RCO Access
Driftsätta

Manualen beskriver hur du förbereder för användandet av mobilapplikationen RCO Access i passersystemet. Gäller även integrationer med tredjepartsprodukter.

RCO Security AB
Box 3130
169 03 Solna

tel 08-546 560 00
info@rco.se
www.rco.se

Innehåll

RCO Access och R-CARD M5 User API

Mobilapplikationen RCO Access ger möjlighet för slutanvändare att se status på och öppna dörrar i RCO-passersystemet. Appen laddas kostnadsfritt ner från Google Play eller AppStore. I appen stöds svenska, norska, finska och engelska.

Passersystemet styrs av programmet R-CARD M5, och för att appen ska fungera krävs tilläggsprogrammet R-CARD M5 User API. Tilläggsprogrammet får man genom att registrera licenser *för varje databas* och *för varje dörr* som användarna ska kunna öppna via appen.

Licenser finns i två varianter:

- R-CARD M5 Access Dörr: Används på dörrmiljöer med kortläsare.
- R-CARD M5 Access Virtuell: Används till virtuella dörrar.

Efter installation och licensregistrering krävs konfigurering i R-CARD M5, som beskrivs i denna manual.

Manualen är användbar även för tredjepartsintegrationer, exempelvis sådana från Precise Biometrics och Accessy AB.

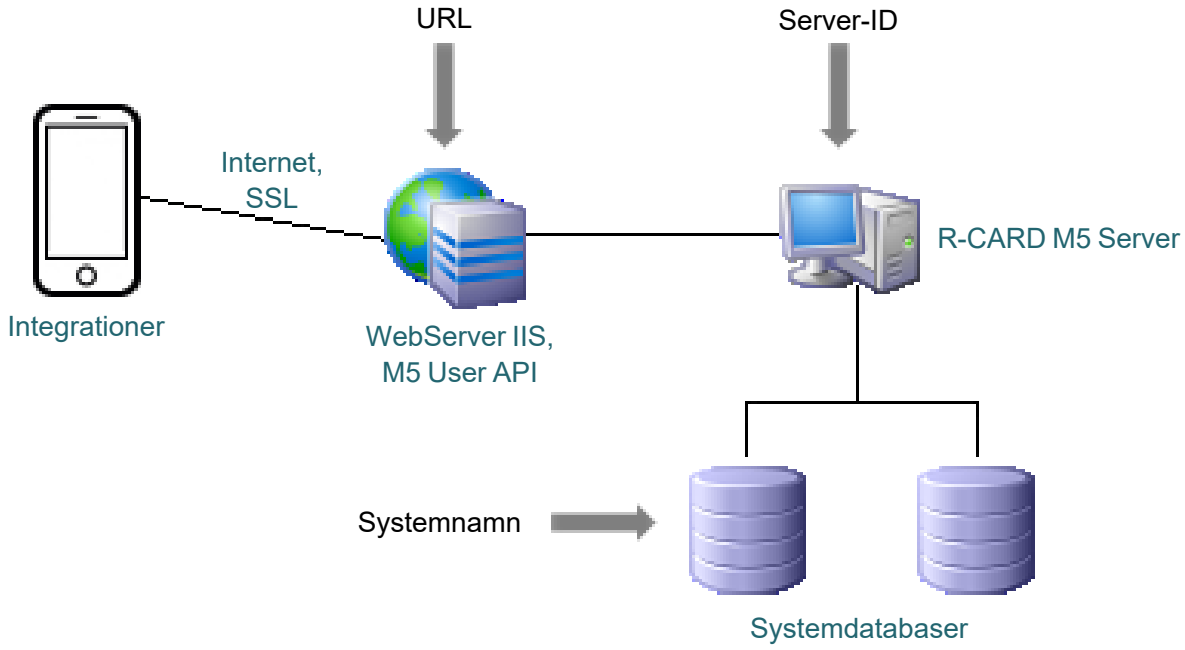
Förutsättningar

- Ett driftsatt och uppkopplat passersystem.
- IP-kommunikation mellan mobil och R-CARD M5.
- Licens för bruk av R-CARD M5 Access Dörr och/eller R-CARD M5 Access Virtuell (se ovan).
- Undercentralen UC-50 version 2.84 F8 eller senare.
- R-CARD M5 version 5.46 eller senare och R-CARD M5 User API version 1.1 eller senare. *Använd senaste version för full funktionalitet.*

Viktigt: Säkerställ att datorn installerar säkerhetsuppdateringar automatiskt eller att den på annat sätt uppdateras regelbundet.

Aktivera IIS och installera mjukvaran

Översikt



R-CARD M5 User API installeras på R-CARD M5-serverdatorn, alternativt på valfri IIS-server. Anrop och kommunikation med IIS-webbservern sker med HTTPS när ett R-CARD M5-system är driftsatt.

För varje session sparas klientens unika nätverksinformation som en *client secret* och förhindrar att en *session access token* kan användas av någon annan än den som loggade in. RCO Access använder ytterligare kryptering för inloggning samt byte av lösenord. Inloggningssessioner stängs efter fem minuters inaktivitet.

Enligt grundinställningarna blir alla passersystem på den lokala datorn tillgängliga för appen. Ingen konfigurering krävs om:

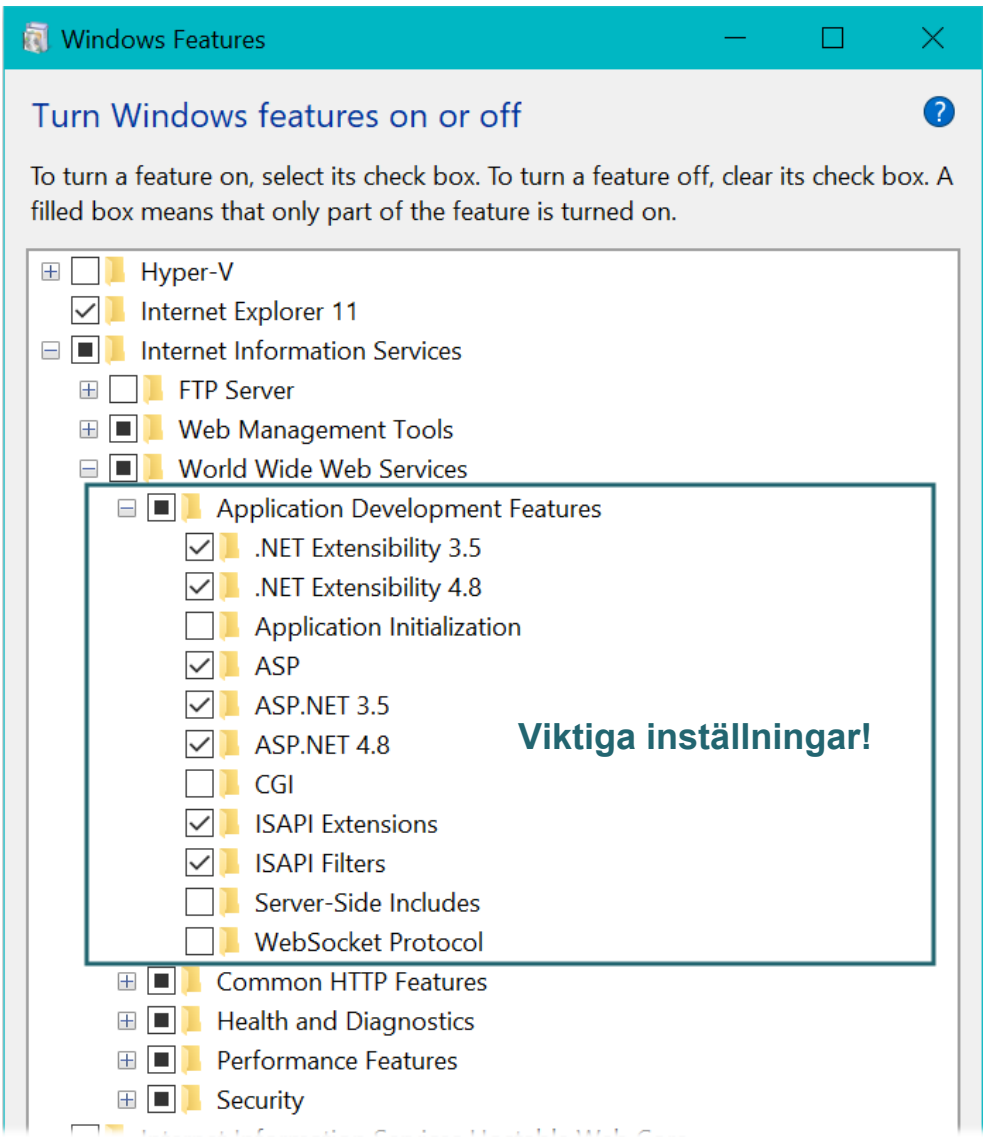
- Alla passersystem på den lokala datorn (och inga andra) ska vara tillgängliga.
- API-operatören (eller operatörerna) skapas med namnet "apitest" och lösenord "1234". (För instruktioner se sidan 17.)

I annat fall krävs anpassningar i konfigurationsfilen **rcoservers.config**. Se "BILAGA 1: Konfigurationsfilen rcoservers.config" på sidan 27 för anvisningar efter installation.

Aktivera IIS

Internet Information Services (IIS) finns att lägga till i de flesta Windows operativsystem. Aktivera IIS på den dator som R-CARD M5 User API ska installeras på:

1. Öppna **Program och funktioner** i Windows kontrollpanelen.
2. Klicka på **Aktivera eller inaktivera Windows-funktioner** på vänster sida.
3. Bläddra i listan och klicka på plustecknet (⊞) vid **Internet Information Services**.
4. Utöver grundinställningarna, säkerställ att de **Programutvecklingsfunktioner (Application Development Features)** som bilden visar är markerade.



