

R-CARD M5

Driftsätta

Manualen beskriver systeminställningar samt programmering av passersystem och MEGA integrerat larmsystem, inkl. offline-enheter, porttelefoni, hisstyrning m.m.

[Klikk for norsk versjon!](#)



[Suomeksi, paina tästä!](#)



Innehåll

Allmänt om R-CARD M5, R-CARD 5000 och R-CARD M5 MEGA	6
Om driftsättningsmanualen	8
Förutsättningar	9
Komma igång	9
Installera R-CARD M5 och tillval	9
Logga in	9
Registrera licenser	12
Aktivera stödprogram och tillvalsfunktioner	14
Kontrollera licensregistrering och aktiveringsläge	15
Systeminställningar	15
Gemensamma systeminställningar	15
Ansluta bordsläsare	17
Ange hur användardata visas för operatörerna (globalt)	18
Upprätta kommunikation med enheterna	19
Förutsättningar	19
Skapa domäner	19
Skapa anknytningar	21
Hämta den nya anknytningen	23
Konfigurera systemenheter	27
Uppgradera mjukvara (firmware) i systemenheter	27
Minneskonfigurera undercentraler	29
Konfigurera undercentralens bussar för nätverksmodulen IP-50	36
Överföra data till enheterna	45
Inställningar i undercentralen	46
Konfigurera dörrmiljöer	49
Konfigurera ingångar och utgångar	51
Visa och aktivera funktioner	54
Allmänt	54
Aktivera funktioner	56
Ta reda på vilka funktioner som används i anläggningen	58

Styra integrerat larm (R-CARD M5 MEGA)	60
Konfigurera larmöverföringsinterface	61
Konfigurera larmsystem med grundinställningar	64
Ingångstyper och utgångstyper – hur hänger de ihop?	66
Konfigurera larmmottagare (kanaler)	67
Konfigurera larmområden	70
Konfigurera larmkaraktärer	83
Konfigurera indikeringar (ljudkaraktärer)	83
Konfigurera ingångstyper	83
Konfigurera utgångstyper	84
Konfigurera enheter anslutna till delningsbox	84
Konfigurera manöverpaneler	87
Konfigurera nödöppning/nödlåsning	88
Konfigurera in- och utpasseringsvägar	89
Anpassa behörighetsnivåer för manöverpaneler	91
Definiera åtkomst till larmsystemets manöverpaneler	92
Planritningar och grafik i R-CONTROL och MapR Touch	95
Testa detektorer i larmsystemet	97
Styra externt larm med larmområde	99
Bra att veta	99
I stora drag	100
Konfigurera undercentralens minne för larmområden	101
Konfigurera ett larmområde	103
Välja in och konfigurera larmområdets kortläsare och ev. larmområden	107
Konfigurera återkopplingsingång för centralapparatens status	109
Konfigurera larmstyrningsutgång	110
Tilldela behörighet att styra larmet	110
Konfigurera porttelefonssystem	111
Översikt och förutsättningar	111

Konfigurera linjekort TEL-50	112
Konfigurera porttelefoner	114
Konfigurera portregister	117
Definiera åtkomst till porttelefoner	118
Lägga in telefonkort	120
Styra hissar	122
Installera hissläsare och in/utenheter	122
Konfigurera undercentral för hisstyrning	123
Knyta våningar till utgångar på IO-50	125
Konfigurera dörrfunktioner till hissläsare och våningsplan	126
Behörighet i hissar	127
Verifiera hissarnas funktion i systemet	128
Tidsscheman: Ange när behörigheter och funktioner ska gälla	129
Begrepp	129
Så här fungerar ett tidsschema	132
Lägga upp ett tidsschema från början	133
Verifiera passersystemets funktion	136
Skapa en behörighetsgrupp	136
Lägga in en användare eller lägenhet med ett passerkort	136
Kontrollera att kortet öppnar dörren	137
Felsökning	138
Allmänt bästa rådet	138
Funktionalitet inte tillgänglig; menyer saknas eller ser annorlunda ut	138
Nyss skapade objekt saknas i ett annat fönster	139
Försvunna användare/lägenheter	140
Kortläsare eller manöverpaneler fungerar inte som programmerat	140
Anpassa händelsetyper	141
Dokumentera och säkerhetskopiera systemet	144
BILAGA 1: Enhetsadresser och adresstyper	145

BILAGA 2: Identifiering av enheter (enhetsbeteckningar)	148
BILAGA 3: Importera data till systemet	150
BILAGA 4: Konfigurera Mifare-kortläsningen	152
BILAGA 5: Dynamisk korthantering	154
BILAGA 6: Kundinloggning / portalinloggning	156
BILAGA 7: Programväxlar	157
BILAGA 8: Några viktiga inställningar i larmsystemet	158
BILAGA 9: Larm- och miljöklassificering	159

Allmänt om R-CARD M5, R-CARD 5000 och R-CARD M5 MEGA

Ett passersystem från RCO Security består av:

- **R-CARD M5:** Mjukvaran som används för administration, datalagring och kommunikation. Programmet kan även hantera porttelefoner samt bokningstavlor. Mjukvaran består av:
 - R-CARD M5 Server (Windows-tjänsten RaServer): Sköter kommunikation med arbetsstationer, databasserver och passersystemet. Installeras automatiskt som en Windows-tjänst i den dator som sköter kommunikationen med passersystemet. Startas automatiskt när datorn startas.
 - R-CARD M5 Arbetsstation (**RaClient.exe**) (kallas även *klient*): Används av operatörer för att administrera systemet. I ett nätverkssystem installeras R-CARD M5 Klient även i serverdatorn så att man kan arbeta med systemet vid ett eventuellt nätverksbortfall.

Man kan även installera systemet i nätverk med önskat antal klienter. R-CARD M5 tillåter obegränsat antal arbetsstationer (begränsas eventuellt av operativsystem och nätverk). Med *fleranvändarlicens* kan flera operatörer logga in samtidigt, annars bara en åt gången.

- En Microsoft SQL Server-databas.
 - Olika stödprogram och tillvalsfunktioner.
 - Programmets onlinehjälp och övrig dokumentation.
 - **R-CARD 5000:** Hårdvaran, som i sin tur består av:
 - Undercentraler (UC-50): Kommunikerar med dator, dörrmiljöer, bokningstavlor etc. samt med varandra.
- Undercentralerna lagrar händelser i sitt batteriuppsbackade internminne tills kontakt med serverdatorn återfås efter ett ström- eller kommunikationsavbrott. Inga händelser går alltså förlorade. (Undantag: Om kommunikationsavbrottet varar så länge att internminnet blir fullt, så skrivs de äldsta händelserna över när nya registreras.)

- Kortläsare: Finns för beröringsfri avläsning av kort¹ med olika teknologier.
- Eventuella bokningstavlor, porttelefonsystem m.m.

Passersystemet är oberoende av datorerna för den dagliga funktionen. Undercentralerna har egen klocka och kalender samt all information som behövs för att kontrollera dörrarna.

För montering, anslutning och specifikationer se manualen *R-CARD 5000 – Installera*.

Från passersystemet kan ett separat (externt) inbrottslarm styras via kortläsare.

Önskas ett *integrerat larmsystem* krävs även följande:

- Tilläggslicens för programvarianten **R-CARD M5 MEGA**.
- DIO-5084.
- Manöverpaneler. (Även manöverpaneler tillhör hårdvaruplattformen **R-CARD 5000**.)

Då kan man även styra anpassade ingångs- och utgångstyper, nödöppningsfunktion m.m.

¹ Kort (passerkort, bricka, tag) är en generell beteckning som används för olika typer av kodbärare som kan se ut på olika sätt.

Om driftsättningsmanualen

Denna manual beskriver driftsättning av passersystemet, med eller utan externt eller integrerat larm.

Vid tidpunkten för denna skrift är R-CARD M5 i version 5.49.4. De allra flesta av manualens instruktioner gäller dock även tidigare programversioner.

Ytterligare några PDF-manualer:

- *R-CARD M5 – Installera*
- *R-CARD M5 – Använda*
- *R-CARD 5000 – Offline-läsare – Driftsätta* (beskriver driftsättning av alla LockR-modeller samt NoKey offline)
- *RCO Access – Driftsätta*
- *Fastighetsboxar – Driftsätta*
- *R-CARD 5000 – Installera*
- *R-CARD 5000 – LockR Cylinder – Installera*
- *R-CARD 5000 – LockR Cabinet – Installera*
- *R-CARD 5000 – LockR Rotary Switch – Installera*
- *R-CARD 5000 – NoKey Offline – Installera*
- *R-CARD 5000 – NoKey Online – Installera*
- *R-CARD 5000 – NoKey Motor – Installera*

Dessa manualer samt övrig produktdokumentation finns i mappen **Document** på installationsmediet för R-CARD M5. Manualer kan även laddas ner från [RCO:s webbplats](#), under **Mediaarkivet > Manualer** (inloggning krävs).

Tips

Merparten av anvisningarna återfinns i online-hjälpen. I hjälpen finns även utförliga anvisningar för speciallösningar som inte tas upp i denna manual, såsom konfigurering av Electrolux Boka och PAYMENT (tidigare Debitering), R-CARD M5 BOKA, R-CARD M5 NAP (Närvaro och antipassback) samt Besökshantering.

Tryck på **F1** i R-CARD M5 för att öppna programmets online-hjälp.

Dokumentet *Exempelsamling R-CARD 5000 och M5* ger idéer och uppslag för dig som projekterar, planerar eller söker information om tekniska lösningar på tillträdesskydd.

Typiska applikationer och installationer är illustrerade som principiella exempel med förklarande text. Exempelsamlingen kan laddas ner från [RCO:s webbplats](#), under **Mediearkivet > Projektering**.

På [RCO:s webbplats](#), under **Mediearkivet > Projektering > Projektregistrering**, kan du ladda ned projektregistreringsblanketter för många olika enheter.

Förutsättningar

- Programmet R-CARD M5 och eventuella tillval ska vara installerade, registrerade och körklara (se "[Installera R-CARD M5 och tillval](#)" nedan).
- Utrustningen (undercentraler, kortläsare etc.) förutsätts vara på plats, inkopplad och körklar. Se manualen *R-CARD 5000 – Installera*.
- Du som sköter driftsättningen ska ha kännedom om komponenterna i passersystemet R-CARD 5000 och hur man arbetar i Windowsmiljö.
- Du som sköter *driftsättning av det integrerade larmsystemet R-CARD M5 MEGA* ska dessutom vara av RCO Security certifierad tekniker, och logga in som tekniker.
- Du ska logga in i R-CARD M5 med alla rättigheter, t.ex. som operatör "rcard".

Komma igång

Installera R-CARD M5 och tillval

Hur du installerar R-CARD M5 och tillhörande moduler och webbapplikationer beskrivs utförligt i manualen *R-CARD M5 – Installera* samt i onlinehjälp (tryck på **F1**).

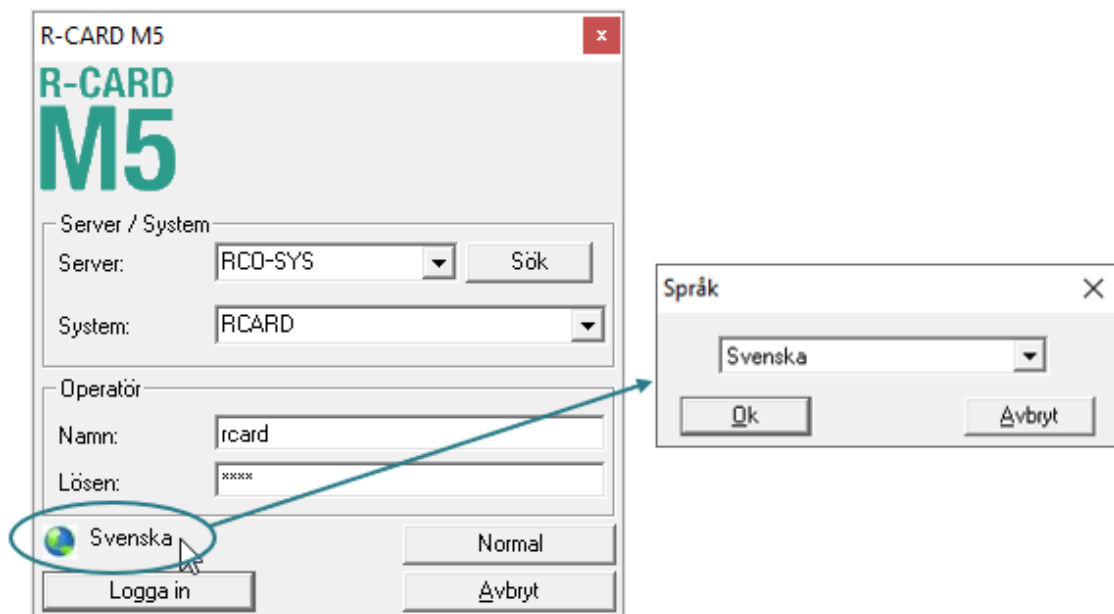
Ett oregistrerat R-CARD M5-program arbetar i demoläge. All kommunikation med passersystemet är stängd. Oregistrerade tillvalsfunktioner fungerar inte alls. Se "[Registrera licenser](#)" på sidan 12.

Logga in

Första inloggning i R-CARD M5

Om DCOM-inställningarna behöver ställas in i R-CARD M5-klienten visas ett meddelande om detta. Klienten kan själv göra dessa inställningar – förutsatt att du loggar in som en operatör med administratörsrättigheter (som *rcard*). Följ instruktionerna som ges av programmet.

1. Klicka på Windows **Start**-knappen och välj **R-CARD M5 > R-CARD M5 Arbetsstation**. Inloggningsdialogrutan visas.
2. Om du kör på en klientinstallation (dvs serverdelen av R-CARD M5 har installerats på en annan dator) måste du ange vilken R-CARD M5 Server som ska användas:
 - a. Första gången du loggar in i systemet måste du ange vilken R-CARD M5 Server som ska användas. Klicka på **Avancerat**. Dialogrutan ändrar utseende:



- b. Skriv in datorns namn eller den IP-adress² där R-CARD M5 Server finns installerad.
 - c. Klicka på **Sök**. Systemnamnet visas.
3. Valfritt: Välj språk genom att klicka på språkikonen (🌐) nere till vänster i inloggningsdialogrutan. Välj språk och klicka på **OK**.
 4. Ange **Namn** och **Lösen** (leveransvärden *rcard* och *1234*) och klicka på **Logga in**.

² Datornamnet föredras. Stödprogram som exempelvis R-CONTROL och AdminBin fungerar inte om IP-adress anges.

Efterföljande inloggningar

1. Klicka på Windows **Start**-knappen och välj **R-CARD M5 > R-CARD M5 Arbetsstation**. Inloggningsdialogrutan visas.
2. Om programmet hanterar flera system, välj vilket av systemen du ska logga in i.
3. Ange **Namn** och **Lösen** (leveransvärden *rcard* och *1234*) och klicka på **Logga in**.



Av säkerhetsskäl ska namn och lösenordet för denna operatör bytas när systemet tas i bruk. Operatören *rcard* och hur man byter lösenord beskrivs utförligt i onlinehjälp (tryck på **F1**).

4. Om du enl. din operatörsprofil är certifierad tekniker (**Tekniker** är markerad) visas ytterligare en dialogruta.
 - a. Välj certifikat.
 - b. Ange ditt tekniker-lösenord.
 - c. Klicka på **Bekräfta**.

Nu har du tillgång till funktioner i det integrerade larmsystemet, möjligen begränsat av den säkerhetsgrupp du tillhör.

Om du klickar på **Avbryt** kommer inloggningen att fullföljas utan rättigheter som certifierad tekniker.

Registrera licenser

Efter installationen registrerar du licenser för R-CARD M5 med det medföljande registreringsprogrammet i den dator där R-CARD M5 Server är installerad. (Registrering via e-post är inte möjlig.) Även vissa tilläggsmoduler kräver registrering.

 Registrera antingen kundlicenser eller teknikerlicens. Om teknikerlicens används, lägg inte in kundlicensen samtidigt. Kundlicensen har högre prioritet.

Vad är en teknikerlicens?

Teknikerlicens för R-CARD M5 innebär följande:

- R-CARD M5 Server är igång och kommunicerar med anläggningen i 4-timmarsintervall. Därefter avslutas serverprogrammet. Det krävs att du startar om och på nytt loggar in i R-CARD M5 Arbetsstation för att få ett nytt 4-timmarspass.

Förvarningsmeddelanden (som måste kvitteras) ges på arbetsstationen med allt kortare intervall ju närmare avstängningstidpunkten man kommer.
- Alla stödprogram och tillvalsfunktioner är aktiverade utom:
 - Electrolux PAYMENT.
 - Tillval som kräver R-CARD M5 DBI-licens ("DBI extern"), dvs import från extern datakälla, M5ToM5 och realtidsimport. (Se "[BILAGA 3: Importera data till systemet](#)" på [sidan 150](#) för mer information om detta.)
- Ett *teknikercertifikat* måste vara registrerat i anläggningen för att R-CARD M5 MEGA-funktionerna ska bli tillgängliga.

För att få en teknikerlicens mejlar du till order@rco.se och begär en teknikerlicens. Licensnumret, som kommer som ett vändande mejl, registrerar du på samma sätt som övriga licenser.

Teknikerlicens, teknikercertifikat och teknikerbehörighet är skilda saker

Teknikerlicens beskrivs ovan.

Teknikercertifikat (eller *MEGA-certifikat*) är ett av RCO utfärdat certifikat till tekniker/installatörer som vid prov har visat erforderliga kunskaper om R-CARD M5 MEGA (integrerat larm). Certifikatet måste vara registrerat för att larmfunktionerna ska bli tillgängliga. Registrering av teknikercertifikat beskrivs i manualen *R-CARD M5 – Installera* och i online-hjälpen i R-CARD M5.

Teknikerbehörighet är ett behörighetstillval som ger kortanvändaren generösa rättigheter i systemet *under en viss tid*. Teknikerbehörighet beskrivs på sidan [93](#).

Registrera licenserna enligt instruktionerna i manualen *R-CARD M5 – Installera* eller onlinehjälp i R-CARD M5 (tryck på **F1**).

Man börjar så här:

1. På datorn där R-CARD M5 Server ska köras (den dator som sköter kommunikationen med passersystemet), logga in i Windows som en användare med administratörsrättigheter.
2. Starta programmet R-CARD M5 Registrering. (Välj **Start > R-CARD M5 > R-CARD M5 Registrering**.)
3. Om en varningsruta från Microsoft Windows visas, klicka på **Ja**.

Aktivera stödprogram och tillvalsfunktioner

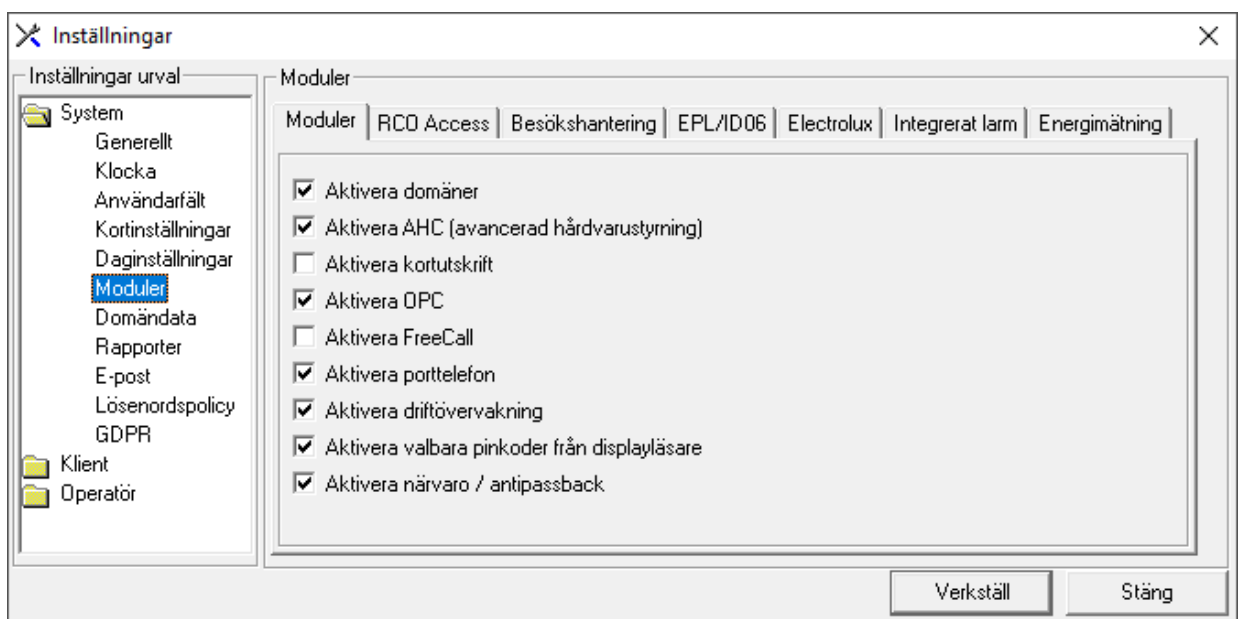
Flertalet R-CARD M5 stödprogram och tillvalsfunktioner behöver *aktiveras* för att kunna användas.



Licensbelagda funktioner visas inte för aktivering förrän aktuell licens är registrerad.

Gör så här:

1. Välj **Inställningar > Inställningar**.
2. Klicka på mappen **System** och välj **Moduler**.



3. Markera de stödprogram och tillvalsfunktioner som ska användas i anläggningen.



Tips: Tryck på **F1** så visas en förteckning över dessa program, med länkar till ytterligare information och instruktioner.

4. Klicka på **Verkställ** och **Stäng**.

Kontrollera licensregistrering och aktiveringsläge

1. Efter inloggning, välj **Hjälp > Om R-CARD M5**.
2. På fliken **Moduler** visas status för registrering av moduler och aktiveringsläge.

Systeminställningar

! **Viktigt:** Gå igenom systeminställningarna först av allt. Vissa inställningar måste göras innan övriga data läggs in i systemet.

Gemensamma systeminställningar

Följande inställningar påverkar alla datorer i systemet. I ett distribuerat system görs dessa inställningar på den dator där R-CARD M5 Server är installerad.

1. I R-CARD M5, välj **Inställningar > Inställningar**.
2. Klicka på mappen **System** och välj **Generellt**.

3. Systeminställningarna är uppdelade i följande inmatningsformulär. Tryck på **F1** på respektive inmatningsformulär för en utförlig beskrivning av alternativen.
 - **Generellt:** Ange systemets benämning och portar (krävs).
 - **Klocka:** Ställa in datum och tid.

- **Användarfält:** Ange vilka användar- eller lägenhetsdata och kortdata som ska behandlas i systemet. Att tänka på:
 - Ska man kunna se status på och öppna dörrar i passersystemet via mobilapplikationen RCO Access eller andra integrationer gäller särskilda krav. Se respektive driftsättningsmanualer.
 - Ska slutanvändare kunna öppna fastighetsboxar med sitt kort gäller ytterligare krav.
 - Det finns även möjlighet att även ange avvikande namn på fälten.
 - R-CARD M5 Server (Windows-tjänsten RaServer) *måste startas om för att dessa ändringar ska gälla.*
 - **Kortinställningar:** Ange hur kort (brickor/taggar) och pinkoder ska användas i systemet. Bland annat kan följande funktioner aktiveras:
 - Länkade kort.
 - Korttyper med långt kort-ID.
 - Dynamisk korthantering. (Se "[BILAGA 5: Dynamisk korthantering](#)" på [sidan 154.](#))
 - Pinkodspolicy, t.ex. minsta längd och minsta antal unika siffror, bytesintervall etc.
 - **Daginställningar:** Definiera specialdagtyper till årskalendern.
 - **Moduler:** Aktivera stödprogram och tillvalsfunktioner. (Se sidan 14.)
 - **Domändata:** Här kan du döpa om domäner samt konfigurera bokningsräknare för användning i anläggningar med integrerad Electrolux Boka.
 - **Rapporter:** Ange hur rapporter ska se ut.
 - **E-post:** Ange systemets e-postkonto.
 - **Lösenordspolicy:** Ange hur operatörers lösenord ska hanteras.
 - **GDPR:** Ange hur personuppgifter ska hanteras. Detta för att uppfylla kraven i dataskyddsförordningen (GDPR) 2018.
4. Klicka på **Verkställ**.

Ansluta bordsläsare

För enkel inläsning av kortnummer (serienummer, kort-ID) från kodbärare (kort, taggar, brickor) kan du använda en av nedanstående bordsläsare i R-CARD M5:

- USB-ansluten RK1 radioknapp (bordsläsare som läser radioknappar; heter PS01 hos underleverantören).
- USB-ansluten PROMAG PCR310U (läser *sektorer* på Mifare-kort).
- USB-ansluten PROMAG PCR300M (läser serienummer på Mifare-kort).
- USB-ansluten PROMAG PCR300A (läser serienummer på prox (EM)-kort).
- RCO:s serieportsläsare Reader-20 (MAG-20, DAL-20, PROX-22 - utgått).

Gör så här på klientdatorn:

1. I R-CARD M5, välj **Inställningar > Inställningar**.
2. Klicka på mappen **Klient** och välj **Kortinläsning**.
3. Tryck på **F1** för att öppna online-hjälpen med detaljerade instruktioner.
4. Klicka på **Verkställ** och **Stäng**.

Installation och användning av bordsläsare beskrivs i manualen *R-CARD M5 – Bordsläsare – Installera och Använda*. Manualen finns i mappen **Document** på installationsmediet för R-CARD M5. Manualen kan även laddas ner från [RCOs webbplats](#), under **Mediaarkivet > Manualer** (inloggning krävs).

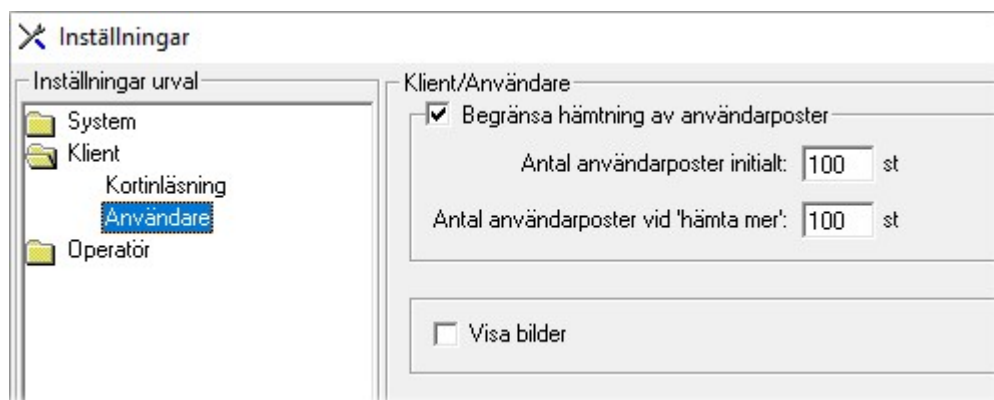
Ange hur användardata visas för operatörerna (globalt)

I ett system med många användare kan det ta lång tid när man byter sorteringsordning, t.ex. från bokstavs- till avdelningsordning. Genom att begränsa antalet poster som hämtas åt gången från databasen snabbas visningen upp.

i **Tips:** Man kan anpassa programmets utseende ytterligare genom att ändra inställningarna under **Operatör**. Visningsalternativ för operatörer beskrivs i onlinehjälp (tryck på **F1**).

Följande görs på varje klientdator som inte ska ha standardinställningarna. Inställningarna är gemensamma för alla operatörer på arbetsstationen.

1. I R-CARD M5, välj **Inställningar > Inställningar**.
2. Klicka på mappen **Klient** och välj **Användare**.



3. Anpassa inställningarna enl. önskemål. Markera **Visa bilder** om bilder på användarna ska visas för operatören.

Tryck på **F1** för att öppna online-hjälp med detaljerade instruktioner.

4. Klicka på **Verkställ** och **Stäng**.

Upprätta kommunikation med enheterna

Förutsättningar

Ett oregistrerat R-CARD M5-program kommunicerar inte med någon undercentral. Registrera en teknikerlicens eller en kundlicens. (Se sidan 12.)

För att kunna göra inställningar och åtgärder som beskrivs i detta kapitel måste man vara inloggad med alla rättigheter. Den fördefinierade operatören rcard, med lösenord 1234, har alla rättigheter.

Skapa domäner

Domäner används för att dela upp ett system i delar som är oberoende av varandra vad gäller årskalender, maximalt antal passerkort etc. Detta är användbart t.ex. i ett system som kontrollerar ett antal skolor med olika årskalendrar eftersom varje domän har sin egen kalender.

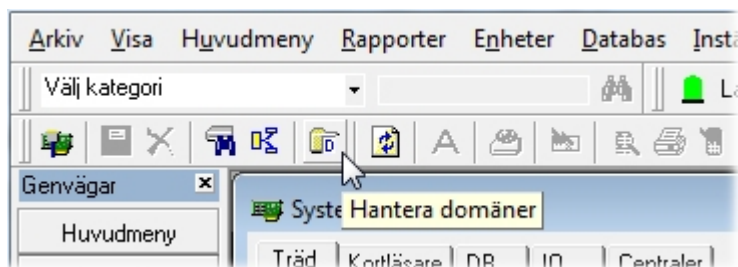
Genom att dela in systemet i domäner behöver man t.ex. inte bestycka alla undercentraler med utökat minne bara därför att några av undercentralerna måste hantera ett stort antal användare. Man skapar då en domän som består av anknytningar med de undercentraler som hanterar det stora antalet användare.

Ett exempel kan vara entrén till en byggnad där flera företag har sina lokaler. Man skapar då dels en domän där bara entrédörrens undercentral ingår, dels en separat domän för varje företag. Eftersom användardata bara sänds ut till domäner där användarna har passagerättigheter blir minneskravet mindre för undercentralerna i respektive företags domän än för undercentralen som styr den gemensamma entrédörren.

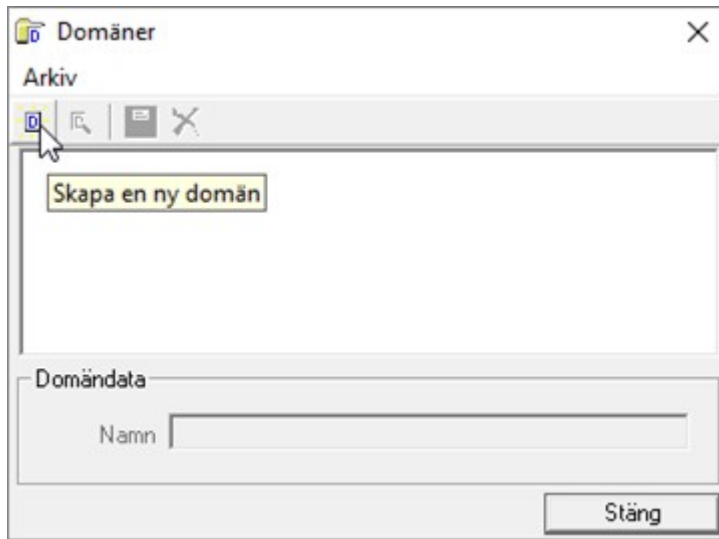
Domäner måste *aktiveras* innan de kan användas. Se sidan 14.

Så här skapar du domäner:

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Klicka på **Hantera domäner** (📁).



3. Dialogrutan **Domäner** visas. Klicka på **Skapa en ny domän** (📁).



4. Rutan för namnet aktiveras. Ge den nya domänen ett beskrivande namn.
5. Klicka på **Spara** (💾).
6. Klicka på **Stäng** för att avsluta.

Skapa anknytningar

En *anknytning* är en kommunikationsförbindelse mellan R-CARD M5 och passersystemet. Minst en anknytning måste skapas i systemet.

Anknytningen etableras med TCP/IP mellan R-CARD M5 Server och *en* undercentral försedd med nätverksmodulen IP-50.

! Om domäner ska användas, skapa dessa innan några anknytningar skapas. Anknytningens domäntillhörighet kan inte ändras när anknytningen väl är skapad. (Domäner kan dock när som helst döpas om.)

En anknytning kan bara höra till en domän.

Så här skapar du en ny anknytning:

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Klicka på **Skapa ny anknytning** (🔧) och välj typ av anknytning (normalt **UC-50 undercentral via TCP/IP**).

Egenskaper	Inställningar
Benämning	Anknytning via IP-modul
Typ	Anknytning via IP-modul
Uppdaterad till och med	
Anknytningsnummer	2
Domän	RCARD
Använd MAC-adressering	☐
IP-adress / DNS	
UDP-port UC-50	1000
UDP-port server	1000
Krypteringsnyckel	12345678
Automatisk händelseinläsning	☒
Fast uppkoppling	☒
Automatisk överföring nytt/ändrat	☒

3. Ange önskade inställningar:
 - **Benämning:** Ge anknytningen ett beskrivande namn. I annat fall får anknytningen ett standardnamn som kan vara förvirrande under driftsättningen.

- **Anknytningsnummer:** Skapas automatiskt i numerisk ordning (1–65 535) och anges normalt inte manuellt.
- **Domän:** Om domäner används, välj domän. (I annat fall visas inte listan.)
- **IP-adress / DNS:** Anknytningens IP-adress behöver inte anges med siffror (t.ex. 192.168.254.12) utan kan anges som ett DNS-namn. DNS-servern behöver inte tilldela IP-modulen samma adress varje gång undercentralen startar om, R-CARD M5 kan hantera dynamiska IP-adresser.

Markera **Erhåll en IP adress automatiskt (DHCP)** för undercentralen (se sidan 41) för att aktivera funktionen. Tänk på att kundens nätverk kan ha brandväggar etc. som ställer krav på adresseringen. Utförlig information ges i manualen *R-CARD M5 – Installera*.

DHCP namnet är UC 50MAC00-05-7c-*nn-nn-nn* där *nn* är unika värden från IP-50-modulens MAC adress på etiketten. Om DHCP- och DNS-servern utbyter information automatisk mellan varandra så fungera detta som DNS-namn.

Kontakta nätverksansvarig och ta reda på det namn som ska användas och skriv in det.

Alternativt kan MAC-adressering användas. Tryck på **F1** för mer information.

- Standardvärden för **UDP-port UC-50** (1000) och **UDP-port server** (1000) behöver vanligtvis inte ändras.
 - **Krypteringsnyckel:** En 80-bitars nyckel som används för att kryptera informationen mellan dator och undercentral. Denna nyckel ger med systemnyckeln en kryptering på totalt 144 bitar (16 tecken) för data. Nyckeln används även för att dator och undercentral ska kunna verifiera varandras äkthet ("authentication"). Nyckeln kan bara ändras om man vet den tidigare nyckeln. Standardinställning 12345678.
 - Övriga inställningar ska normalt vara valda.
4. Klicka på **Spara** (📁).
 5. Hämta anknytningen (se nästa avsnitt).

Hämta den nya anknytningen

Detta är en fortsättning på föregående avsnitt.

Hämtning av en anknytning innebär att etablera kontakt med undercentralerna och deras anslutna enheter.



I en driftsatt anläggning: Gör aldrig hämtning av en anknytning som har kommunikationsproblem! Enheter som inte svarar anses då vara ohämtade enheter och servern slutar att kommunicera med dem. Redan hämtade och programmerade enheter kan förlora sina inställningar. Kontrollera i händelsefönstret att inga kommunikationsproblem finns innan hämtning görs.

Hämtning ska aldrig göras som kommunikationstest. Servern rapporterar automatiskt eventuella kommunikationsfel.

Avbryt inte påbörjad hämtning, utan vänta tills den avslutas. Om du redan har avbrutit en hämtning, starta om Windows-tjänsten RaServer (eller starta om datorn) för att kunna fortsätta arbeta i anläggningen.

Standardinställningar för hämtade enheter

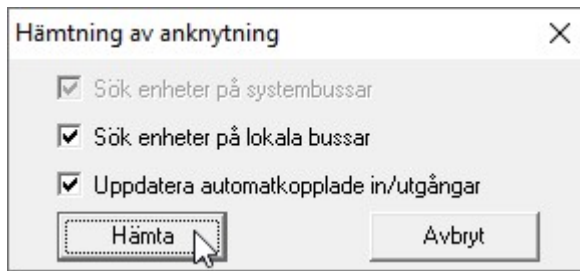
I en ny anläggning får varje enhet som svarar vid hämtning av anknytningen en uppsättning standardinställningar. Enheternas adress, typ etc. avläses automatiskt och läggs in i databasen tillsammans med standardegenskaper för resp. enhetstyp. Kortläsare ställs in för att kräva kort³ + pinkod för passage. Du behöver alltså inte själv skapa nya poster eller lägga in grunddata för enheterna.

