perskaitė, suprato jos turinį ir pasekmes, priėmė ją kaip atitinkančią jų tikslus.

Tiekėjo atstovas		**Subtiekėjo atstovas**		**Pirkėjo atstovas**	
Vardas, Pavardė:		Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:		Pareigos:	
Parašas:		Parašas:		Parašas:	
Data:		Data:		Data:	

T33238

1 priedas

TRIŠALĖS ATSISKAITYMO SUTARTIES PERDAVIMO - PRIĖMIMO AKTO FORMA

PERDAVIMO - PRIĖMIMO AKTAS NR. ----------

(data)

Pirkimo sutarties Nr.:	
Pirkimo sutarties pavadinimas:	
Pirkimo sutarties pasirašymo data:	
Trišalės sutarties Nr.:	
Trišalės sutarties pasirašymo data:	
Tiekėjas:	
Subtiekėjas:	
Pirkėjas:	

Visos [*tiekiamos prekės*] [*suteiktos paslaugos*] nurodytos [*prekių*] [*paslaugų*] sąraše, buvo [*pristatytos*] [*suteiktos*], pateikti visi reikalingi dokumentai (sertifikatai, naudojimo ir priežiūros instrukcijos ir panašiai).

Pirkėjas [*pristatytas prekes*] [*suteiktas paslaugas*] priėmė ir patvirtina, kad [*pristatytos prekės*] [*suteiktos paslaugos*] atitinka sutarties sąlygas.

[Prekių] [Paslaugų] sąrašas:

								Valiuta:	**Eur**
Eil. Nr.	**[*Užsakymo data*]**	**[*Pristatymo*] [*Suteikimo*] data**	**Vietos adresas**	**[*Garantinis terminas*]**	**[Prekės] [Paslaugos] pavadinimas (įvardinant tikslius gamintojų ir modelių pavadinimus)**	**Mato vnt.**	**Kiekis**	**Vieneto kaina be PVM**	**Suma be PVM**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10=8×9**
								Iš viso be PVM:	
								PVM [*tarifas*]*:	
								Iš viso su PVM:	

Šis aktas neatleidžia Tiekėjo bei Pirkėjo nuo likusių jų sutartinių įsipareigojimų pagal nurodytą Pirkimo sutartį vykdymo.

Perdavė Subtiekėjo atstovas		**Patvirtino Tiekėjo atstovas**		**Priėmė Pirkėjo atstovas**	
Vardas, Pavardė:		Vardas, Pavardė:		Vardas, Pavardė:	
Pareigos:		Pareigos:		Pareigos:	
Parašas:		Parašas:		Parašas:	
Data:		Data:		Data:	

A.V. A.V.

** - tais atvejais, kai pagal galiojančius teisės aktus tiekėjui nereikia mokėti PVM, atitinkamos skiltys nepildomos ir nurodomos priežastis, dėl kurių tiekėjas PVM nemoka.*

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	VĮ Ignalinos atominė elektrinė (102 / 103) 255450080, Elektrinės g.4, K 47, Drūkšinių k., 31152 Visagino sav., Lietuvos Respublika UAB Spectra Baltic 304635904, Baltų pr. 145, LT-47125 Kaunas
Dokumento pavadinimas (antraštė)	Patekimo kontrolės sistemos viešojo pirkimo-pardavimo sutartis
Dokumento registracijos data ir numeris	2025-09-03 Nr. PSt-271(13.66E)/2025
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	2025-09-01 14:26:55 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-09-01 14:27:15 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	SK ID Solutions EID-Q 2021E, SK ID Solutions AS EE
Sertifikato galiojimo laikas	2024-10-31 13:54:50 – 2029-10-31 23:59:59
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	
Sertifikatas išduotas	
Parašo sukūrimo data ir laikas	2025-09-02 17:19:47 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2025-09-02 17:20:43 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2023-03-15 10:50:39 – 2028-03-13 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Ignalinos atominė elektrinė, VĮ, į.k. 255450080 LT", sertifikatas galioja nuo 2024-12-18 09:12:37 iki 2027-12-18 09:12:37
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.79.2
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2025-09-03 07:58:10)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2025-09-03 07:58:11 Dokumentų valdymo sistema Avilys