5. Klicka på **OK**.

Installera R-CARD M5 User API på R-CARD M5 Server

1. Ladda ned "R-CARD M5 User API" från RCO:s hemsida. (Gå in under **Mediearkivet** > **Mjukvara** > **Programvara R-CARD M5**.)

   Nedladdningsfilen finns även i mappen **M5Web** på R-CARD M5-installationsmediet.

2. Packa upp filen.
3. Högerklicka på filen **SetupM5UserAPI.exe** och välj **Kör som administratör**.
4. Följ anvisningarna på skärmen och slutför installationen.

Konfigurera IIS

HTTPS gör att kommunikationen mellan klient och webbserver är krypterad. Att använda ett signerat servercertifikat säkerställer att klienten kommunicerar med den server man angett adressen till.

Från 4:e oktober 2020 är det inte längre möjligt att använda självsignerade SSL-certifikat i Google Android-plattformar. Certifikatet måste istället vara signerad av en s.k. *certification authority* (CA), eller certifikatutfärdare. I annat fall kommer slutanvändare inte kunna styra dörrar via Android-appen.

Om din organisation inte har ett SSL-certifikat kan du följa RCO:s instruktioner för att skaffa ett sådant. Se "BILAGA 2: Skaffa och tillämpa SSL-certifikat" på sidan 30.

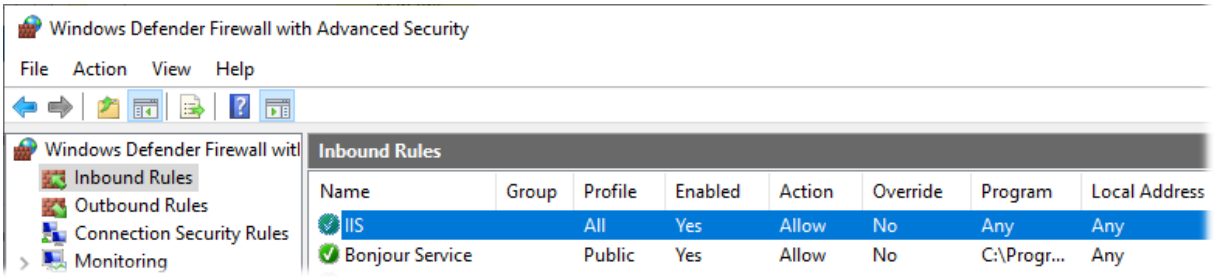
Observera att det finns olika tillvägagångssätt, olika lösningar och olika prisklasser på certifikat. Saknar man kunskap inom området finns mycket information att hämta via nätet.

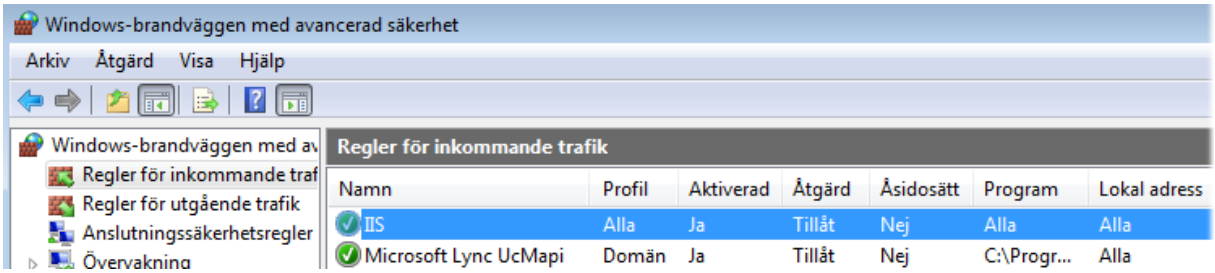
Konfigurera brandväggen

Används den inbyggda brandväggen i Windows så kan den stängas av tillfälligt för test. För en produktionsmiljö behöver brandväggen öppnas för inkommande trafik på HTTPS-port 443.

Gör så här:

1. Öppna Windows Defender-Brandväggen i Windows Kontrollpanelen.
2. Klicka på **Avancerade inställningar**.
3. Klicka på **Regler för inkommande trafik**.
4. Kontrollera att det finns en regel för IIS. Konfigurera i annat fall en sådan regel (öppna brandväggen för inkommande trafik på port 443).





Registrera RCO-licenser

Följande licenser krävs:

- R-CARD M5 Access Dörr: Licens för det antal *dörrar med kortläsare* som ska kunna öppnas via appen.
- R-CARD M5 Access Virtuell: Licens för det antal *dörrar utan kortläsare* som ska kunna öppnas via appen.

Registrera licenserna på samma sätt som övriga RCO-licenser. För steg-för-steg instruktioner se manualen *R-CARD M5 – Installera* eller onlinehjälpen 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**.

Konfigurera loggning

Loggning via R-CARD M5 User API

R-CARD M5 User API sköter sin loggning med hjälp av Apache Log4net. Konfigurationen ligger i slutet av **web.config**-filen för R-CARD M5 User API. Standardsökvägen för denna fil:

C:\inetpub\wwwroot\M5UserAPI

Elementet **<level>** styr vilka fel som ska loggas.

```
<log4net debug="false">
  <root>
    <!-- ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF -->
    <level value="INFO" />
    <appender-ref ref="RollingLogFileAppender" />
  </root>
```

Värdet INFO (standardinställningen) innebär loggning av applikationstrafik, dörrhändelser och fel.

Under installationen har en loggkatalog (**logs**) skapats i samma mapp som konfigurationsfilen. Den kan även skapas manuellt om den saknas. Exempel:

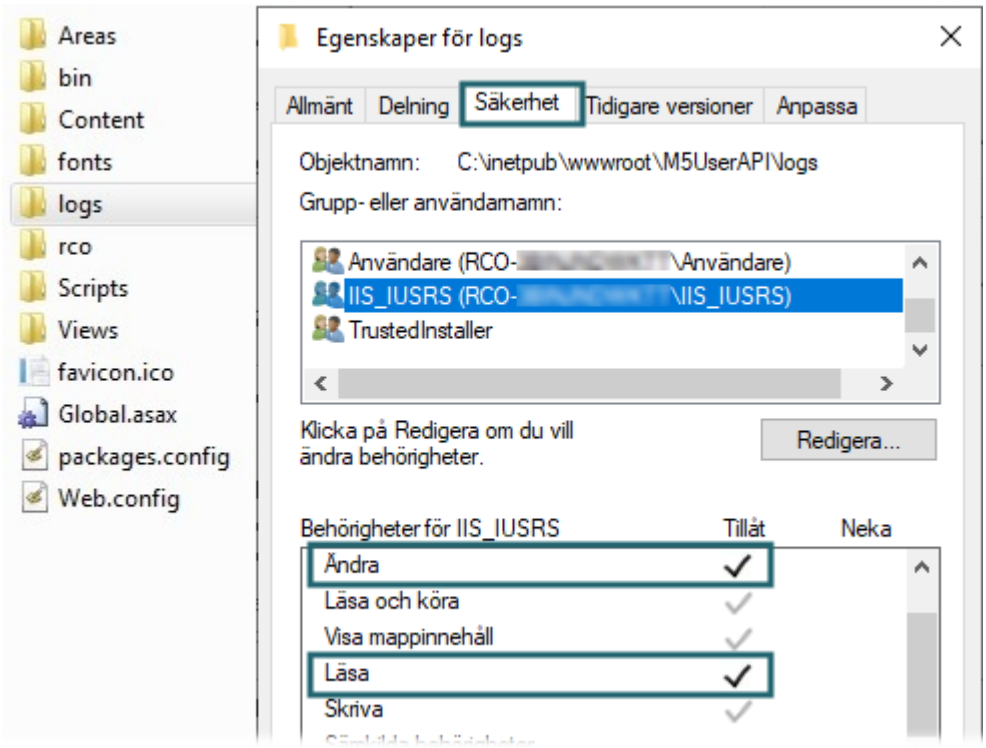
C:\inetpub\wwwroot\M5UserAPI\logs

Värden OFF, FATAL, ERROR, WARN, DEBUG, INFO, ALL är nivåer. Sätter man nivå till INFO får man också med DEBUG, WARN, ERROR och FATAL.

För att loggning ska ske krävs att användaren IIS_IUSRS får skriv- och ändringsrättigheter i loggkatalogens egenskaper.

Gör så här:

1. Högerklicka på katalogen **logs** och välj **Egenskaper**.
2. På fliken **Säkerhet**, välj användaren **IIS_IUSRS**.
3. Klicka på **Redigera**.



4. Markera **Ändra** och **Skriva**.
5. Klicka på **Verkställ** och **OK**.

Utökad loggning via RaServiceHost

Även RaServiceHost-tjänsten sköter sin loggning med hjälp av Apache Log4net. Det är valfritt att aktivera denna loggning, som då visar eventuella anropsfel.

Loggningen styrs via konfigurationsfilen **log4net.config**. Standardsökvägen för denna fil:

C:\Program Files (x86)\RCO Security AB\R-CARD M5\RcardService

Elementet **<level>** styr vilka fel som ska loggas.

Loggarna skrivs normalt till följande katalog:

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\RCO Security AB\R-Card M5\Logs

Konfigurera R-CARD M5

Hantering av användare/lägenheter

För att användare/boende ska kunna styra dörrar i passersystemet via sitt kort (alltså utan appen RCO Access) krävs följande:

- Personen eller lägenheten måste de vara inlagd som användare eller lägenhet.
- Användaren/lägenheten måste ha minst ett giltigt kort inlagt.
- Kortet måste via sin behörighetsgrupp vara behörigt att öppna dörren vid den aktuella tidpunkten.

I onlinehjälpen i R-CARD M5 ges detaljerade instruktioner för ovanstående.

För att användare/boende ska kunna styra dörrar via RCO Access krävs *dessutom* nedanstående.