Däremot finns inga användardata, kortdata eller behörigheter i systemet från början. Därför måste man efter driftsättningen lägga in minst en behörighetsgrupp och en användare med kort för att kunna verifiera systemets funktion (beskrivs under "[Verifiera passersystemets funktion](#)" på sidan 136).

Så här hämtar du en anknytning

1. Klicka på **Hämta anknytning** (🖨️) och välj den anknytning som ska hämtas.
2. Markera **Sök enheter på lokala bussar** och **Uppdatera automatkopplade in/utgångar**. Detta görs för att alla data för samtliga enheter, även kortläsare och IO-50, ska hämtas och läggas upp i databasen.

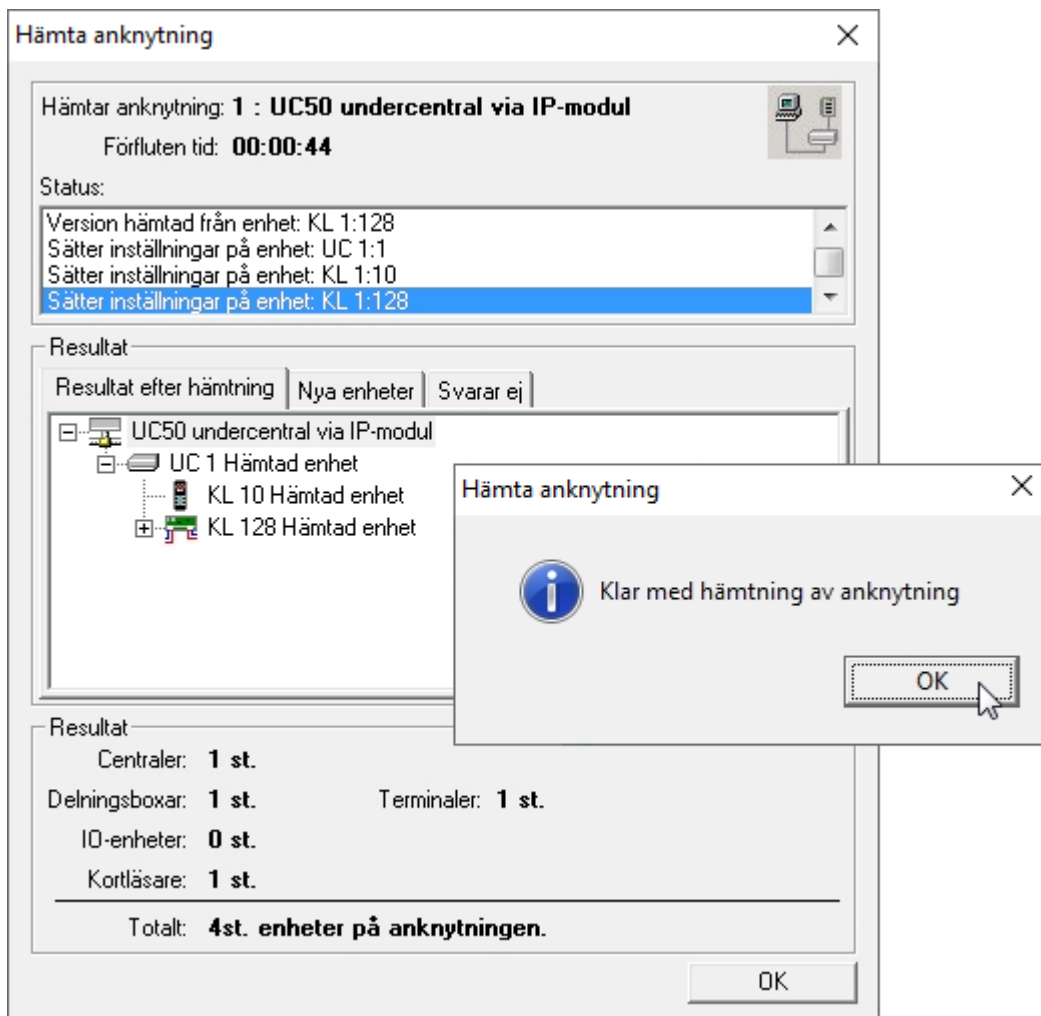
³ Kort (passerkort, bricka, tag) är en generell beteckning som används för olika typer av kodbärare som kan se ut på olika sätt.



3. Klicka på **Hämta**.

Vänta tills hämtningen är avslutad. Det kan ta allt från sekunder till minuter beroende på antalet enheter på anknytningen. Vänta tills meddelandet "Klar med hämtning av anknytning" visas.

I **Status**-rutan visas löpande vad som sker.

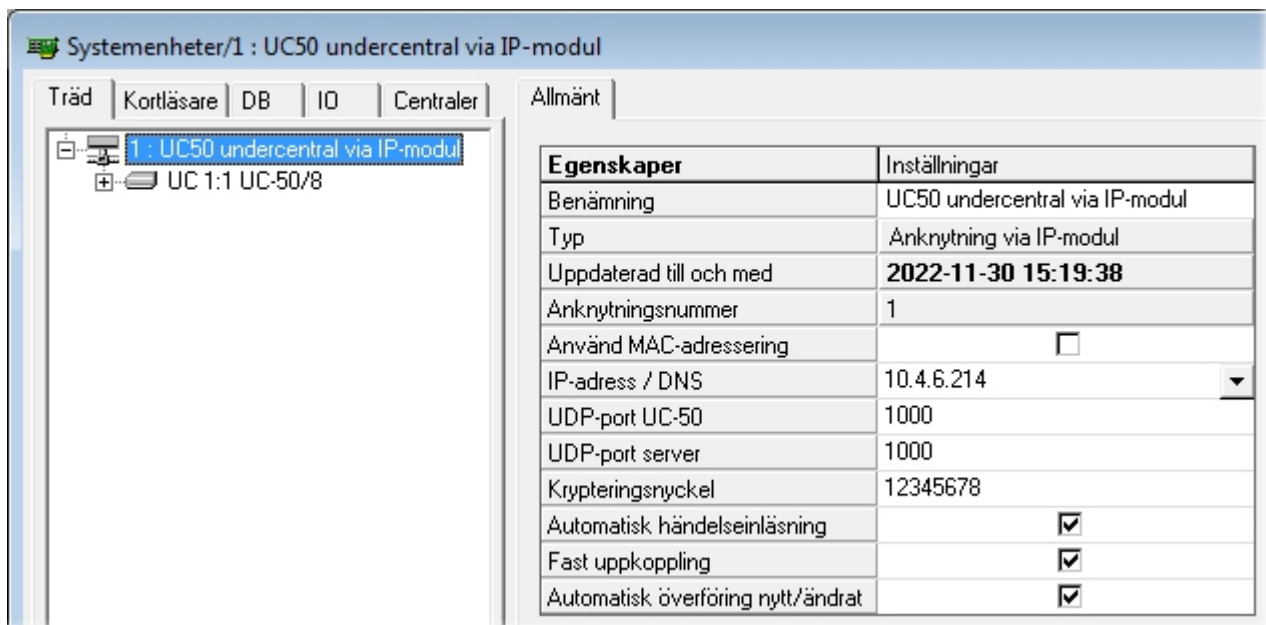


Under **Resultat** finns tre flikar:

- **Resultat efter hämtning:** Redovisar samtliga enheter. Enheter som fanns före hämtningen men nu inte svarar markeras med ett gult utropstecken i listan. Dessa enheter redovisas även på fliken **Svarar ej**.
- **Nya enheter:** Redovisar enheter som tillkommit.
- **Svarar ej:** Redovisar enheter som tidigare har kommunicerat men nu inte svarar på anrop. En sådan situation kan uppstå om man har installerat ytterligare enheter på en befintlig lokalbuss och installationen är felaktig så att lokala bussen inte fungerar. Gäller även lokalbuss via TCP/IP. En ny hämtning måste göras efter att kommunikationsfelet åtgärdats för att enheterna ska kunna konfigureras och tas i drift.

4. Avsluta med **OK**.

Om du markerar anknytningen i trädet syns anknytningens egenskaper på fliken **Allmänt**. I exemplet nedan visas en IP-anknytning. Andra anknytningstyper har något olika inställningar.



The screenshot shows a software interface for configuring system units. The title bar reads 'Systemenheter/1 : UC50 undercentral via IP-modul'. Below the title bar are tabs: 'Träd', 'Kortläsare', 'DB', 'IO', 'Centraler', and 'Allmänt'. The 'Träd' tab is active, showing a tree structure with '1 : UC50 undercentral via IP-modul' selected. Below this, a sub-entry 'UC 1:1 UC-50/8' is visible. The 'Allmänt' tab is also visible, showing a table of properties and settings.

Egenskaper	Inställningar
Benämning	UC50 undercentral via IP-modul
Typ	Anknytning via IP-modul
Uppdaterad till och med	2022-11-30 15:19:38
Anknytningsnummer	1
Använd MAC-adressering	☐
IP-adress / DNS	10.4.6.214
UDP-port UC-50	1000
UDP-port server	1000
Krypteringsnyckel	12345678
Automatisk händelseinläsning	☒
Fast uppkoppling	☒
Automatisk överföring nytt/ändrat	☒

Felsökning

Kommunikationsfel vid hämtning indikeras med ett gult utropstecken (!). (Om en enhet visas med rött utropstecken (!) i listan under normal drift betyder det kommunikationsavbrott med enheten.)

Hänvisning om "Internt fel 4" efter hämtning av anknytningen kan bero på följande:

- Programmet tror att IP-adressen på anknytning redan finns, vilket i sin tur kan bero på att det finns flera anknytningar med samma IP-adress eller t.ex. att datorns nätverkskort har hängt sig eller är trasigt.
- IP-adressen på anknytningen är ogiltig.

Prova följande:

- Starta om datorn.
- Kontrollera att IP-adressen i anknytningens inställningar är korrekt.
- Starta om Windows-tjänsten RaServer.

Under hämtningen kontrolleras att minneskonfigurationen är lika för alla undercentraler som hör till anknytningen. Om olikheter upptäcks visas ett meddelande:

"Minneskonfigurationen för en eller flera centraler skiljer sig från domänens konfiguration. Konfigurering av anknytningen rekommenderas."

Konfigurera om anknytningens samtliga undercentraler.

Konfigurera systemenheter

Uppgradera mjukvara (firmware) i systemenheter

RCO:s produkter utvecklas kontinuerligt, vilket innebär att nya versioner av firmware lanseras. Nya versioner kan dels innebära att ny funktionalitet implementerats, eller att redan existerande har optimerats. *Därför rekommenderas alltid senaste version av firmware för respektive enhet.*

Det krävs ingen licens eller datumgräns för uppgradering ("flashning") av hårdvara. Ny funktionalitet som uppgraderingen innehåller kan dock kräva uppgradering av R-CARD M5, som i sin tur kräver licens.

Viktigt / Varningar

- **Det får inte förekomma några kommunikationsfel på den anknytning där uppgraderingen ska ske!**
- Vid uppstart kan larmstyrningar m.m. påverkas som vid en normal omstart. I en anläggning med larm bör man ta hänsyn till detta.
- Om det är den första undercentralen på en anknytning som uppgraderas kopplas anknytningen ner under uppgraderingen, och en ny uppkoppling sker.
- Vid forcerad *nedgradering* av undercentralen kan minnet totalraderas (som att lyfta batteriet). Detta inträffar om minnessignaturerna är olika för den nya och den befintliga programvaran.
- När du har startat uppgraderingen, *avvakta slutmeddelandet*. Om sekvensen avbryts finns risk för att serviceläget kan ligga kvar. (Detta avslutas i så fall automatiskt efter 30 minuter.) Normal tidsåtgång för uppgraderingen är upp till 10 minuter.
- Rekommendation: Alla undercentraler i systemet bör ha samma version (helst senast möjliga version). Man bör konfigurera alla undercentraler samtidigt i ett system, inom en domän eller en anknytning.

Tips inför uppgradering

- Särskilda instruktioner finns för uppgradering av offline-läsare. Se programmets hjälpfunktion eller manualen *Offline-läsare – Driftsätta*.
- MapR Touch, R-TOUCH 50 och Electrolux Easy kan även uppgraderas via USB. Steg-för-steg instruktioner i PDF-format ligger ihop uppgraderingsfilerna. (Se steg 1 nedan.)
- Electrolux Vision kan *endast* uppgraderas via USB. Steg-för-steg instruktioner (manualen *Uppgradera Electrolux Vision*) ligger ihop med uppgraderingsfilerna.

Gör så här:

1. Kopiera programfilen (med filnamnstillägg BFF) från installationsmediet för R-CARD M5.

Alternativt, ladda ned den från [RCO:s webbplats](#), **Mediearkivet > Mjukvara > Firmware**. (Inloggning krävs.)

2. I R-CARD M5, välj **Enheter > Uppgradera mjukvara**.

3. Välj **Programfil** (filnamnstillägg BFF).

Filinformation visas.

Enhets typ väljs automatiskt.

4. Tryck nu på **F1** för vidare instruktioner och information.

Minneskonfigurera undercentraler

Översikt

Här bestäms hur undercentralernas minne ska allokeras. Minneskonfigurering görs med:

- Gemensamma grundvärden (i rutan **Domänkonfiguration**) för samtliga undercentraler inom anknytningen/domänen, t.ex. antalet behörighetsgrupper.

Undercentraler från version 2.60 är vid leverans minneskonfigurerade för 20 000 kort och 500 behörigheter. De behöver konfigureras endast om andra värden önskas eller om individuell minneskonfigurering behövs.

Se instruktioner på sidan [30](#).

- Individuella värden (i dialogrutan **Zonägende**) för undercentraler som ska:
 - Kontrollera larmområden
 - Hantera Electrolux Boka
 - Mäta energiförbrukning
 - Kontrollera närvaro/lokal tidsantipassback

Se instruktioner på sidan [33](#).

 Om undercentralen har konfigurerats tidigare kan man hämta dessa värden och se dem i dialogrutan. Högerklicka på undercentralen och välj **Visa info om central**.

Förutsättningar

- Undercentralen måste vara hämtad.
- Kommunikationen med undercentralen måste fungera.
- AHC är aktiverat (leveransläge).

Observera!

- Minneskonfigurering raderar allt minnesinnehåll i undercentralen. Om Electrolux bokningstavlor redan finns i drift i anläggningen, säkerhetskopiera bokningar från alla bokningstavlor i den domän som ska konfigureras för att spara eventuella bokningar. Återställa sedan bokningarna efter konfigurering. För anvisningar se onlinehjälp i R-CARD M5. (Tryck på **F1** när du använder programmet.)
- Värden som anges för **Aktivera korttyper med långt kort-ID** och **Längd på kort-ID** i systemets kortinställningar *påverkar minneskonfigurationen*.

- Efter en minneskonfigurering måste normalt en komplett överföring till de konfigurerade enheterna göras. (Det kan utföras automatiskt. Programmet frågar innan konfigureringen verkställs.) Undantag: När du konfigurerar undercentraler för systembuss via TCP/IP bör överföring i vissa lägen inte göras.
- Om systembuss via IP ska användas: Konfigurera först alla undercentraler som ska anslutas till systembussen för TCP/IP mellan centraler. Tryck på **F1** för att öppna programmets onlinehjälp, där konfigureringen för denna typ av kommunikationsbuss beskrivs.

Gemensamma grundvärden

1. I R-CARD M5, välj **Enheter > Konfigurera enheter**.
2. Dra–släpp domänen eller anknytningen till den tomma rutan.

Ändring av de gemensamma inställningarna i rutan **Domänkonfiguration** påverkar alla undercentraler i domänen. Därför ska hela domänen dras in. Alla undercentraler ska vara markerade.

Om domäner inte används måste istället *alla anknytningar* inkluderas i listan.

Undantagen är vid inkoppling av en ny undercentral på befintlig anknytning eller om individuella värden (se lista ovan) ska konfigureras.

Domänkonfiguration - RCARD

Antal användarkort: 10000 st. Antal kortgrupper: 0 st. Antal offline-dörrgrupper: 10 st.
☒ Behörighetsgrupper: 500 st. Antal informationstexter: 0 st. Antal offline-enheter: 100 st.
☐ Behörighetszoner: 10 st. Läsarbehörigheter på kort: 3 st. ☐ Versionsstyrda läsarbehörigheter
☒ Tidszoner: 10 st.

Markerade centraler kommer att konfigureras:
☒ Markera alla/ingen

Enhet	Larmområden	Närvaroområden	Fria närvaroområden	Förval	Integrerat larm	Centralapparat	Händelser
☒ UC... 5	4	2	0	Ja	Ja	8959	
☒ UC... 4	0	0	0	Nej	Nej	923	
☒ UC... 1	0	0	0	Nej	Nej	17501	

Information om minnet

Namn	Antal valda	Storlek
Användarkort	10000	78
Behörighetsgrupper	500	168
Behörighetszoner		
Tidszoner	10	74
Kortgrupper	0	44
Infotexter	0	50
Händelser	923	12

Verkställ Stäng

3. Anpassa nedanstående inställningar som gäller för alla markerade undercentraler:

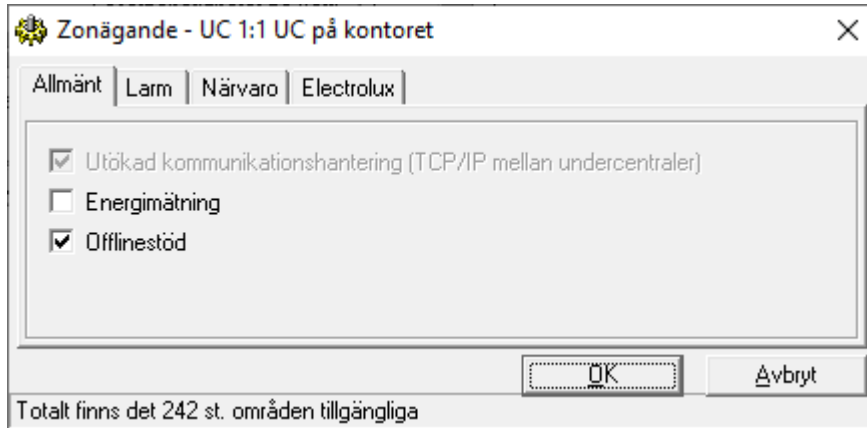
Inställning	Beskrivning
Antal användarkort	Antalet kort i systemet.
Behörighetsgrupper	Antalet behörighetsgrupper.
Behörighetszoner	Max. 255 behörighetszoner per domän.
Tidszoner	Tidszoner (maximalt antal. 199 per domän) behövs om läsarbehörigheter ska ges.
Antal kortgrupper*	Kortgrupper behövs endast vid integration med Electrolux Boka. Beräkna antalet kortgrupper så här: antalet lägenheter/användare (vanligast är en kortgrupp per lägenhet) + några för servicetekniker, städpersonal osv + marginal för framtida ökning <i>Välj 0 om Electrolux inte används.</i>
Antal informationstexter*	Gäller Electrolux Boka. Det handlar om textmeddelanden som anges per kortgrupp. För mer information se programmets hjälpfunktion. <i>Välj 0 om Electrolux inte används.</i>
Läsarbehörigheter på kort	Brukar behövas i system med offline-enheter. Max. 3 st. läsarbehörigheter per kort.
Versionsstyrda läsarbehörigheter	Används för att hantera in- och utflyttning från lägenheter med offline-läsare. Observera att detta val inte kan <i>avaktiveras</i>. Har man en gång aktiverat den i en domän eller anknytning så kan det inte ångras.

Inställning	Beskrivning
Antal offline dörrgrupper	<i>Dörrgrupper</i> används till att gruppera offline-läsare för tilldelning av behörigheter. Påverkar minnesutrymmet på kort. Max. antal dörrgrupper är 255 st.  Rekommendation: Skapa några fler dörrgrupper än vad som krävs för tillfället, så slipper man konfigurera om undercentralerna om behovet skulle öka.  Tips: Om anläggningen består av ett stort antal dörrar där bara en eller ett fåtal personer ska beviljas tillträde (t.ex. privata kontor) rekommenderas att nyttja funktionen Läsarbehörigheter på kort (se ovan) istället för att skapa ett stort antal dörrgrupper.
Antal offline-enheter	Ange hur många offline-läsare som ska kunna skapas för domänen. Max. antal 2047 st. Påverkar minnesutrymmet på kort. För full funktion av offline-system, aktivera offlinestöd på fliken Allmänt i dialogrutan Zonägande (se nedan) på de undercentraler som har initieringsläsare.

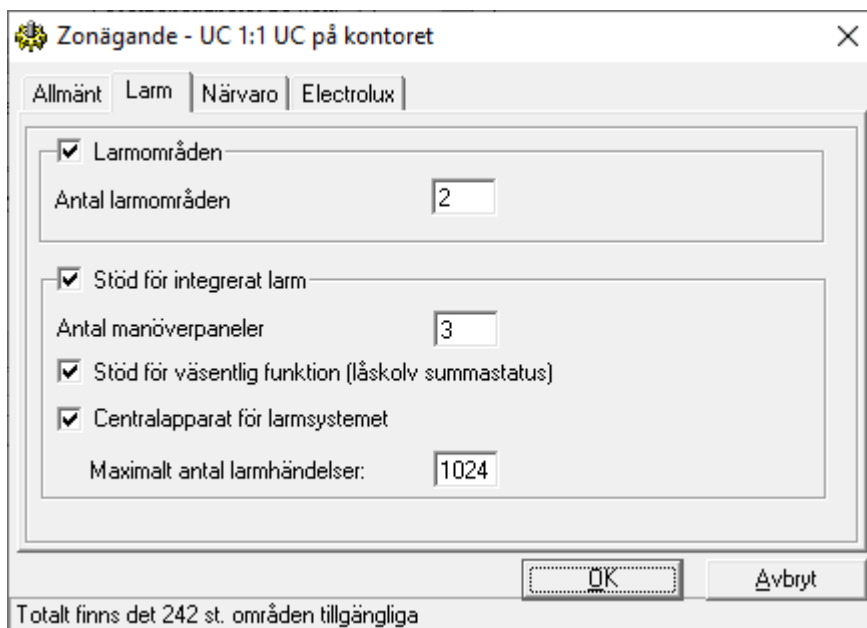
* Dessa värden kommer att påverka minnesallokeringen i samtliga undercentraler på anknytningen/domänen, oavsett om de kontrollerar bokningstavlor eller ej.

Individuella värden

1. Dubbelklicka på en undercentral som ska konfigureras individuellt. Dialogrutan **Zonägande** visas.



2. Ange önskade inställningar på fliken **Allmänt**:
 - **Utökad kommunikationshantering** möjliggör användning av systembuss via IP (beskrivs i programmets onlinehjälp – tryck på **F1**).
 - **Energimätning** möjliggör för centralen att hantera förfrågan mot energimätningsserver.
 - **Offlinestöd** måste markeras på samtliga UC-50 som har kortläsare som ska användas som *initieringsläsare*.
3. På fliken **Larm** finns inställningar för undercentraler som ska kontrollera ett eller flera larmområden:



Inställning	Beskrivning
Antal larmområden	Antal larmområden som ska kontrolleras av undercentralen. Om undercentralen ska "äga" larmområden, gör den med fördel även till centralapparat för larmsystemet (se nedan).
Stöd för integrerat larm	Måste alltid markeras om integrerat larm ska konfigureras. (Om externt larm ska styras ska alternativet inte markeras.)
Antal manöverpaneler	Antalet manöverpaneler anslutna till just denna undercentral.  Tips: Om MapR Touch eller R-TOUCH 50 ska anslutas mot denna undercentral med lokalbuss via TCP/IP, passa på att markera Utökad kommunikationshantering på fliken Allmänt.
Stöd för väsentlig funktion (låskolv summastatus)	Krävs på samtliga undercentraler som på något sätt kommer att beröras av väsentlig funktion. <i>För utförlig information om väsentlig funktion se programmets hjälpfunktion.</i>
Centralapparat för larmsystemet Maximalt antal larmhändelser	Används om undercentralen ska vara centralapparat och kontrollera larmsystemet. <i>Endast en UC-50 i larmsystemet kan ha denna inställning och vara centralapparat.</i> Den undercentral som "äger" larmområden bör vara centralapparat. TCP/IP-modulen ger utökad minne; dessutom kan trafiken på systembussen hållas ner. Larmloggen lagras i centralapparaten och är gemensam för alla centraler på anknytningen. Ange därför hur många larmhändelser som ska kunna buffras i larmloggen. Rekommenderat värde: 1000. <i>Larmklass 3/4 kräver minst 1000.</i> Undercentralen kan spara maximalt 2040 larmhändelser.  Larmloggen förbrukar minne i undercentralen. Välj inte högre värde än nödvändigt.

4. På fliken **Närvaro** finns inställningar för undercentraler som ska kontrollera närvaroområden. Tryck på **F1** och läs i programmets hjälpfunktion om att minneskonfigurera undercentral för närvaro.
5. På fliken **Electrolux** finns inställningar för undercentraler ska kontrollera en eller fler Electrolux-bokningstavlor och bokningsobjekt. Tryck på **F1** och läs i programmets hjälpfunktion om att minneskonfigurera undercentral för Electrolux Boka.
6. Klicka på **OK** för att spara undercentralens individuella data.

Verkställ minneskonfigureringen

Följden av dina val visas i kolumnerna i det underliggande fönstret.

Nertill finns **Information om minnet** som visar antal valda poster och hur stor minnesdel varje enskild post tar. T.ex. kortens storlek ökar om **Aktivera korttyper med långt kort-ID** markeras i systemets kortinställningar, samt om kortgrupper eller närvaroområden används.

Om en rad visas **rött** räcker undercentralens minne inte till för de valda värdena, som då måste minskas. Obs: Om enheterna har olika mycket minne baseras beräkningarna på den undercentral som har minst minne.

Rosa betyder att undercentralens individuella konfigurationen inte överensstämmer med domänkonfigurationen (dvs de gemensamma inställningarna för alla undercentraler i domänen)

Blått betyder att undercentralen saknar stöd för de tillval som gjorts.

Verkställ minneskonfigureringen:

1. Klicka på **Verkställ**.
2. Svara **Ja** på kontrollfrågan "Är du säker..."
3. Minnesinnehållet kommer att raderas vid konfigureringen. Svara därför **Ja** på följdfrågan "Du måste göra en överföring... Ska detta göras?" Överföringen görs då automatiskt. Om du svarar **Nej** måste överföring göras manuellt. Annars kommer undercentralerna att vara utan data.
4. *Avvakta klarmeddelandet.* Tiden för minneskonfigureringen varierar och påverkas även av ev. återställning av data.

 **Tips:** Är du osäker på om alla undercentraler måste konfigureras? Undrar du vad som händer när du klickar på **Konfigurera** eller vad **Överföring allt** innebär? Information finns i programmets hjälpfunktion!

Konfigurera undercentralens bussar för nätverksmodulen IP-50

Vid leverans är modulen inställd på **Erhåll en IP adress automatiskt (DHCP)**. Får den inget svar från DHCP-servern vid uppstart så genererar den en IP-adress **169.254.254.0**, nätmask 255.255.0.0, gateway 0.0.0.0. Detta görs efter ca. 75–90 sekunder (APIPA).

Nollan i sista adressegmentet ersätts av den inställda fysiska adressen (2–254) på UC-50. En undercentral som har en inställd adress 122 kommer alltså att få IP-adressen 169.254.254.122.

Förutsättningar

- IP-50-modulen ska vara monterad på undercentralen. Instruktioner finns i manualen *R-CARD 5000 – Installera*.
- Undercentralen måste vara hämtad.
- Kommunikationen med undercentralen måste fungera.

Rekommendationer och varningar

- TCP/IP-modulens IP-adress och övriga IP-parametrar lagras i undercentralen. Om man tar bort matningsspänning och batteri i UC-50 försvinner konfigurering. Det kan även ske vid t ex. demontering/byte av IP-50 pga utökat minneskapacitet till undercentralen.
- IP-50-modulens MAC-adress (som är unik och fast inprogrammerad i modulen) följer IP-50-modulen. Att flytta/byta modulen till en annan undercentral kan påverka IP-adresstilldelning om IP-adressen är låst till MAC-adressen i nätverkets DHCP-server. Se "MAC-adressering" i onlinehjälpen.
- **Rekommendation för att undvika problem:** Anslut inte en okonfigurerad undercentral/nätverksmodul till kundens nätverk. Använd t.ex. en bärbar dator om konfigurering ska göras via IP-anslutning. Anslut undercentral/IP-50 till kundens nätverk först när busskonfigureringen är genomförd!
- Busskonfigureringen kan göras via annan dator än den som används i kundsystemet eftersom IP-adressen finns kvar i undercentralen även när man kopplar bort matningsspänningen (förutsatt att undercentralens reservbatteri är OK och sitter på plats).
- Vid konfigurering via en nätverksanknytning: Om TCP/IP-modulen ges en IP-adress som inte ligger inom den konfigurerande datorns adressegment så bryts kommunikation mot den konfigurerade undercentralen. Kommunikationen fungerar igen när undercentralen ansluts till kundens nätverk.

Undercentralen kan sköta tre sorters IP-kommunikation – men bara två samtidigt

- Kommunikation med R-CARD M5 via TCP/IP.
En anknytning görs alltid till serverdatorn via en undercentral. Eventuella ytterligare undercentraler kommunicerar med den första undercentralen via systembussen eller routing.
- Kommunikation med andra undercentraler över systembuss via TCP/IP.
Systembussen kan förlängas genom s.k. routing.
- Kommunikation med MapR Touch eller R-TOUCH 50 över lokalbuss via TCP/IP.



Oavsett konfigurering kan undercentralen endast sköta två av dessa samtidigt. Om man konfigurerar undercentralen för alla tre så fungerar ändå bara de första två som konfigurerades. Inget felmeddelande visas.

Upprätta kommunikation med undercentraler inför busskonfigurering

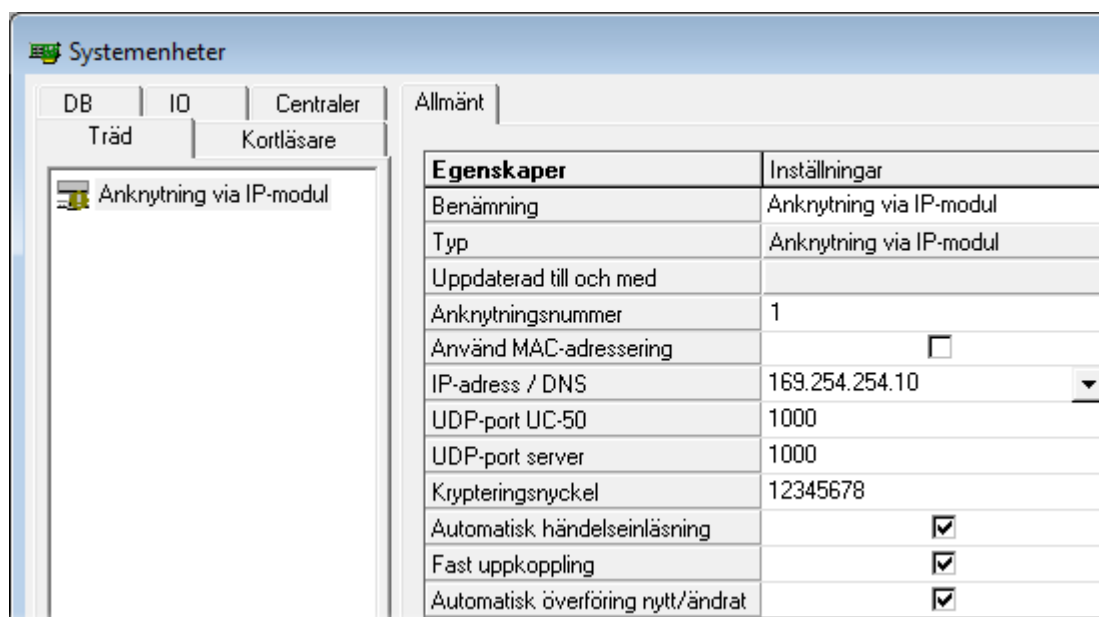
Det finns olika sätt att komma i kontakt med en ny UC-50 där busskonfigurering ska göras. I A) till C) nedan beskrivs olika sätt att få kontakt med en UC-50 så att busskonfigurering kan göras. I samtliga alternativen gäller att UC-50 måste ha fått en enhetsadress tilldelad via DIP-omkopplaren. Busskonfigureringen görs sedan på samma sätt oavsett hur du kommunicerar med undercentralen.

A) Använda nätverkskabel mellan teknikerdatorn och UC-50

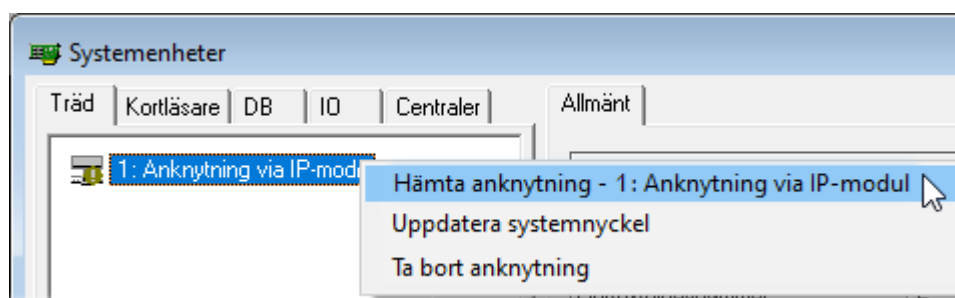
Om UC-50 har en IP-modul, skapa en temporär anknytning på en teknikerdator och anslut via en nätverkskabel direkt mellan datorn och UC-50. Använd standard APIPA-adresser 169.254.254.x.

När du har anslutat kabeln mellan datorn och undercentralen, gör så här:

1. Välj **Enheter > Systemenheter**.
2. På fliken **Träd**, högerklicka på en fri yta och välj **Ny anknytning > UC-50 undercentral via TCP/IP**.
3. Ange undercentralens IP-adress i fältet **IP-adress / DNS**. Här är undercentralen adresserad som enhet 10, standard IP-adress blir då 169.254.254.10:



- Högerklicka på anknytningen och välj **Hämta anknytningen**. Siffran (1 i nedanstående bild) kan vara olika beroende på antalet redan skapade anknytningar i systemet.



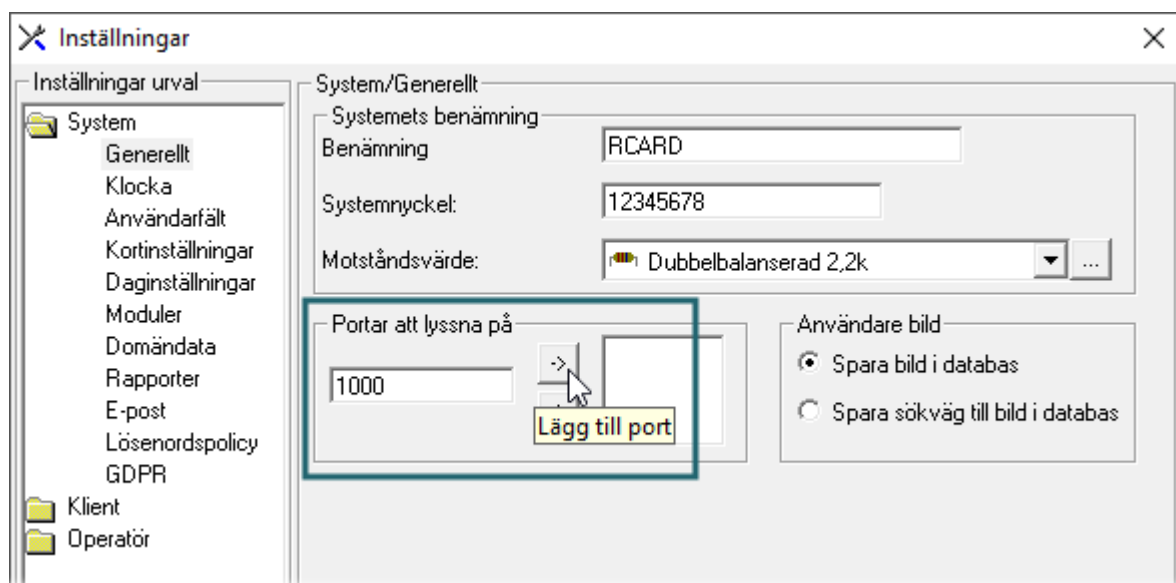
- Fortsätt nu med busskonfigureringen. (Se "[Konfigurera bussar](#)" på sidan 41.)