- *Unik identifiering av användaren/lägenheten.*

  Identifieringen av användaren/lägenheten måste vara unik. Skulle två användare eller lägenheter registreras med samma identifierare (t.ex. e-postadress eller efternamn) kommer ingen av dem att kunna logga in i RCO Access. Se nedan.

- *Webblösenord.*

  Varje användare/lägenhet måste ges ett webblösenord ("lösen för webb") på minst 4 tecken. **Lösen för webb** anges av operatören när användaren eller lägenheten läggs in.

Välja fält för inloggning i RCO Access

Välj vilket fält som användare ska skriva som inloggningsnamn i mobilapplikationen RCO Access.

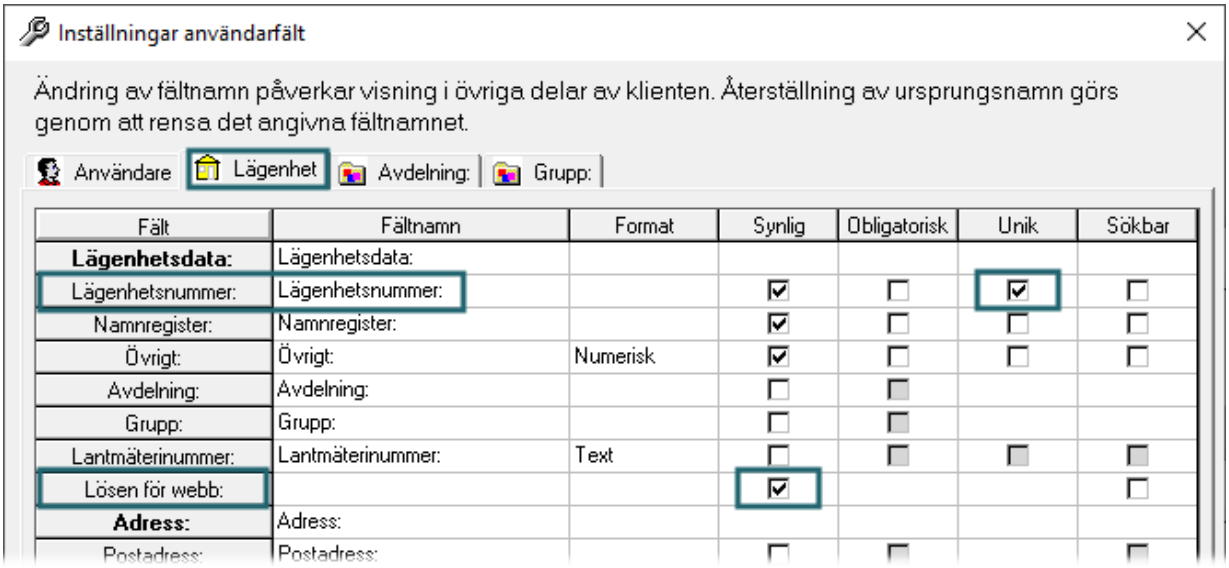
Om lägenheter registreras i systemet

I anläggningar där man lägger in lägenheter istället för användare används alltid *lägenhetsnummer* för inloggning.

Det går bra att skapa upp till 10 aktiva inloggningssessioner med samma användarnamn/lösenord i appen. (Om ytterligare inloggningar görs så tas den äldst uppdaterade sessionen bort.) Detta för att alla medlemmar i en familj ska kunna öppna en entréport. I ett normalt flerbostadssystem är varje "användare" en lägenhet med ett lägenhetsnummer. Inloggningsuppgifter delas då av alla boende i lägenheten.

Gör så här:

1. Välj **Inställningar** > **Inställningar**.
2. Klicka på mappen **System** och välj **Användarfält**.
3. Klicka på **Konfigurera användarfält**. Dialogrutan **Inställningar användarfält** visas.
4. Välj fliken **Lägenhet**.



5. Rekommendation: Markera kryssrutan i kolumnen **Unik** för fältet **Lägenhetsnummer**.

> Inställningen **Unik** är inget krav. Däremot måste den information som matas in i fältet för varje användare vara unik, annars kommer RCO Access att blockera inloggning för berörda användare. Att markera **Unik** är därför ett bra hjälpmedel då det förhindrar inmatning av icke-unik information.

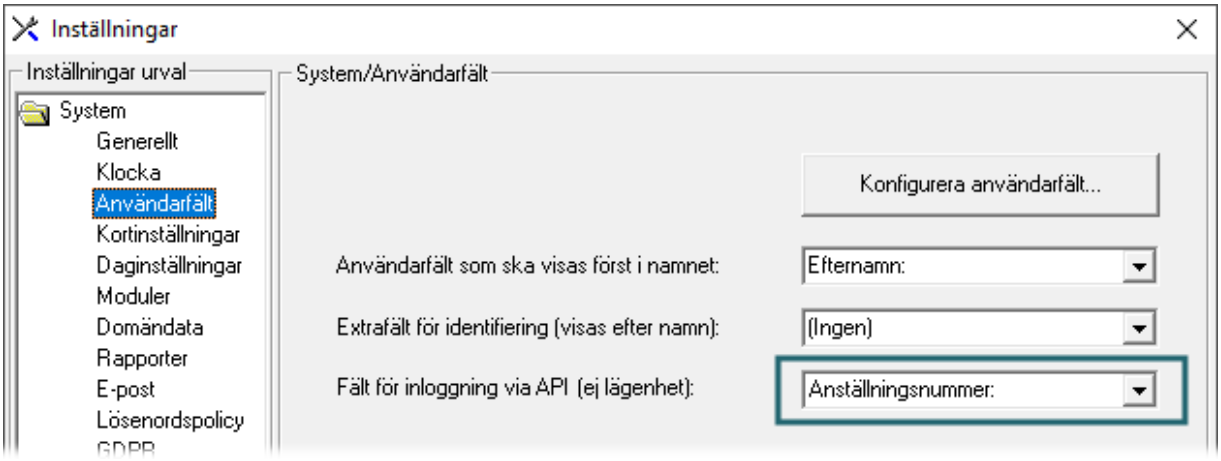
6. Markera kryssrutan i kolumnen **Synlig** för fältet **Lösen för webb**. (Fältet **Lösen för webb** visas endast efter aktivering av licenser för R-CARD M5 Access Dörr/Virtuell.)
7. Klicka på **Verkställ** och **Stäng**.

Om användare registreras i systemet

Du väljer vilket fält som slutanvändarna ska ange som inloggningsnamn i RCO Access. Väljs inget fält så kan användarna inte använda appen.

Gör så här:

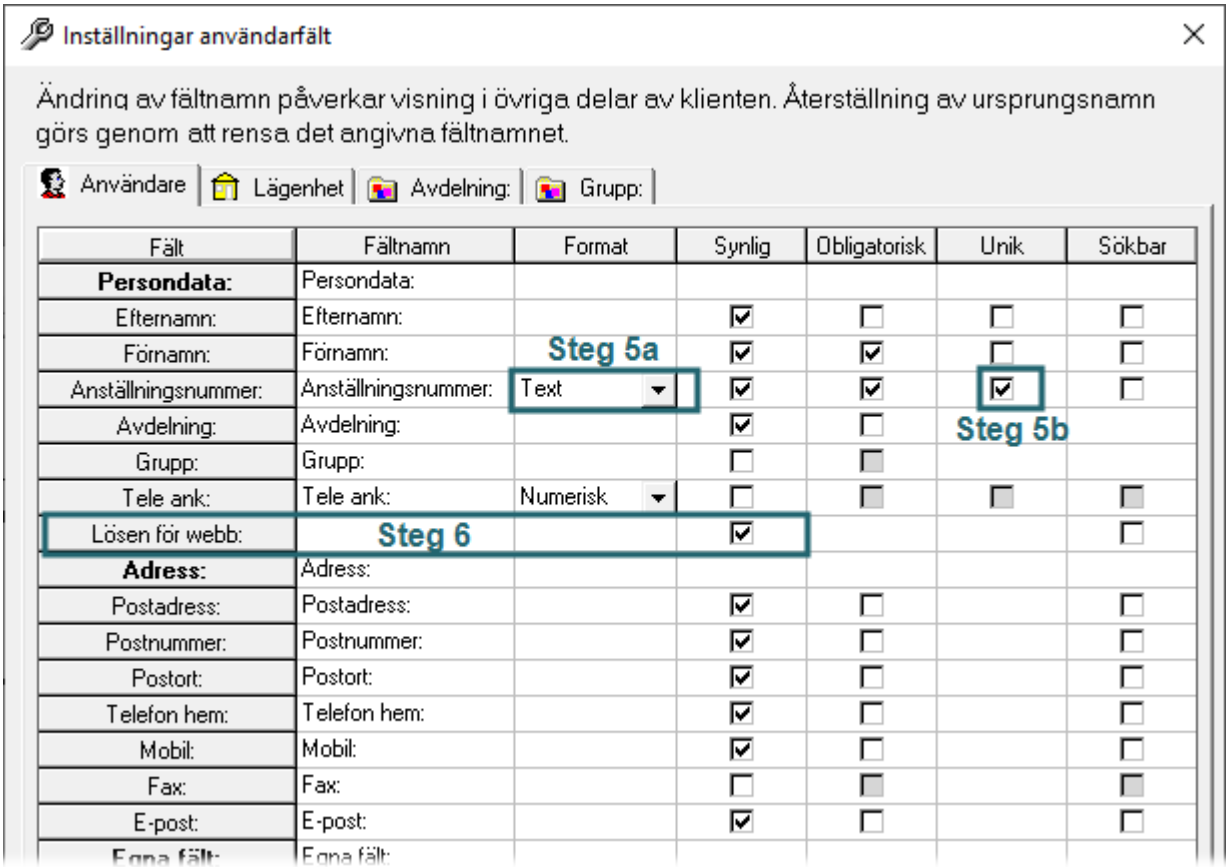
1. Välj **Inställningar** > **Inställningar**.
2. Klicka på mappen **System** och välj **Användarfält**.
3. I fältet **Fält för inloggning via API**, välj ett fält som har unik information såsom anställningsnummer eller e-post.