B) Använda nätverksanslutning med DHCP

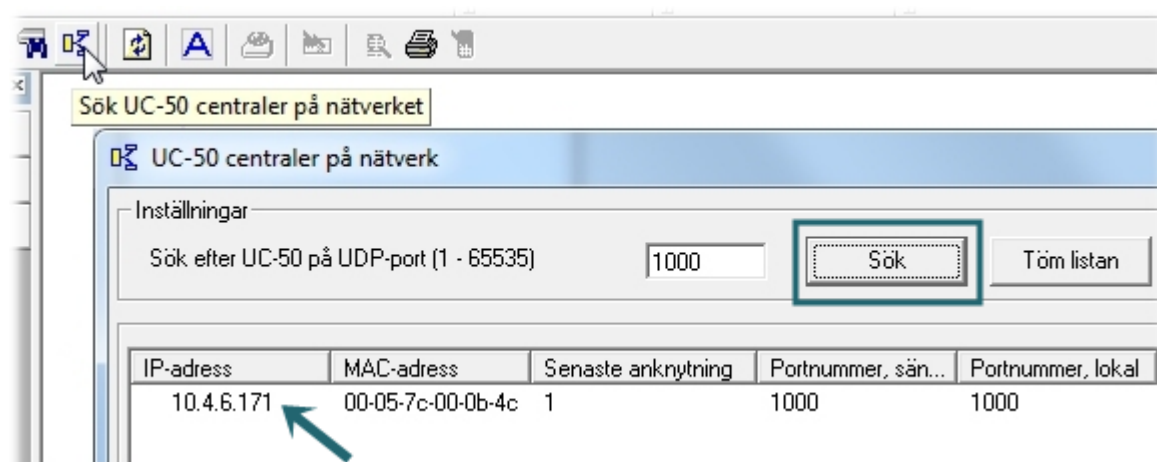
Anslut den nya UC-50 med IP-modul och en teknikerdator till ett nätverk med DHCP, dynamisk tilldelning av IP-adresser. I teknikerdatorn, sätt **Portar att lyssna på** till 1000. Sök sedan UC-50 på nätverket under **Systemenheter**, och skapa en temporär anknytning till IP-adressen som undercentralen har blivit tilldelad.

När du har anslutit undercentralen till ditt lokala nätverk, gör så här:

- Välj **Inställningar > Inställningar**.
- Klicka på mappen **System** och välj **Generellt**.
- I fältet **Portar att lyssna på**, ange port 1000.
- Klicka på **-> (Lägg till port)**.



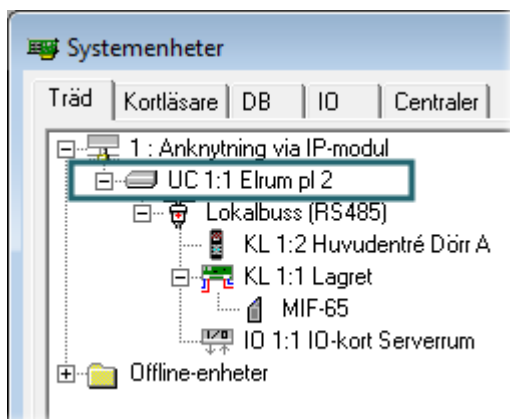
5. Klicka på **Verkställ** och **Stäng**.
6. Välj **Enheter > Systemenheter**.
7. Klicka på **Sök UC-50 centraler på nätverket**.
8. I dialogrutan som visas, klicka på **Sök**.



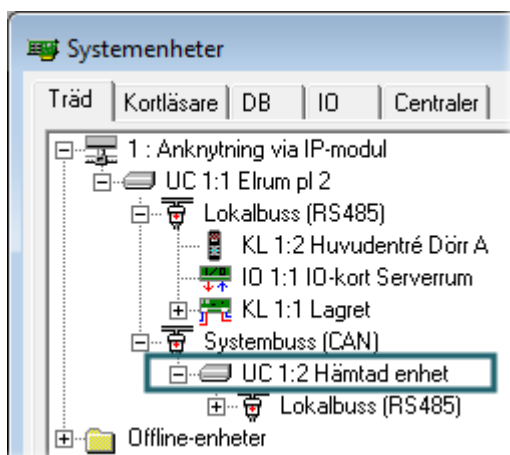
9. Notera IP-adressen från sökresultatet och stäng dialogrutan.
10. Skapa anslutningen på samma sätt som i steg 2–3 på sidan 37, men ange IP-adressen från sökresultatet.
11. Hämta den nya anslutningen som i steg 4 på sidan 38.
12. Fortsätt nu med busskonfigureringen. (Se "[Konfigurera bussar](#)" på sidan 41.)

C) Använda CAN-bussen på en befintlig anknytning

1. Anslut den nya undercentralen via CAN-buss till den befintliga. (Anvisningar hittar du i manualen *R-CARD 5000 – Installera*.) Se till att terminera på ett korrekt sätt!
2. Så här kan det se ut på en hämtad anknytning. Just nu finns endast en undercentral:



Hämta anknytningen på nytt: Högerklicka på anknytningen och välj **Hämta anknytningen**. Nu ser vi den nya UC-50 inkopplad via systembuss:



3. Fortsätt nu med busskonfigureringen. (Se "[Konfigurera bussar](#)" på sidan 41.)

Konfigurera bussar

1. På fliken **Träd**, högerklicka på aktuell undercentral och välj **Konfigurera bussar**.
2. Välj fliken **TCP/IP egenskaper**.

Konfigurera - UC 1:1 Elrum pl 2

TCP/IP egenskaper | TCP/IP mot PC | TCP/IP mellan undercentraler | Lokalbuss via TCP/IP

☒ Erhåll en IP adress automatiskt (DHCP)

Ange en IP-adress

IP-adress: 169 . 254 . 254 . 0

Nätmask: 255 . 255 . 0 . 0

Gateway: 0 . 0 . 0 . 0

☒ Erhåll adress till DNS-server automatiskt

Använd följande DNS-serveradresser

Önskad DNS-server . . .

Alternativ DNS-server . . .

MAC-adress: 00-05-7C-00-34-86

Nätverksbeskrivning: Cirrus CS8900 Ethernet

Spara Avbryt

3. Om dynamisk adresstilldelning ("DHCP") ska användas, kontrollera att **Erhåll en IP adress automatiskt (DHCP)** är markerad.

Då behöver man inte fylla i IP-parametrarna **IP-adress**, **Nätmask** och **Gateway**. Då får man också möjligheten att välja **Erhåll adress till DNS-server automatiskt** och behöver inte fylla i IP-adressen.

4. Om DHCP inte ska användas, fyll i IP-parametrarna.



Om du anger 0 i den minst signifikanta adressdelen kommer undercentralens egen fysiska adress (2–254, inställd med DIP-omkopplaren SW1 på undercentralens kretskort) att ersätta nollan.



Adresserna 1 och 255 ska inte användas. De kan ha speciella funktioner i ett nätverk (broadcastadress, serveradress etc.). Även andra adresser kan vara reserverade i nätverket. Kontrollera med nätverksansvarig.

5. Om DNS-server används, markera **Erhåll adress till DNS-server automatiskt**. (Tillgänglig bara om **Erhåll en IP-adress automatiskt** markerats.)

Alternativt, skriv in adressen till DNS-servern och ev. alternativ DNS-server.

Om DNS inte används, lämna DNS-inställningarna blanka.

6. Välj fliken **TCP/IP mot PC** och ange följande inställningar:

- a. Markera **Aktivera protokoll**.
- b. **Port** avser TCP/IP-modulen. Välj ett nummer i samråd med nätverksansvarig. Standardvärdet är 1000.
- c. I fältet **Tid för nyckeluppdatering**, ange hur ofta kodnyckeln för anknytnings kommunikation ska uppdateras. Standardvärde är 60 sekunders intervall.

- d. Rekommendation: Markera **Svara på nätverkssökning** så att undercentralen kan svara på serverns sökning.
- e. Om **Dynamisk server IP** markeras kan kontakt upprättas mellan undercentralen och R-CARD M5 oavsett vilken IP-adress datorn med servern har. Då behöver ingen serveradress eller port anges.

IP-adress ska vara 0.0.0.0 om **Dynamisk server IP** är markerad. Annars är markeringen borta nästa gång dialogrutan visas.

Om **Dynamisk server IP** inte markeras måste serverdatorns IP-adress och port anges. Detta ger högre säkerhet än dynamisk adress eftersom bara den dator som har rätt IP-adress och -port kan kommunicera med undercentralen.

Dessa inställningar sparas inte i databasen utan bara i undercentralen.

7. Om MapR Touch eller R-TOUCH 50 ska anslutas, konfigurera lokalbuss via TCP/IP:
 - a. Välj fliken **Lokalbuss via TCP/IP** och ange följande inställningar:

Konfigurera - UC 1:1 Elrum pl 2

TCP/IP egenskaper | TCP/IP mot PC | TCP/IP mellan undercentraler | **Lokalbuss via TCP/IP**

☒ Aktivera lokalbuss via TCP/IP

Port:

Krypteringsnyckel

Antal sekunder för kontroll av kom.avbrott: Sekunder

Antal omsändningsförsök: gånger

Kommunicera med dessa enheter

Enhet	Adressering	Port:
Ny enhet...		

Spara Avbryt

- b. Fyll i lämpligt värde om inte standardnummer (9001) för **Port** ska användas. Önskat portnummer måste då också anges på manöverpanelen.

- c. Om det finns flera MapR Touch eller R-TOUCH 50 på nätverket kan det vara klokt att ändra krypteringsnyckeln för att låsa panelen och UC mot varandra. Det går bra att ha olika nycklar för olika undercentraler på samma anknytning.
- d. Inställningarna **Antal sekunder för kontroll av kom.avbrott** och **Antal omsändningsförsök** gäller för lokalbuss via IP:s bussegment. Rekommenderade värden: 3 sekunder, 3 försök.
- e. Under **Kommunicera med dessa enheter**, dubbelklicka på **Ny enhet**. Dialogrutan **Egenskaper lokalbuss enhet via TCP/IP** visas.⁴
- f. Ange samma **Port** som angivits i enheten (standardnummer 9001).
- g. Välj **Adresseringsmetod** mot enhet och ange värdet för vald metod:
 - **Enhetsadress (1–255)**
 - **MAC-adress** (Tryck på **F1** för att öppna online-hjälpen med detaljerade instruktioner.)
 - **IP-Adress**

Alla tre alternativen fungerar i ett lokalt nät (nätsegment) som inte är begränsat med router eller brandvägg. I annat fall gäller alternativet **IP-Adress**.



Om undercentralen och enheten är åtskilda av en brandvägg ska i vissa fall inte den faktiska IP-adressen till enheterna läggas in. För information om användningen av brandväggar i systemet se manualen *R-CARD M5 – Installera*.

- h. Avsluta med **OK**.
8. Klicka på **Spara**.
 9. Vid vissa ändringar visas en uppmaning om att "Reset av centralen krävs för att nya inställningarna ska börja gälla..." Man kan välja **Ja** eller **Nej**. I vissa fall kan det krävas att trycka på undercentralens **Reset**-knapp.

Om ingen reset/omstart av undercentral utförs så är det inte säkert att alla förändringar genomförs. De är dock sparade i undercentralen.
 10. Hämta anknytningen på nytt.

⁴ Observera att en UC-50 endast klarar två TCP/IP-protokoll samtidigt. Mer information på sidan [36](#).

Överföra data till enheterna

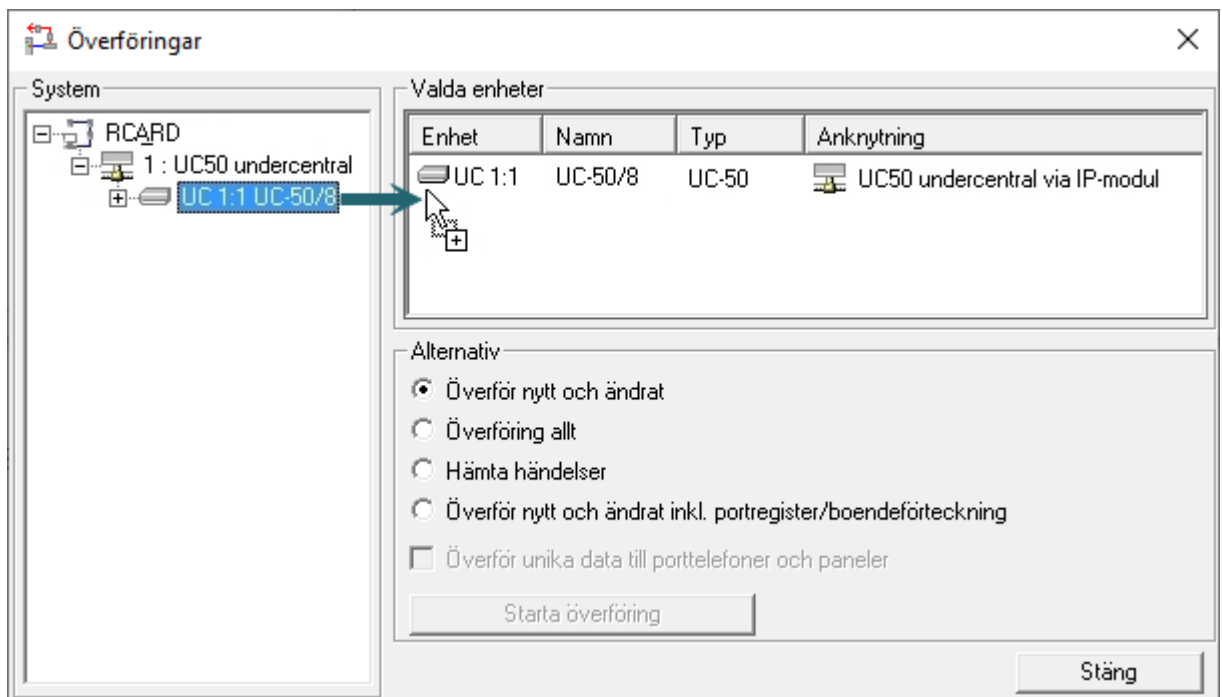
När du sparar data så överförs nya och ändrade data automatiskt ut till undercentralerna. Men dataöverföring kan även beordras manuellt om du misstänker att undercentraler inte fått alla data.

Överföra data till en enhet som du arbetar med

1. Enheten är vald under **Enheter > Systemenheter**.
2. Klicka på **Överför till enhet** (📡).

Överföra data till flera enheter

1. Välj **Enheter > Överföringar**.
2. Dra-släpp domän, anknytning eller enheter till **Valda enheter**.



3. Välj ett alternativ:
 - **Överför nytt och ändrat** överför ändrad och ny information som inte blivit skickad till enheter.
 - **Överföring allt** behövs normalt endast på enheter som är nya i systemet, efter utbyte av trasiga enheter eller om misstanke finns att enheter saknat kommunikation.

- **Hämta händelser** avläser loggdata från undercentralerna.
 - **Överför unika data till porttelefoner och paneler** behövs vid driftsättning av porttelefoner eller Electrolux bokningstavlor.
4. Klicka på **Starta överföring** för att starta överföring till (och/eller hämtning från) enheterna.
 5. Bekräfta att överföring ska ske.
 6. *Avvakta klarmeddelandet.*

Inställningar i undercentralen

 Man måste först ha hämtat anknytningen där enheterna (delningsboxar, in-utenheter, kortläsare och virtuella dörrar) är anslutna för att de ska bli tillgängliga för konfigurering. (Hämtning beskrivs på sidan 23.) Det går inte att lägga in nya enheter "manuellt".

 **Tips:** Om systembuss via IP ska användas: Konfigurera först alla undercentraler som ska anslutas till systembussen för TCP/IP mellan centraler. Tryck på **F1** för att öppna programmets onlinehjälp, där konfigureringen för denna typ av kommunikationsbuss beskrivs.

Gör så här:

1. Välj **Enheter > Systemenheter**.
2. Markera aktuell enhet i systemträdet.
3. Huvuddelen av inställningarna görs på fliken **Allmänt**.

Inställning	Beskrivning
Summalarm	Ange vilka händelser som ska ge summalarm. Om undercentralens summalarm-utgång ska användas till annan funktion, se "fliken Ingångar/Utgångar " på sidan 48.

Inställning	Beskrivning
Virtuella enheter	En <i>virtuell enhet</i> (eller virtuell kortläsare) kan enklast beskrivas som en dörrmiljö av typ "Reader-50" utan kortläsare. En UC-50/8 kan kontrollera upp till 8 virtuella enheter, vanliga dörrmiljöer och hissar (även i blandning). Om man behöver fler virtuella enheter måste ytterligare undercentraler kopplas in. I rullgardinslistan Antal virtuella enheter, välj Ange antal (1 - 2/4/8). Ange antalet virtuella enheter som ska skapas. Ange Adress för första enheten. Virtuella enheter har adresstyp A3 och följer de regler som gäller för denna typ. Exempel: Antal virtuella enheter: 4 Adress för första enheten: 50 Adresserna 50, 51, 52 och 53 kommer att upptas av de virtuella enheterna.  Adresserna för virtuella enheter, hissenheter och befintliga dörrmiljöer får inte kollidera med varandra.
Hissenheter	Se " Styra hissar " på sidan 122 för utförliga instruktioner.
Energimätning	Denna inställning visas när undercentralen är del av ett system som är konfigurerad för energimätning. Normalt står den på Använd global inställning . Ska en del av systemet använda t.ex. en annan mätserver så kan dess värden anges här.
Övrigt	
Serieport	Automatiskt val rekommenderas.
Sekvensöppningsintervall	För att förebygga strömrusning vid samtidig aktivering av t.ex. flera motorlås kan man fördröja utgångarnas aktivering.

Inställning	Beskrivning
Lokal tidsanti-passback	<i>Tidsantipassback</i> förhindrar att en kortläsare används igen inom en definierad tid. Oftast används tidsantipassback för att förhindra att en person överlämnar sitt kort till en efterföljande person (passback). Dörrar som ska ingå i antipassback måste konfigureras för detta. Steg-för-steg instruktioner ges i programmets hjälpfunktion. Tryck på F1 och sök på "Konfigurera lokal tidsantipassback".
Spänningsvarning	Undercentralen rapporterar om matningsspänningen ligger utanför tillåtna värden. Vid otillåten spänning lagras en felrapport i händelseloggen.

På fliken **Minneskonfig** redovisas hur minnet används och vilka moduler som ingår. Inga inställningar kan göras. För mer information se "[Minneskonfigurera undercentraler](#)" på sidan 29.

- Välj fliken **Ingångar/Utgångar**. Här kan du välja vilken funktion som ska kopplas till undercentralens reläutgång (P16).

Förutsättning: AHC är aktiverat (leveransläge).

Dubbelklicka på utgången. Dialogrutan **Egenskaper** visas. Välj **Egenskap**:

Inställning	Beskrivning
Summalarmutgång UC-50	Standard. Se Summarlarm ovan.
Central: Blinkande statusutgång, system OK	Utgången indikerar att undercentralen har startat utan problem. Inga systemfel med omstart har registrerats. Utgången kan väljas att vara sluten för att signalera OK (aktivt hög, NO) eller att vara öppen. Ett UC-fel indikeras på systemstatusutgången samt av lysdiod D2 (7 återkommande blink) på kretskortet. Felet kan bestå av t.ex. oscillatorfel, minnesfel etc. För att återställa statusindikeringen, tryck på RESET-knappen på undercentralens kretskort. Lysdiod D2 ska slockna och reläutgången ska åter indikera status OK. Om felindikeringen kvarstår kan det bli nödvändigt att byta ut undercentralen.

Alternativt, koppla utgången till valfri enhet/funktion.

5. Avsluta med **OK**.
6. Klicka på **Spara** .

Konfigurera dörrmiljöer

Med *dörrmiljö* menas oftast systemenheter (oftast kortläsare men även delningsboxar, manöverpaneler och bokningstavlor) som har adresstyp 3. Se "[BILAGA 1: Enhetsadresser och adresstyper](#)" på sidan 145.

Inställningarna varierar beroende på enhet. För inställningar specifikt för manöverpaneler se "[Konfigurera manöverpaneler](#)" på sidan 87. För inställningar specifikt för porttelefoner se "[Konfigurera porttelefoner](#)" på sidan 114. För inställningar specifikt för bokningstavlor se programmets hjälpfunktion.

Inställningar som inte stöds av aktuell undercentralversion eller aktuell enhet syns inte i R-CARD M5.

Som alltid kan du trycka på **F1** för utförlig information om tillgängliga inställningar.

Gör så här:

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Markera aktuell enhet i systemträdet.
3. Enheternas grundegenskaper:
 - Ange ett beskrivande namn i fältet **Benämning**.
 - **Typ**: Enhetstyp och programversion. Ej ändringsbart.
 - **Enhetsnummer**: Enhetens fysiska, inställda adress (1–255). Ej ändringsbart här.
 - **Pos**: Enhetsbeteckningen. (Se "[BILAGA 2: Identifiering av enheter \(enhetsbeteckningar\)](#)" på sidan 148.)
 - **Logotypbild** kan väljas till enheter med display: Klicka på dialogöppnaren () till höger om inställningen **Logotypbild**. Bläddra fram till och välj bilden och klicka på **Öppna**. Kontrollera bilden genom att välja fliken **Grafik**.
4. Inställningarna på fliken **Allmänt** är grupperade enligt nedan:
 - **Dörrmiljö** – konfigurera dörrstyrning. Här anger du hur kortläsare och ev. bokningstavlor ska styra dörrarnas lås. Här ingår typ av låsning, dörröppningstid, dag/nattlåsning, öppning för funktionshindrade och

separat styrning för utpassage. Inställningarna varierar beroende på enhet.

- **Fri text** kan väljas till enheter med display. För Reader-509 och MapR 509 gäller max. 2 rader med 30 tecken var.

- **Motorlås (dag-/nattnläge)** – konfigurera motorlåsstyrning.

Med NoKey motor-enhetens inbyggda kontroll av tryckesfallet i kombination med motorstyrning av regeln erhåller man dag- och nattnläsning i en och samma enhet.

- **Dörrlarm** – konfigurera dörrlarmstyrning. Här anger du hur kortläsare och ev. bokningstavlor ska styra dörrlarm (dvs fungera som larmförbikopplare). Funktion är beroende av att dörravkänning är ansluten. Inställningarna varierar beroende på enhet.

- **Lokal larmstyrning** – styra externt larm från kortläsare.

Rekommendation: I stället för att styra det externa larmet från kortläsaren, konfigurera ett larmområde för styrning av externt larm. (Se sidan 99.) Så slipper man dra kablage till varje dörrmiljö för att sköta larmstyrningen/återkopplingen. Det behövs endast en kabel till en in/utgång.

De dörrmiljöer som ingår i ett larmområde ska under **Lokal larmstyrning** ha inställningarna *avstängda*.

- **Dörrmiljö lokal larmstyrning/larmområden** – Här kan du bestämma:

- Om kortläsarens larvindikeringsdiod eller display ska visa larmets status konstant.
- Larmvarning vid larmtillkoppling.
- Säkerhetsnivå vid pågående larmtillkoppling.
- Automatisk larmfrånkoppling vid in- eller utpassage.

- **Summalarm** – En utgång kan fås att aktivera som ett *summalarm* om någon av ett antal valbara händelser eller fel inträffar. Exempel på summalarm är dörr uppbruten eller uppställd, sabotage, kommunikationsavbrott m.m. Ange vilka händelser ska ge summalarm.

- **Terminal 1, Terminal 2** – ansluta kortläsare till delningsbox (se sidan 84).

- **Nödöppning** – konfigurera nödöppning/nödlåsning i ett integrerat larmsystem (MEGA), se sidan 88.

- **Indikeringar** – ange lampornas och summerns funktion. Alla indikeringar är markerade som standard. Avmarkera indikeringar som inte tillåts i ett larmsystem i enlighet med vald larmklass.
- **Inställningar för offline-enheter** – aktivera kortläsare som initieringsläsare.
- **Övrigt:**
 - Konfigurera hotlarm, inslagsbegränsning m.m.
 - Konfigurera lokal tidsantipassback
 - Gäller enheter med display: Ange ljusstyrkan.
 - Integrationer: Knyt dörrar till licenser

5. Klicka på **Spara** (💾).

Konfigurera ingångar och utgångar

Enheternas ingångar och utgångar har inställningar som bestämmer deras funktion. Funktionerna kan finnas antingen inom enheten/området själv eller i en annan enhet (kortläsare, virtuell enhet etc).

In/utenheter används i kombination med "Reader-50", som inte har några egna in- eller utgångar.

För varje in- och utgång definieras:

- Funktion.
- Vilken annan enhet/område/typ som påverkas av ingången.
- Vilken annan enhet/område/typ som påverkar utgången.

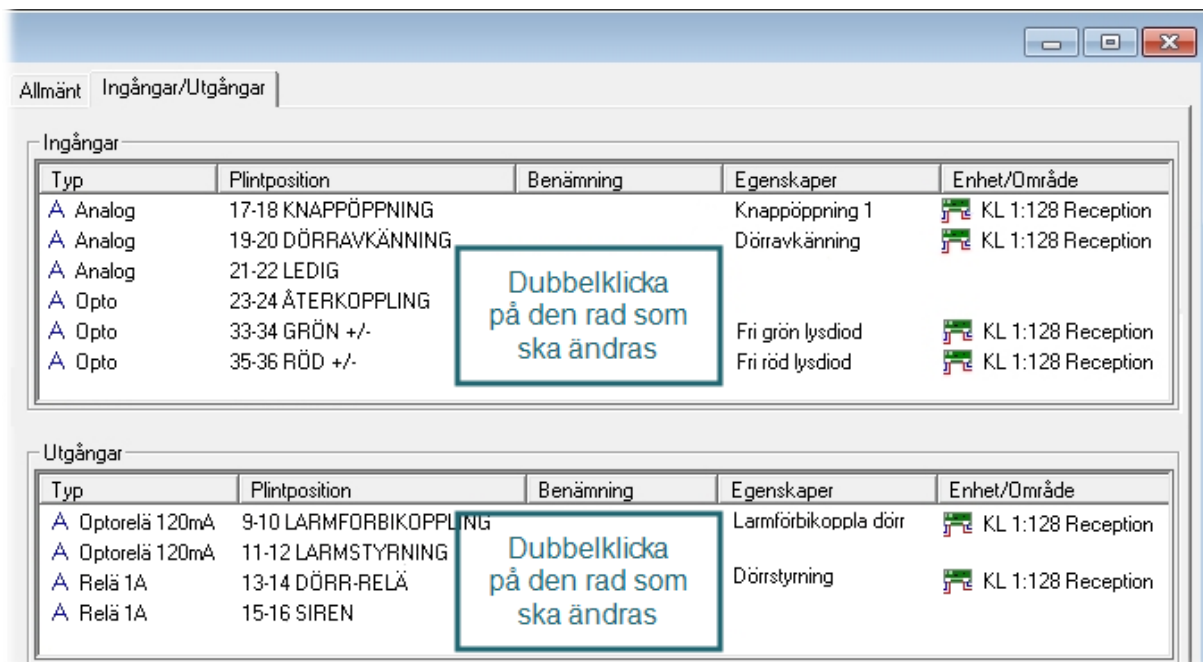
Genom att välja andra enheter på in- eller utgångarna kan man "korskoppla" signaler mellan olika enheter.

En del in- och utgångar kan konfigureras aktivt höga (NO) eller aktivt låga (NC). Vissa ingångar kan även sättas till dubbelbalanserad funktion.

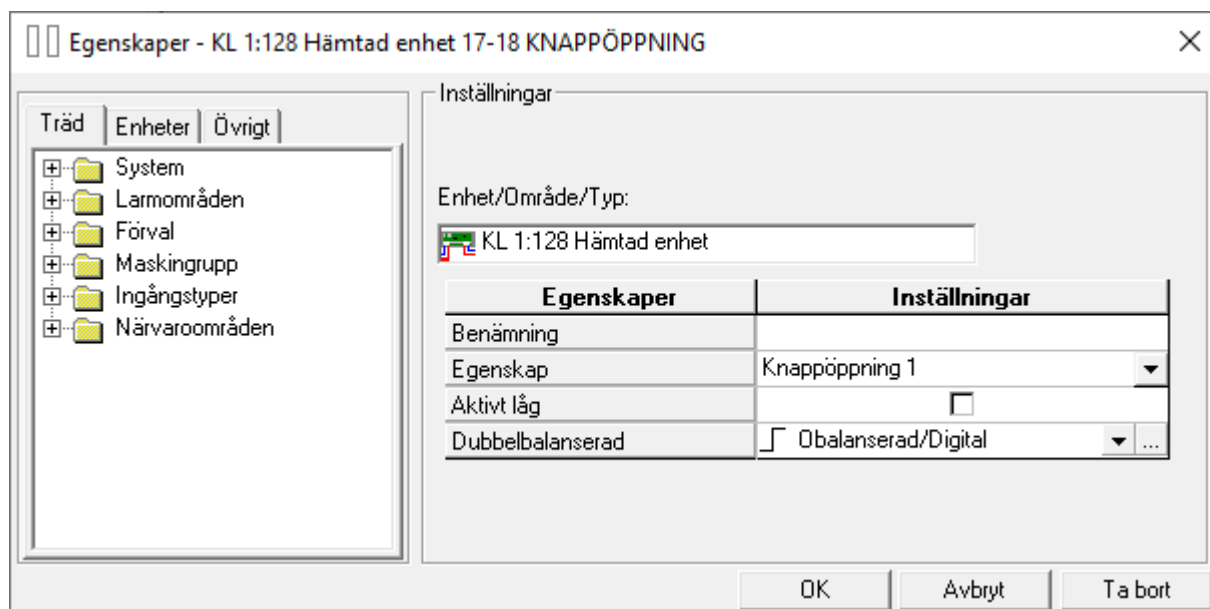
Gör så här för att konfigurera in- och utgångar, exempelvis på en delningsbox:

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Välj den enhet som ska konfigureras.
3. Välj fliken **Ingångar/Utgångar**.

Om enheten inte redan har omprogrammerade in- och utgångar ser det ut ungefär enl. nedan. Listan över egenskaper anpassas efter vilken typ av enhet man valt.

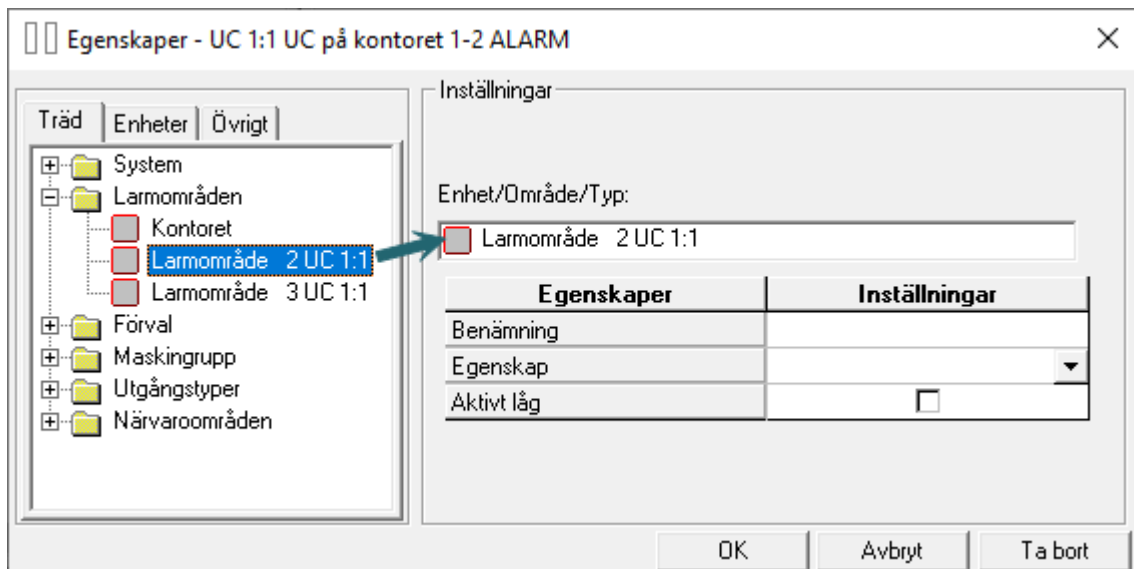


4. Dubbelklicka på den ingång eller utgång vars funktion ska ändras. Dialogrutan **Egenskaper** visas. Den funktion som kopplats syns i rutan **Egenskap**. Exempel:



5. Klicka på plustecknet (+) vid trädlistan så att enheterna syns.
Alternativt, välj fliken **Enheter**.

6. Dra den enhet eller det larmområde eller närvaroområde som ska använda in- eller utgången och släpp det på **Enhet/Område/Typ**.



7. I fältet **Egenskap**, välj den funktion hos aktuell enhet/område som ska styra in- eller utgången.

 Ingångs- och utgångsegenskaperna beskrivs utförligt i programmetts hjälpfunktion (tryck på **F1**).

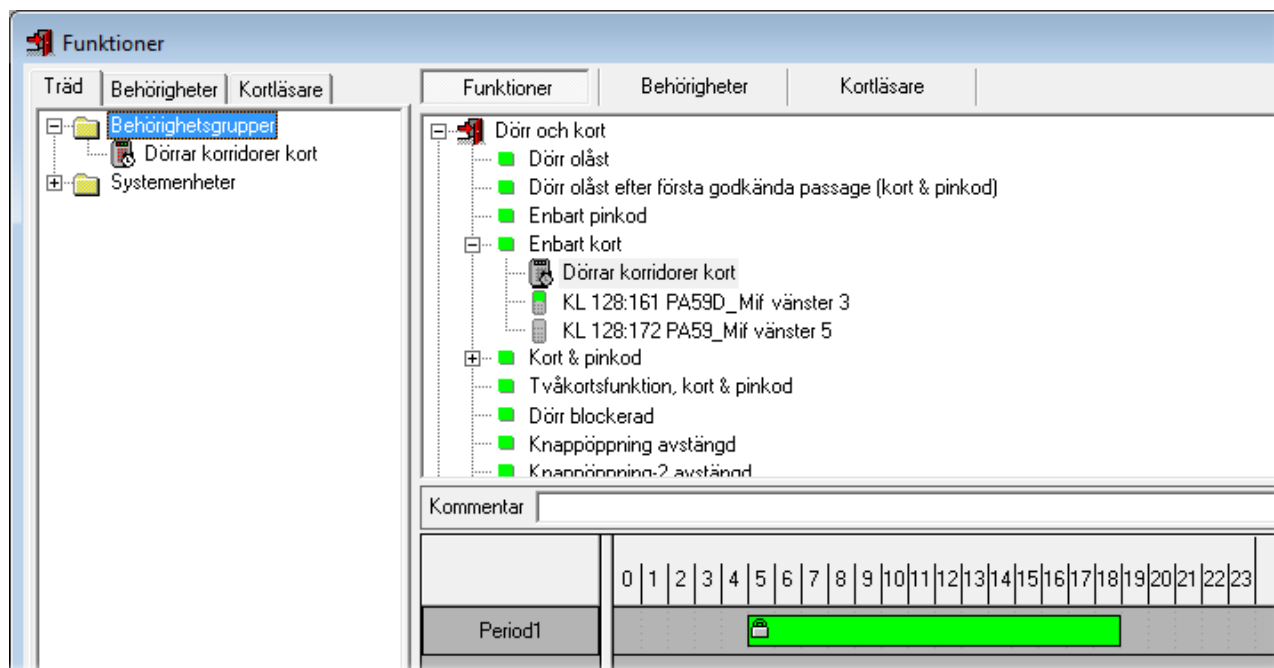
8. Ange övriga egenskaper.
- Vissa typer av ingångar kan definieras för aktivt hög (NO) eller aktivt låg (NC) funktion.
 - Vissa typer av ingångar är analoga och kan därför ställas in för dubbelbalanserad funktion. *Motståndet måste vara 2,2 kΩ vid dubbelbalansering.*
9. Avsluta med **OK**.
10. Klicka på **Spara** (.

Visa och aktivera funktioner

Allmänt

När vi pratar om *funktioner* i R-CARD M5-systemet så menas sådant som påverkar dörrmiljöer (vanligtvis kortläsare), t.ex. att en dörr får stå olåst eller att knappöppningen är avstängd.

Att *aktivera* en funktion innebär att välja *vilka kortläsare som ska ha den och när den ska gälla*. Det kan man göra på två olika sätt:



- Man kan koppla funktionen direkt till utvalda kortläsare. I exempelbilden är funktionen **Enbart kort** knutna till kortläsarna **KL 128:161** och **KL 128:172**. (**Enbart kort** innebär att dessa kortläsare inte kräver pinkod för passage.) Skapa sedan ett tidsschema som bestämmer när funktionen ska gälla. (För instruktioner se sidan [129](#).)
- Man kan koppla funktionen till utvalda *behörighetsgrupper*. Följden blir att *alla kortläsare som valts in i behörighetsgruppen* kopplas till funktionen. Funktionen följer i detta fall behörighetsgruppens tidsschema.

I exempelbilden är funktionen **Enbart kort** knuten till behörighetsgruppen **Dörrar korridorer kort**. Alla kort som kopplas till behörighetsgruppen **Dörrar korridorer kort** kan därför öppna dörrarna med enbart kortet. Dessa användare slipper alltså slå sin pinkod på de dörrar som omfattas av behörighetsgruppen.

i Funktioner som kräver kort *gäller ändå själva kortläsarna*. Det innebär att *alla* kort som är behöriga att passera dörren, oavsett om de fått denna behörighet via just denna behörighetsgrupp eller via en annan behörighetsgrupp, som inte är knuten till funktionen, *kan göra passage på det sättet som funktionen anger*.

Det är möjligt—men rekommenderas inte, för att det komplicerar administrationen—att koppla kort till samma behörighetsgrupp som du kopplar till funktionen, och på det sättet ge korten passage i de valda kortläsare under valda dagar och tider.

Men kort som kopplas endast till en annan behörighetsgrupp—en som *inte* är knuten till funktionen—kommer ändå att kunna göra passage på det sättet som funktionen anger. Funktionen gäller de *kortläsare* som valts in i behörighetsgruppen, oavsett vilka kort som används i dem.

Exempel:

En behörighetsgrupp som kopplats till en funktion. Behörighetsgruppen har också kopplats till ett kort för att tillåta passage vid entrén:

 Behörighetsgrupp för passage och för funktion **Enbart kort**

Tider: Måndag-fredag kl. 9–16

Kortläsare entré

Sven Svenssons kort

En behörighetsgrupp som endast kopplats till kort och alltså endast används för att tillåta passage vid entrén:

 Behörighetsgrupp för passage

Tider: Alla dagar kl. 6–20

Kortläsare entré

Anna Johanssons kort

Innebörden:

- Om Sven Svensson inte tillhör någon annan behörighetsgrupp så får han endast passera entrén kl. 9–16.

Han behöver endast visa kort, eftersom det är den funktion som gäller för kortläsaren då.

- Anna Johansson får passera entrén kl. 6–20.

Kl. 9–16 behöver hon endast visa kort, eftersom det är den funktion som gäller för *kortläsaren* under de tiderna.

Vissa funktioner är aktiverade som standard. De är inbyggda i systemet. Exempel: Kortläsare med knappsats kräver kort och pinkod (**Kort + kod** i dialogrutan) som standard.



Viktigt: Se till att flera funktioner inte aktiveras samtidigt. Det är en vanlig anledning till att enheter inte fungerar så som man tror att man har programmerat dem. Vid felsökning se "Kortläsare eller manöverpaneler fungerar inte som programmerat" på sidan 140.

Aktivera funktioner

Koppla funktioner direkt till utvalda kortläsare

1. Välj **Huvudmeny > Funktioner**.
2. Välj visningssätt i vänster ruta (**Kortläsare** eller **Träd**).
3. Välj fliken **Funktioner** i höger ruta (se bild på sidan 54). Sök reda på och markera önskad typ av funktion i listan.

Exempel: *Fri tidsstyrd utgång* är en funktion som kan användas för valfritt ändamål, t.ex. att tända belysning enligt ett tidsschema. Den har ingen inverkan på dörrens säkerhetsnivå.

4. Dra önskad kortläsare och släpp den *på* den funktion som ska användas.



Tips: Du kan även dra en kortläsare från ett träd eller en lista som visas i något annat fönster.

Enheten syns nu under funktionens namn.

5. Valfritt: Lägg in en beskrivning i fältet **Kommentar**.
6. Ange nu när funktionen ska gälla (skapa ett tidsschema).

Tidsscheman används av flera objekt i systemet. Se gemensamma instruktioner på sidan 129.

7. Klicka på **Spara** (💾).

Koppla funktioner till behörighetsgrupper

1. Välj **Huvudmeny > Funktioner**.

2. Välj visningssätt i vänster ruta (**Behörigheter** eller **Träd**).

Behörighetsgrupper som inte är avsedda för funktioner är överkryssade och inte användbara.

3. Välj fliken **Funktioner** i höger ruta (se bild på sidan 54). Sök reda på och markera önskad typ av funktion i listan.

Exempel: *Fri tidsstyrd utgång* är en funktion som kan användas för valfritt ändamål, t.ex. att tända belysning enligt ett tidsschema. Den har ingen inverkan på dörrens säkerhetsnivå.

4. Dra önskad behörighetsgrupp och släpp den på den funktion som ska användas.



Tips: Du kan även dra en behörighetsgrupp från ett träd eller en lista som visas i något annat fönster.

Behörighetsgruppen syns nu under funktionens namn. Även behörighetsgruppens tidsschema visas (skrivskyddat).

5. Valfritt: Lägg in en beskrivning i fältet **Kommentar**.

6. Klicka på **Spara** (📁).

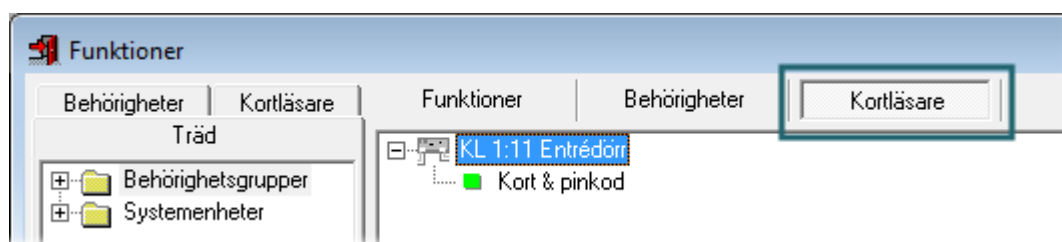
Funktionen kommer nu att påverka behörighetsgruppens kortläsare under de tider som bestäms av behörighetsgruppens tidsschema.

Ta reda på vilka funktioner som används i anläggningen

Visa funktioner för en utvald kortläsare

Gör så här för att kontrollera vilka funktioner som har kopplats direkt till en utvald kortläsare:

1. Välj **Huvudmeny > Funktioner**.
2. Välj fliken **Kortläsare** i höger ruta.

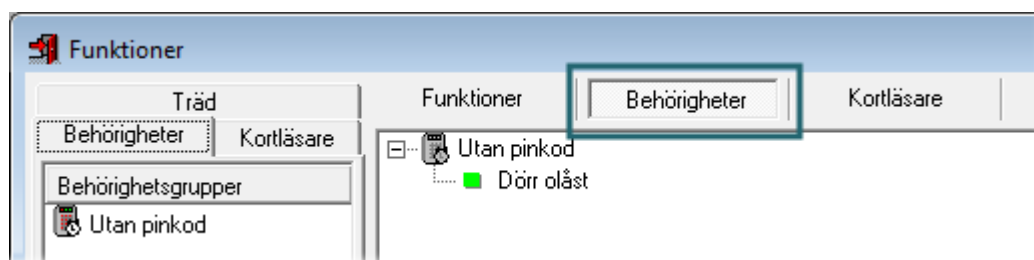


3. Klicka på  vid aktuell kortläsare.

Visa funktioner för behörighetsgrupp

Gör så här för att kontrollera vilka funktioner som är kopplade till *alla* kortläsare i en utvald behörighetsgrupp:

1. Välj **Huvudmeny > Funktioner**.
2. Välj fliken **Behörighetsgrupper** i höger ruta. Här visas en lista med de behörighetsgrupper som använder någon funktion.



3. Klicka på  vid aktuell behörighetsgrupp.

Visa kortläsare och behörighetsgrupper som använder en viss funktion

Gör så här för att kontrollera vilka kortläsare och behörighetsgrupper som är kopplade till en utvald funktion:

1. Välj **Huvudmeny > Funktioner**.
2. Välj fliken **Funktioner** i höger ruta (se bild på sidan [54](#)).
3. Klicka på plustecknet (+) i funktionslistan.

Styra integrerat larm (R-CARD M5 MEGA)

Följande steg ska utföras. Alla beskrivs i efterföljande avsnitt.

1. En undercentral i varje larmsystem konfigureras som centralapparat och för att hantera larmöverföringsinterface. Både larmområden och själva larmsystemet och skapas vid minneskonfigurering. Samtidigt skapas utrymme för larmloggen. Se steg 3 på sidan [33](#).
2. [Konfigurera larmöverföringsinterface](#) (se nedan).
3. [Konfigurera larmsystem med grundinställningar](#) (se sidan [64](#)).
4. [Konfigurera larmmottagare \(kanaler\)](#) (se sidan [67](#)).
5. [Konfigurera larmområden](#) (se sidan [70](#)).
6. [Välja in och konfigurera larmområdets in- och utgångar och ev. larmområden](#) (se sidan [78](#)).
7. Valfritt: [Konfigurera larmkaraktärer](#) (se sidan [83](#)).
8. Valfritt: [Konfigurera indikeringar \(ljudkaraktärer\)](#) (se sidan [83](#)).
9. Valfritt: [Konfigurera ingångstyper](#) (se sidan [83](#)).
10. Valfritt: [Konfigurera utgångstyper](#) (se sidan [84](#)).
11. [Konfigurera nödöppning/nödlåsning](#) (se sidan [88](#)).
12. [Konfigurera in- och utpasseringsvägar](#) (se sidan [89](#)).
13. Valfritt: [Anpassa behörighetsnivåer för manöverpaneler](#) (se sidan [91](#)).
14. [Definiera åtkomst till larmsystemets manöverpaneler](#) (se sidan [92](#)).

Se även [BILAGA 8: Några viktiga inställningar i larmsystemet](#) och [BILAGA 9: Larm- och miljöklassificering](#) på sidorna [158–159](#).

Konfigurera larmöverföringsinterface

Larmöverföringsinterfacet LS-50 monteras på kretskortet till larmsystemets centralapparat (undercentral som är minneskonfigurerad att vara centralapparat). Det larmar vid linjefel och överföringsfel.

LS-50 kan endast anslutas till det vanliga trådbundna telenätet (PSTN).

Larmöverföringsprotokoll som stöds av LS-50:

- SIA-II/SIA-III
- Contact ID



Protokoll väljs i fältet **Typ av mottagare** i larmkanalen. Se "[Konfigurera larmmottagare \(kanaler\)](#)" på sidan 67.

För montering, anslutning och specifikationer se manualen *R-CARD 5000 – Installera*.

Så här konfigurerar du LS-50

1. Välj **Larm > Larmsystem/larmområden**.
2. Välj fliken **Larmområden**.
3. Markera aktuellt larmsystem för att visa dess inställningar.
4. Klicka på plustecknet (+) vid **LS-50 Larmöverföringsinterface**.
5. I förekommande fall: Välj **SIA nivå**.
 - **Sia nivå 2** – mindre utförlig jämfört med nivå 3.
 - **Sia nivå 3** – innehåller maximal information i klartext.
 - **Sia nivå 3 med konfigurationsblock L3** – väljs endast om larmmottagaren begär det.
6. I fältet **SIA konfigureringssträng**, ange i förekommande fall hur data i ett SIA-meddelande ska formateras.

Använd fyra kommaseparerade parametrar:

<Kundnummer>,<Larmområde>,<Larmkaraktär>,<Sektionsadress>

Var och en av parametrarna kan beskrivas så här: <flagga><antal tecken><.precision><typvärde>

Formateringen följer samma regler som i funktionen **printf()** i programspråket C:

flagga	Inget värde = högerjusterat Minustecken (-) = vänsterjusterat # = 0x eller 0X förre hexadecimalt värde
antal tecken	Antalet tecken som resultatet ska vara, med inledande <i>blanktecken</i> till angivet antal tecken. Om 0 står först ska utfyllnad göras med inledande <i>nollor</i> .
.precision	Max. antalet tecken i strängen.
typvärde	s = strängvärde u = decimalt värde (unsigned) x = hexadecimalt värde, små bokstäver (ff) X = hexadecimalt värde, stora bokstäver (FF)

Exempel:

- 03u ger för värdet 11 slutresultatet 011 (tresiffrigt värde med inledande nollor).
- 04u ger för värdet 123 slutresultatet 0123 (fysiffrigt värde med inledande nollor).

Exempel: s,01u,s,03u

- s = kundnummer som text.
- 01u = ensiffriga larmområden, utfyllnad med inledande nollor.
- s = larmkaraktär som text.
- 03u = tresiffriga sektionsadresser (001–999), utfyllnad med inledande nollor.

En blank formatsträng ger standardvärden s,03u,s,04u vilket innebär:

- s = kundnummer som text.
- 03u = tresiffriga larmområden (001–999), utfyllnad med inledande nollor.
- s = larmkaraktär som text.
- 04u = fysiffriga sektionsadresser (0001–9999), utfyllnad med inledande nollor.

7. Ange PSTN-parametrar (trådbunden telelinje):

Inställning	Beskrivning
PSTN aktiverad	Aktiverar PSTN. Indikeras på kretskortet med tänd (fast eller blinkande) lysdiod D1.
PSTN prefix telefonnummer	Används t.ex. när uppringningen går via företagsväxel och LS-50 måste komma i kontakt med det externa telenätet innan meddelandet kan sändas. Prefixet ska följa modemstandard. Exempel på prefix: 0W – LS-50 slår siffran 0 och väntar tills linjeton detekteras.
PSTN prioritet	Prioritering mellan PSTN och GSM (utgått).
PSTN SIA baudrate	Kommunikationshastighet vid överföring av SIA-data.
PSTN Linjekontroll PSTN antal minuter mellan linjekontroll	Kontrollerar teleledningen regelbundet genom att LS-50 kortvarigt lyfter luren. Ange antal minuter mellan kontroller. <i>Linjen bryts under kontrollen.</i>

8. Klicka på **Spara** .

Konfigurera larmsystem med grundinställningar

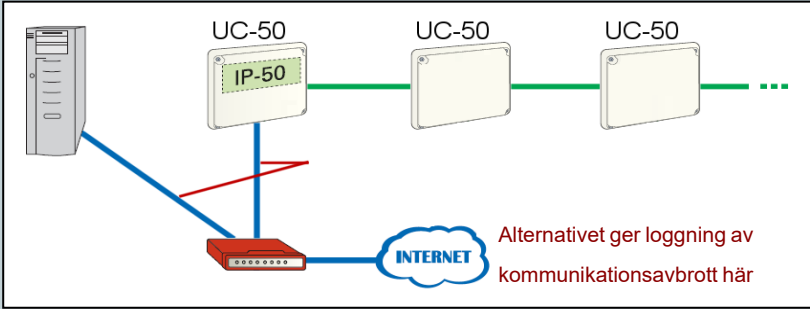
1. Välj **Larm > Larmsystem/larmområden**.
2. Välj fliken **Larmområden**.
3. Markera ett larmsystem för att visa dess inställningar.



Tips: Inställningarna för hela eller delar av ett larmsystem kan importeras från en databasfil i Access-format (.mdb). Tryck på **F1** för att öppna online-hjälpen med detaljerade instruktioner.

4. Ange grundinställningarna:

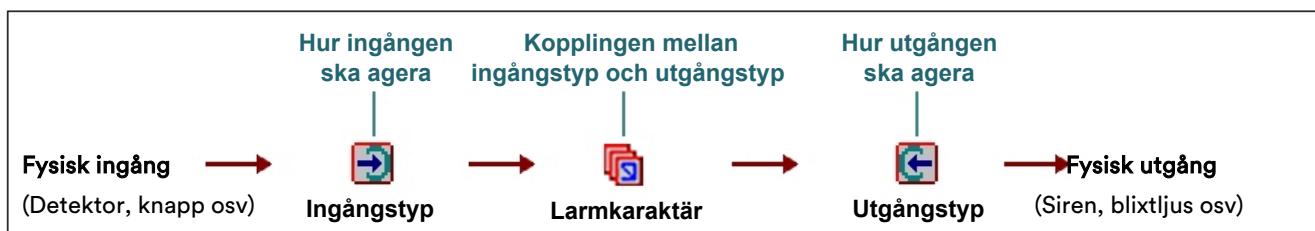
Inställning	Beskrivning
Benämning	Ange ett beskrivande namn. Om SIA III-koder sänds till larmmottagaren så följer benämningen med. Därför kan det vara lämpligt att ange företagsnamn eller adress i detta fält, som information till larmmottagaren.
Fördröjningstid för larmsändning	Antal sekunder innan larmöverföringsinterfacet startar vid ett larm. Funktionen aktiveras när larmsektionens ingångstyp har Fördröjd larmöverföring markerad. (Se " Konfigurera ingångstyper " på sidan 83.)
Fördröjningstid mellan första och andra sändningsförsöket	Om larmsändning misslyckas: Antal sekunder mellan första och andra sändningsförsök. Om även andra försöket misslyckas: Antal sekunder mellan efterföljande sändningsförsök.
Fördröjningstid mellan övriga sändningsförsök	 Vid användning av certifierade larmsändare är det larmsändarens inställningar som är relevanta; dessa två fördröjningstider i R-CARD M5 ignoreras.
Maximal rapporteringstid för larm	Larmsändningar som inte kan genomföras inom vald tid eller misslyckas dessförinnan kommer att häva eventuell sirenfördröjning i larmområden.

Inställning	Beskrivning
Max. antal larm per tillkoppling	Hur många larm (1–15) som sänds vid flera larm på en ingång. Funktionen aktiveras när Begränsning av antalet larm är satt till Begränsning i larmlogg i ingångstypens inställningar. Värdet ska vara 3 för Larmklass 3/4.
Standard motståndsvärde	Välj vilket motståndsvärde som ska vara standard för sektionsanslutningarna. Om inget av värdena passar kan du definiera egna värden. Detta påverkar alla ingångstyper som inte redan har individuellt inställda motståndsvärden. Detta åsidosätter den övergripande standard som valts i systemets grundinställningar. Inställningen Standard motståndsvärde påverkas inte heller av en eventuell ändring där. ! Motståndet måste vara 2,2 kΩ vid dubbelbalansering.
Behörighetstid för vaktarkort (min)	Hur många minuter kort med väktarbehörighet ska vara är aktiva när de aktiverats. Standardtiden är 60 minuter. i Även kortens behörighetsgrupp(er) påverkar. För mer information se "Hantera väktare och deras kort" i programmets hjälpfunktion.
Generera kom.avbrott när kontakt mot server saknas	Loggar kommunikationsavbrott mellan R-CARD M5 Server och anknytnings första undercentral.  Relevant exempelvis om användarna tillåts välja sin egen pinkod, vid dynamisk korthantering eller vid öppning via mobilapplikationen RCO Access.

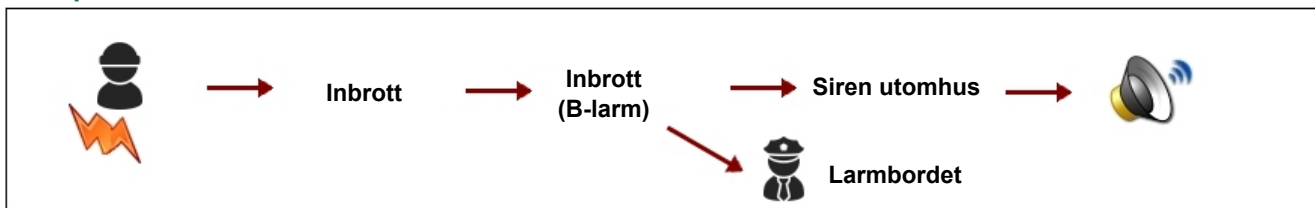
Inställning	Beskrivning
Åtgärdstext	Meddelande som visas i MapR Touch, R-TOUCH 50 och R-CONTROL när larm har skickats. Texten ska förklara för personalen vad man ska göra när larmet skickats. Förväxlas inte med Varning för fel innan tillkoppling, som visas i manöverpanelen <i>innan</i> larmet skickas. Den förklarar vad personalen ska göra för att <i>undvika</i> larmsändning. Varning för fel innan tillkoppling anges inte i karaktären utan i ingångsegenskaperna. Rekommendation: Välj åtgärdstext per ingång, per ingångstyp eller per larmkaraktär i stället för att ha samma åtgärdstext för hela larmsystemet.

5. Klicka på **Spara** (💾).

Ingångstyper och utgångstyper – hur hänger de ihop?



Exempel:



Konfigurera larmmottagare (kanaler)

Larmöverföring görs via larmöverföringsinterfacet LS-50. LS-50 förutsätts vara installerad och konfigurerad. (Se "[Konfigurera larmöverföringsinterface](#)" på sidan 61.)

Upp till 8 larmmottagare kan definieras per larmsystem. Till varje mottagare kan man rapportera en unik kundidentitet.

Gör så här:

1. Välj **Larm > Larmsystem/larmområden**.
2. Markera aktuellt larmsystem för att visa dess inställningar.
3. Klicka på plustecknet (+) vid **Larmmottagare**. Nu visas 8 "kanaler".
4. Klicka på dialogöppnaren (...) för den "kanal" som ska konfigureras. Dialogrutan **Larmmottagare** visas.
5. Klicka på **Ny**.
6. Ange ett beskrivande namn.
7. Välj protokoll (t.ex. SIA III) och mottagarens telefonnummer eller IP-adress.
8. Klicka på **Spara** och **Stäng**.
9. Den nya larmmottagaren är inte vald per automatik. Välj larmmottagaren i rullgardinslistan för den "kanal" som ska konfigureras.
10. Klicka på plustecknet (+) vid kanalen och konfigurerera mottagaren med hjälp av följande inställningar:

Inställning	Beskrivning
Typ av linje för uppkoppling	Behöver inte ändras från standardinställningen Automatisk . (GSM-varianten av LS-50 har utgått.)
Kundidentitet	Kundnummer eller sifferkod för anläggningen. Identifierar anläggningen för larmcentralen. Kundidentiteten kan åsidosättas för ett larmområde genom att ange en Avvikande kundidentitet för larmområdet. (Se sidan 77.) Detta påverkar uppringningen till <i>alla</i> larmmottagare från larmområdet.

Inställning	Beskrivning
Ett uppkopplingsförsök innan alternativ mottagare rings upp	<i>Vid användning av certifierade larmsändare är det larmsändarens inställningar som är relevanta; inställningar kring uppkopplingsförsök i R-CARD M5 ignoreras.</i> Normalt görs nytt uppkopplingsförsök direkt efter det föregående tills antalet uppkopplingsförsök har förbrukats. Sedan kommer nästföljande alternativa mottagare att ringas upp det antal gånger som anges för den mottagaren. Detta fortsätter tills uppringningsförsök har gjorts för samtliga mottagare som är programmerade. Om du markerar detta alternativ anropas nästa mottagare efter ett misslyckat försök. Detta upprepas för varje mottagare tills antalet uppkopplingsförsök har gjorts.
Antal uppkopplingsförsök	Hur många uppringningsförsök som görs innan uppringningen anses misslyckad. Ange 1–15 eller Avstängd.
Filtrering	Välj vilka typer av händelser som ska meddelas till mottagaren. Fördefinierade ingångstyper som är karaktärstyrda har fördefinierad filtrering. Inställningarna kan ändras: - Klicka på dialogöppnaren (...). Dialogrutan Urval filter visas. - Tillgängliga filter visas till vänster, valda filter till höger. Dra–släpp önskade filter från vänstra till högra rutan. För att ångra en tilldelning, dra–släpp i motsatt riktning. Filtergrupp 1 till Filtergrupp 6 används när man vill göra egna larmöverföringsalternativ. - Klicka på OK.

Inställning	Beskrivning
Alternativa kanaler	<i>Vid användning av certifierade larmsändare ignoreras dessa alternativa kanaler.</i> Om en viss larmmottagare inte svarar kan upp till 7 alternativa mottagare istället ringas upp. Observera: ◦ I listan över valbara alternativa kanaler saknas alltid den som just konfigurerats eftersom en kanal inte kan ha sig själv som alternativ. ◦ Den alternativa kanalens konfiguration påverkas: Om t.ex. kanal 1 tilldelas kanal 2 som alternativ kommer kanal 2 att få kanal 1 som alternativ. ◦ Filtringen för de alternativa mottagarna bör vara identiska med förstahandsmottagarens. ◦ För att den alternativa kanalen ska fungera måste både primära och alternativa aktiveras på larmområdet.
Automatisk schemalagd testöverföring	Välj in behörighetsgrupp som styr när testöverföring ska utföras. Tidsintervallernas starttid triggar testöverföringen. Filtreringen Testöverföring måste också väljas för kanalen.

11. Klicka på **Spara** (.

Konfigurera larmområden

Larmområden skapas vid minneskonfigurering av undercentralen. Det finns alltså ingen **Ny**-knapp för larmområden.

Förutsättningar:

- Den undercentral som "äger" larmområdet ska vara minneskonfigurerad för larm och det antal larmområden som ska användas. (Se sidan 33.)
- De dörrmiljöer som ingår i ett larmområde ska under **Lokal larmstyrning** ha inställningarna *avstängda*.

Så här konfigurerar du larmområden för styrning av integrerat larm:

1. Välj **Larm > Larmsystem/larmområden**.
2. Välj fliken **System**.
3. Klicka på plustecknet (+) vid den undercentral som kontrollerar larmområdet.
Nu visas ikoner (□) för de larmområden som undercentralen konfigurerats för.
4. Markera det aktuella larmområdet.
5. Ange önskade inställningar:



Tips: Inställningarna för hela eller delar av ett larmsystem kan importeras från en databasfil i Access-format (.mdb). Tryck på **F1** för att öppna online-hjälpen med detaljerade instruktioner.

Övergripande inställningar, varningstider, larmmanövrering, larmområdesgrupp:

Benämning	Ange ett tydligt beskrivande namn, t.ex. Kontoret plan 1.
Annan benämning i terminal	Benämning som ska visas i enheternas ev. display. Max. 30 tecken. Om detta fält lämnas blankt visas det namn som angetts i Benämning .

Inkluderande

Markera **Inkluderande** om kortläsare som tillhör flera larmområden ska blockeras när aktuellt larmområde tillkopplas, oavsett läget för övriga larmområden som kortläsarna ligger i.

Om **Inkluderande** är markerat: Samtliga kortläsare i larmområdet blockeras så snart det området är tillkopplat. Rekommenderas.

Om **Inkluderande** *inte* är markerat (= "exkluderande"): Kortläsare blockeras först då alla larmområden de ligger i är tillkopplade.

(Det kan även vara en larmsektion i stället för en kortläsare.)

Exempel:



Förråd är beroende av både Kontoret och Butiken.

Butiken är *inkluderande*. Det innebär följande:

- När Butiken tillkopplas blir Förråd blockerat för passage, oavsett läget för Kontoret.
- När Kontoret tillkopplas men inte Butiken så kan Förråd ändå användas. Det innebär att kortläsaren Förråd skulle kunna användas för *passage in i ett larmat område*.

Om Butiken hade varit *exkluderande* (**Inkluderade** inte markerat) så hade Förråd blockerats först när Butiken *och* Kontoret tillkopplats.



Kräver att **Direkt till- och fråkoppling av larmområde** markerats för kortläsaren/sektionen på fliken **Enheter/Ingångar/Utgångar**.

Larmstyrning latch/puls (sek)

Normalt **Avstängt** i en integrerad larmanläggning.

Varningstid vid automatisk larmtillkoppling (sek) Varningstid vid manuell larmtillkoppling (sek)	Förvarningstid vid larmtillkoppling. Ange hur många sekunder summern ska ljuda vid automatisk resp. manuell tillkoppling.  Enheter som ska ge förvarning ska ha Aktivera larmvarning markerad. Larmområdet har utgångsegenskap Varning vid larmtillkoppling som kan kopplas till valfri utgång. Se "Ge varning och status från larmområdet via en utgång" i programmens hjälpfunktion.
Fördröjd återkoppling (sek)	Antalet sekunder som avkänningen av återkopplings-signalen fördröjs (på larmområdets återkopplingsingång). Exempel: Ett kontorsområde tillkopplas från en kort-läsare inom området. Normalt fungerar inte Knappöppning 1 efter tillkoppling. Sätts Fördröjd återkoppling till 30 sekunder så hinner man ut via knappöppningen trots att undercentralen anser att larmet är tillkopplat. Används vanligtvis endast vid styrning av externt larm, om man utnyttjar centralapparatens egen inbyggda varningstid vid tillkoppling. Vid styrning av integrerat larm, observera att <i>integrerat larm inte kan hantera elektrisk återkoppling från extern centralapparat.</i> Se även Ignorera fördröjd återkoppling och utpasseringstid på fliken Enheter/Ingångar/Utgångar.
Manöver för att växla / tillkoppla / frånkoppla larmet	Behövs om någon av larmområdets enheter ingår i flera larmområden. Se "Anpassa larmmanövrering" i programmens hjälpfunktion.
Integrerad larmstyrning	Måste vara valt.
Larmområdesgrupp (0–255)	Vid brandvarning kan flera larmområden (t. ex. gemensam huskropp) som tillhör samma larmområdesgrupp tystas med en ingång, eller ett handhavande.

Väntetider för återkoppling, dubbelpulstid, in- och utpasseringstider, siren:

Väntetid återkoppling larmtillkoppling (sek)	Fördröjning innan återkoppling registreras.
Väntetid återkoppling larmfrånkoppling (sek)	Standardvärdet är 10 sekunder, vilket är ett rekommenderat minimivärde. Använd inte kortare tid.
Tidsgräns verifierat larm (på områden med denna egenskap, sek)	Om en larmsektion larmar två gånger inom denna tidsgräns så genereras ett verifierat larm (A-larm). Första larmet (B-larmet) kommer att behandlas. Se även motsvarande inställning för ingångstypen.
Dubbelpulstid för att generera larm (sek)	Om givare signalerar två gånger inom denna tid på en larmsektion genereras larm på den andra signalen. Detta kräver att använd ingångstyp har Dubbelpuls markerat. Undantag: Det går inte att använda dubbelpuls på ingångar med funktion för brandvarning, eftersom DIO-5084 återställer automatiskt efter 14 sekunder. Detta skapar då Brand verifierat.
Inpasseringstid 1 (sek) Inpasseringstid 2 (sek)	Du kan definiera två inpasseringsvägar. Varje inpasseringsväg har sin egen tidsgräns.
Inbrottsfördröjning under inpasseringstid	Antal sekunder som inbrottslarm (A- och B-larm) fördröjs om de inträffar under inpasseringstiden (se ovan). Larmen läggs fördröjda i larmkön. Utomhussiren startar inte under fördröjningstiden. Övriga sirener och indikeringar fungerar dock som vanligt.  Om larmområdet inte frånkopplas inom fördröjningstiden aktiveras utomhussiren och larmsändning.
Utpasseringstid (sek)	Den tid man har på sig att lämna larmområdet via utpasseringsvägen när larmet har tillkopplats. Tiden är gemensam för båda utpasseringsvägarna och avslutas när man passerar. Den kan förlängas (omstartas) automatiskt beroende på vald Typ av utpasseringssektion under Ingångstyper .
Siren fördröjningstid (sek)	Siren startar inte förrän efter denna tid.

Direkt/villkorsstyrda områden:

För att kunna skapa beroenden måste de styrda larmområdena dras in i det styrande. Dessutom måste **Till- och frånkopplas villkorsstyrt av larmområden** markeras för det inkluderade larmområdet på fliken **Enheter/Ingångar/Utgångar**.

Endast tillkoppling av direktstyrda larmområden

När det aktuella larmområdet tillkopplas så tillkopplas även larmområden som ingår i det. Exempel: När Kontoret tillkopplas så tillkopplas även Förråd och HR. (Frånkoppling tillåts inte.)



Kräver även att **Direkt till- och frånkoppling av larmområde** markeras (på fliken **Enheter/Ingångar/Utgångar**) för det inkluderade larmområdet.

Tillkopplingsfel vid direktstyrning av larmområden

Hur larmområdet ska hantera styrda larmområden:

- **Följ tillkopplingsfel:** Om styrt larmområde blir felaktigt får även det styrande larmområdet felstatus.



Manöverpanelerna saknar stöd för inställningen **Följ tillkopplingsfel**. Den fungerar som **Ignorera**.

- **Ignorera:** Gör tillkoppling även om styrt område har felstatus.
- **Fel om inte tillkopplat:** Det styrda området måste vara tillkopplat för att det styrande området ska kunna tillkopplas. Används ofta på larmområden som inte ska tillkopplas förrän styrda områden är tillkopplade, för att undvika att personer blir inlarmade.

Kräver även att **Direkt till- och frånkoppling av larmområde** markeras (på fliken **Enheter/Ingångar/Utgångar**) för det inkluderade larmområdet.

Automatisk tillkoppling när beroende larmområden tillkopplade	Det aktuella larmområdet tillkopplas automatiskt när inkluderade larmområden tillkopplas. Exempel (se bild ovan): När Förråd och HR tillkopplas så tillkopplas Kontoret automatiskt.
Automatisk frångkoppling när beroende larmområden frångkopplade	Det aktuella larmområdet frångkopplas automatiskt när inkluderade larmområden frångkopplas. Exempel (se bild ovan): När Förråd eller HR frångkopplas så frångkopplas Kontoret automatiskt.

Brandvarning:

Tid för att aktivera verifierad brandvarning (sek)	Två brandvarningar inom denna tid ger verifierad brand. Standardtid 120 sekunder.
Tid för att aktivera verifierad brandvarning om larm från en detektor (sek)	Tid 0 sekunder = avstängd. Ingen verifierad brand från en adress/larmsektion. Tid 1–14 sekunder blir alltid 15 sekunder, vilket är den minsta tiden för att göra en kontrollåterställning på detektor. Standardtid 120 sekunder.
Tvådetektors beroende brand giltig från samma sektion	Två larm från olika givare på en och samma larmsektion krävs för verifierad brand. Fungerar endast om brandgivaren inte är återställningsbar.
Tysta inbrottslarm vid brandvarning i larmområdesgrupp	Alla larm med prioritet på indikering mellan 5 och 16 (även nya larm med brandkaraktär) ignoreras tills larmområdet återställs.

Automatisk till- och frånkoppling:



Tips: Se "Konfigurera automatisk till- och frånkoppling av larm" och "Konfigurera tillkopplingsfördröjning ('köpa tid'-funktion)" i programmet hjälpfunktion.

Tider för automatisk tillkoppling (behörighetsgrupp)	Välj en behörighetsgrupp med användningsområde Funktioner .
Aktivera automatisk tillkoppling	Tillkoppling sker vid den i behörighetsgruppen angivna starttid.
Aktivera automatisk frånkoppling	Frånkoppling sker vid den i behörighetsgruppen angivna sluttid.
Standardtid för tillkopplingsfördröjning (min)	Om du ska konfigurera tillkopplingsfördröjning, ange standardtiden som ska kunna "köpas": ◦ Antal minuter (1–230). Klicka sedan i fältet och ange antalet minuter för fördröjningen. Tiden räknas från handhavandet. ◦ Antal timmar (1–24). Klicka sedan i fältet och ange antalet timmar för fördröjningen. Tiden räknas från handhavandet. ◦ Hela tillkopplingstiden = ingen tillkoppling sker. Används Automatisk larmfrånkoppling vid passage i enheten så aktiveras tillkopplingsfördröjning istället för larmfrånkoppling. Tiden används även vid tillkopplingsfördröjning via en fysisk ingång på enhet (Tillkopplingsfördröjning standardtid väljs i fältet Egenskap). Högsta valbara tid kan anges i behörighetsgrupper.
Om tillkopplingsfel genomför nytt försök (min)	Ange med hur många minuters fördröjning ett nytt tillkopplingsförsök ska göras vid ev. misslyckad automatisk tillkoppling (maximal tid 255 minuter). Anger du 0 görs inga nya försök.

Larmöverföring:

Avvikande kundidentitet

Om kundidentiteten som är kopplad till larmmottagaren ska åsidosättas vid uppringning från det aktuella larmområdet så anger du en annan kundidentitet här. I annat fall ska fältet vara blankt.

Endast siffror tillåts.



Detta påverkar uppringningen till *alla* larmmottagare från larmområdet.

Kanal 1 ...**Kanal 8**

Markera de larmmottagare som ska kunna ringas upp. Både den primära mottagaren och ev. alternativa som har konfigurerats måste markeras.



Markeras ingen kanal så kan inte larmområdet larma.

6. Klicka på **Spara** (💾).

Välja in och konfigurera larmområdets in- och utgångar och ev. larmområden

Gör enligt nedan för att välja vad som ska ingå i larmområdet.