> Det valda fältet måste vara ett textfält (inte numeriskt). Du kan kontrollera om ett fält är numeriskt eller text i dialogrutan **Konfigurera användarfält** (se nästa steg). Om du väljer ett fält som vanligtvis är numeriskt måste formatet ändras till **Text**.

Inställningen visas endast om lämpliga licenser har registrerats eller program aktiverats.

4. Klicka på **Konfigurera användarfält**. Dialogrutan **Inställningar användarfält** visas.



Fält	Fältnamn	Format	Synlig	Obligatorisk	Unik	Sökbar
Persondata:	Persondata:					
Efternamn:	Efternamn:		☑	☐	☐	☐
Förnamn:	Förnamn:		☑	☑	☐	☐
Anställningsnummer:	Anställningsnummer:	Text	☑	☑	☑	☐
Avdelning:	Avdelning:		☑	☐		
Grupp:	Grupp:		☐			
Tele ank:	Tele ank:	Numerisk	☐			
Lösen för webb:			☑			☐
Adress:	Adress:					
Postadress:	Postadress:		☑	☐		☐
Postnummer:	Postnummer:		☑	☐		☐
Postort:	Postort:		☑	☐		☐
Telefon hem:	Telefon hem:		☑	☐		☐
Mobil:	Mobil:		☑	☐		☐
Fax:	Fax:		☐			
E-post:	E-post:		☑	☐		☐
Egna fält:	Egna fält:					

5. Anpassa det valda inloggningsfältet vid behov:
    a. Om fältets standardformat är **Numerisk**, ändra formatet till **Text**.
    b. Rekommendation: Om möjligt, markera kryssrutan i kolumnen **Unik** för det valda inloggningsfältet.

> Inställningen **Unik** är inget krav. Däremot måste den information som matas in i fältet för varje användare vara unik, annars kommer RCO Access att blockera inloggning för berörda användare. Att markera **Unik** är därför ett bra hjälpmedel då det förhindrar inmatning av icke-unik information.

6. Markera kryssrutan i kolumnen **Synlig** för fältet **Lösen för webb**.
7. Klicka på **Verkställ** och **Stäng**.

Hantering av behörighetsgrupper

För dörrstyrning via appen måste app-användarnas kort via sin behörighetsgrupp vara behörigt att öppna dörren vid den aktuella tidpunkten.

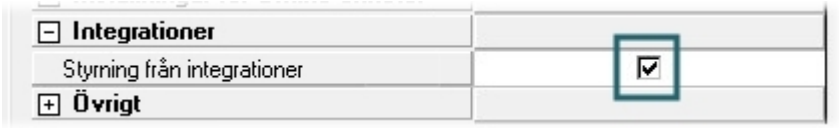
I behörighetsgruppernas egenskaper måste dessutom inställningen **Styrning från integrationer** vara markerad.

Rekommenderat är att ej ha fler än 15 dörrar/enheter i varje behörighetsgrupp. Prestandan beror på antal samtida användare och bör utvärderas innan fler dörrar läggs till.

Knyta dörrar till licenser

Varje dörr som ska kunna styras via appen måste knytas till en licens av typen R-CARD M5 Access Dörr eller R-CARD M5 Access Virtuell. Det görs via enhetens inställningar:

1. Välj **Enheter** > **Systemenheter**.
2. Markera aktuell enhet
3. Klicka på plustecknet (⊞) vid **Integrationer**.
4. Markera **Styrning från integrationer**.



5. Klicka på **Spara** ( ).

Definiera rättigheter för API-operatören

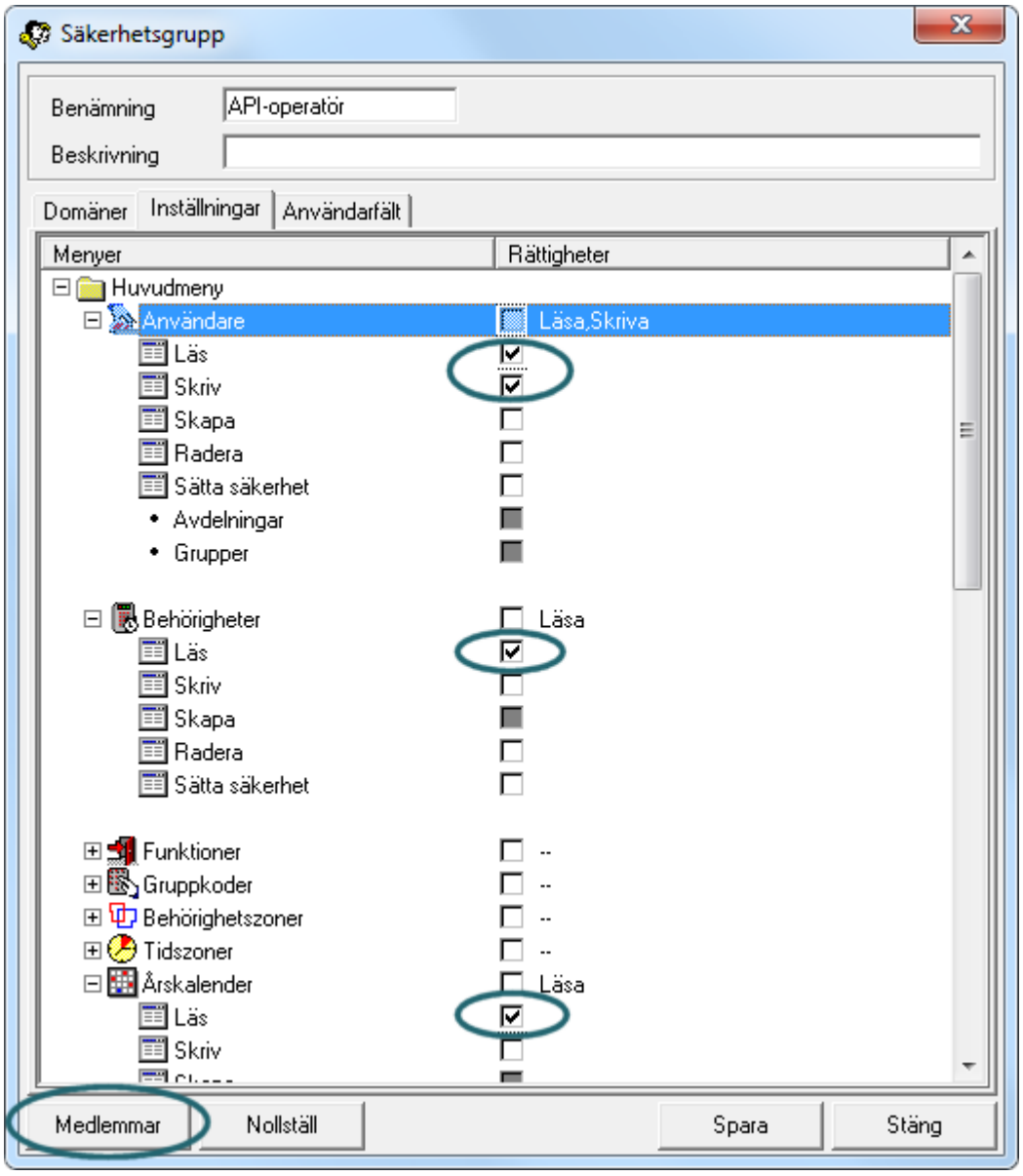
R-CARD M5 User API använder en *operatörsprofil* för att logga in mot R-CARD M5 Server. Av den anledningen måste en operatör läggas in i R-CARD M5.

Varje API-operatörsprofil knyts i sin tur till en *säkerhetsgrupp* som avgör vilka handlingar som får utföras och vilka dataposter (som exempelvis användare och behörighetsgrupper) som får hanteras.

Det rekommenderas att skapa en särskild säkerhetsgrupp för API-operatören, med syfte att begränsa åtkomst. *Undantag: Om det redan finns flera operatörer med olika säkerhetsgrupper som administrerar användare och kort i systemet, rekommenderas i stället att använda standardsäkerhetsgruppen* ***SystemAdmin*** *för API-operatören.*

API-operatören behöver följande rättigheter:

Objekt	Rättigheter
Användare/lägenheter	Läs- och skrivrättigheter
Behörighetsgrupper	Läsrättigheter
Årskalendrar	Läsrättigheter
Kortläsare som relateras till de dörrmiljöer som ska kunna öppnas via appen	Läsrättigheter



Det är sedan också möjligt att ytterligare begränsa vilka användare eller lägenheter som ska få styra dörrar via denna API-operatör. (Markera **Användare** och klicka på **Medlemmar**.)

Gör så här:

1. Välj **Huvudmeny** > **Operatörer**.
2. Markera **Säkerhetsgrupper** i trädet.
3. Klicka på ikonen **Definiera ny säkerhetsgrupp** () som nu blivit åtkomlig. Dialogrutan **Säkerhetsgrupp** visas.
4. Skriv in ett namn för säkerhetsgruppen i fältet **Benämning**.
5. Tryck nu på **F1** för vidare instruktioner och information.

Skapa operatörsprofil för API-operatören

API:et använder en *operatörsprofil* för att logga in mot R-CARD M5 Server. Skapa en separat API-operatörsprofil för ändamålet.

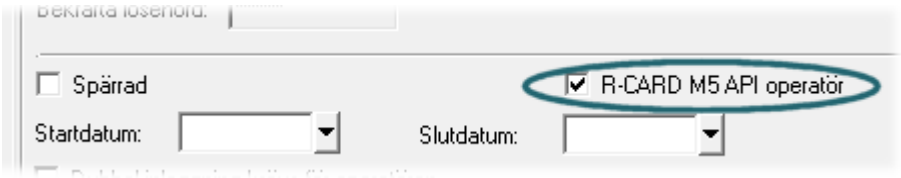
Om grundinställningen används där alla system är åtkomliga, så måste denna operatör finnas inlagd *i varje system* för att API:et ska kunna logga in.