(Alla *virtuella* ingångar är automatiskt inkluderade med sina standardegenskaper.)

De dörrmiljöer som ingår i ett larmområde ska under **Lokal larmstyrning** ha inställningarna *avstängda*.

1. Välj **Larm > Larmsystem/larmområden**.
2. Klicka på plustecknet (+) vid larmsystemet i vänster panel och markera det larmområde där in- eller utgången ska läggas till.
3. Välj fliken **Enheter/Ingångar/Utgångar** och "underfliken" **System**.

Längst ner i fönstret kan du anpassa visningen enligt önskemål:



= Visa radvis.



= Gruppera på ingångstyper och utgångstyper.



= Gruppera på ägande enheter.

Längst ner till höger kan du klicka på **Visa / dölj sektioner** (🔍) och välja vad som ska visas. Om du döljer alla larmsektioner så finns endast kortläsare och larmområden kvar.

4. Gör följande i valfri ordning:

Välj in och konfigurera in- och utgångar:

- a. Klicka på + vid den enhet vars ingång eller utgång ska användas.

Längst ner i fönstret kan du välja vilka virtuella ingångar som ska visas eller döljas:



= Visa/dölja in- och utgångar som är kopplade till en enhet (för passage).



= Visa/dölja in- och utgångar som är kopplade till minst ett larmområde (oavsett vilket).



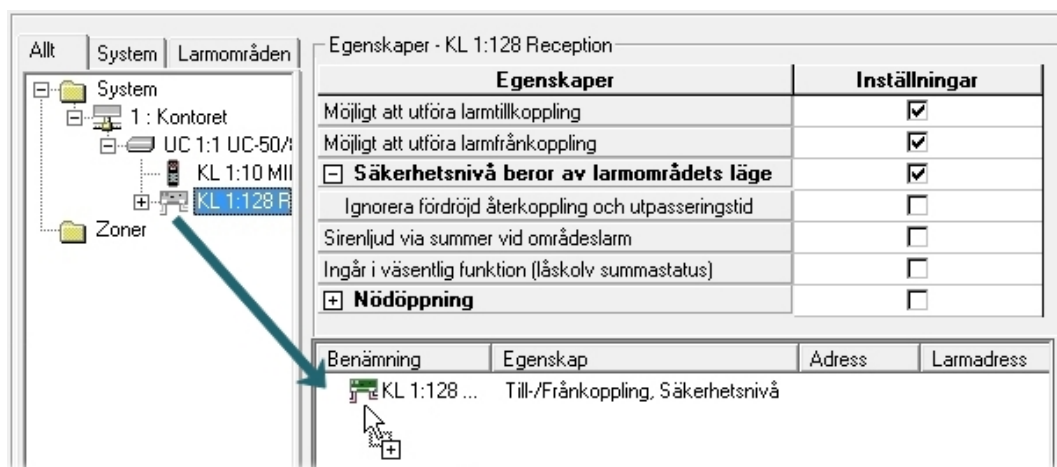
= Visa/dölja in- och utgångar som inte är kopplade till någon enhet (för passage) eller något larmområde.

- b. Dra–släpp en ingång eller utgång från trädet till nedre delen av högerpanelen.

- c. Klicka på ingången/utgången så att dess inställningar visas.
- d. Välj ingångstyp eller utgångstyp.
- e. Markera **Kopplad mot alla larmområden** om in- eller utgången ska kopplas till alla larmområden.
- f. I fältet **Varning för fel innan tillkoppling**, ange ev. text som kan hjälpa personalen att undvika att utlösa larm.
- g. Ingångar kan ges andra värden än ingångstypens standardvärden: Klicka på plustecknet (+) vid **Ingångstyp (nedanstående värden ersätter ingångstypens standardvärden)** och anpassa ingången. Tryck nu på **F1** för vidare instruktioner och information.
- h. Upprepa ovanstående för varje ingång och utgång som ska vara med i larmområdet.

Välj in och konfigurera kortläsare:

- a. Dra-släpp en kortläsare från trädet till nedre delen av högerpanelen.
- b. Klicka på kortläsaren så att dess inställningar visas. Exempel:



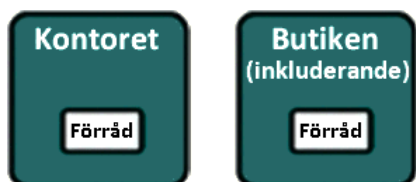
c. Ange önskade inställningar:

Möjligt att utföra larmtillkoppling	Välj om det ska vara möjligt att tillkoppla resp. frångkoppla larmet på vald enhet.
Möjligt att utföra larmfrångkoppling	 Tips: För att blockera kortläsare för passage när området är tillkopplat, inkludera dem i larmområdet och <i>avmarkera</i> dessa två inställningar.
Säkerhetsnivå beror av larmområdets läge	Ska normalt inte väljas i ett integrerat larmsystem.
Ignorera fördröjd återkoppling och utpasseringstid	Om ett larmområde har flera dörrar som är anslutna till centralapparatens statusutgång kan du välja att låta en eller flera dörrar ignorera den fördröjning som ställs in i fältet Fördröjd återkoppling . Denna eller dessa dörrar spärrar då omedelbart passage vid tillkoppling av larmet.
Sirenljud via summer vid områdeslarm	De olika sirenljuden på sirenutgångar i larmområdet kommer ut på enhetens summer.
Ingår i väsentlig funktion (låskolv summastatus)	Låsets kolvläge (låst eller olåst) kontrolleras och används till summerad utgång för larmområdet. Tryck på F1 för att öppna online-hjälpen med detaljerade instruktioner.
Dörrfunktion vid nödöppning	<i>Markera själva inställningen Nödöppning först. I annat fall sparas inte inställningen.</i> Ange sedan hur dörrmiljön ska fungera: ○ Lås öppnas ○ Dörrmiljö låses (enbart kort) ○ Dörrmiljö blockeras ○ Lås öppnas (häver slussfunktion) ○ Dörrmiljö låses (enbart kort, häver slussfunktion) Ingen (förvalt) innebär att ingen nödöppning eller nödlåsning sker.

- d. Om någon av larmområdets kortläsare ingår i flera områden blir kortläsaren som standard blockerad för passage först då alla områden den ligger i är tillkopplade.

Om däremot något av områden den ligger i är *inkluderande* så blockeras alla kortläsarna i det larmområdet då det tillkopplas, oavsett lägen för övriga larmområden som kortläsaren tillhör.

Exempel:



Förråd är beroende av både Kontoret och Butiken.

Butiken är *inkluderande*. Det innebär följande:

- När Butiken tillkopplas blir Förråd blockerat för passage, oavsett läget för Kontoret.
- När Kontoret tillkopplas men inte Butiken så kan Förråd ändå användas. Det innebär att kortläsaren Förråd skulle kunna användas för *passage in i ett larmat område*.

Om Butiken hade varit *exkluderande* (**Inkluderade** inte markerat) så hade Förråd blockerats först när Butiken och Kontoret tillkopplats.

Gör så här om det aktuella larmområdet ska vara *inkluderande*:

- a. Välj fliken **Inställningar**.
 - b. Markera **Inkluderande**.
 - c. Klicka på **Spara** (💾).
- e. Upprepa ovanstående för varje kortläsare som ska vara med i larmområdet.

Välj in och konfigurera andra larmområden:

- a. Dra-släpp ett larmområde från trädet till nedre delen av högerrutan.
- b. Klicka på larmområdet så att dess inställningar visas.
- c. Markera **Direkt till- och fränkoppling av larmområde** om det invalda larmområdet ska följa det område som det ligger i.

- d. I förekommande fall: Markera **Till- och fråkopplas villkorsstyrt av larmområden**.
 - e. Upprepa ovanstående för varje larmområde som ska vara med i det aktuella larmområdet.
5. Klicka på **Spara** (.

Konfigurera larmkaraktärer

Varje ingångstyp är knuten till en larmkaraktär. *Larmkaraktären* definierar vilken kod som ska sändas via larmöverföringsinterfacet när ingången detekterar ett larm eller när larmet återställs.

Karaktären kan även påverka hur utgångar fungerar. Läs om utgångstypen **Karaktärsstyrd utgång** i programmets hjälpfunktion.

Det finns en mängd fördefinierade larmkaraktärer som kan anpassas för varje larmsystem/anknytning. Du kan också definiera egna. För instruktioner se programmets hjälpfunktion. (Välj **Larm** > **Karaktärer**. Tryck sedan på **F1**.)

 Inställningen **Obligatorisk händelse** ingår i larmcertifiering. *Obligatoriska händelser* lagras i en reserverad del av larmloggen och kan inte skrivas över av icke-obligatoriska händelser. Antalet larmhändelser som kan sparas i undercentralen anges när den minneskonfigureras (inställning **Maximalt antal larmhändelser** – se sidan 34). Läs mer om larmloggen i programmets hjälpfunktion.

Konfigurera indikeringar (ljudkaraktärer)

Ljudkaraktärer definierar ljudet (indikeringar) i olika situationer. Dessa ljud används om **Standardljud** väljs som **Typ av ljud** i ingångstypens inställningar.

Det finns en mängd konfigurerbara indikeringar. För instruktioner och exempel se programmets hjälpfunktion.

Konfigurera ingångstyper

En *ingångstyp* kan ses som en grupp standardinställningar för ingångar. När du [väljer in larmområdet ingångar](#) så väljer du även ingångstyp. Den bestämmer vilken typ av larm den hanterar, avkänningsteknik m.m.

Till ingångstypen kopplas en larmkaraktär för tillkopplat resp. fränkopplat läge. (Se "[Konfigurera larmkaraktärer](#)" ovan.)

Det finns en mängd fördefinierade ingångstyper som kan anpassas för varje larmsystem/anknytning. Du kan också definiera egna. För instruktioner se programmets hjälpfunktion. (Välj **Larm** > **Ingångstyper**. Tryck sedan på **F1**.)

 Rekommendation: Anpassa inte fördefinierade ingångstyper. Gör i stället en kopia på ingångstypen (se nedan) och anpassa den.

Konfigurera utgångstyper

En *utgångstyp* kan ses som en grupp standardinställningar för utgångar. När du väljer in larmområdets utgångar så väljer du även utgångstyper. De bestämmer vilken funktion utgången ska ha.

Det finns en mängd fördefinierade utgångstyper som kan anpassas för varje larmsystem/anknytning. Du kan också definiera egna (max. 128). För instruktioner se programmets hjälpfunktion. (Välj **Larm > Utgångstyper**. Tryck sedan på **F1**.)

 **Rekommendation: Anpassa inte fördefinierade utgångstyper. Gör i stället en kopia på utgångstypen (se nedan) och anpassa den.**

Konfigurera enheter anslutna till delningsbox

Delningsbox DB-50 är en styrenhet för fullständig kontroll över dörr och larm:

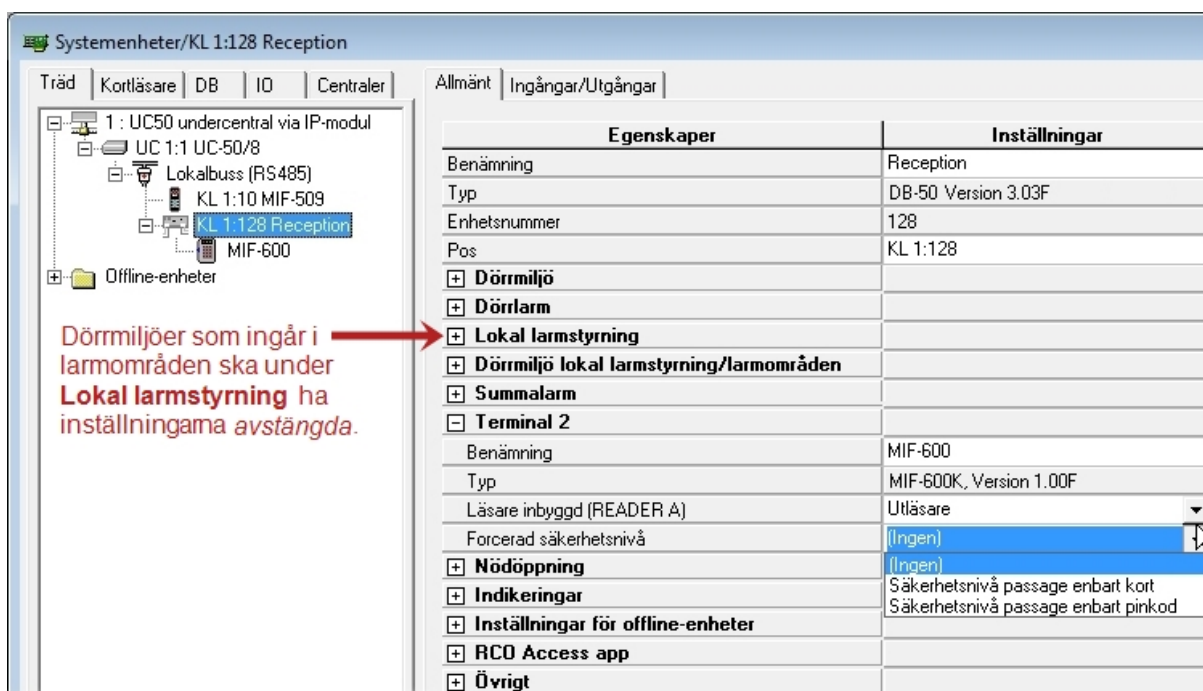
- Förbikoppling av dörrlarm
- Automatisk och manuell larmstyrning med förvarning, återkoppling från centralapparat samt indikering av larmstatus.
- Dagläge och nattläge. Sirenutgången används då normalt för nattlåsen.

Den ansluts via lokalbuss till undercentral UC-50 och har adresstyp A3. (Se "[BILAGA 1: Enhetsadresser och adresstyper](#)" på sidan 145.)

Två kortläsare av typen "Reader-60" (med ev. slavläsare) kan anslutas till delningsbox DB-50, DB-50 Light eller DIO-5084. Om två läsare är anslutna visas båda **Terminal 1** och **Terminal 2** i inställningarna.

 Delningsboxar har, lite oegentligt, prefixet **KL** (kortläsare – se "[BILAGA 2: Identifiering av enheter \(enhetsbeteckningar\)](#)" på sidan 148). I exemplet betecknas den KL 1:128 Reception, en delningsbox som här har en kortläsare av typ MIF-600.

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Markera aktuell delningsbox i systemträdet.



- Klicka på plustecknet (+) vid **Terminal 1** och/eller **Terminal 2** och ange önskade inställningar:

Inställning	Beskrivning
Benämning	Här kan du ge enheten ett beskrivande namn.
Läsare inbyggd (Reader A)	Välj om huvudläsaren ska behandlas som in- eller utläsare. Passage loggas normalt som "Passage In". Genom att definiera om Reader-A till utläsare loggas istället "Passage Ut".  Omkonfigurering av Reader-A/Reader-B påverkar ev. antipassbackfunktion!

Inställning	Beskrivning
Forcerad säkerhetsnivå	 Om dörren har en forcerad säkerhetsnivå kan användare inte skapa tillfälliga koder i mobilapplikationen RCO Access. Ange om ev. programmerade dörrfunktioner (under Dörr och kort) ska åsidosättas på aktuell enhet. Följande alternativ finns: ◦ Säkerhetsnivå passage enbart kort. Vid utpassage krävs ingen pinkod, även om knappsats finns.  Tips: Snarlik funktion kan åstadkommas genom att aktivera funktionen Enbart kort vid utpassage. ◦ Säkerhetsnivå passage enbart pinkod. Vid passage krävs inget kort, även om kortläsare finns. Detta alternativ fungerar enbart med UC-50 version 3.01 eller senare. Används med försiktighet. Det är viktigt att pinkoderna är unika. Om det finns flera kort med samma pinkod gäller följande: Vid passage med pinkod registreras händelsen <i>på det kort som fick pinkoden först</i>, även om det kortet inte är behörigt i kortläsaren. Exempel: Kalle och Karin har pinkod 1234. Kalle fick sin pinkod först men är inte behörig i kassaskåpsdörren. När Karin slår 1234 för att öppna kassaskåpet visar händelseloggen att Kalles kort har använts för det, trots att endast Karins kort är behörigt. ◦ Ingen. Standard säkerhetsnivå för enheten gäller, alternativt programmerad dörrfunktion.

4. Om terminalerna har slavläsare visas ytterligare inställningar:

Inställning	Beskrivning
Läsare slav (Reader B)	Välj om slavläsaren ska behandlas som in- eller utläsare.
Läsare slav (Reader B) använder tangentbord	Läs av korten i slavläsaren men använd huvudläsarens knappsats för t.ex. pinkod.

5. Klicka på **Spara** .

Övriga inställningar beskrivs i avsnittet "[Konfigurera dörrmiljöer](#)" på [sidan 49](#).

Konfigurera manöverpaneler

Med en *manöverpanel* kan man till- och fränkoppla eller återställa larmområden, kvittera larm, testa sirener, utföra gångtester och annat – allt beroende på vilka behörigheter du har i systemet. Man kan även styra dörrmiljöer.

Inställningarna varierar beroende på enhet. Inställningar som inte stöds av aktuell undercentralversion eller aktuell enhet syns inte i R-CARD M5.

Antalet manöverpaneler måste anges individuellt för varje undercentral vid minneskonfigureringen. Se **Antal manöverpaneler** på sidan [33](#).

Som alltid kan du trycka på **F1** för utförlig information om tillgängliga inställningar.

En stor del av konfigurationen är identisk med övriga dörrmiljöer, se "[Konfigurera dörrmiljöer](#)" på sidan [49](#). Här beskrivs vanliga inställningar för manöverpaneler.

Gör så här:

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Markera aktuell enhet i systemträdet.
3. Vanliga inställningar för manöverpaneler:

Inställning	Beskrivning
Logotypbild	Klicka på dialogöppnaren (...) till höger om inställningen Logotypbild. Bläddra fram till och välj bilden och klicka på Öppna. Bildkrav MapR 509: Filformat JPEG/JPG eller BMP. (BMP kräver längre överföringstid.) Bredd 240 pixlar, höjd 160 pixlar. Svart bakgrund. Bildkrav för MapR Touch: Filformat JPEG/JPG. Max. bredd 700 pixlar, max. höjd 350 pixlar.
Fri text	Kan väljas till enheter med display. För MapR 509 och MapR Touch gäller max. 2 rader med 30 resp. 50 tecken var.
Kort tid för automatisk utloggning (sek)	När man loggat in måste man trycka på någon knapp inom denna tid för att inte bli automatiskt utloggad. Standardtid 10 sekunder.
Tid för automatisk utloggning (sek)	När man loggat in och börjat manövrera blir man automatiskt utloggad om ingen manövrering sker eller knapp trycks inom denna tid. Standardtid 60 sekunder.

Inställning	Beskrivning
Aktivera inslagsbegränsning	För att förhindra att någon ska kunna testa fram en pinkod för inpassage kan man begränsa antalet inslag som går att göra. Det finns speciella in- och utgångstyper för inslagsbegränsning.

Manöverpaneler kan också kontrollera en dörrmiljö och har motsvarande inställningar. De kan inkluderas i passerbehörigheter precis som en vanlig kortläsare.

4. Klicka på **Spara** (💾).

Konfigurera nödöppning/nödlåsning

Du anger när nödöppning (eller nödlåsning) ska initieras och om även larmade/blockerade dörrar ska öppnas.

Två alternativ:

- Bara dörrar i det larmområde som sektionen tillhör nödöppnas.
- Nödöppning sker oberoende av om dörren ingår i ett larmområde.

Som standard initieras nödöppning av larmkaraktärerna Brand och Brand verifierad. Detta kan ändras valfritt.

 **Varje dörr som ska nödöppnas eller nödlåsas måste programmeras för detta.**

Steg-för-steg instruktioner ges i programmets hjälpfunktion. Tryck på **F1**.

Konfigurera in- och utpasseringsvägar

Ett larmområde kan ha två inpasseringsvägar och två utpasseringsvägar. Dörrar som ingår kan vara försedda med kortläsare (se nedan) eller bara magnetkontakt.

Aktivera dörrlarm

Börja med att aktivera dörrlarm i den enhet som ska kontrollera dörrarna i in- och utpasseringsvägarna. Då skapas den virtuella ingången **Dörravkänning uppbruten** på enheten.

Du hittar **Aktivera dörrlarm** under **Dörrlarm** i enhetens inställningar.

Ange tidsgränser för in- och utpassage

1. Välj **Larm > Larmsystem/larmområden**.
2. Klicka på plustecknet (+) vid larmsystemet. Klicka sedan på det larmområde som ska styras. Larmområdets aktuella status (tillkopplat eller fränkopplat) indikeras.
3. Ange **Inpasseringstid 1** eller **Inpasseringstid 2**.
4. Ange **Utpasseringstid** (gemensam för båda vägarna).

Definiera inpasseringsväg



Vid användning av inpasseringsväg får inte manöverpanelen tillhöra samma dörrmiljö som inpasseringsläsaren.

1. Välj fliken **Enheter/Ingångar/Utgångar**.
2. Välj "underfliken" **System**.
3. Dra–släpp den kortläsare som kontrollerar den dörr som är först i inpasseringsvägen från systemträdet till listan över ingångar/utgångar/enheter i larmområdet.
4. Klicka på plustecknet (+) vid systemträdet så att kortläsarens ingångar visas.
5. Klicka på **Visa virtuella ingångar** (🔗) längst ner i fönstret.
6. Dra–släpp den virtuella ingången **Dörravkänning uppbruten** till listan över larmområdets in- och utgångar.

Alternativt, använd **Dörr öppen**.

7. Kontrollera att den virtuella ingången är markerad och att inställningarna för ingångstypen visas ovanför listan. Ingångstypen ska vara **Inbrott/dörr uppbruten**.

8. Klicka på plustecknet (+) framför ingångstypen för att få tillgång till alternativa inställningar.
9. Välj ingångstypens inställning **Typ av inpasseringssektion**, t.ex. **Start1** och **Följande**.
10. För varje ytterligare dörrmiljö som ska passeras, upprepa steg 3–9, men välj **Följande** i steg 9.
11. Klicka på **Spara** (💾).

Starta inpassage

Inpassering startas med en manöver för larmfrånkoppling vid första dörren, normalt # + kort + pinkod.

Om dörren ingår i flera larmområden, konfigurera manöverkommando:

1. Välj fliken **Inställningar för larmområdet**.
2. Ange hur **Manöver för larmtillkopplingar** ska utföras för larmområdet. (Se "Anpassa larmmanövrering" i programmets hjälpfunktion.)

Larmet måste nu frånkopplas via manöverpanel inom inpasseringstiden för att inte larm ska utlösas.

Definiera utpasseringsväg

1. Välj fliken **Enheter/Ingångar/Utgångar**.
2. Välj "underfliken" **System**.
3. Klicka på **Visa virtuella ingångar** (🔗) längst ner i fönstret.
4. Dra–släpp en kortläsare som ska kontrollera en dörr i utpasseringsvägen från systemträdet till listan över ingångar/utgångar/enheter i larmområdet.
5. Markera kortläsaren i listan och markera inställningarna **Manöver för larmfrånkopplingar** och **Säkerhetsnivå beror av larmområdets läge**.
6. Klicka på plustecknet (+) vid systemträdet så att kortläsarens ingångar visas.
7. Klicka på **Visa virtuella ingångar** (🔗) längst ner i fönstret.
8. Dra–släpp den virtuella ingången **Dörravkänning uppbruten** till listan över larmområdets in- och utgångar.
9. Kontrollera att den virtuella ingången är markerad och att inställningarna för ingångstypen visas ovanför listan. Ingångstypen ska vara **Inbrott/dörr uppbruten**.

10. Välj ingångstypens inställning **Typ av utpasseringssektion**, t.ex. **Avsluta efter aktivering**. Larmet kommer då att tillkopplas så snart sista dörren har passerats på utvägen.
11. För varje dörr i utpasseringsvägen, upprepa steg 4–10.
12. Klicka på **Spara** .

Starta utpassage

Utpassage startas med larmtillkoppling, t.ex. via manöverpanel.

Ange säkerhetsnivå (passermöjlighet)

1. Välj **Enheter > Systemenheter**.
2. Markera en kortläsare som ingår i utpasseringsvägen.
3. På fliken **Allmänt**, expandera **Dörrmiljö lokal larmstyrning/larmområden**.
4. För **Säkerhetsnivå vid pågående larmtillkoppling (In/Ut)**, ange vilken passermöjlighet dörren ska ha under övergång från olarmat till larmat läge.

Om dörren har två kortläsare går det att välja kombinationer av nivåer för in- och utpassage.

5. Klicka på **Spara** .

Anpassa behörighetsnivåer för manöverpaneler

Användarnas *behörighetsnivå* avgör vilka operationer som tillåts vid manöverpanelen. Den kan även begränsa vilka manöverpaneler som är tillgängliga.

Behörighetsnivån anges när du definierar åtkomst till larmsystemets manöverpaneler, dvs när du skapar MAP-behörighetsgrupper (se nedan).

Larmsystemet har åtta fördefinierade behörighetsnivåer. Nivåerna är fritt programmerbara och har ingen inbördes prioritetsordning. I programmets hjälpfunktion finns en tabell som visar vilka funktioner och menyer som är tillgängliga för varje nivå vid leverans. Nivåerna är fritt programmerbara (se hjälpen) och har ingen inbördes prioritetsordning.

Ju högre behörighetsnivå, desto högre prioritet. Om en användare har två MAP-behörigheter med t.ex. behörighetsnivå 6 och 7 så kommer rättigheter enligt nivå 7 att gälla.

Definiera åtkomst till larmsystemets manöverpaneler

För att ge åtkomst till larmsystemets manöverpaneler skapar du en behörighetsgrupp av varianten "MAP". Sedan kopplas behörighetsgruppen till kort.

 Vissa manöverpaneler innehåller kortläsare och kan därmed även styra dörrar. *Passermöjligheterna* styrs av den "vanliga" behörigheten, inte av MAP-behörigheten. Kort som ska användas både för rättigheter i manöverpaneler och för passage måste följaktligen ha två olika behörigheter.

 Inställningar med stjärna (*) här nedan finns även för individuella kort. Anges ett annat värde när man lägger in kort så åsidosätts behörighetsgruppens värde.

Gör så här:

1. Välj **Huvudmeny > Behörigheter**.
2. Högerklicka på en fri yta i behörighetslistan och välj **Ny MAP-behörighet**.
Alternativt, markera en befintlig behörighetsgrupp och välj **Skapa ny behörighet baserad på denna** (🔄). Kopian kan sedan ändras enl. önskemål.
I ett domänsystem, välj även den domän med de enheter som ska ingå i behörighetsgruppen.
3. Ange ett beskrivande namn i fältet **Benämning**.
4. Ange **Giltighet**.*
5. Ange önskade inställningar:

Inställning	Beskrivning
Behörighetsnivå	Behörighetsnivån avgör vilka operationer som tillåts vid manöverpanelen. Den kan även begränsa vilka manöverpaneler som är tillgängliga.
Semesterstyrd*	Spärrar behörigheten under semesterperioden. (Semesterperioden bestäms domänvis i årskalendern.)
Väktarbehörighet	Ger väktarbehörighet, som vanligtvis aktiveras när larm eller sabotage inträffar.

Inställning	Beskrivning
Teknikerbehörighet	Används för tekniker som gör tillfälliga besök. (Förväxla inte <i>teknikerbehörighet</i> och <i>certifierad tekniker</i>. Läs mer om teknikerbehörighet i programmets hjälpfunktion.) Observera att Teknikerbehörighet innebär en <i>begränsning</i> av användarens rättigheter i systemet. Teknikerkort kan bara användas när teknikern anges vara på plats.  Om både Väktarbehörighet och Teknikerbehörighet är markerade blir behörighetsgruppen giltig bara om villkoren för <i>båda</i> är uppfyllda.
Tvåkortsfunktion1 Tvåkortsfunktion2	Innebär att det krävs att två olika kort används inom 6 sekunder (fast tidsgräns) för att öppna en dörr. Samma kort kan inte visas två gånger. För tvåkortsfunktion måste kortens behörighetsgrupper tillsammans ha både Tvåkortsfunktion 1 och Tvåkortsfunktion 2 markerade. Det godkänns inte att båda kortens behörigheter bara har samma tvåkortsfunktion markerad. Det ena eller båda korten kan däremot ha behörighet med båda funktionerna markerade.
Valbar pinkod från displayläsare	Ger möjlighet att byta pinkod direkt i Reader-509 eller MapR 509.
Låsa/återställa dörrmiljö (*0*)	Ger möjlighet att låsa dörren, alternativt återställa en tillfälligt låst dörr. (På äldre kortläsare låsas dörren genom att slå *0* på knappsatsen. På nyare enheter väljer man Lås dörr eller Återställ dörr.) För att få låsa en dörr som är olåst med funktion krävs det att Aktivera 'Lås dörr'-funktion (*0*) väljs i dörrens inställningar.
Högsta valbara tid tillslagsfördröjning (tim)	Ger möjlighet att skjuta upp larmtillkoppling. Förutsätter att automatisk till- och fränkoppling är konfigurerad. (Se sidan 76 .)

6. Välj fliken **Kortläsare/Områden** och lägg nu in de manöverpaneler, kortläsare och larmområden som ska vara åtkomliga. Dra–släpp enheter från listan/trädet till behörighetens förteckning. (Gör tvärtom för att ta bort en enhet från behörighetsgruppen.)



Om en enhet som är del av ett larmområde inkluderas kommer även larmområdet att inkluderas.

7. Om kortinnehavarna ska kunna tillkoppla eller frånkoppla ett larm *från en manöverpanel som ingår i flera larmområden* så kan du ange standardlarmområde: I högra rutan, högerklicka på larmområdet () och välj **Ange som standard**.
8. Välj fliken **Tidsschema** och ange när behörigheterna ska gälla. (För instruktioner se sidan [129](#).)
9. Klicka på **Spara** ()

Nu kan du koppla behörighetsgruppen till kort.

Planritningar och grafik i R-CONTROL och MapR Touch

I Planritningsverktyget kompletteras utvalda ritnings- och bildfiler med de dörrar, larmområden och larmpunkter som ska övervakas och styras ifrån R-CONTROL⁵ och/eller från manöverpanelen MapR Touch. (Även R-TOUCH 50, som utgått.)



Visning av en planritning i MapR Touch

Observera / tips

- Om R-CARD M5 körs på en separat klient behöver vissa inställningar göras innan Planritningsverktyget kan användas. Dessa beskrivs i manualen *R-CARD M5 – Installera*.
- Man kan importera en befintlig INDIGRAF-ritning. Steg-för-steg instruktioner ges i programmets hjälpfunktion. Tryck på **F1**.
- Ritningarna presenteras i manöverpanelen i samma ordning som de skapas i Planritningsverktyget. Det går inte att ändra deras inbördesordning.
- För personal som övervakar en eller flera anläggningar är det ibland önskvärt att presentera ett larm på en översiktsbild över anläggningen, för att därefter kunna klicka sig vidare till en mer detaljerad ritning. I Planritningsverktyget kan detta åstadkommas via funktionen **Tillåt att larm fortsätter i länkar till denna ritning** tillsammans med **Överordnad** ritning. Länkningen kan ske i flera steg.
- Se även "[Konfigurera manöverpaneler](#)" på sidan 87.

⁵ R-CONTROL är ett grafiskt komplement till R-CARD M5. Det används för att från en central punkt styra och övervaka anläggningens dörrar, larmområden, närvaroområden, kameror och larmgivare/larmpunkter. R-CONTROL rekommenderas för större anläggningar, och för styrning av olika domäner. Du kan skapa *scenarier* där du genom en tangenttryckning eller ett knapptryck styr en eller flera dörrar, larmområden, eller närvaroområden till alternativa funktioner. R-CONTROL är licensbelagd. Om licens finns till modulen R-CONTROL och för flera R-CARD M5-klienter kan R-CONTROL användas på flera datorer. Handhavandet beskrivs i onlinehjälp i R-CARD M5.

Förbereda ritningarna

Texter och benämningar (utöver objektens benämning i R-CARD M5) som ska synas på ritningen kan inte skapas i Planritningsverktyget. Använd ett separat program för bildhantering.

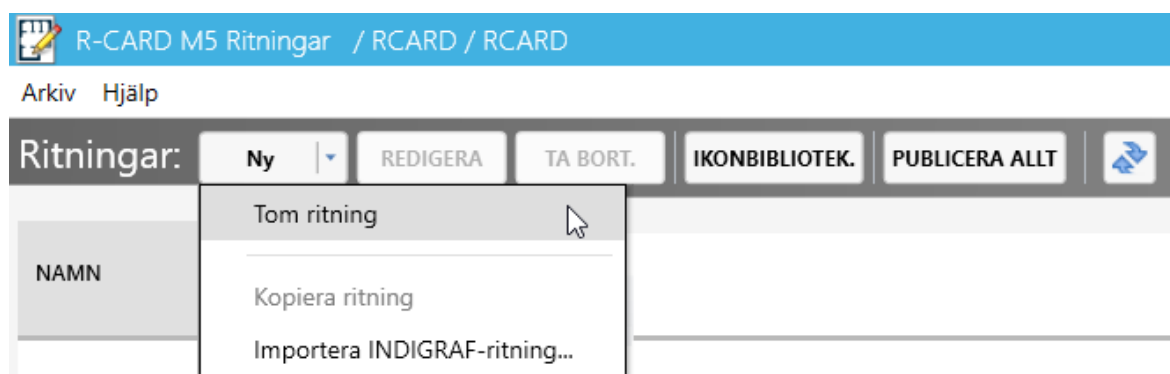
- Bildformaten som stöds är BMP, PNG och JPG/JPEG.
- Rekommenderad bildstorlek för MapR Touch och R-TOUCH 50 är 1024 x 768 pixlar.

Bildstorlek för R-CONTROL väljs efter datorbildskärmens storlek och upplösning.

- Prestanda gynnas av en låg upplösning (96 DPI rekommenderas), vilket inte påverkar presentationen på skärmen negativt.

Konfigurera ritningarna i Planritningsverktyget

1. Starta Planritningsverktyget genom att välja **Inställningar > Planritningar** i R-CARD M5.
2. Klicka på **Ny** i övre vänstra hörnet och välj **Tom ritning**.



Alternativt, importera en INDIGRAF-ritning. För instruktioner se programmets hjälpfunktion.

Till höger visas olika knappar och fält med inställningar för den aktuella ritningen. Utförliga instruktioner ges i programmets hjälpfunktion. Tryck på **F1** inifrån programmet. Glöm inte att exportera ("publicera") ritningarna när de är klara.

Testa detektorer i larmsystemet

Gångtestläge används när man ska testa detektorer i larmsystemet (dock inte brand, systemfel eller larmkaraktärer för sabotage).

I gångtestläge gäller:

- Inga larm överförs.
- Inga sirener ljuder.
- Händelser visas inte i händelsefönstret utan bara i manöverpanelen.
- Minimitid, dubbelpuls och fördröjning ignoreras för snabbare respons.

Larmområdet måste vara frånkopplat.

i För att kunna sätta ett larmområde i gångtestläge måste du ha teknikerbehörighet eller ha en behörighetsnivå som inkluderar **Gångtest**. (Som standard är det endast behörighetsnivån 7 (Tekniker) som gör det.) Val av behörighetsnivå beskrivs på sidan 92.

i **Viktigt:** Följande larmkaraktärer aktiveras (genererar larm) som vanligt även under gångtest. Om de ska ingå i gångtestet, *stäng av sirener och meddela larmcentralen*.

- Batterifel (ackumulator extern)
- Brand och Brand, verifierad
- Linjefel (generell), PSTN-fel, GSM-fel
- Nätfel
- Larmsändningsfel
- Sabotage (generell), Sabotage avbrott (normalt sabotage)
- Sabotage kortsluten, Sabotage manipulering, Sabotage tamper, Sabotage kom.avbrott, Sabotage siren
- Systemfel (systemfel, batterifel minnesbackup, felaktig inspänning)
- Överfall (hotlarm) tyst, ljudande, dolt

I följande beskrivs hur du utför gångtest från manöverpanelerna MapR 509, MapR Touch och R-TOUCH 50. Gångtest kan också utföras från MAP-59 och MAP-50; anvisningar hittar du i onlinehjälpn i R-CARD M5 (tryck på **F1**).

Gångtestläge upphör automatiskt efter 30 minuter om man inte aktivt återgår till vanlig drift.

Gångtest från MapR 509

1. Logga in med kort och pinkod.
2. Bläddra till **Servicemeny** och bekräfta med #.
3. Bläddra till **Gångtest** och bekräfta med #.
4. Om inga ljudsignaler ska höras i manöverpanelen, välj **Ljudlös**.



Övriga manöverpaneler ljuder. Endast den aktuella manöverpanelen blir tyst.

5. Välj larmområden som ska testas. Gångtest av valda larmområden börjar direkt.
6. Välj **Visa sektioner** för att visa alla sektioner i valda områden. Bekräfta med #.
7. Utför gångtest. Testade punkter försvinner från listan.
8. Avsluta gångtest genom att backa (med X), välja **Avsluta gångtest** och bekräfta med #.

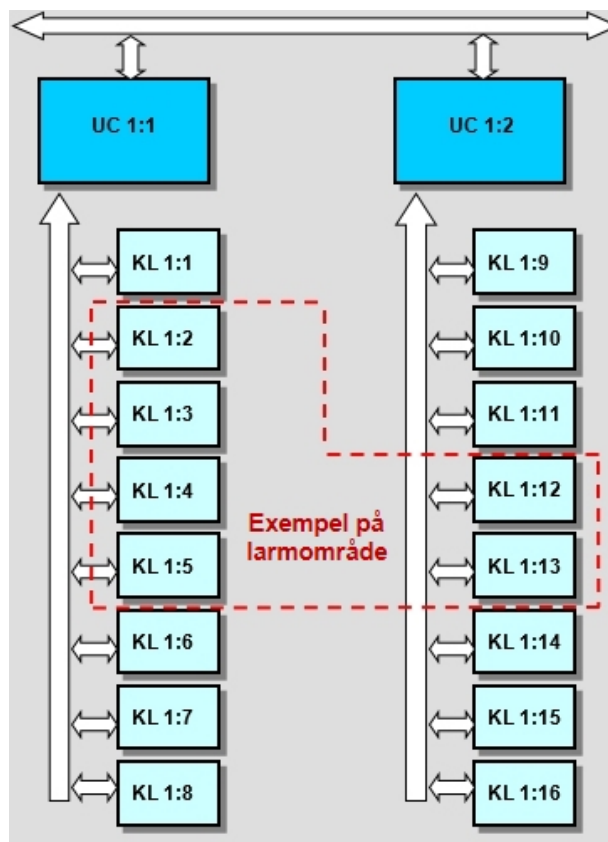
Gångtest från MapR Touch och R-TOUCH 50

1. Logga in med kort och pinkod. (Pinkod kan vara tillräcklig om användarens kort saknar kortnummer [kort-ID] men pinkoden måste då vara unik för användaren.)
2. Välj **Larmområden** och sedan **Frånkoppla**.
3. Välj **Tillbaka**.
4. Välj **Servicemeny**.
5. Välj **Gångtest**.
6. Bläddra ev. till önskat larmområde.
7. Välj **Gångtest** längst ner till vänster.
8. Utför gångtestet.
Sektioner som aktiverats vid test försvinner från listan.
9. För att återgå till vanlig drift, välj **Normalläge**.

Styra externt larm med larmområde

För att slippa dra kabel till samtliga dörrar som ska styra ett externt larm kan man skapa ett larmområde bestående av dessa dörrar. Du väljer gemensamt för larmområdet en utgång för manöversignalen och en ingång för återkopplingssignalen. Kabel dras nu bara från larmets centralapparat till dessa två anslutningar. Du kan välja fritt om pulsad eller latchad styrning ska gälla. De dörrmiljöer som ingår i larmområdet får information om larmstatus via den gemensamma ingången och styr gemensamt utgången.

Vill du istället styra ett externt larm från endast *en* kortläsare där inga andra kortläsare ska påverkas av larmet, se programmets hjälpfunktion för anvisning.



Bra att veta

- Larmområden skapas vid minneskonfigurering av undercentralen. Det finns alltså ingen **Ny**-knapp för larmområden.
- Larmområden konfigureras under **Larm > Larmsystem/Larmområden**.
- Larmområdet kan bestå av enheter från olika undercentraler, men bara på samma anknytning.
- Användning av larmområden reducerar minnesresurserna för *alla* undercentraler på anknytningen.
- Ett larmområde kan inkludera ett annat larmområde eller ingå i ett annat larmområde.

Funktion

De inramade kortläsare kontrollerar ett område som är larmat med extern centralapparat. Man vill kunna slå av och på larmet från vilken som helst av dessa kortläsare.

Man vill också att centralapparatens status ska indikeras i teckenfönstret på områdets alla kortläsare.

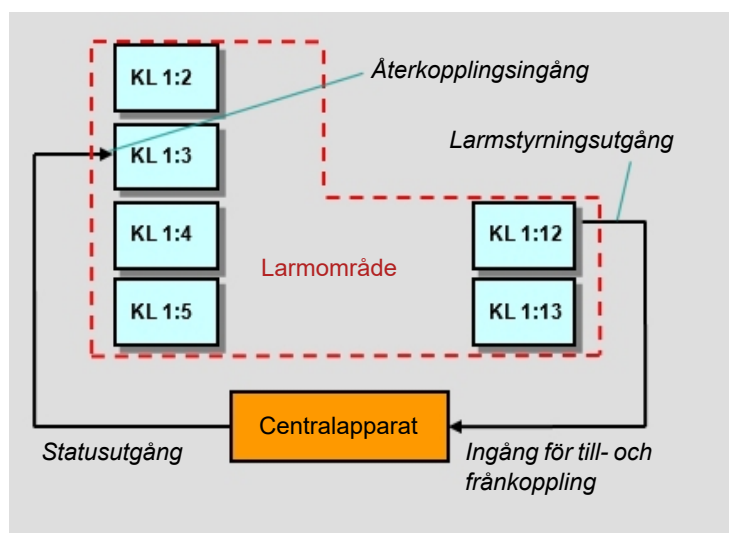
Utförande

1. En utgång på en av kortläsarna konfigureras som områdets larmstyrningsutgång.
2. En ingång på en av larmområdets kortläsare konfigureras som återkopplingsingång för centralapparatens statussignal.

(Det naturliga är givetvis att en och samma enhet både styr larmet och tar emot återkopplingssignalen. Exemplet vill bara visa möjligheterna med områden.)

3. Skapa ett larmområde som består av de inramade kortläsarna.
4. Konfigurera larmområdets och kortläsarnas egenskaper.

Kablar för larmstyrning behöver bara dras till de två plintar som är anslutna till centralapparatens.



I stora drag

Följande steg ska utföras. Alla beskrivs i efterföljande avsnitt.

1. [Konfigurera undercentralens minne för larmområden](#) (se nedan).
2. [Konfigurera ett larmområde](#) (se sidan 103).
3. [Välja in och konfigurera larmområdets kortläsare och ev. larmområden](#) (sidan 107).
4. [Konfigurera återkopplingsingång för centralapparatens status](#) (sidan 109).
5. [Konfigurera larmstyrningsutgång](#) (sidan 110).
6. [Tilldela behörighet att styra larmet](#) (sidan 110).

Konfigurera undercentralens minne för larmområden

1. I R-CARD M5, välj **Enheter > Konfigurera enheter**.
2. Dra–släpp den anknytning där undercentralen finns till **Markerade centraler**.
3. Dubbelklicka på den undercentral som ska "äga" larmområdet. Om de enheter som ska ingå i området är uppdelade på flera undercentraler kan man välja vilken som helst av undercentralerna som "ägare". Dialogrutan **Zonägande** visas.

i Tips: Larmområden förbrukar mest minne i den "ägande" undercentralen. Om någon av centralerna är försedd med TCP/IP-modul, låt den om möjligt vara ägare till området/områden eftersom TCP/IP-modulen bidrar med minne. Minnesutrymme tas från händelsebufferten i första hand.

4. Välj fliken **Larm**, markera **Larmområden** och skriv i antalet önskade larmområden centralen ska kunna hantera.

Markera *inte* **Stöd för integrerat larm**, annars visas alternativ som bara gäller för integrerat larmsystem.

5. Spara med **OK**.
6. Ändra ev. övriga, gemensamma inställningar.

Följden av dina val visas i kolumnerna i det underliggande fönstret.

Nertill finns **Information om minnet** som visar antal valda poster och hur stor minnesdel varje enskild post tar. T.ex. kortens storlek ökar om **Aktivera korttyper med långt kort-ID** markeras i systemets kortinställningar, samt om kortgrupper eller närvaroområden används.

Om en rad visas **rött** räcker undercentralens minne inte till för de valda värdena, som då måste minskas. Obs: Om enheterna har olika mycket minne baseras beräkningarna på den undercentral som har minst minne.

Rosa betyder att undercentralens individuella konfigurationen inte överensstämmer med domänkonfigurationen (dvs de gemensamma inställningarna för alla undercentraler i domänen)

Blått betyder att undercentralen saknar stöd för de tillval som gjorts.

7. Klicka på **Verkställ**.
8. Svara **Ja** på kontrollfrågan samt på frågan om **Överföring allt** ska utföras efter konfigureringen. Överföringen görs i så fall automatiskt.



Om överföring inte görs (automatiskt eller manuellt vid senare tidpunkt) kommer de konfigurerade undercentralerna inte att ha komplett information!

9. *Avvakta klarmeddelandet.* Tiden för minneskonfigureringen varierar och påverkas även av ev. återställning av data.
10. Klicka på **Stäng** för att avsluta konfigureringen.

Konfigurera ett larmområde

Larmområden skapas vid minneskonfigurering av undercentralen. Det finns alltså ingen **Ny**-knapp för larmområden.

Förutsättningar:

- Den undercentral som "äger" larmområdet ska vara minneskonfigurerad för larm och det antal larmområden som ska användas. (Se sidan 33.)
- De dörrmiljöer som ingår i ett larmområde ska under **Lokal larmstyrning** ha inställningarna *avstängda*.

Så här konfigurerar du larmområden för styrning av externt larm:

1. Välj **Larm > Larmsystem/larmområden**.

2. Välj fliken **Larmområde**.

Nu visas ikoner (□) för de larmområden som undercentralen konfigurerats för.

3. Välj larmområde. Larmområdets inställningar visas.

Inställningar Enheter/Ingångar/Utgångar	
Larmområde	
Egenskaper	Inställningar
Benämning	Larmområde 2 UC 1:1
Annan benämning i terminal	
Inkluderande	
Larmstyrning latch/puls (sek.)	Latch 
Varningstid vid automatisk larmtillkoppling (sek.)	Avstängt 
Varningstid vid manuell larmtillkoppling (sek.)	Avstängt ☐ 
Fördrojd återkoppling (sek.)	Avstängt 
☒ Manöver för att växla larmet	
☒ Manöver för larmtillkoppling	
☒ Manöver för larmfrånkoppling	
☐ Direkt/villkorsstyrda larmområden	
Endast tillslag av direktstyrda larmområden	☐

4. Ange önskade inställningar:

Inställning	Beskrivning
Benämning	Ange ett tydligt beskrivande namn, t.ex. Kontoret plan 1.
Annan benämning i terminal	(Ingen funktion i larmområde som styr externt larm.)

Inställning	Beskrivning
Inkluderande	Markera Inkluderande om kortläsare som tillhör flera larmområden ska blockeras när aktuellt larmområde tillkopplas, oavsett läget för övriga larmområden som kortläsarna ligger i. Om Inkluderande är markerat: Samtliga kortläsare i larmområdet blockeras så snart det området är tillkopplat. Rekommenderas. Om Inkluderande <i>inte</i> är markerat (= "exkluderande"): Kortläsare blockeras först då alla larmområden de ligger i är tillkopplade. Exempel: Förråd är beroende av både Kontoret och Butiken. Butiken är <i>inkluderande</i>. Det innebär följande: ◦ När Butiken tillkopplas blir Förråd blockerat för passage, oavsett läget för Kontoret. ◦ När Kontoret tillkopplas men inte Butiken så kan Förråd ändå användas. Det innebär att kortläsaren Förråd skulle kunna användas för <i>passage in i ett larmat område</i>. Om Butiken hade varit <i>exkluderande</i> (Inkluderade inte markerat) så hade Förråd blockerats först när Butiken <i>och</i> Kontoret tillkopplats.  Kräver att Direkt till- och frånkoppling av larmområde markerats för kortläsaren/sektionen på fliken Enheter/Ingångar/Utgångar.

Inställning	Beskrivning
Larmstyrning latch/puls (sek)	Välj hur larmstyrningen (utgångsegenskap Larmstyrning (Puls/Latch)) ska fungera: ◦ Latch: Bistabil styrsignal. Återkoppling är inget krav men rekommenderas. Utgången växlar vid tillkoppling av larmområdet och ligger kvar i samma läge tills larmområdet fränkopplas. ◦ Pulstid: Monostabil styrsignal. Måste väljas om flera delningsboxar ska styra samma larmområde. Kräver återkoppling från larmsystemet. Väljer du Pulstid så ändras rullgardinsmenyn till ett inmatningsfält. Ange pulslängden i sekunder. Utgången drar under inställd tid vid larmstyrningsmanöver och återgår sedan.
Varningstid vid automatisk larmtillkoppling (sek)	Förvarningstid vid larmtillkoppling. Ange hur många sekunder summern ska ljuda vid automatisk resp. manuell tillkoppling.
Varningstid vid manuell larmtillkoppling (sek)	 Enheter som ska ge förvarning ska ha Aktivera larmvarning markerad. Larmområdet har utgångsegenskap Varning vid larmtillkoppling som kan kopplas till valfri utgång. Se "Ge varning och status från larmområdet via en utgång" i programmets hjälpfunktion.

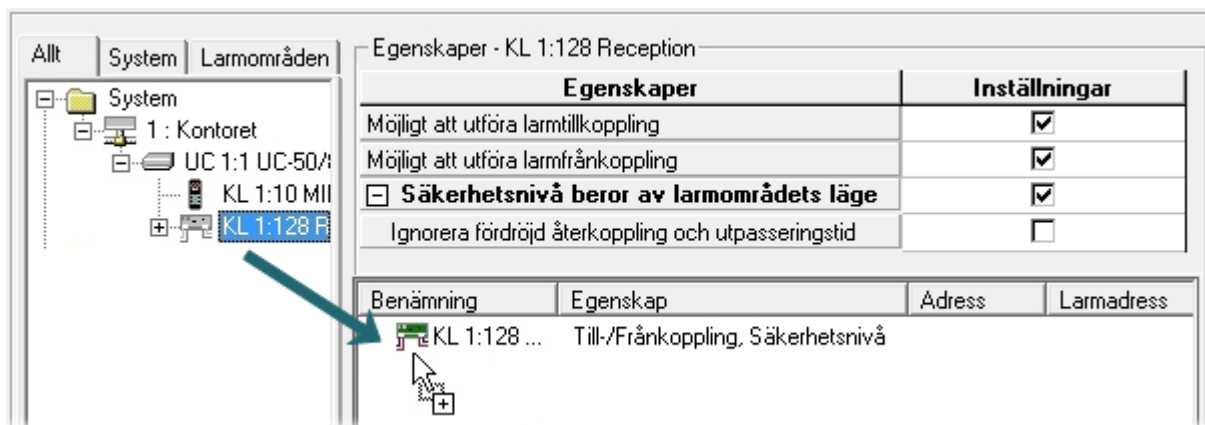
Inställning	Beskrivning
Fördröjd återkoppling (sek)	Antalet sekunder som avkänningen av återkopplings-signalen fördröjs (på larmområdets återkopplingsingång). Exempel: Ett kontorsområde tillkopplas från en kort-läsare inom området. Normalt fungerar inte Knappöppning 1 efter tillkoppling. Sätts Fördröjd återkoppling till 30 sekunder så hinner man ut via knappöppningen trots att undercentralen anser att larmet är tillkopplat. Används om man utnyttjar centralapparatens egen inbyggda varningstid vid tillkoppling. Vissa centralapparater signalerar redan under förvarningstiden att larmet är tillkopplat. Det gör att passersystemet spärrar passage under förvarningen. Åtgärda problemet med fördröjd avläsning av återkopplingssignalen. Återkopplingssignalen från centralapparaten avläses då inte förrän efter det antal sekunder som anges här. Antalet sekunder måste vara minst lika många som centralapparatens egen varningstid. Fungerar i latch-läge och utan återkoppling. (Latchens läge kopplas internt till återkopplingen, som därmed också kan fördröjas om detta är valt.) Gäller bara vid larmtillkoppling.
Manöver för att växla / tillkoppla / frånkoppla larmet	Behövs om någon av larmområdets enheter ingår i flera larmområden. Se "Anpassa larmmanövrering" i programmets hjälpfunktion.
Direkt/villkorsstyrda områden > Endast tillkoppling av direktstyrda larmområden	När det aktuella larmområdet tillkopplas så tillkopplas även larmområden som ingår i det. Exempel: När Kontoret tillkopplas så tillkopplas även Förråd och HR. (Frånkoppling tillåts inte.)



5. Klicka på **Spara** (💾).

Välja in och konfigurera larmområdets kortläsare och ev. larmområden

1. Välj fliken **Enheter/Ingångar/Utgångar**.
2. I vänster ruta, välj fliken **System**.
3. Dra–släpp de enheter som ska ingå i larmområdet från trädet till nedre delen av högerutrymmet. Exempel:



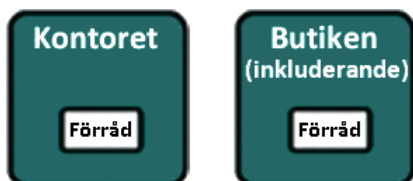
4. Ange önskade inställningar för varje enhet:

Inställning	Beskrivning
Möjligt att utföra larmtillkoppling	Välj om det ska vara möjligt att tillkoppla resp. frånkoppla larmet på vald enhet.
Möjligt att utföra larmfrånkoppling	
Säkerhetsnivå beror av larmområdets läge	Normalt styrs dörrens säkerhetsnivå (passermöjlighet) av återkopplingssignalen som är ansluten till dörrmiljön. Med detta alternativ styrs passermöjligheten istället av larmområdets återkopplingsstatus.
Ignorera fördröjd återkoppling och utpasseringstid	Om ett larmområde har flera dörrar som är anslutna till centralapparatens statusutgång kan du välja att låta en eller flera dörrar ignorera den fördröjning som ställs in i larmområdets inställning Fördröjd återkoppling . Denna eller dessa dörrar spärrar då omedelbart passage vid tillkoppling av larmet.

5. Om någon av larmområdets kortläsare ingår i flera områden blir kortläsaren som standard blockerad för passage först då alla områden den ligger i är tillkopplade.

Om däremot något av områden den ligger i är *inkluderande* så blockeras alla kortläsarna i det larmområdet då det tillkopplas, oavsett lägen för övriga larmområden som kortläsaren tillhör.

Exempel:



Förråd är beroende av både Kontoret och Butiken.

Butiken är *inkluderande*. Det innebär följande:

- När Butiken tillkopplas blir Förråd blockerat för passage, oavsett läget för Kontoret.
- När Kontoret tillkopplas men inte Butiken så kan Förråd ändå användas. Det innebär att kortläsaren Förråd skulle kunna användas för *passage in i ett larmat område*.

Om Butiken hade varit *exkluderande* (**Inkluderade** inte markerat) så hade Förråd blockerats först när Butiken och Kontoret tillkopplats.

Gör så här om det aktuella larmområdet ska vara *inkluderande*:

- a. Välj fliken **Inställningar**.
 - b. Markera **Inkluderande**.
 - c. Klicka på **Spara** (💾).
6. Välj in eventuella *larmområden* som ska ingå i det aktuella larmområdet.
 7. Ange hur det inkluderade larmområdet ska styras:

Markera **Direkt till- och frånkoppling av larmområde** om det invalda larmområdet ska följa det område som det ligger i.

Om endast tillkoppling ska direktstyras:

- a. Välj fliken **Inställningar**.
- b. Klicka på plustecknet (+) vid **Direkt/villkorsstyrda områden**.

- c. Markera **Endast tillkoppling av direktstyrda larmområden**. Nu gäller:

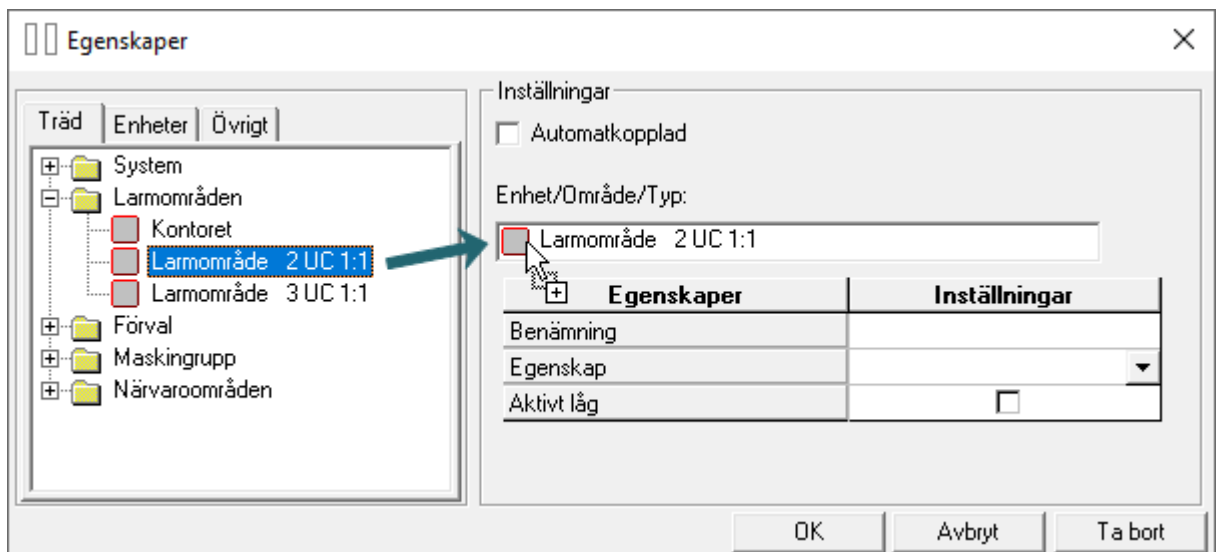
När det aktuella larmområdet tillkopplas så tillkopplas även larmområden som ingår i det. Exempel: När Kontoret tillkopplas så tillkopplas även Förråd och HR. (Frånkoppling tillåts inte.)



8. Klicka på **Spara** (ikon).

Konfigurera återkopplingsingång för centralapparatens status

1. Välj **Enheter > Systemenheter**.
2. Välj den enhet som ska kopplas till centralapparatens statusutgång för att känna av om larmet är till- eller frånkopplat. Enhetens egenskaper visas.
3. Välj fliken **Ingångar/Utgångar**.
4. Under **Ingångar**, dubbelklicka på den ingång som ska vara avkänningsingång – på DB-50 exempelvis **23–24 Återkoppling**. Dialogrutan **Egenskaper** visas.
5. Eftersom det är återkopplingsfunktionen i larmområdet som ska påverkas av larmstatus, expandera mappen **Larmområden** i vänster rutan. Dra aktuellt larmområde och släpp det på **Enhet/Område/Typ**.



6. Välj egenskapen **Återkoppling** från centralapparat i rullgardinslistan.
7. Avsluta med **OK**.
8. Klicka på **Spara** (ikon).

Konfigurera larmstyrningsutgång



Det naturliga är givetvis att en och samma enhet både styr larmet och tar emot återkopplingssignalen.

1. Välj **Enheter > Systemenheter**.
2. Välj den enhet som ska kopplas till centralapparatens styringång för att koppla från larmsektionen. Enhetens egenskaper visas.
3. Välj fliken **Ingångar/Utgångar**.
4. Dubbelklicka på önskad utgång. Dialogrutan **Egenskaper** visas.
5. Eftersom det är larmstyrningsfunktionen i larmområdet som ska påverka centralapparaten, expandera mappen **Larmområden** i vänster rutan.
6. Dra aktuellt larmområde och släpp det på **Enhet/Område/Typ**.
7. Välj **Larmstyrning (Puls/Latch)** i rullgardinslistan.
8. I förekommande fall: Välj **Aktivt låg (NC)**.
9. Avsluta med **OK**.
10. Klicka på **Spara** (💾).

Nu kan du göra eventuella inställningar på enheterna, t.ex. **Konstant larmdiod**.

Inställningarna under **Lokal larmstyrning** ska vara *avstängda*.

Tilldela behörighet att styra larmet

1. Lägg in larmområdet i behörighetsgrupper.
2. Markera **Larmtillkoppling** och/eller **Larmfrånkoppling** i behörighetsgruppen för att medge larmstyrning.
3. Tilldela alla användare som ska kunna styra larmområdet ovanstående behörighetsgrupp.



Tips: Utförliga instruktioner ges i programmets hjälpfunktion. Tryck på **F1** inifrån programmet.

Konfigurera porttelefonsystem

Översikt och förutsättningar

RCO:s porttelefonsystem är helt integrerad i R-CARD 5000 hårdvara och R-CARD M5. Porttelefoner installeras vid varje port. Se manualen [R-CARD 5000 – Installera](#). Ingen separat licens krävs.

Varje porttelefon upptar en dörrplats i undercentralen. Varje porttelefon har en ingång för öppn knapp och en utgång för låsöppning.

Förutsättningar

- Linjekort TEL-50 version 2.09.
- PA-519: R-CARD M5 version 5.40.4. (Version 5.40.5 eller senare rekommenderas.)
- Porttelefon är aktiverad (se sidan [14](#)).
- Anknytningen är spänningssatt och hämtad så att enheterna är åtkomliga för konfigurering.

I stora drag

Följande steg ska utföras. Alla beskrivs i efterföljande avsnitt.

1. [Konfigurera linjekort TEL-50](#) (se nedan).
2. [Konfigurera porttelefoner](#) (se sidan [114](#)).
3. [Definiera åtkomst till porttelefoner](#) (se sidan [118](#)).
4. [Lägga in telefonkort](#) (se sidan [120](#)).
5. Valfritt: [Konfigurera portregister](#) (se sidan [117](#)).

Konfigurera linjekort TEL-50

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Välj det linjekort som ska konfigureras.
3. Ge linjekortet en **Benämning**.

Allmänt Ingångar/Utgångar	
Egenskaper	Inställningar
Benämning	TEL-50 Strandgatan
Typ	TEL-50 G, Version 2.09F
Enhetsnummer	34
Pos	TEL 1:34
Riktnummerområde	
Prefix för externa telefonnummer	
Samtalstid för att ange manuellt ID	Avstängt ▼
Kortast tid DTMF	Standardinställning ▼
Lås upp dörrar efter 2 ringsignaler	☒
Tillfällig kod efter 4 ringsignaler	☒
Polväxling på telelinje	☐
Porttelefoner	...
Fri text	

4. Ange önskade inställningar:

Inställning	Beskrivning
Riktnummer-område	Området där anläggningen är belägen, t.ex. 08 för Stockholmsområdet. Riktnumret gäller hela domänen. <i>Om flera riktnummer ingår måste flera domäner användas.</i> Om flera linjekort TEL-50 ingår i domänen räcker det att ange riktnummer för ett av korten. De övriga linjekorten får automatiskt samma riktnummer. Även nya telefonkort får riktnumret automatiskt.
Prefix för externa telefonnummer	Anger den eller de siffror som ska användas för att komma ut på linjen, exempelvis om uppringning sker via en företagsväxel. Bara kort med Externt telefonnummer markerat påverkas. (Se sidan 121.) Kan också användas för att ge styrkoder för uppringningsfunktionen: ◦ W betyder "Vänta på kopplingston i max. 2 sekunder. Avbryt därefter om ton uteblir." ◦ Kommatecken (,) betyder "Vänta två sekunder". Uppringningen fortsätter sedan oavsett om ton har uppfattats eller ej. Exempel: 0W12121234 betyder "Slå 0 för linje. Vänta på ton i max. två sekunder. Slå abonnentnumret."
Kortast tid för DTMF	Välj mellan Standardtid och 65, 80 eller 100 millisekunder. Detta värde kan behöva justeras beroende av svarsapparatens tonlängd vid porttelefonöppning. Ska inte vara längre än telefonens tonlängd.
Polväxling på telelinje	Polväxling används för att avgöra om och när telefonluren lyfts. Vissa telefonväxlar och IP-baserade telefoner använder inte polväxling. Det gäller även teleanslutning via så kallade ATA-boxar. Vanligast är att polväxling inte finns på telelinje, allra helst om det är ATA box alternativ analog linje telefonväxel. Funktionen blir något olika beroende på om polväxling används. Tryck på F1 för mer information.

Inställning	Beskrivning
Porttelefoner	Knyter samman porttelefoner och linjekort. Klicka på dialogöppnaren (...). Dialogrutan Välja enheter visas. Porttelefoner som sitter på samma anknytning som linjekortet visas under Alla enheter. Dra–släpp önskade porttelefoner från listan till Valda enheter. Klicka på OK.
Fri text	Plats för egna noteringar om t.ex. utförd service. Texten visas ingen annanstans än i denna dialogruta.

5. Klicka på **Spara** (💾).

Konfigurera porttelefoner

i **Tips:** Mikrofonens förstärkning kan sänkas m.h.a. två DIP-omkopplare på porttelefonens kretskort (från revision F). Det kan vara till hjälp i bullriga miljöer. För mer information se manualen [R-CARD 5000 – Installera](#).

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Klicka på plustecknet (+) vid anknytningen och markera aktuell porttelefon.

i I fältet **Enhetsnummer** visas "(Terminerad)" eller "(Ej terminerad)" beroende på tillstånd vid senaste hämtningen. (Uppdateras f.n. inte i realtid.)

3. Rekommendation: Ange en beskrivande **Benämning** (portens namn, gatuadress, etc.).
4. Under **Språk**, välj standardspråk för enheten. Alternativt, välj **Samma som serverns operativsystem** för att följa operativsystemets språk.
5. Under **Telefoni** finns ett antal speciella egenskaper för porttelefoner:

Inställning	Beskrivning
Antal ringsignaler	Maximalt antal ringsignaler som går fram innan systemet anser att inget svar fås. Besökaren behöver alltså inte tänka på att själv avbryta uppringningsförsöket. 2–30 eller obegränsat antal. Alternativet visas bara om det TEL-50-kort som är knutet till porttelefonen har Polväxling på telelinje markerad (ej standard).
Samtalstid vid uppringning till hyresgäst	Hur långt ett samtal får vara. Upp till 255 sekunder eller obegränsat. Fr.o.m UC-50 version 2.84 så blir "obegränsad" samtalstid lika med 255 sekunder. Valet Obegränsat visas då inte längre. Det visas endast om det var valt och sparat från tidigare version. Valet Obegränsat visas inte heller om det TEL-50-kort som är knutet till porttelefonen <i>inte</i> har Polväxling på telelinje markerad. Samtalstiden kommer då att räknas från första ringsignalen.
Låsöppningstangent från telefon	Den siffra hyresgästen ska trycka på sin telefon för att öppna porten. Möjliga värden: #, 0–9 eller Avstängt. Obs: Funktionen måste aktiveras i behörighetsgruppen. Se sidan 119.
Kopplad mot TEL-50	Välj det linjekort som ansluter till den publika telefonlinjen. Om du vid programmering av linjekortet (TEL-50) redan har definierat vilka porttelefoner som hör ihop med linjekortet (se Porttelefoner på sidan 114) behöver du inte göra något här. (TEL-50-kortet som är valt visas i detta fält.)
Volym porttelefon	Om tendenser till akustisk återkoppling (rundgång) finns kan enhetens funktion påverkas negativt. För att bli av med rundgången, minska Volym porttelefon under Telefoni i porttelefonens egenskaper. Välj ett värde mellan Avstängd (0) och Högst (15). Standardvärdet är 10.

6. Även under **Registerhantering** finns speciella egenskaper för porttelefoner:

Inställning	Beskrivning
Fältkopplingar	Om portregister önskas, ange vad som ska visas i portregistret ("fältkopplingar"). Tryck på F1 för att öppna online-hjälpen med detaljerade instruktioner. Se även " Konfigurera portregister " på sidan 117.
Infotext	Infotexten visas när enheten inte används. Det kan t.ex. vara en välkomsttext eller portens benämning eller gatunummer.

7. Om TELE-dioden ska visa larmsystemets status i stället för telelinjens status: Klicka på plustecknet (+) vid **Indikeringar** och markera **TELE-diod används för larmlägesindikering**.
8. Ange övriga egenskaper som för vanliga enheter (se sidan 49):
- **Dörrmiljö**
 - **Lokal larmstyrning** (se programmets hjälpfunktion).
 - **Dörrmiljö lokal larmstyrning/larmområden**
 - **Summalarm**
9. Ange följande under **Övrigt**:
- **Bakgrundsljus vid tänt fönster**
 - **Bakgrundsljus vid släckt fönster**
 - **Tid innan fönster släcks (sek)**

Övriga inställningar under **Övrigt** är som för vanliga enheter. Tryck på **F1** för mer information.

10. På fliken **Ingångar/Utgångar** kan du se hur in- och utgångarna är kopplade i likhet med t.ex. en in/utenhet. Se "[Gör så här för att konfigurera in- och utgångar, exempelvis på en delningsbox:](#)" på sidan 51.
11. Klicka på **Spara** (💾).
12. Vid behov, överför data till enheterna genom att klicka på **Överför till enhet** (📶). (I vanliga fall sker överföring automatiskt.)

Konfigurera portregister

Översättning på gång. Portregister (boendeförteckning, trappregister) kan visas i porttelefoner med display samt i bokningstavlor. Portregister konfigureras enligt nedan.

 **Tips:** Se "Visa portregister (boendeförteckning): Översikt" i programmet's hjälpfunktion.

Ange våningsbenämningar

Observera:

- **Viktigt:** Våningsbenämningarna presenteras i samma ordning i enheterna som du ser dem i R-CARD M5. Ändring i efterhand av den inbördes ordningen mellan våningsbenämningarna eller antalet våningar i tabellen innebär mycket arbete. Tänk därför igenom hur många våningar som maximalt ska ingå och se till att det finns en rad per våning i tabellen. *Våningsbenämningar för samtliga våningar i alla trappuppgångar läggs i samma tabell.*
- Flera användare/lägenheter kan knytas till en våning.
- Bara våningar som har knutits till minst en användare/lägenhet visas i portregistret.

Gör så här:

1. Välj **Inställningar > Våningsbenämningar**.
2. För varje våning, lägg in en benämning eller ett våningsnummer (max. 8 tecken).
3. Klicka på **Spara**.
4. Klicka på **Exportera** för att skicka benämningarna till berörda enheter ("registerenheter"). Dialogrutan **Urval registerenheter** visas.
5. Dra–släpp önskade enheter från **Tillgängliga registerenheter** till **Valda registerenheter**.
Bara enheter som kan hantera våningsregistret visas.
6. Klicka på **OK**.
7. Spara och stäng.

Fylla i uppgifter i användardata/lägenhetsdata och kortdata

Portregistret "skapas" när du kopplar våningar till användare eller lägenheter. Detta kan göras när som helst under driftsättningen:

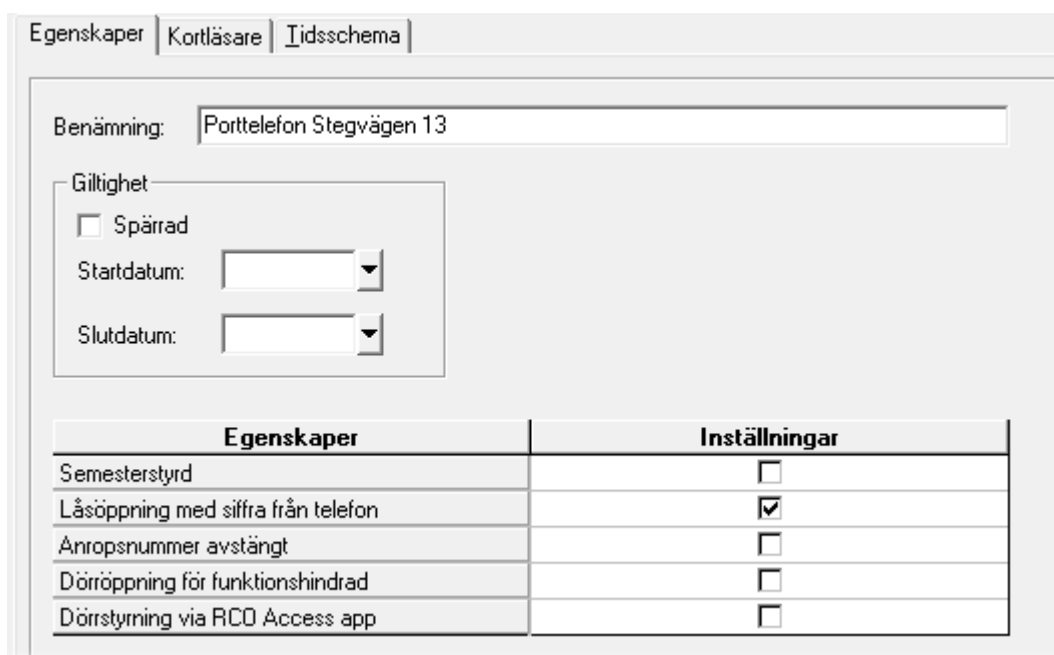
- I användarnas/lägenheternas egenskaper, välj fliken **Användare** och välj våning under **Portregister**.
- I användarens/lägenhetens telefonkort, se till att markera **Visa i portregister** (se sidan 121) samt fylla i alla fält som angetts för visning i portregistret (se **Fältkopplingar** på sidan 116).