Gör så här:

1. Välj **Huvudmeny** > **Operatörer**.
2. Markera **Operatörer** i trädet.
3. Högerklicka på en fri yta under **Operatörer** och välj **Skapa ny operatör**.
4. Ange namn och lösenord för operatören.

   Som standard används namnet **apitest** och lösenordet **1234**. Ska ett annat namn eller lösenord användas så krävs anpassningar i konfigurationsfilen **rcoservers.config**. För anvisningar se "BILAGA 1: Konfigurationsfilen rcoservers.config" på sidan 27.

5. Markera **R-CARD M5 API operatör**.



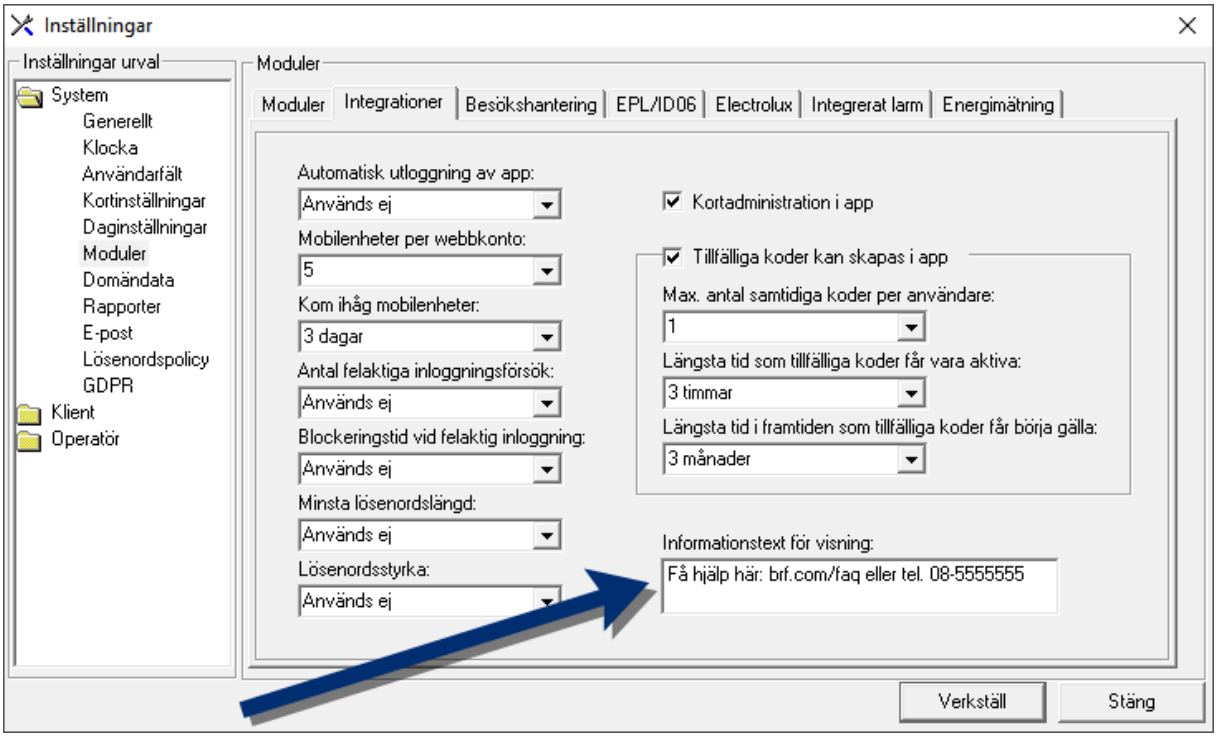
   Den här operatören kommer härmed inte kunna logga in i R-CARD M5-klienten.

6. På fliken **Medlem i**, klicka på **Ändra** och dra in den säkerhetsgrupp som skapades i föregående sektion (alternativt **SystemAdmin**).
7. Avsluta med **OK** och **Spara**.

Konfigurera säkerheten

Gör så här för att anpassa säkerheten:

1. Välj **Inställningar** > **Inställningar**.
2. Klicka på mappen **System** och välj **Moduler**.
3. Välj fliken **Integrationer**.
4. Ange önskade inställningar:



Rekommendation: Skriv ett meddelande som ska visas när slutanvändare klickar på informationsikonen på inloggningssidan i applikationen. Används för att ange vart användarna ska vända sig vid problem. Max. 50 tecken.

Inställningar för tillfälliga koder kräver R-CARD M5 version 5.48 eller senare. Om dörren har inställningen **Forcerad säkerhetsnivå** kan användare inte skapa tillfälliga koder i RCO Access.

Inställningarna beskrivs utförligt i programmets hjälpfunktion. Klicka var som helst i inställningarna och tryck på **F1**.

5. Klicka på **Verkställ** för att spara.

Hjälpa användare/boende komma igång med RCO Access

Slutanvändarna hämtar RCO Access-appen från Apple AppStore (iOS) eller Google Play (Android).

Inställningar i appen

I appens inställningar anger användarna följande:

- **Namn**: Ett beskrivande namn på den aktuella uppsättning av inställningar.
- **URL**: Adress till IIS-servern. Måste stämma överens med **server.url** i konfigurationsfilen **rcoservers.config**.
- **Server-ID**: Måste stämma överens med **server.id** i **rcoservers.config**.
- **Systemnamn**: R-CARD M5-systemnamn. Måste stämma överens med **system.name** i **rcoservers.config**.

  Alternativt (om inga system har lagts in i konfigurationsfilen) måste denna stämma exakt överens med namnet på ett system som finns på den angivna servern.

  Systemnamnet är skiftlägeskänsligt i appen men inte i **rcoservers.config**. Exempel: Om systemnamnet i R-CARD M5 är *RCARDSYSTEM* så går det bra att ange *rcardsystem* i konfigurationsfilen. I applikationen krävs dock att systemnamnet anges som *RCARDSYSTEM*.

I appen stöds svenska, norska, finska och engelska. Språket följer operativsystemets språk. I Android-applikationen kan man dock byta språk.

Tips!

- När ett system finns sparat i appen kan man dela med sig inställningarna till övriga hyresgäster utan att behöva kunna detaljerna som IP-adress och server-ID. Det görs genom att välja systemet i menyn och sedan klicka på dela-knappen i iOS (⎙) eller Android (<). (Observera att Android-appen kräver nyaste Android-operativsystem för funktion.) Alternativt kan man klicka på QR-koden för att visa en större version för skanning.
- **Rekommendation:** Underlätta inställning av URL, server-ID och systemnamn genom att skapa en QR-kod eller en applikationsspecifik länk som innehåller dessa uppgifter. Gör som ovan. Skicka sedan denna QR-kod via e-post till slutanvändarna. Alternativt, använd formuläret *RCO Access – komma igång* som

innehåller instruktioner till slutanvändarna. (Inloggning krävs för nedladdning.) Spara PDF-filen lokalt, fyll i uppgifterna och lämna till de boende.

- Manualen *RCO Access – Använda* beskriver handhavandet i appen och kan anpassas till anläggningen eller målgruppen. (Inloggning krävs för nedladdning.)

Inloggning via appen sker så här

- Boende (dvs om man lagt in *lägenheter*)
  - Användarnamn: Som inloggningsnamn anges lägenhetsnumret.
  - Lösenord: Webblösenordet (värdet i fältet **Lösen för webb**) som angetts för lägenheten. Minst 4 tecken.
- Användare (dvs om man lagt in *användare*)
  - Användarnamn: Som inloggningsnamn anges det namn som angetts i det fält man angett som inloggningsnamn. Det kan vara efternamn, epostadress, telefonnummer osv.
  - Lösenord: Webblösenordet (värdet i fältet **Lösen för webb**) som angetts för användaren. Minst 4 tecken.

Det går bra att skapa upp till 10 aktiva inloggningssessioner med samma användarnamn/lösenord i appen. (Om ytterligare inloggningar görs så tas den äldst uppdaterade sessionen bort.) Detta för att alla medlemmar i en familj ska kunna öppna en entréport. I ett normalt flerbostadssystem är varje "användare" en lägenhet med ett lägenhetsnummer. Inloggningsuppgifter delas då av alla boende i lägenheten.

Tips: Missa inte att ange i appens inställningar vart användarna ska vända sig vid problem. Se rekommendationen på sidan 18.

Viktigt vid ändring eller uppgradering av R-CARD M5 User API

Spara undan en säkerhetskopia på konfigurationsfilen **rcoservers.config**. *Filen kan raderas vid avinstallation eller uppgradering.*

Filen ligger i IIS-katalogen. Standardsökvägen är **C:\inetpub\wwwroot\M5UserAPI\rco**.

Filen beskrivs på sidan 27.

Felsökning

"Ett SSL-fel har uppstått"

Symptom

Ett meddelande visas i RCO Access:

> Fel: Ett SSL-fel har uppstått och en säker anslutning till servern kan inte göras.

Det visas endast i iOS-appen och inte i Android. Meddelandet kommer från operativsystemet iOS när R-CARD M5 Server körs på en Microsoft Windows 7-dator.