Definiera åtkomst till porttelefoner

Behörighetsgruppen bestämmer vilka boenden man kan ringa upp från en porttelefon. Den uppringande porttelefonen kommer att öppna när den boende trycker på låsöppningssiffran på sin telefon.

 **Inställningar med stjärna (*)** här nedan finns även för individuella kort. Anges ett annat värde när man lägger in kort så åsidosätts behörighetsgruppens värde.

1. Välj **Huvudmeny > Behörigheter**.
2. Högerklicka på en fri yta i behörighetslistan och välj **Ny porttelefonsbehörighet**.
I ett domänsystem, välj även den domän med de enheter som ska ingå i behörighetsgruppen.
3. Ange ett beskrivande namn i fältet **Benämning**.



Egenskaper	Inställningar
Semesterstyrd	☐
Låsöppning med sifra från telefon	☒
Anropsnummer avstängt	☐
Dörröppning för funktionshindrad	☐
Dörrstyrning via RCO Access app	☐

4. Ange **Giltighet**.*
5. Ange övriga *egenskaper*:

Inställning	Beskrivning
Semesterstyrd*	Spärrar behörigheten under semesterperioden. (Semesterperioden bestäms domänvis i årskalendern.)
Låsöppning med siffra från telefon	Den boende kan öppna porten från sin telefon. Siffran som ska användas för låsöppning anges i fältet Låsöppningstangent från telefon i porttelefonens inställningar. (Se sidan 115.)
Anropsnummer avstängt	Blockerar så att uppringning inte kan ske med anropsnummer utan hela abonnentnumret måste slås på porttelefonen. Rekommendation: Använd antingen telefonnummer <i>eller</i> anropsnummer i systemet. Risk finns annars att ett anropsnumret rings upp istället för det telefonnummer man tänkte ringa upp. Orsaken är att uppringning görs så snart man knappat in ett nummer som motsvarar ett anropsnummer. Se exempel på sidan 121.  Tips: Liknande funktion kan uppnås med hjälp av funktionen Anropsnummer avstängt .
Dörröppning för funktionshindrad*	Gäller endast dörrar som har dörrautomatik. Ger utökad öppningstid. Tiden anges i dörrinställningarna.
Styrning från integrationer	Ger möjlighet att öppna dörrar m.h.a. mobilapplikationen RCO Access. Inställningen visas endast om lämpliga licenser har registrerats eller program aktiverats.

6. Välj fliken **Kortläsare** och lägg nu in de porttelefoner som ska vara åtkomliga.
Dra–släpp porttelefoner från listan/trädet till behörighetens förteckning.
7. Välj fliken **Tidsschema** och ange när behörigheterna ska gälla. (För instruktioner se sidan 129.)
8. Klicka på **Spara** .

Nu kan du koppla behörighetsgruppen till kort.

Lägga in telefonkort

Ett *telefonkort* är ett virtuellt "kort" som har inställningar för telefonnummer och anropsnummer i stället för kortnummer.

Du lägger in ett telefonkort för varje användare/boende som ska kunna öppna porten via sin telefon.

Användardata förutsätts vara inlagt tidigare. Instruktioner ges t.ex. under "[Lägga in en användare eller lägenhet med ett passerkort](#)" på [sidan 136](#). Förvaltning av passerkort beskrivs i detalj i programmets hjälpfunktion. Här ges bara kortfattade instruktioner med egenskaper specifika för telefonkort.

1. Välj **Huvudmeny > Användare**.
2. Högerklicka på den användare/lägenhet som ska ha kortet och välj **Nytt kort > Telefonkort**.
3. Ange önskade inställningar:

Funktion	Inställning
Spärrat	☐
Visa i portregister	☒
Extern telefonnummer	☐

Portregister

Efternamn

Förnamn

Behörigheter

Porttelefon Stegvägen 13

Benämning	Larm till	Larm från

Inställning	Beskrivning
Telefonnummer Anropsnummer	I fältet Telefonnummer, ange lägenhetsinnehavarens telefonnummer. Alternativt, i fältet Anropsnummer, ange 1–6 siffror som kan användas istället för telefonnumret vid anrop till boende från en porttelefon. Rekommendation: Använd antingen telefonnummer <i>eller</i> anropsnummer i systemet. Risk finns annars att ett anropsnumret rings upp istället för det telefonnummer man tänkte ringa upp. Orsaken är att uppringning görs så snart man knappat in ett nummer som motsvarar ett anropsnummer. Exempel: Om ett av anropsnumren är 123 får det inte också finnas telefonnummer som börjar på 123, t.ex. 1230087. Anropsnummer 123 kommer att ringas upp så snart man har knappat in de första tre siffrorna i telefonnummer 1230087. Om båda nummertyperna ska användas bör alla anropsnummer börja med 00.
Visa i portregister	Visar namnuppgift i portregister/boendeförteckning. Villkor för visning: - Porttelefonen eller bokningstavlan ingår i kortets behörighetsgrupp. (Se Kortläsare/Områden på sidan 136.) - Det måste även anges vad som ska visas i portregistret/boendeförteckningen. (Se Fältkopplingar på sidan 116.) Beroende på hur fältkopplingarna ser ut visas t.ex. Efternamn och Förnamn i inställningarna här, och du får ange vad som ska visas i displayen.
Externt telefonnummer	Markera om uppringning sker via växel. Värdet i Prefix för externa telefonnummer i TEL-50-kortets egenskaper (se sidan 112) slås före telefonnumret vid uppringning.

4. Dra–släpp den eller de behörigheter som kortet ska ha från listan **Behörigheter** till kortets behörigheter. Endast behörigheter för porttelefon visas.
5. Klicka på **Spara** (📁).

Styra hissar

I varje hisskorg finns en *hissläsare* (vanligen en Reader-50) där användaren identifierar sig. Undercentralen aktiverar då under inställbar tid (**Styrtid**) via en eller flera in/utenheter de våningsknappar som motsvarar användarens behörighetsgrupp. Utgångarna på IO-50 styr varsin våningsknapp.

Hissläsaren använder ingen egen utgång på IO-50, men upptar en dörrplats i undercentralen.

Alla hissar anses ha samma antal våningar. Varje våningsplan är gemensamt för alla hissar som styrs av samma undercentral. Det innebär att om en användare har behörighet att åka till t.ex. våning 5 så kan denne åka till våning 5 i alla hissar som styrs av denna undercentral.

Förutsättning: AHC är aktiverat (leveransläge).

 **Tips:** I onlinehjälp finns ett utförligt exempel på hisstyrning, inkl. adressering av enheter och våningar. Tryck på **F1** och sök på "Exempel på hisstyrning".

I stora drag

Följande steg ska utföras. Alla beskrivs i efterföljande avsnitt.

1. Installera hissläsare och in/utenheter (se nedan).
2. [Konfigurera undercentral för hisstyrning](#) (se sidan 123).
3. [Knyta våningar till utgångar på IO-50](#) (se sidan 125).
4. [Konfigurera dörrfunktioner till hissläsare och våningsplan](#) (se sidan 126).
5. [Behörighet i hissar](#) (se sidan 127).
6. [Verifiera hissarnas funktion i systemet](#) (se sidan 128).

Installera hissläsare och in/utenheter

Om man vill ha olika behörighet till våningsplanen i olika hissar behöver man skapa unika hisstyrningar. Maximalt antal unika hisstyrningar på en undercentral är **64 / antal dörrmiljöer på undercentralen**.

1. Gör undercentralen strömlös.
2. Installera en "Reader-50" som hissläsare i hisskorgen. Det behövs bara en hissläsare per hiss, oavsett antal våningar i hisschaktet.
3. Installera erforderligt antal in/utenheter (max. 8 våningar per in/utenhet).

Bygga utgångarna för den typ av anslutning som används till hissknapparna.
(Använd helst mellanrelä för att isolera systemen.)

Anslutningen till hissautomatiken görs i samråd med hissleverantören.

Det behövs minst en in/utenhet per hiss. Varje utgång på enheten motsvarar en våning.

- Utgångarna på IO-50 består av halvledarreläer, som endast är avsedda för svagströmsapplikationer.
- För anslutning till hisselektroniken, använd potentialfri NO eller matande utgång *med mellanrelä*.



Använd inte matande utgång utan mellanrelä. Då kommer passersystemet att sammankopplas elektriskt med hissens elektronik.

- Om utgångarna styr induktiv last (t.ex. mellanreläer) måste skyddsdiод anslutas på reläspolarna precis som när man ansluter elslutbleck.



Se data för IO-50 i manualen *R-CARD 5000 – Installera*.

4. Spänningssätt undercentralen.

Konfigurera undercentral för hisstyrning

En undercentral för hisskontroll kan anslutas på en befintlig anknytning tillsammans med andra undercentraler.

Undercentraler kan kontrollera hissar i kombination med både virtuella enheter och vanliga dörrmiljöer. Rekommendationen är dock att *inte blanda vanliga dörrmiljöer med hisstyrning i en undercentral*.

Summan av antalet virtuella enheter, vanliga dörrmiljöer och hissläsare kan inte överstiga undercentralens maximala antal dörrar (2, 4 eller 8 dörrar beroende på UC-variant). En undercentral kan alltså inte kontrollera fler hissläsare än det maximala antalet dörrmiljöer den kan hantera. (Maximalt antal våningsknappar är alltid 64.)

1. I R-CARD M5, välj **Enheter > Systemenheter**.
2. Markera den undercentral som ska sköta hisskontrollen.
3. Klicka på plustecknet (+) vid **Hissenheter** och ange önskade inställningar:

Inställning	Beskrivning										
Antal hissenheter	Ange hur många våningsknappar som undercentralen ska kontrollera (max. 64). Våningar i hisstyrningen använder en annan typ av plats på undercentralen. Finns det bara en kortläsare kan man ha upp till 64 våningar på undercentralen. Har man två kortläsare halveras antalet våningsplatser. Har man fyra kortläsare ryms bara 16 våningsplatser. Detta för att antalet dörrmiljöer anslutna på lokalbussen (även ev. DB-50) <i>antas vara antalet hissar</i>. Produkten av antalet hissar och antalet våningsknappar får alltså inte överstiga 64, oavsett om det är en 2-, 4- eller 8-dörrars undercentral som används. Några kombinationer, avseende en 8-dörrars undercentral: <table> <tr> <th>Antal hisschakt (=hissläsare)</th><th>Max. antal våningar</th></tr> <tr> <td>1</td><td>64/1 = 64</td></tr> <tr> <td>2</td><td>64/2 = 32</td></tr> <tr> <td>4</td><td>64/4 = 16</td></tr> <tr> <td>8</td><td>64/8 = 8</td></tr> </table>	Antal hisschakt (=hissläsare)	Max. antal våningar	1	64/1 = 64	2	64/2 = 32	4	64/4 = 16	8	64/8 = 8
Antal hisschakt (=hissläsare)	Max. antal våningar										
1	64/1 = 64										
2	64/2 = 32										
4	64/4 = 16										
8	64/8 = 8										
Startadress (första hissenhet)	Våningsknapparna räknas adressmässigt som dörrmiljö. Ange första våningsknappens adress. Hisskontrollen kommer att uppta startadressen + antal våningsknappar - 1. Exempel: Om startadress är 100 och antalet våningsknappar är 8 kommer adresserna 100–107 att användas för hisskontrollen.  Adresserna för virtuella enheter, hissenheter och befintliga dörrmiljöer får inte kollidera med varandra.										
Styrtid	Hur många sekunder våningsknapparna ska hållas aktiva vid godkänd "passage".										

- Klicka på **Spara** .
- Gör nu en hämtning. **Sök enheter på lokala bussar** ska markeras. (Hämtning beskrivs på sidan [23](#).)

Knyta våningar till utgångar på IO-50

Gör manuella kopplingar mellan IO-utgångarna och hissenheterna. Utgångarna på IO-50 styr varsin våningsknapp. En in/utenhet kan delas mellan flera hissar.

Hissläsaren använder ingen egen utgång på IO-50, men upptar en dörrplats i undercentralen.

Alla hissar anses ha samma antal våningar. Varje våningsplan är gemensamt för alla hissar som styrs av samma undercentral. Det innebär att om en användare har behörighet att åka till t.ex. våning 5 så kan denne åka till våning 5 i alla hissar som styrs av denna undercentral.

1. Välj **Enheter > Systemenheter**.
2. Markera den in/utenhet som ska styra våningsknapparna.
3. Välj fliken **Ingångar/Utgångar**.
4. Dubbelklicka på en utgång som ska anslutas till en våningsknapp.
5. Dra–släpp den kortläsare som ska vara hissläsare från trädet till rutan **Enhet/Zon**.
6. Under **Egenskap**, välj vilken våning utgången ska styra.



Egenskaperna **Våningsstyrning 1** osv finns inte förrän man har hämtat anknytningen *efter* inställning av hissparametrarna i undercentralen (se ovan).

7. Spara med **OK**.
8. Upprepa steg 4-6 för varje våning. Om det finns fler våningar än utgångar på in/utenheten, upprepa från steg 2 med nästa in/utenhet men samma hissläsare.
9. Upprepa från steg 2 med nästa hissläsare och nästa in/utenhet.

Konfigurera dörrfunktioner till hissläsare och våningsplan

För att kortinnehavare ska kunna använda en våningsknapp måste de först godkännas i hissläsaren. Det sker enligt den funktion som är aktiv i kortläsaren.

Enheter som styrs av en hisscentral kan använda maximalt 4 av dörrmiljöns funktioner.

Följande funktioner kan användas både i hissläsare och för våningsplanen:

- **Dörr olåst** (*använd aldrig på hissläsaren, utan endast på våningsplan!*)
- **Dörr blockerad**
- **Enbart pinkod**
- **Enbart kort**
- **Kort & pinkod** (gäller om ingen annan funktion är konfigurerad)

Övriga funktioner ignoreras.

Tänkbara funktionskombinationer för hissläsare och våningsplan

Funktion i hissläsare	Funktion på våningsplan	Resultat
Ingen funktion aktiv eller Enbart kort, Enbart pinkod, Kort & pinkod	Ingen funktion aktiv	Kortinnehavaren måste vara godkänd både i hissläsaren och till våningen.
Oavsett funktion (utom Dörr olåst)	Dörr blockerad	Våningsknappen avstängd.
Dörr blockerad	Alla (utom Dörr olåst)	Alla våningsknappar avstängda.
Oavsett funktion (utom Dörr olåst)	Dörr olåst	Våningsknappen aktiverad.

För steg-för-steg-instruktioner se "[Allmänt](#)" på sidan 54.

Ge tillträde till våningsplan utan kortläsning



Använd aldrig funktionen **Dörr olåst** på hissläsaren, utan endast på våningsplan ("hissvåningar" i gränssnittet)!

Så här gör du hissknappar tillgängliga utan att kortläsaren i hissen behöver användas:

1. Skapa en behörighetsgrupp för ändamålet.
 - När du väljer användningsområde, välj **Funktioner**.
 - På fliken **Kortläsare/Områden**, lägg in de "hissvåningar" som ska vara åtkomliga.
 - Ange i tidsschemat när tillträde utan kortläsning ska gälla.

Spara.

2. Under **Huvudmeny > Funktioner**, koppla funktionen **Dörr olåst** till behörighetsgruppen.

Spärra hissknappar

Använd samma metod som ovan, men koppla funktionen **Dörr blockerad** till behörighetsgruppen.

Behörighet i hissar

Hissvåningar läggs in i behörighetsgrupperna precis som vanliga kortläsare.

Gör så här för att komplettera befintliga behörigheter med hissvåningar:

1. Välj **Huvudmeny > Behörigheter**.
2. Markera aktuell behörighetsgrupp.
3. Välj fliken **Kortläsare/Områden** och lägg nu in de hissvåningar som ska vara åtkomliga.

Listan i mitten visar tillgängliga objekt och kan visas på olika sätt (välj flik).

Dra–släpp enheter från listan/trädet till behörighetens förteckning. (Gör tvärtom för att ta bort en enhet från behörighetsgruppen.)



Tips: Använd en mall för att lägga in flera våningar samtidigt. Steg-för-steg instruktioner ges i programmets hjälpfunktion. Tryck på **F1**.



Även *hissläsaren* måste ingå i behörigheten för att användaren ska kunna nyttja hissen.

4. Klicka på **Spara** (💾).

Man kan enkelt spärra behörighet till alla våningar i en hiss genom att i behörigheten inte inkludera hissläsaren.

Verifiera hissarnas funktion i systemet



Om ett våningsplan har funktionen **Dörr olåst** aktiv kan man använda motsvarande hissknapp utan att först använda hissläsaren.

Hissläsaren används enligt nedan.

1. Visa kort och/eller ange pinkod.

Om dina behörighetsgrupper inkluderar hissläsaren kommer de hissknappar som ingår i din behörighetsgrupp (vid aktuell tidpunkt, styrt av behörighetsgruppens tidsschema) att vara aktiverade under styrtiden (anges i fältet **Styrtid** – se sidan 124). **Grön lysdiod**, "grön gubbe" eller  är även tänd.

Om dina behörighetsgrupp(er) inte inkluderar aktuell hissläsare kommer **röd lysdiod**, "röd gubbe" eller **X** att visas i kortläsarens display och ingen av hissknapparna aktiveras.

2. Tryck på hissknappen för önskad våning innan styrtiden går ut.

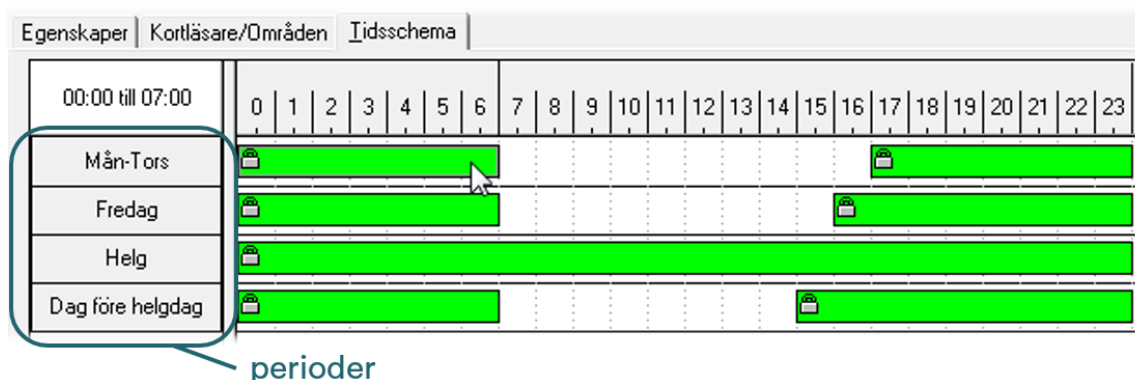
Tidsscheman: Ange när behörigheter och funktioner ska gälla

Begrepp

Tidsscheman

När ska systemets behörighetsgrupper och funktioner gälla? Det styr du med hjälp av ett *tidsschema* som konfigureras för resp. objekt.

Ett *tidsschema* i R-CARD M5 består av en eller flera *perioder* plus de *tidsintervall* under vilka perioderna ska gälla.



Ett tidsschema kan innehålla max. 32 tidsintervaller med en minuts noggrannhet, fördelat på max. 12 perioder.

Perioder och tidsintervall

En *period* består av en eller flera *dagtyper* som ska gälla samma tider i systemet.

Hänglåsymbolen (🔒) betyder att tiderna inte kan ändras eller tas bort. För att ta bort låsningen, avmarkera **Lås tider** i dialogrutans nederkant. (**Lås tider** förhindrar oavsiktlig ändring av inställda tider.)

Löparen under **Tidsintervall** bestämmer upplösningen på tidvisningen. I bilden nedan är upplösningen halvtimmar.

I exemplet har man definierat *perioder* som heter **Mån-Tors**, **Fredag** och **Dag Före Helgdag**. Om du placerar muspekaren på en tidsstapel visas exakta tider i rutan ovanför namnen på perioderna:

i **Tips:** Om du avmarkerar **Lås tider** och dubbelklickar på ett tidsintervall kan du ange exakta tider i siffror. Du kan också ange en valfri text som visas i eller intill tidsintervallet.

Tidsintervallen är de tider på dagen under vilka *perioderna* ska gälla.

Dagtyper

För att skilja veckodagarna åt i systemets *årskalender* har varje veckodag en unik *dagtyp*. Givetvis heter de som standard **Måndag**, **Tisdag**, **Onsdag** osv.

Att varje kalenderdag har en motsvarande *dagtyp* innebär exempelvis att du kan ange att en utvald onsdag ska behandlas som en lördag. (Det gör du genom att dra-släppa dagtypen **Lördag** till den onsdagen i kalendern.)

Förutom de sju standarddagtyperna finns det fem *specialdagtyper* som du kan konfigurera enligt önskemål och använda när avvikande tider ska gälla. Exempel:

- Helgdag
- Dag före helgdag
- Öppet hus-dag
- Studiedag
- Dag i semesterperiod

Dagtyperna har ingen egen funktion. De fungerar i stället som "strömbrytare" som kopplar in olika tidsscheman enligt årskalendern. Tekniskt sett är de inkopplingssignaler för tidsstyrda behörigheter och funktioner i systemet.

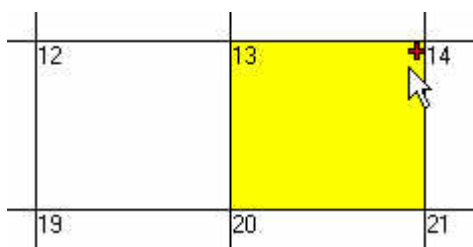
En specialdagtyp kan vara generell eller kompletterande

- *Generell* betyder att dagtypen gäller för hela domänen (eller hela systemet om domäner inte används). Om du lägger en generell dagtyp på ett datum som har en annan generell dagtyp, kommer den befintliga dagtypen ersättas av den nya.

De fördefinierade dagtyperna **Måndag** till **Söndag** är alltid generella.

- En *kompletterande* dagtyp påverkar bara det tidsschema där den används. Den *kompletterar* den generella dagtypen. Om du lägger en kompletterande dagtyp på ett datum kommer befintliga dagtyper *inte* att ersättas, oavsett om de är generella eller inte.

En eller flera kompletterande dagtyper kan alltså läggas på ett datum i årskalendern som redan har en annan dagtyp oavsett om denna är generell eller ej. Om ett datum har fler än en dagtyp visas ett plus i övre högra hörnet:

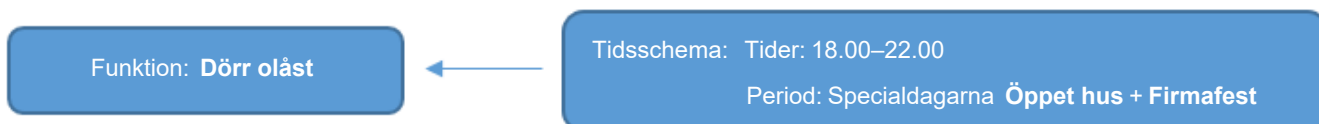


Genom att lägga en kompletterande dagtyp på samma datum som en annan dagtyp kan du aktivera funktioner som normalt inte skulle vara igång den dagen. Det kan användas för att t.ex. hålla en dörr olåst längre än normalt ett valfritt datum.

Flera kompletterande dagtyper kan läggas på samma datum, även om det redan finns en generell dagtyp för datumet.

Hur hänger det ihop?

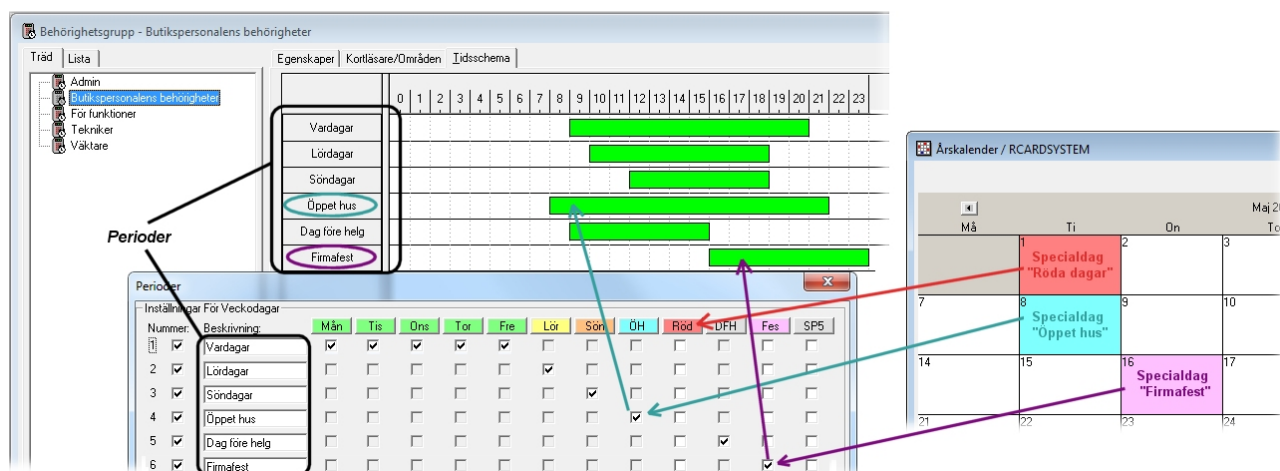
Systemets *behörighetsgrupper* och *funktioner* styrs med hjälp av *tidsscheman*. Ett tidsschema bestämmer vilka tider som gäller för olika *perioder*. En *period* består av en eller flera *dagtyper* under vilka samma tider ska gälla. Här anges de egendefinierade specialdagtyperna **Öppet hus** och **Firmafest** i tidsschemat till funktionen **Dörr olåst**:



Lägger du specialdagen **Öppet hus** eller **Firmafest** på en viss dag i årskalendern så kommer dörren att stå olåst kl. 18–22 den dagen.

Så här fungerar ett tidsschema

Du kan definiera ett tidsschema per behörighetsgrupp eller funktion:



Exemplet illustrerar följande:

- För kalenderdagen den 1:a maj har man i årskalendern lagt in specialdagstypen **Röda dagar**. Alla perioder som har en markering för dagstypen **Röda dagar** börjar gälla vid midnatt mot tisdagen den 1:a maj.

Om vi antar att **Röda dagar** enligt systeminställningarna är en *generell* specialdagstyp så gäller endast de tider som definierats för **Röda dagar**. Dvs tiderna för **Tisdag** (fördefinierad dagstyp som ingår i perioden **Vardagar**) gäller inte.

Här finns inga perioder med en markering för **Röda dagar**. Eftersom tiderna för dagstypen **Tisdag** inte gäller så har butikspersonalen ingen åtkomst den 1:a maj.

Om **Röda dagar** hade varit en *kompletterande* specialdagstyp så hade butikspersonalen åtkomst som på en vanlig tisdag.

- För kalenderdagen den 8:e maj har man lagt in specialdagstypen **Öppet hus**. Alla perioder som har en markering för dagstypen **Öppet hus** börjar gälla vid midnatt mot tisdagen den 8:e maj.

Notera perioden med markering för **Öppet hus**. (Perioden har av praktiska skäl också fått namnet **Öppet hus**.)

Om vi antar att specialdagstypen **Öppet hus** enligt systeminställningarna är en *kompletterande* specialdagstyp så gäller de tider som definierats för **Öppet hus** och de tider som definierats för **Tisdag** (fördefinierad dagstyp som ingår i perioden **Vardagar**).

Om **Öppet hus** hade varit en *generell* specialdagtyp så hade butikspersonalen endast haft åtkomst från kl. 8–22. Eftersom den tiden överlappar med de tider som gäller en vanlig tisdag så hade det inte spelat någon roll.

- För kalenderdagen den 16:e maj har man lagt in specialdagtypen **Firmafest**. Alla perioder som har en markering för dagtypen **Firmafest** börjar gälla vid midnatt mot tisdagen den 16:e maj.

Notera perioden med markering för **Firmafest**. (Perioden har av praktiska skäl också fått namnet **Firmafest**.)

Om vi antar att specialdagtypen **Firmafest** enligt systeminställningarna är en *kompletterande* specialdagtyp så gäller de tider som definierats för **Firmafest** och de tider som definierats för **Onsdag** (fördefinierad dagtyp som ingår i perioden **Vardagar**).

Om **Firmafest** hade varit en *generell* specialdagtyp så hade butikspersonalen endast haft åtkomst från kl. 16–24.

För andra behörighetsgrupper (exempelvis **Väktare**) kan helt andra tider ha definierats.



Bra att veta: De behörigheter som styrs av tidsschemat börjar gälla när tidsschemat sparas.

Lägga upp ett tidsschema från början

1. Öppna en behörighetsgrupp och välj fliken **Tidsschema**.
2. Klicka på **Perioder** i dialogrutans nederkant. Dialogrutan **Perioder** visas.
På översta raden syns de dagtyper som konfigurerats i systemet. Klicka på **Visa dagtypsfärg** för att få etiketterna med dagtypsnamnen visade i färg som i exemplet.
3. Om du vill använda en periodmall, välj den i fältet **Basera på** i periodfönstrets nedre högra hörn, och klicka på **Hämta mall**. Dialogrutan fylls i med de i mallen konfigurerade perioder.



Periodmallar innehåller inga tider utan bara dagar. Därför måste tidsintervall konfigureras som vanligt enligt nedan. Du kan även ändra perioderna som i nästa steg utan att påverka mallen.

- Skapa nya perioder genom att markera oanvända kryssrutor t.v. i dialogrutan.

Inställningar För Veckodagar		Mån	Tis	Ons	Tor	Fre	Lör	Sön	SP1	SP2	SP3	SP4	SP5
1	☒ Mån-Tors	☒	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐
2	☒ Fredag	☐	☐	☐	☐	☐	☒	☒	☐	☐	☐	☐	☐
3	☒ Dag Före Helg	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐
4	☐												
5	☐												
6	☐												
7	☐												
8	☐												
9	☐												
10	☐												
11	☐												
12	☐												

☒ Lås dagtyp till period
☒ Visa dagtypsfärg

Basera på

- Markera vilka dagtyper som respektive period ska gälla under.

i Om **Lås dagtyp till period** är markerad kan du bara ha ett kryss per dagtyp (lodrät rad). Avmarkera rutan för att kunna använda en dagtyp till flera perioder. Här används exempelvis dagtypen **Måndag** i två perioder:

Inställningar För Veckodagar		Mån	Tis	Ons
1	☒ Mån-Tors	☒	☒	☒
2	☒ Fredag	☐	☐	☐
3	☒ Dag Före Helg	☐	☐	☐
4	☒ Utbildningsdagar	☒	☐	☐
5	☐			

- Rekommendation: Namnge perioderna.
- Klicka på **OK**.

8. Lägg in de tidsintervall som ska gälla för respektive period: Klicka vid startpunkten, håll ned vänster musknapp och dra markören till sluttiden.

Hängglåssymbolen (🔒) betyder att tiderna inte kan ändras eller tas bort. För att ta bort låsningen, avmarkera **Lås tider** i dialogrutans nederkant. (**Lås tider** förhindrar oavsiktlig ändring av inställda tider.)

Löparen under **Tidsintervall** bestämmer upplösningen på tidvisningen. I bilden nedan är upplösningen halvtimmar.

I exemplet har man definierat *perioder* som heter **Mån-Tors**, **Fredag** och **Dag Före Helgdag**. Om du placerar muspekaren på en tidsstapel visas exakta tider i rutan ovanför namnen på perioderna:

i **Tips:** Om du avmarkerar **Lås tider** och dubbelklickar på ett tidsintervall kan du ange exakta tider i siffror. Du kan också ange en valfri text som visas i eller intill tidsintervallet.

9. Klicka på **Spara** (💾).

Verifiera passersystemets funktion

När driftsättningen är klar, gör en kontroll av systemets funktion genom att:

1. Skapa en behörighetsgrupp.
2. Lägga in en användare eller lägenhet med ett passerkort och tilldela passerkortet en behörighetsgrupp som inkluderar åtminstone alla dörrar och ev. larmområden.
3. Kontrollera att kortet öppnar dörren.

Förvaltning av behörighetsgrupper, användare/lägenheter och passerkort beskrivs i detalj i programmets hjälpfunktion samt i manualen *R-CARD M5 – Använda*. Manualen finns på installationsmediet för R-CARD M5. Manualer kan även laddas ner från [RCO:s webbplats](#) under **Mediaarkivet > Manualer** (inloggning krävs). Här ges bara en kortfattad instruktion.

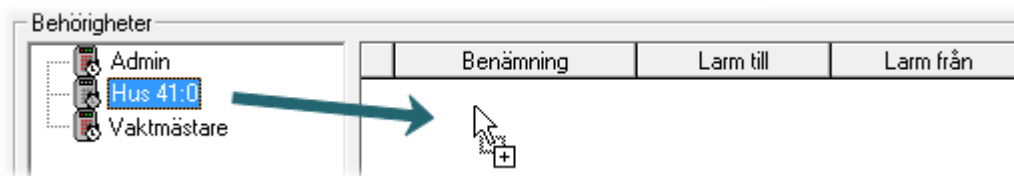
Skapa en behörighetsgrupp

1. Välj **Huvudmeny > Behörigheter**.
2. Högerklicka på en fri yta i behörighetslistan och välj **Ny behörighetsgrupp**.
3. Ange ett beskrivande namn i fältet **Benämning**.
4. Om larmstyrning ska testas, markera **Larmtillkoppling** och **Larmfrånkoppling**.
5. På fliken **Kortläsare/Områden**, dra– släpp alla kortläsare och ev. larmområden till behörighetsgruppen.
6. Välj fliken **Tider** och skapa ett tidsschema för behörighetsgruppen. För instruktioner se sidan 129.
7. Klicka på **Spara** (💾).

Lägga in en användare eller lägenhet med ett passerkort

1. Välj **Huvudmeny > Behörigheter**.
2. Högerklicka på en fri yta under **Användare** och välj **Ny > Användare > (Tom)** eller **Ny > Lägenhet > (Tom)**.
3. Fyll i grundläggande personuppgifter eller lägenhetsuppgifter och ev. övriga data.
4. Klicka på **Spara** (💾).
5. Högerklicka på den användare/lägenhet som ska ha kortet och välj **Nytt kort > Normalt**.
6. Klicka på kortet som nu visas knutet till användaren i trädet.

7. Skriv in ID-kod (kortnumret, som standard 9 siffror). Alternativt läs in ID-koden med bordsläsare.
8. Lägg in pinkod.
9. Dra–släpp den nyss skapade behörighetsgruppen från listan **Behörigheter** till kortets behörigheter:



10. Klicka på **Spara** (💾).

Sparade data sänds automatiskt ut till undercentralerna.

Kontrollera att kortet öppnar dörren

Använd passerkortet vid dörrarna. Knappa in pinkoden för att kontrollera att dörrarna öppnar.

Testa tillkoppling resp. fränkoppling av ev. larmsystem.

När systemfunktionerna är verifierade kan det vara lämpligt att säkerhetskopiera databasen, se "[Dokumentera och säkerhetskopiera systemet](#)" på sidan 144.

Felsökning

Allmänt bästa rådet

Är det något i systemet som inte verkar fungera som det ska, går det ofta att hitta ledtrådar i händelsefönstret: Välj **Visa > Händelsefönstret**.

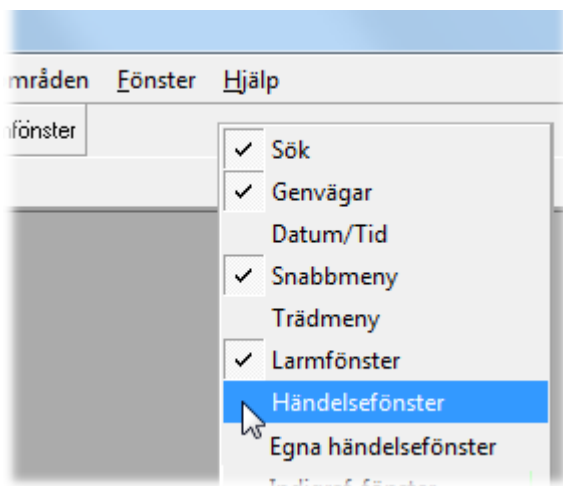
Olika typer av data visas:

- *Operatörsdata* är sådant som operatören företar sig, t.ex. in- och utloggning, inläggning och redigering av användardata etc. Välj fliken **Operatör** för att se operatörsdata.
- *Systemdata* är t.ex. loggning av passager, sabotagelarm etc. Välj fliken **System** för att se systemdata.
- Beroende på systeminställningar kan även egna händelsefönster och närvaroområden visas.

Tryck på **F1** i programmet för mer information.

Funktionalitet inte tillgänglig; menyer saknas eller ser annorlunda ut

För att visa eller dölja paneler eller vissa fönster, högerklicka på en fri yta i menyraden. En popupmeny med möjliga alternativ visas:



Markera vad som ska visas, avmarkera det som ska döljas.

Några faktorer som påverkar vilka menyer och inställningar som syns i R-CARD M5:

- Aktiverad funktionalitet. Många funktioner måste aktiveras för att bli synliga. I vissa fall krävs licensregistrering. Kontrollera vad som krävs i förteckningen över stödprogram och tillvalsfunktioner.
- Hur systemet har ställts in. Exempelvis ledtexter för användare och lägenheter kan ha anpassats.
- Inställningarna på din arbetsstation.
- Din säkerhetsgrupp som operatör. Är du inte inloggad som en operatör som är medlem i säkerhetsgruppen **SystemAdmin** kan dina behörigheter i R-CARD M5 vara begränsade. I så fall saknas menyer eller menyval, och inställningar kan vara inaktiverade (gråa). Kontakta din systemadministratör.
- Inställningar i din operatörsprofil.

Läs mer om detta i programmets hjälpfunktion.

Nyss skapade objekt saknas i ett annat fönster

Exempel på problemet:

- Du lägger in kort och skapar behörighetsgrupper samtidigt. Nyskapade behörighetsgrupper syns inte i användarfönstret när du ska knyta dem till korten. Det berör på att två fönster är öppna. Information från det ena fönstret uppdateras inte alltid i det andra.
- Du tittar på tidbokningar men det saknas bokningar. Det kan bero på att bokningsfilen har lästs in sedan fönstret öppnades.

Så här uppdaterar du fönstret:

1. Se till att nya objekt är sparade (.
2. Klicka på **Uppdatera** () eller tryck på **F5** i det fönstret där data inte har uppdaterats.
3. Om det inte löser problemet, stäng fönstret där data inte har uppdaterats genom att klicka på **Stänga** () i övre högra hörnet *samtidigt som du trycker ned skifftangenten*. Öppna sedan fönstret igen.

Försvunna användare/lägenheter

Användare eller lägenheter kan verka ha försvunnit när man gjort en sökning i användarlistan eller använt en bordsläsare.

Så här återställer du visningen:

1. Välj kategori **-Alla-** som sökbegrepp.
2. Klicka på kikaren (.

Se även "[Nyss skapade objekt saknas i ett annat fönster](#)" ovan.

Kortläsare eller manöverpaneler fungerar inte som programmerat

När enheter inte fungerar som konfigurerat beror det oftast på att enhetens *funktioner* krockar med de *behörigheter* som slutanvändarnas kort tilldelats.

Programmets hjälpfunktion innehåller information som hjälper dig att:

- Ta reda på vad som gäller för ett kort som inte fungerar som det är tänkt.
- Ta reda på vilka funktioner som gäller för aktuell kortläsare eller manöverpanel.

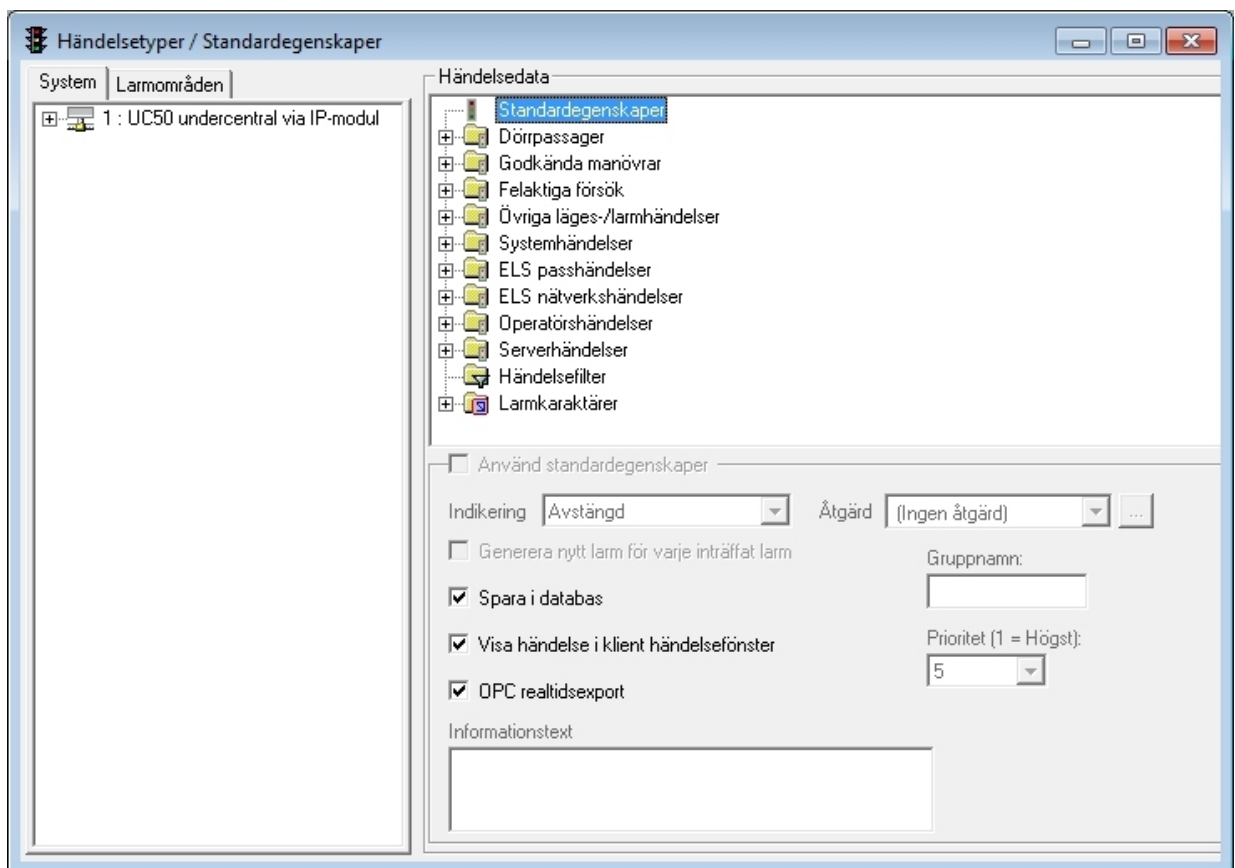
Tryck på **F1** och sök på detta.

Anpassa händelsetyper

Händelsetyper används i händelseloggen och i driftövervakning. Alla typer av händelser har efter programinstallationen en standardinställning som gäller för alla enheter. Du kan anpassa dem, t.ex. om en viss händelse ska generera larm eller om en anpassad text ska visas i händelsefönstret. Möjligheterna är många.

Gör så här för att anpassa händelsetyper:

1. Välj **Inställningar > Händelsetyper**.
2. Händelserna är sammanförda under gemensamma mappar beroende på händelsetyp. Klicka på plustecknet (+) vid respektive mapp för att se vilka händelser som ingår. Ett blått utropstecken (!) syns om händelsens standardegenskaper är ändrade.



3. Ange vad du ska ändra:
 - Standardegenskaper för alla händelser: Markera **Standardegenskaper**, som i bilden ovan.
 - Standardegenskaper för alla händelser som ingår i en mapp: Markera händelsemappen.

- Egenskaper för en enskild händelse: Klicka på plustecknet (+) vid händelsemappen och markera händelsen.
- Egenskaper för en viss händelse på en utvald enhet:
 - a. Klicka på plustecknet (+) vid händelsemappen.
 - b. Expandera även enhetsmappen i vänster rutan.
 - c. Dra–släpp enheten från trädet till önskad händelsetyp.
 - d. Markera enheten i höger rutan.

(Används exempelvis för att skapa anpassade informationstexter för olika enheter.)

4. Avmarkera inställningen **Använd standardegenskaper**. Då aktiveras inställningsmöjligheterna.
5. Anpassa önskade egenskaper. (Listan kan ha olika innehåll beroende på licens, aktivering och programversion.)

Indikering	Hur händelsen ska hanteras och visas i larmfönstret:
	◦ Avstängd: Ingen indikering sker. Saftblandaren förblir grön (1). Ingen åtgärd kan aktiveras (standardinställning). ◦ Läge: Läge (t.ex. dörr öppen, dörr blockerad) indikeras med 1 utan att larm skickas till larmcentral. ◦ Larmgenererande: När händelsen inträffar genereras ett larm som skickas till larmcentral och indikeras med 1 i programfönstret. När du klickar på symbolen öppnas larmfönstret, där händelsen kan ses. Larmet behöver inte kvitteras. ◦ Larmgenererande med kvittering: Som ovan, men larmet måste kvitteras. ◦ Larmgenererande med kvittering och lösen: Som ovan, men larmet måste kvitteras med operatörens inloggningslösenord.
	Om du har valt Larmgenererande med kvittering eller Larmgenererande med kvittering och lösen kan du skriva i fältet Informationstext den text som ska visas när man ska kvittera ett larm.

Generera nytt larm för varje inträffat larm	Om du valt något Larmgenererande -alternativ i fältet Indikering (se ovan) så ger detta alternativ en ny rad för varje larm även om det handlar samma larmpunkt/enhet.
Spara i databas	Händelsen sparas i databasen. Krävs om epost ska sändas i åtgärd.  Om åtgärden innebär att sända epostmeddelande krävs det att Spara i databas är markerad för både händelsefiltret och den underliggande händelsetypen.
OPC realtidsexport	Händelsen rapporteras till överordnat presentationssystem via OPC-anslutning. Syns bara om OPC aktiverats under Inställningar > Moduler .
Visa händelse i klient händelsefönster	Händelsen visas i händelsefönstret, oberoende av valet under Indikering .  Om händelser ska övervakas med hjälp av R-CONTROL, undvik att spärra händelser från visning i klienterna. Det kan få oväntade konsekvenser för presentationen i R-CONTROL.
Informationstext	Text som visas vid de två alternativen Larmgenererande med kvittering och Larmgenererande med kvittering och lösen .
Åtgärd	Kopplar en händelsetyp till en <i>åtgärd</i> – antingen att skicka e-post eller att starta en applikation.
Gruppnamn*	Grupperar olika händelser / larm i listorna för visning i R-CONTROL.
Prioritet*	Styr vilka som ligger överst i listorna. Valbart 1–5. 1 ger högst prioritet, 5 lägst. Tidssortering sker inom varje prioritet. T ex. larmkaraktär Inbrott med prioritet 3 skulle visas högre upp i listorna än Sirenfel med prioritet 5, även om inbrottet hände efter sirenfelet.

* Tillgängligt för R-CONTROL på händelsetyper som har något **Larmgenererande**-alternativ valt i fältet **Indikering** (se ovan).

- Klicka på **Spara** (📁).

Dokumentera och säkerhetskopiera systemet

Under **Rapporter > Rapporter** finns möjlighet att skriva ut valda delar av systemets information. Rapporter kan göras till bildskärm eller skrivare. Man kan skapa egna urval och redigera befintliga. För en översikt, tryck på **F1** i dialogrutan **Rapport**.

Gör en säkerhetskopia av systemet: Välj **Databas > Säkerhetskopiera**. Tryck på **F1** om du behöver mer information.

En databas som körts i en nyare version av SQL Server går inte att ansluta eller återställa i en tidigare version av SQL Server. Detta gäller även mellan SQL Server 2008 och 2008 R2. Mer information om detta finns hos Microsoft.

BILAGA 1: Enhetsadresser och adresstyper

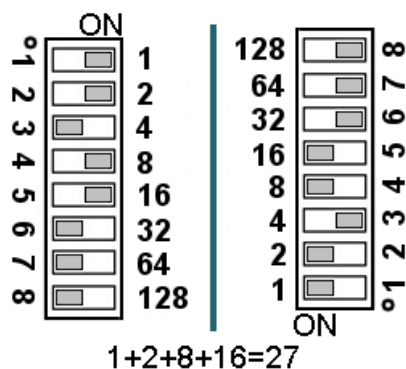
Enhetsadresser

Varje enhet har en adress mellan 0 och 255.

- På enheter med display ställs adressen in via menyn.
- På enheter utan display ställs adressen in med en 8-polig omkopplarbanks, en så kallad DIP-omkopplare.

Omkopplarna motsvarar vardera värdet 1-2-4-8-16-32-64-128, skrivet bredvid respektive omkopplare i omkopplarbanken. När man sluter en omkopplare (sätter den i läge ON) adderas dess värde till adressen.

Exempel: Här visas adress 27. Omkopplare i ON-läge: Nr. 1, 2, 4, 5 ($1+2+8+16 = 27$).



Adresstyper

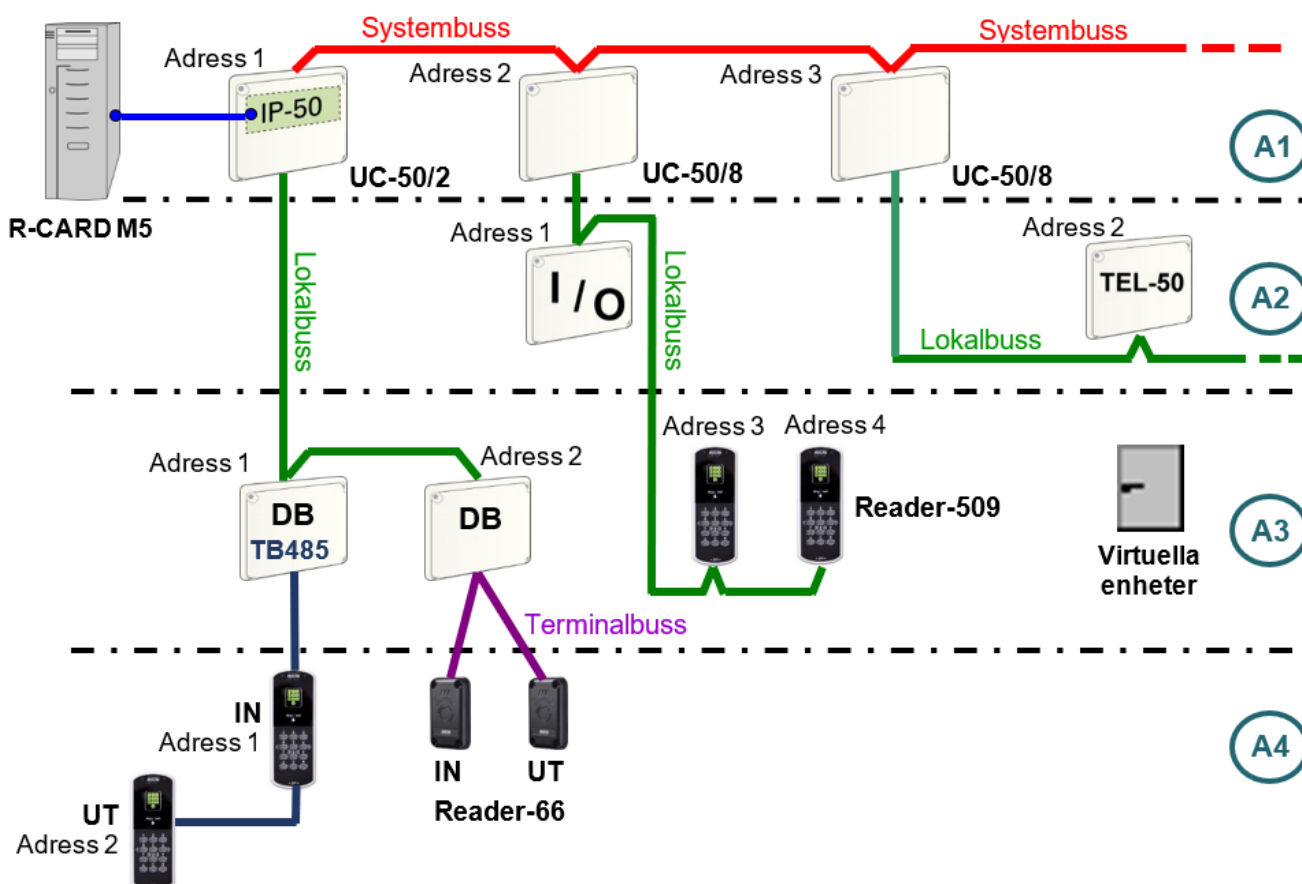
Det finns fyra adresstyper (här betecknade A1 – A4) beroende på enhetstyp och vilken kommunikationsbuss enheten använder:

Adresstyp	Enhetstyp och inställbara adresser
A1	Undercentral UC-50, 1–255 per anknytning
A2	Styrenheter: In/utenhet IO-5004/5008/5044, linjekort TEL-50, in/utenhet DIO-5084 byglad som in/utenhet. 1–255 per anknytning
A3	Enheter (Reader-50 m.m.) som kan anslutas på lokalbuss och tar en kortläsarplats på undercentralen, 1–255 per anknytning: • Kortläsare MIF-509 och PROX/MIF-509 • Porttelefon PA-519 • Manöverpanelerna MapR Touch och MapR 509 • Bokningstavlan Electrolux Easy • NoKey online, NoKey motor • Delningsbox DB-50, DB-50 Light, DB-50W • In/utenhet DIO-5084 byglad som delningsbox • Virtuella enheter, t.ex. virtuella dörrar, våningar i hisstyrning. Observera att hissvåningar tar adresser av typ A3 av anknytningens max 255, men inte dörrplatser av UC-50 max 2, 4 eller 8 dörrar.⁶ Det är dessa enheter som i en stor anläggning först kommer att förbruka de maximalt 255 adresserna och framtvinga användning av ytterligare en anknytning. I ritningen nedan visas enheter på en anknytning. Inställd enhetsadress betecknas med #, t.ex. #2.
A4	Enheter (Reader-60) som tar en kortläsarplats på DB-50 (även DB-50 Light) eller in/utenhet DIO-5084 byglad som delningsbox: • Kortläsare MIF-509 och PROX/MIF-509: Adress 1 = Terminal 1; Adress 2 = Terminal 2. • MIF-66 • Manöverpanelen MapR 509

⁶ Våningar i hisstyrningen använder en annan typ av plats på undercentralen. Finns det bara en kortläsare kan man ha upp till 64 våningar på undercentralen. Har man två kortläsare halveras antalet våningsplatser. Har man fyra kortläsare ryms bara 16 våningsplatser. Detta för att antalet dörrmiljöer anslutna på lokalbussen (även ev. DB-50) *antas vara antalet hissar*. Se "[Styra hissar](#)" på sidan 122.

Regler för adressering av enheter

- Högsta enhetsadress är 255, vilket också är maximalt antal enheter av samma *adresstyp* (utom A4, som kan ha två enheter per delningsbox) som kan tillhöra en anknnytning.
- Enheter inom samma anknnytning och adresstyp får inte ha samma adress.
- Enheter inom adresstyp A4 anslutna via TB-485 kan bara ha adress 1 eller 2. Det kan finnas fler än 255 sådana enheter i en anknnytning om man har både in- och utläsare. Det är delningsboxens adress som representerar dörrmiljön.
- *Bara adresstyp A4 får ha adress 0.*
- Samma enhetsadress kan återfinnas hos flera enheter av a) samma adresstyp men i olika slingor/grupper; b) olika adresstyper i samma anknnytning.



BILAGA 2: Identifiering av enheter (enhetsbeteckningar)

Enhetsbeteckningen består av tre delar:

1. Prefix. Några exempel:

- **UC:** Undercentraler
- **KL:** Står för *kortläsare* men följande enheter får beteckningen KL: Virtuella enheter, hiss våningar, porttelefoner, DIO-5084 inställd som delningsbox.

Även delningsbox DB-50 i kombination med kortläsare får beteckningen KL. (Terminaler anslutna till delningsboxar har inget eget prefix.)

Delningsboxar med kortläsare visas på olika sätt i träd och listor: I trädvisningen kan man expandera delningsboxen till att även visa kortläsaren. I listor visas delningsboxen som två enheter.

Bokstaven **K** efter läsarbenämningen betyder att kortläsaren har knappsats.

- **MAP:** Manöverpaneler.
- **BT:** Electrolux bokningstavlor.
- **IO:** In/utenheter.
- **TEL:** Linjekort TEL-50.
- **OL:** Offline-läsare.

2. Anknytningsnummer.

3. Den adress man ställt in på enhetens adressomkopplare.

Exempel: **KL 2:27** betyder kortläsare ansluten till anknytning 2, med inställd adress 27.

Enhetsbeteckningen påverkas inte av vilken domän enheten tillhör.

Enheter av olika typ kan ha samma *anknytning:inställd adress* i enhetsbeteckningen, t.ex.

UC 4:1, **KL 4:1** och **IO 4:1**, eftersom de har olika adresstyper. (Se "[BILAGA 1: Enhetsadresser och adresstyper](#)" på sidan 145.)

Enheter av samma typ kan också ha samma inställda adress om de är anslutna till olika anknytningar. Exempel: **UC 4:1** och **UC 5:1** kan finnas i samma system.

Adresstyper beskrivs på sidan 145. Systemets hårdvara beskrivs i manualen *R-CARD 5000 – Installera*. Manualen finns på installationsmediet för R-CARD M5.

Manualer kan även laddas ner från [RCOs webbplats](#), under **Mediaarkivet > Manualer** (inloggning krävs).

Ikon/symbol	Enhetsstyp	Info i manualen
	Domän	"Skapa domäner" på sidan 19.
	Anknytning	"Skapa anknytningar" på sidan 21.
	Undercentral	"Minneskonfigurera undercentraler" på sidan 29; "Konfigurera undercentralens bussar för nätverksmodulen IP-50" på sidan 36.
	In/utenhet IO-5022	"Konfigurera dörrmiljöer" på sidan 49.
	In/utenhet IO-50xx (ej IO-5022)	
	Delningsbox	"Konfigurera enheter anslutna till delningsbox" på sidan 84.
	Kortläsare Reader-509	"Konfigurera dörrmiljöer" på sidan 49.
	Diverse kortläsare	
  	NoKey offline, NoKey online, NoKey motor	Se programmets hjälpfunktion eller <i>manualen R-CARD 5000 – Offline-läsare – Driftsätta</i> .
  	LockR Cylinder, LockR Cabinet, LockR Rotary Switch	
	Manöverpanel MapR 509	"Definiera åtkomst till larmsystemets manöverpaneler" på sidan 92; "Planritningar och grafik i R-CONTROL och MapR Touch" på sidan 95.
	Manöverpanel MAP-59 (utgått)	
	Manöverpanel MapR Touch	
	R-TOUCH 50 (utgått)	
	Linjekort TEL-50	"Konfigurera linjekort TEL-50" på sidan 112
	Porttelefoner	"Konfigurera porttelefonsystem" på sidan 111.
	Electrolux bokningstavlor	
	Larmområde	"Konfigurera larmområden" på sidan 70; "Styra externt larm med larmområde" på sidan 99.
	Dörrgrupp	Se Antal offline dörrgrupper under "Gemensamma grundvärden" på sidan 30.

BILAGA 3: Importera data till systemet

Följande möjligheter finns att importera data till (eller ändra data i) Microsoft SQL Server-databasen i R-CARD M5:

- Programmet M5ToM5 används för att sammanföra två R-CARD M5-system till ett, d.v.s. importera vissa data från en R-CARD M5-databas till en annan R-CARD M5-databas.

M5ToM5 installeras tillsammans med R-CARD M5 och kräver R-CARD M5 DBI-licens ("DBI extern")⁷ för användning. Kräver även en klientlicens (för en nätverksoperatör) eftersom två R-CARD M5-instanser körs samtidigt.

Utförliga instruktioner ges i manualen *R-CARD M5 – Importera data*. Manualen finns på installationsmediet för R-CARD M5. Manualer kan även laddas ner från [RCOs webbplats](#), under **Mediaarkivet > Manualer** (inloggning krävs).

- Programmet Import från Excel används för att importera valda kolumner och rader från ett Excel-ark eller en textfil till R-CARD M5-databasen. Inget licenskrav. Utförliga instruktioner ges i manualen *R-CARD M5 – Importera data* (se ovan).
- Tillägsprogrammet R-CARD M5 BOKA används vid integrering av externa tidbokningsprogram med R-CARD M5, exempelvis för att kontrollera användning av en kommunal idrottsanläggning. Idrottsföreningar ges tillträde vissa tider till de olika delarna av anläggningen. Insläpp kontrolleras av passersystemets vanliga kortläsare.

Själva bokningarna görs med hjälp av ett externt bokningsprogram, som sparar informationen till en *bokningsfil*. Programmet R-CARD M5 BOKA kontrollerar bokningsfilen varje minut och importerar innehållet. Eventuella nya bokningar läggs omedelbart in i R-CARD M5-databasen och skickas ut till passersystemets undercentraler. Bokningar som inte längre är giltiga raderas automatiskt. Inget manuellt ingripande behövs för att hålla databasens bokningar aktuella.

Namn och sökväg till bokningsfilen anges när du aktiverar R-CARD M5 BOKA. Registrera licensen först. Gå sedan in under **Inställningar > Inställningar > System > Moduler > Tidbokning**.

Både inställningarna och bokningsfilens utseende och innehåll beskrivs utförligt i programmets hjälpfunktion (tryck på **F1**).

⁷ Licensen kan beställas från RCO, tel. 08-54656010 eller e-post order@rco.se eller webbutiken på www.rco.se (inloggning krävs). Artikelnumret är **20021075** och man får ett serienummer vid ordertillfället. Licensregistrering beskrivs på sidan 12 samt i onlinehjälp i R-CARD M5.

- Till dataimport kan även R-CARD M5 Admin API ("M5AdminAPI") och i mindre utsträckning R-CARD M5 User API ("M5UserAPI") användas. Dessa Representational State Transfer (REST)-APIer använder JavaScript Object Notation (JSON) för dataöverföring.

APIerna beskrivs utförligt i manualerna *R-CARD M5 – Integration using M5AdminAPI* resp. *R-CARD M5 – Integration using M5UserAPI*. Dessa manualer är f.n. endast tillgängliga på engelska. De kan laddas ner från [laddas ner från RCOs webbplats](#), under **Mediaarkivet > Manualer** (inloggning krävs).

BILAGA 4: Konfigurera Mifare-kortläsningen

Översikt

Vad som ska lagras på och läsas ifrån Mifare-korten, och hur, programmeras i R-CARD M5 med hjälp av *offline-profiler* och *profilgrupper*.

En *profilgrupp* anger ett eller flera dataformat (t.ex. serienummer).

I system med offline-läsare: Till varje dataformat kopplas 1–2 *offline-profiler*. Offline-profilerna anger kortstorlek, hur passageinformation ska lagras, krypteringsnyckel för att skriva till och läsa från sektorer m.m.

I onlinehjälpfinns exempel på upplägg med och utan offline-läsare.

Det absolut vanligaste förfarandet är läsning av serienumret med tillhörande uppgifter om hur data ska tolkas. Vid användning av kort köpta från RCO Security överensstämmer numret som finns påtryckt med läsning inställd för block.

Konfigurationen (dvs Mifare-profilerna) överförs sedan till kortläsarna. Ska offline-läsare användas i systemet måste Mifare-profilen överföras till dessa via ODM.

Ska du ansluta en Mifare-bordsläsare krävs en *separat* Mifare-profil till den. Du väljer sedan Mifare-profilen när du ansluter bordsläsaren.

Kortläsare som inte har programmerats med någon profilgrupp läser som standard Mifare UID, ett 4-bytes serienummer med datatyp block.



Viktigt: Du som ska driftsätta en anläggning med Mifare-läsare måste vara väl medveten om—och göra klart för slutkunden—om och hur Mifare- eller kombikorten innehåller information utöver serienummer som ska nyttjas av systemet. Stäm av med slutkunden i vilken utsträckning korten ska användas till annat än passersystemet, exempelvis till kopieringsmaskiner eller annan utrustning. Det kan annars innebära ett stort merarbete att rätta till felaktiga profiler.

Allt detta beskrivs i programmets hjälpfunktion.

Om det finns kort med data formaterad på olika sätt i samma system

Mifare-läsarna kan lagra en *profilgrupp* om upp till 15 olika Mifare-profiler.

Vid avläsning av ett Mifare-kort testas först om första profilen är användbar. Om det misslyckades försöker den med nästa profil osv. Läsningen avslutas efter första lyckade avläsningen.

Om ett UID (kortets unika produktionsserienummer) finns som profil i gruppen så läses detta sist, efter att alla andra profiler har testats.

Anvisningar

Följande beskrivs utförligt i onlinehjälp (tryck på **F1**):

- Aktivera korttyper med långt ID
- Skapa profilgrupp och Mifare-profiler till kortläsare
- Skapa Mifare-profil till bordsläsare
- Konfigurera hur data lagras på offline-kort (skapa offline-profiler)
- Överföra Mifare-profiler till kortläsare
- Överföra Mifare-profiler till offline-läsare
- Välja Mifare-profil i bordsläsarinställningar
- Radera Mifare-profiler från kortläsare

BILAGA 5: Dynamisk korthantering

Dynamisk korthantering gör R-CARD 5000 obegränsat i avseende på antalet användbara kort i systemet.

Principen för dynamisk korthantering

1. En domäns undercentraler fylls med kort så långt det går.
2. Kort som därefter behöver passera i denna domän uppdateras från R-CARD M5 Server.

Om nedanstående krav uppfylls är målsättningen att passage med ett kort som behöver läras in ska ske inom 5 sekunder. Vid ogynnsamma förhållanden ska det aldrig ta mer än 20 sekunder.

3. Kortet ersätter det kort som har äldst passertid i domänens undercentraler.

Observera

- Dynamisk korthantering fungerar inte i domäner där kort på ett mer permanent sätt ska hanteras i utrustningen. Exempel:
 - Electrolux Boka kräver kortgrupper. Med dynamisk korthantering skulle systemet blanda ihop bokningar m.m. eftersom allokeringen kan byta plats.
 - Domäner med porttelefoner uppdateras inte dynamiskt.
- Domäner med dynamisk korthantering fungerar inte autonomt vid t.ex. kommunikationsavbrott mot servern.
- Att inläringen sker domänvis innebär att ett kort inte nödvändigtvis finns i alla domäner bara för att det är inlärt på ett ställe.

Förutsättningar

- Alla undercentraler (UC-50 version 2.52 eller senare) i berörda domäner måste ha ständig kontakt med R-CARD M5 Server.
- För att få en pålitlig funktion med bra prestanda ska uppkopplingen vara via TCP/IP med snabba svarstider.
- Datorn där R-CARD M5 körs måste vara kraftfull med god prestanda för databashantering.

Rekommendation

- Eftersom den dynamiska uppdateringen av kort sker domänvis kan det vara klokt att dela in ett stort system i logiska regioner. Då kommer i princip inpasseringsfördröjningen endast ske när ett kort för första gången är utanför "sin egen" region.

Aktivera dynamisk korthantering

1. Välj **Inställningar > Inställningar**.
2. Klicka på mappen **System** och välj **Kortinställningar**.
3. Klicka på **Dynamisk korthantering**. Dialogrutan **Dynamiska kort** visas.
4. Välj domän.
5. Markera **Dynamiska kort**.
6. Klicka på **Spara**.

BILAGA 6: Kundinloggning / portalinloggning

R-CARD M5 Kundinloggning används som en inloggningsportal in i R-CARD M5 Arbetsstation. Vid konfigurering parar man ihop domän + användargrupp till "kunder". Operatörer kan då logga in mot sitt system på två olika sätt:

- Operatören startar inloggningsportalen (**RaPortalClient.exe**), väljer vilken kund hen ska logga in som och klickar på **Logga in**.

Ett användningsområde skulle vara vid ett larmbord, för att snabbt kunna växla mellan olika system.

- Operatören kör klienten (**RaClient.exe**) via kommandoraden och loggas in direkt som förvald kund.

Denna lösning skulle exempelvis kunna tillämpas om man är värd för ett antal flerbostads-anläggningar, vars administratörer ska kunna logga in i sitt system utan att se övriga system.

Efter inloggning administreras systemet som vanligt.

RCO:s portalprogram ingår i installationen och installeras i samma katalog som R-CARD M5 Server.

Konfigurering beskrivs utförligt i onlinehjälp i R-CARD M5 (tryck på **F1**).

BILAGA 7: Programväxlar

Använd följande parametrar när du vill starta programmet via exempelvis ett skript eller en bat-fil.

Exempel: RaClient.exe /RaLogin /Server localhost /System RCARDSYSTEM /Username rcard /Password 1234 /Domain Torg stugan

Parameter	Beskrivning, attribut
/RaLogin	Startar inloggningen.
/Server	Localhost eller IP-adress. Kravfält.
/System	Systemnamnet. Kravfält. Skiftlägeskänsligt.
/Username	Operatör. Kravfält.
/Password	Lösenord. Om lösenord inte anges visas inloggningsdialogrutan och man måste ange lösenordet manuellt. (Övriga fält i inloggningsdialogrutan är utgråade.)
/Lang	Språkval: sv, no, fi, en eller dk.
/Domain	Vald domän (endast en domän). Skiftlägeskänsligt. Inga citationstecken krävs vid mellanslag. Används inte i ett system utan domäner.

BILAGA 8: Några viktiga inställningar i larmsystemet

Inställning/parameter	Beskrivning
Antalet manöverpaneler som kan inkopplas per system (=anknytning)	Bestäms av sammanlagda antalet tillgängliga (oanvända) dörrmiljöer på anknytningens undercentraler. Exempel: En 8-dörrars UC 50 som kontrollerar 5 dörrar kan ansluta 3 st. manöverpaneler. Antalet manöverpaneler anges individuellt för varje undercentral vid minneskonfigureringen – se sidan 33.
Begränsning av antalet larm per tillkopplingstillfälle	Om ingångstypen har Begränsat antal larm satt till Begränsning i larmlogg så bestäms detta av larmsystemets inställning Max. antal larm per tillkoppling (se sidan 65).
Teknikerbehörighet	Aktiveras av en systemadministratör och spärras antingen automatiskt efter 24 timmar eller efter omstart av undercentralen. Kan även spärras av operatör. Se Teknikerbehörighet på sidan 93.
Möjliga kortnummer (kort ID)	9 siffror (0, 1 ... 9). 1 – 999999999. Långa ID-koder: 1 – 340282366920938463463374607431768211455
Möjliga pinkoder	6 siffror (0, 1 ... 9). 000000 – 999999. Systemet stöder pinkod med 3, 4, 5 eller 6 siffror per användare. Max. antal kodkombinationer med 6 siffror (beräknas som $10^{\text{antal siffror}}$) 1.000.000.
Otillåtna koder	Endast inprogrammerade koder är tillåtna i systemet.
Prioritet mellan larmhändelser i larmloggen	Kan anpassas genom att anpassa händelsetyper i R-CARD M5. Inställningen Prioritet bestämmer ordningsföljden för händelserna. Se " Anpassa händelsetyper " på sidan 141. Se även "Larmloggen" i onlinehjälp i R-CARD M5 (tryck på F1).

För utförlig information om konfigurering av larmsystem och manöverpaneler, inmatning av person- och lägenhetsinformation samt kort och pinkoder m.m., se onlinehjälp i R-CARD M5 (tryck på F1).

BILAGA 9: Larm- och miljöklassificering

SSF 1014 larmklass: 4

Security grade: 4

Manöverpanelerna MapR Touch och R-TOUCH 50 tillhör miljöklass 1, type A.

MapR 509 tillhör miljöklass 3, type A.

Indikeringar, Larmklass 3–4, Security Grade 4

Anläggningen ska uppfylla minst ett av nedanstående alternativ enligt EN 50131-1 utgåva 2.

X = Frivilligt alternativ. Siffrorna anger antalet signaldon/system som krävs för respektive alternativ.

	Alternativ A	Alternativ B	Alternativ C
Fjärrmatat akustiskt larmdon	2	X	X
Självförsörjande akustiskt larmdon	X	1	X
Larmsändare	ATS 5	ATS 5	ATS 5
Alternativ larmsändare	X	X	ATS 4