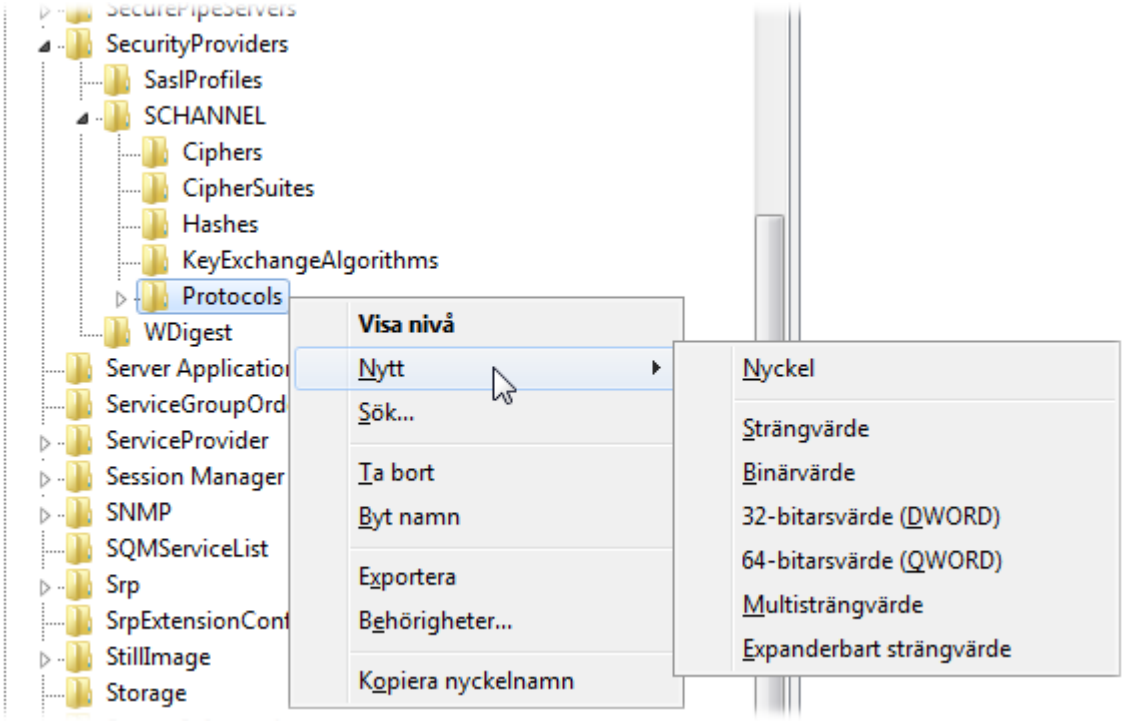
Åtgärd

Lösningen är att aktivera TLS (Transport Layer Security) 1.1 och 1.2 på R-CARD M5 serverdatorn. Det gör du genom ändringar i Windows-registret. *Använd inte Microsofts guide för detta ändamål, då den gör för mycket.*

Gör så här:

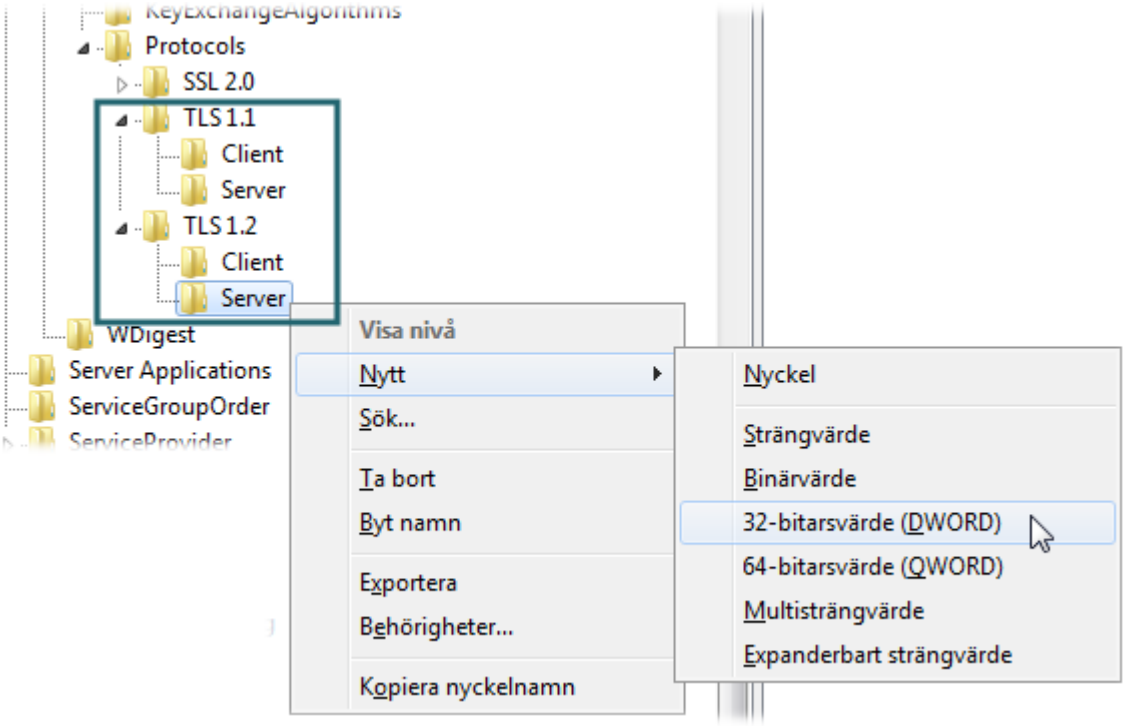
1. Öppna Windows-registret på serverdatorn. (Öppna **Kör**-fönstret och starta programmet RegEdit.)
2. Navigera till och markera följande rad:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
3. Säkerhetskopiera registret – eller mappen **Protocols** – innan du gör några ändringar! Välj **Arkiv** > **Exportera** och ange målkatalog och filnamn.
4. Lägg till **TLS 1.1** och **TLS 1.2** under **Protocols** genom att högerklicka på **Protocols** och välj **Nytt** > **Nyckel**.



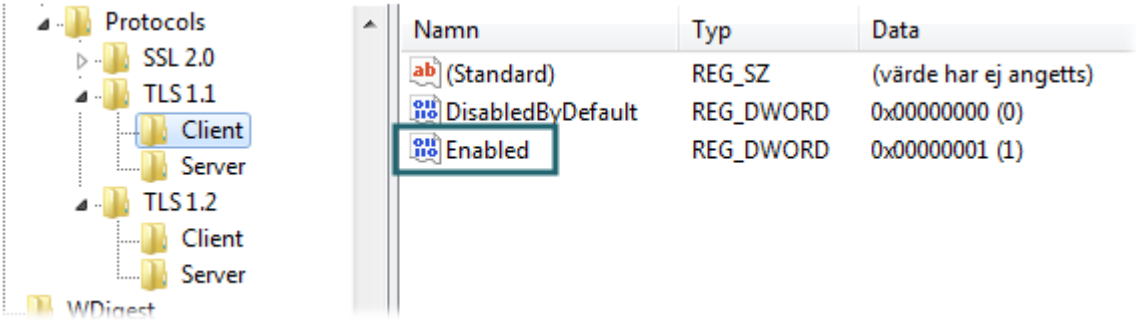
TLS 1.1 och **TLS 1.2** kommer att visas som mappar under **Protocols**, som i nedanstående bild.

5. Skapa ytterligare två nycklar under **TLS 1.1: Client** och **Server**.
6. Skapa ytterligare två nycklar under **TLS 1.2: Client** och **Server**.
7. Under var och en av **Client**- och **Server**-nycklarna, skapa ett **32-bitarsvärde (DWORD)** med namnet **DisabledByDefault**.



Ändra inte standardvärdet (0).

8. Under var och en av **Client**- och **Server**-nycklarna, skapa ett **32-bitarsvärde (DWORD)** med namnet **Enabled**.
9. Dubbelklicka sedan på varje **Enabled**-värde och ändra värdet till 1.



10. Starta om datorn.
11. Besök https://casecurity.ssllabs.com/analyze.html och testa om SSL-felet är åtgärdat.

Om problemet kvarstår

Om ovanstående förfarande inte löser problemet finns följande uppdatering från Microsoft att tillgå:

> Update to add RDS support for TLS 1.1 and TLS 1.2 in Windows 7 or Windows Server 2008 R2

Den kan behövas för att få RDP (Remote Desktop Services) över TLS 1.2 att fungera, speciellt om man tar bort 1.0 stöd.

Starta om datorn efter åtgärd.

> Om andra klientprogram använder RDP på denna dator så kontrollera om de fortfarande fungerar, speciellt om du har installerat en uppdatering. Det finns olika Microsoft Knowledge Base-artiklar för Outlook m. fl. som beskriver hur man får andra klientprogram att fungera med TLS 1.1 och 1.2.

Misslyckad uppgradering av M5UserAPI

Efter uppgradering, kontrollera att den nyare versionen faktiskt har installerats: Starta en webbläsare och ange adressen https://localhost/M5UserAPI. Kontrollera versionsnumret.

Om det äldre versionsnumret visas, avinstallera R-CARD M5 User API via **Kontrollpanelen** > **Program och funktioner**. Installera sedan en fullversion på nytt.

Kontrollera loggarna

Allmänt bästa rådet vid fel är att kontrollera loggen.

Som standard sparar R-CARD M5 API loggfiler i följande mapp:

C:\inetpub\wwwroot\M5UserAPI\logs

Det förutsätter att användaren IIS_IUSRS har skriv- och ändringsrättigheter i loggkatalogen. Se "Konfigurera loggning" på sidan 9.

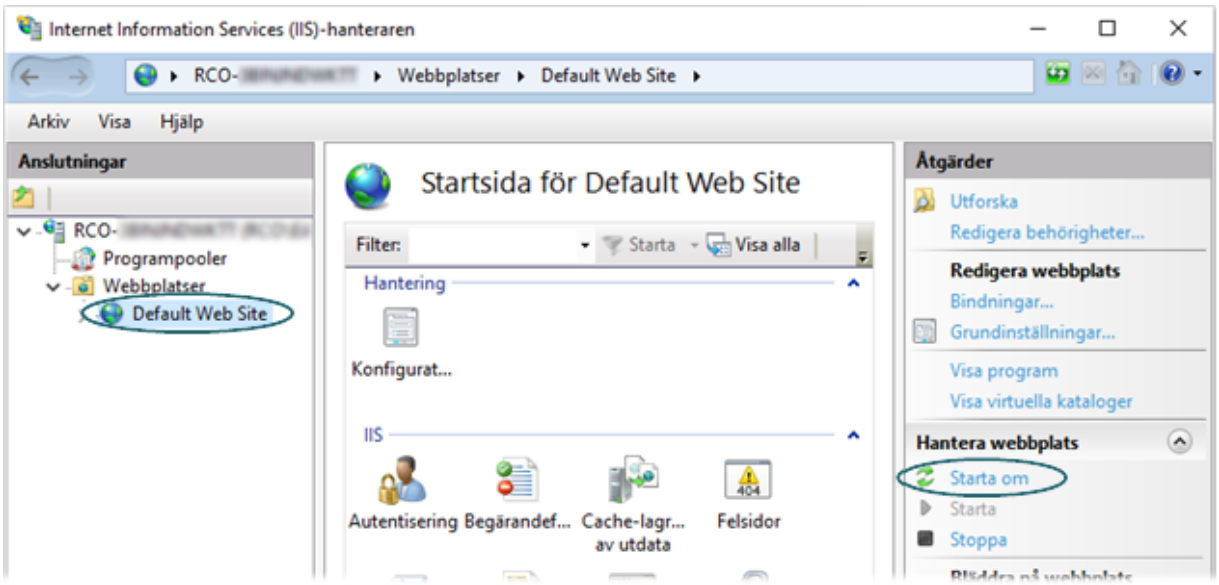
Utökad loggning via RaServiceHost är också möjlig – se sidan 10.

Starta om IIS

En omstart behövs vanligtvis vid ändringar i webbapplikationernas konfigurationsfiler.

Bilden nedan är från 64-bitars Windows 10. Det faktiska utseendet är olika beroende på OS.

1. Starta programmet Internet Information Services (IIS)-hanteraren.
2. Expandera **Webbplatser** och markera **Default Web Site**.



3. Klicka på **Starta om** i högra rutan.

"Inga platser finns"

Felbeskrivning: Nya användare eller lägenheter läggs in och ges behörighet att öppna dörrar via RCO Access, men användarna får felmeddelandet ”Inga platser finns” i appen.

Om detta förekommer i ett system med flera operatörer beror det sannolikt på att den operatör som lagt in användarna tillhör en annan säkerhetsgrupp än API-operatören, och att de två säkerhetsgrupperna ger motstridiga rättigheter.

För att lösa problemet, ge API-operatören säkerhetsgruppen **SystemAdmin** enligt nedan. Du måste själv vara inloggad som systemadministratör för att göra detta.

1. Välj **Huvudmeny** > **Operatörer**.
2. Markera **Operatörer** i trädet.
3. Välj API-operatören (dvs den som har inställningen **R-CARD M5 API-operatör** markerad).
4. Välj fliken **Medlem i**.

5. Klicka på **Ändra**.
6. Dra–släpp **SystemAdmin** till **Valda säkerhetsgrupper**.
7. Ta bort den nuvarande säkerhetsgruppen som API-operatören använder genom att dra–släppa den i motsatt riktning.
8. Avsluta med **OK** och **Spara**.

BILAGA 1: Konfigurationsfilen rcoservers.config

Översikt

R-CARD M5 User API installeras på R-CARD M5-serverdatorn, alternativt på valfri IIS-server. Konfigurationsfilens grundinställning **localhost** innebär att alla passersystem på den lokala datorn är tillgängliga från appen:

```
<?xml version="1.0" encoding="UTF-8"?>
<rcoservers>
  <server id="1" url="net.tcp://localhost:8090/RcardServices/RcardService"
    identity="" username="apitest" password="1234">
  </server>
</rcoservers>
```

Konfigurationsfilen kan ändras så att IIS-webbservern betjänar flera serverinstallationer som är åtkomliga på nätverket. Varje R-CARD M5 server pekas ut med ett valbart unikt server-ID i konfigurationsfilen **rcoservers.config**. Exempel:

```
<?xml version="1.0" encoding="UTF-8"?>
<rcoservers>
  <server id="1" url="net.tcp://localhost:8090/RcardServices/RcardService"
    identity="" username="rcard" password="1234">
    <systems>
      <system name="Fastighet A" username="apia" password="4444"/>
      <system name="Fastighet B" username="apib" password="6666"/>
    </systems>
  </server>
  <server id="987654321" url="net.tcp://server1:8090/RcardServices/RcardService"
    identity="" username="rcard" password="1234" />
</rcoservers>
```

För att få åtkomst till ett R-CARD M5-system måste man veta vilken DNS/IP-adress som webbservern har samt server-ID och systemnamn.

I ett passersystem kan man administrera ett helt bestånd av fastigheter uppdelat i flera *domäner*. Domänindelning separerar hårdvara och vissa funktioner för att kunna hantera olika funktioner och resurser. För dörrstyrning via appen och R-CARD M5 User API är åtkomsten inte domänspecifik.

Man kan också begränsa eller utesluta passersystem på den lokala datorn så att de inte blir tillgängliga från appen.

Viktigt vid ändring eller uppgradering av R-CARD M5 API: Spara undan en säkerhetskopia på konfigurationsfilen **rcoservers.config**. *Filen kan raderas vid avinstallation eller uppgradering.*

Redigera rcoservers.config

1. Öppna filen **rcoservers.config** i Anteckningar eller annan text- eller XML-redigeringsprogram.

   Filen ligger i IIS-katalogen. Standardsökvägen är **C:\inetpub\wwwroot\M5UserAPI\rco**.

2. För varje R-CARD M5-serverdator som R-CARD M5 User API ska ha åtkomst till, lägg till ett **<server>**-element.

   Identifiera servern med hjälp av attributen **id** och **url**. (Se nästa sektion. Se även exemplet ovan.)

3. Grundinställningen är att R-CARD M5 User API har åtkomst till alla passersystem på angivna servrar. För att *begränsa* vilka system som ska vara åtkomliga, peka ut dem med hjälp av elementet **<systems>**.

   Ange systemnamnet i attributen **name**. *Namnet måste stämma överens med det systemnamn som syns i R-CARD M5.*

4. Ange vilka inloggningsuppgifter som R-CARD M5 User API ska använda vid inloggning i R-CARD M5.

   De anges i attributen **server.username** och **server.password** eller i element. (Se beskrivningar nedan.)

5. Spara och stänga filen.

6. **Viktigt:** Anpassade config-filer kan vid uppgradering eller ominstallation försvinna. Har du ändrat filen, gör en säkerhetskopia och spara kopian någon annanstans.

Referens: Element och attribut i rcoservers.config

XML Element.Attribut	Beskrivning
server	Pekar ut en R-CARD M5-serverinstans.
server.id	Valfritt unikt nummer för en R-CARD M5-server (max. 9 siffror). Används vid inloggning. Standardvärdet är 1 (localhost).
server.name	Används inte.
server.url	Adress till RaServerHost-tjänsten. Används för åtkomst till R-CARD M5 Server ("localhost" eller en IP-adress).
server.identity	Används inte.
server.username	API-operatör som R-CARD M5 User API ska använda för anslutning till alla system på denna server (om den inte överrids per system). Standardnamnet är "apitest". API-operatören måste läggas in i varje system manuellt. Instruktioner ges på sidan 17.
server.password	Lösenordet för API-operatören, som standard "1234".
systems	Anger ett eller flera system (passersystem, larmsystem, anläggning) på servern. Grundinställningen är att R-CARD M5 User API har åtkomst till alla system på utpekade servrar. För att *begränsa* vilka system som ska vara åtkomliga läggs elementet **<systems>** till. Alla system därunder som är rätt namngivna i ett **<system>**-element kommer att vara åtkomliga och inga andra.
system	Pekar ut en ett system på serverinstansen.
system.name	Systemnamnet. Måste stämma överens med det systemnamn som syns i R-CARD M5 (under **Inställningar** > **System** > **Generellt**, i fältet **Benämning**).
system.username	API-operatör att använda för systemåtkomst. Valfritt att ange. Åsidosätter i så fall **server.username** (se ovan) för detta system. API-operatören måste läggas in i varje system manuellt. Instruktioner ges på sidan 17.
system.password	Lösenord för API-operatören. Krävs om **system.username** anges.

BILAGA 2: Skaffa och tillämpa SSL-certifikat

Från 4:e oktober 2020 är det inte längre möjligt att använda självsignerade SSL-certifikat i Google Android-plattformar. Certifikatet måste istället vara signerad av en s.k. *certification authority* (CA), eller certifikatutfärdare. I annat fall kommer slutanvändare inte kunna styra dörrar via Android-appen.

Skaffa certifikat

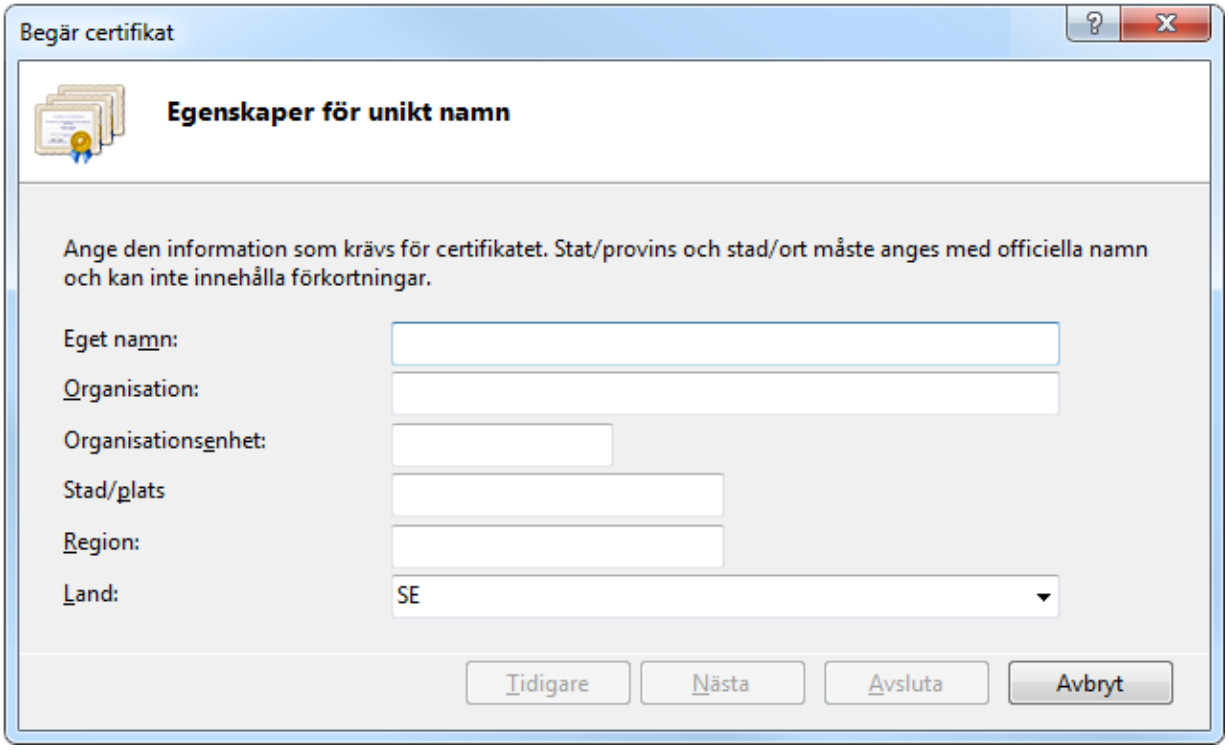
Om din organisation inte har ett SSL-certifikat kan du göra enligt nedan för att skaffa ett sådant.

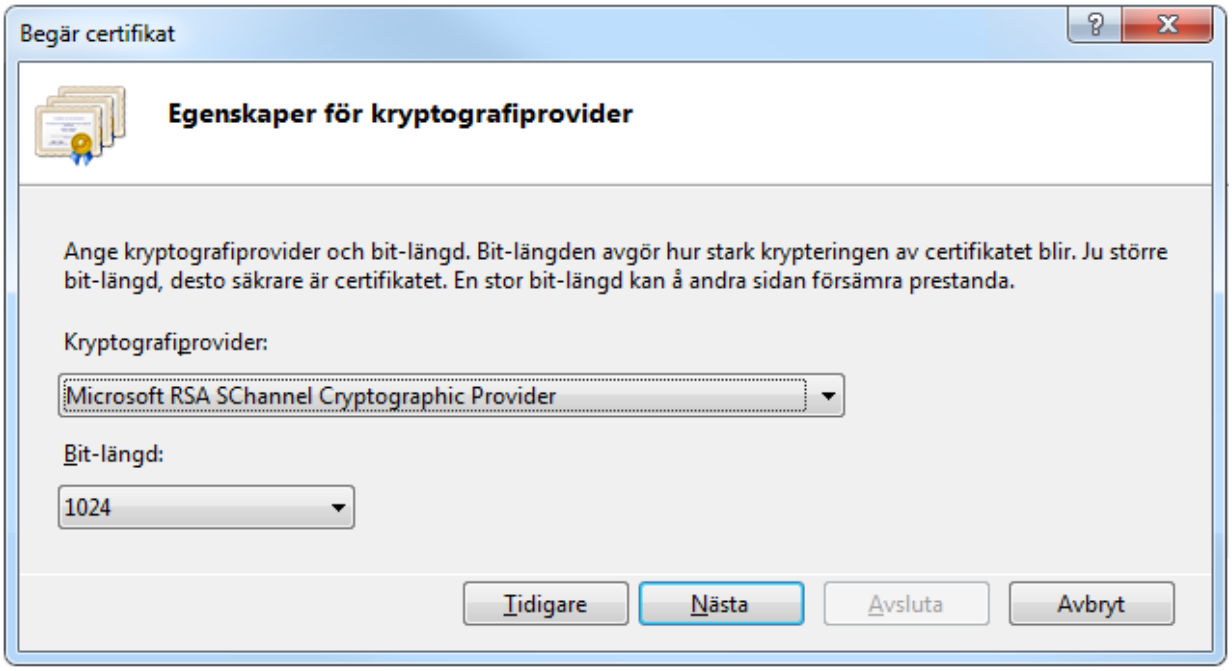
Du kan också skaffa ett certifikat från exempelvis någon av följande organisationerna och sedan ange det som under "Ange certifikatet i IIS-inställningarna" nedan.

- Lets Encrypt
- GoDaddy
- VERISIGN

Observera att det finns olika tillvägagångssätt, olika lösningar och olika prisklasser på certifikat. Saknar man kunskap inom området finns mycket information att hämta via nätet.

1. Starta programmet Internet Information Services (IIS)-hanteraren.
2. Markera översta noden till vänster.
3. Dubbelklicka på **Servercertifikat** längst ner i mittpanelen.
4. I menyn till höger, klicka på **Skapa certifikatbegäran** och följ guiden för att begära ett certifikat.





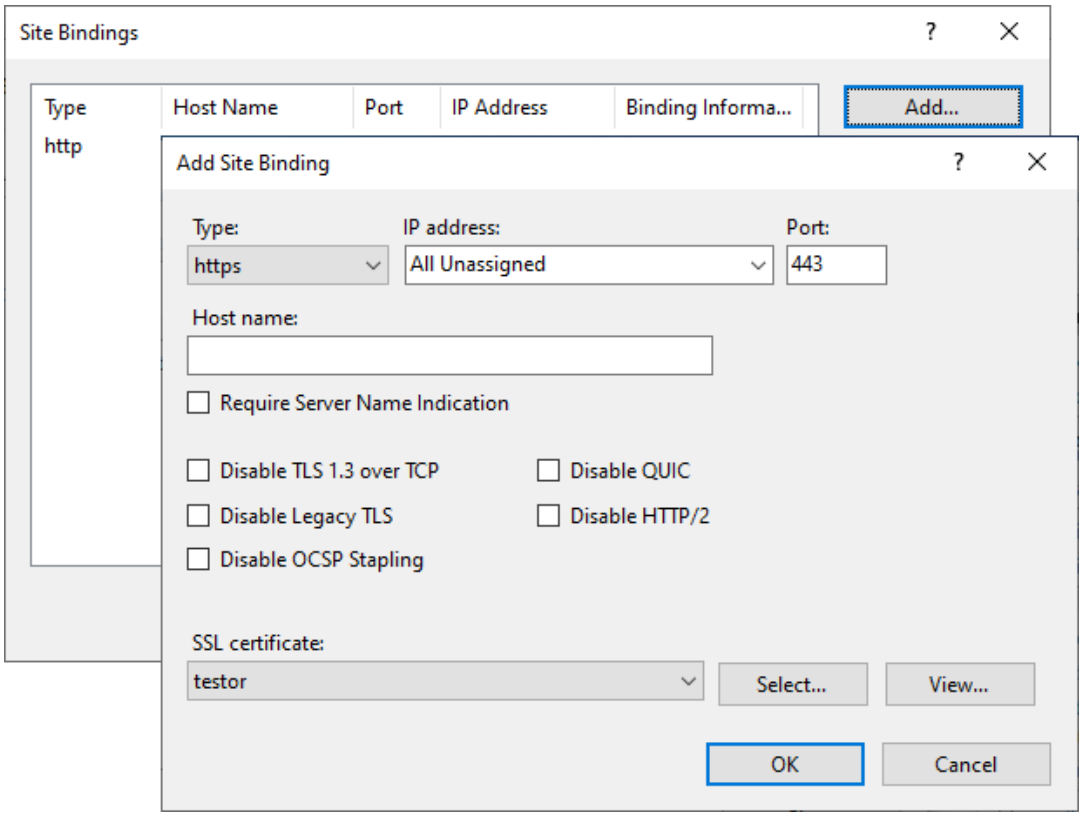
Avsluta certifikatbegäran

När du får svar från certifikatutfärdaren går du in på samma ställe som ovan och väljer **Avsluta certifikatbegäran** i steg 4. Följ instruktionerna.

Ange certifikatet i IIS-inställningarna

När certifikatet har registrerats enl. ovan måste det också anges i webbplatsens bindning:

1. Starta programmet Internet Information Services (IIS)-hanteraren.
2. På vänstra sidan, klicka på plustecknet (⊞) vid **Områden** eller **Webbplatser** och markera noden med jordgloben (🌎).
3. I menyn till höger, välj **Bindningar**. Dialogrutan **Bindningar för webbplats** visas.
4. Lägg till bindningen:
    a. Klicka på **Lägg till**.



    b. I fältet **Typ**, välj **https**.

    I fältet **IP-adress**, låt **Alla ej tilldelade** vara kvar. I fältet **Port**, låt 443 vara kvar.

    c. I fältet **SSL-certifikat**, välj det nya certifikatet.

    d. Klicka på **OK** och **Stäng**.

5. Expandera **Default Web Site** i vänstra rutan och markera **M5UserAPI**.
6. Dubbelklicka på **SSL-inställningar**.

7. Markera **Kräv SSL**. (Låt de övriga inställningarna vara som de är.)
8. I menyn till höger, klicka på **Använd**.

Frågor?

Förfarandet krävs vid användning av alla mobilapplikationer på Android-plattformen, och snart även appar på iOS-plattformen. Det finns därför gått om information att hämta från nätet.

Läs mer om certifikat på exempelvis https://https.se/faq.php.

Du kan även kontakta RCO:s Supportavdelning.