Installation och administration

Lokala Säkerhetstjänster 2.0

Innehållsförteckning

1 INLEDNING 5
1.1 Allmänt 5
1.2 Konventioner 5
1.3 Referenser 5
2 PLATTFORM OCH TREDJEPARTSPRODUKTER 6
2.1 Operativsystem 6
2.2 Java 6
2.2.1 JCE, Java Cryptography Extension 6
2.3 MySQL 6
2.4 Lastbalanserare 6
2.5 Tidssynkronisering 7
2.6 Certifikat 7
2.6.1 Ytterligare certifikat 7
2.7 CSP, Cryptographic Service Provider 7
2.8 Delad diskyta 8
2.9 Terracotta 8
2.10 Beroenden till externa system 8
2.10.1 HSA-WS 8
2.10.2 Revokeringskontroll av certifikat 9
2.10.3 SPAR-tjänsten* 9
2.10.4 Nationell Spärrtjänst* 9
2.10.5 Tjänsteplattformen* 10
3 SYSTEMÖVERSIKT 11
3.1 Ingående servrar 11
3.2 Portöversikt 13
3.3 Adressöversikt gränssnitt 14
3.4 Flera instanser 16
4 INSTALLATION AV DATABASSERVER 17
4.1 Installationsanvisningar för MySQL 17
4.1.1 Skapa ny användare. 17
5 INSTALLATION AV APPLIKATIONSSERVER 19
5.1 Installera Java och JCE 19
6 INSTALLATION AV LOKALA SÄKERHETSTJÄNSTER 20
6.1 Installera systemet på Windowsmiljö 20
6.1.1 Installation 20
6.1.2 Installation av SingleServer 21
6.1.3 Installation på första noden i en fail-over lösning 24
6.1.4 Installation på andra noden i en fail-over lösning 29
6.1.5 Installation på övriga noder (nod3- nodx) i en fail-over lösning 31
7 Uppstart av server 32

7.1 Uppstart av Terracotta 32
7.2 Uppstart av Lokal säkerhetstjänst på första noden 32
7.3 Anslut till webbgränssnittet 35
7.4 Uppstart av Lokal säkerhetstjänst på övriga noder 36

8 SYSTEMKONFIGURATION 37
8.1 Kopplingar mot externa system 37
8.1.1 HSA-WS 37
8.1.2 Spar-tjänsten* 38
8.1.3 Synkronisering till nationell spärrtjänst* 39
8.2 Sätta upp behörighet för användare 42
8.2.1 Allmänt 42
8.3 Ge externa vårdsystem behörighet 44
8.4 Ta bort root-certifikat för test vid en produktionssättning 44
8.5 Konfigurera upp anslutning till autentiseringstjänst 47
8.5.1 Extern autentiseringstjänst 47
8.5.2 Lokal autentiseringstjänst 47
8.5.3 Inläsning av IdP/SP Metadata 47
8.6 Aktivering av filter och åtkomstkontroll 49

9 ANVÄNDNING, START OCH STOPP 50
9.1 Logga in i lokala Säkerhetstjänster 50
9.2 Start och stopp 50
9.3 Hantera aktiviteter i OSGI 50
9.3.1 Aktivering och avaktivering av SAML filter 51
9.3.2 Inläsning av behörighetsregler 51
9.3.3 Aktivering och avaktivering av behörighet 51
9.4 Systemloggning 52
9.4.1 Loggning via loggtjänsten 52
9.5 Felsökning 52

10 FÖRVALTNING OCH UNDERHÅLL 53
10.1 Periodiskt underhåll 53
10.2 Övervakning 53
10.3 Uppgradering 54

11 HSA-WS 55

12 Avinstallation 56

13 Appendix A Skapa separat servicekonto 58

14 Appendix B Användning av generell konfiguration 75

Revisionshistorik		
Version	**Författare**	**Kommentar**
0.1	Logica	Dokument upprättat
0.2	Logica	Förtydligande i text
0.3	Logica	Uppdaterat portbeskrivning
0.4	Logica	Uppdaterat installation, övervakning
0.5	Marcus Tinnsten	Uppdaterat installationsguide
0.6	Marcus Tinnsten	Uppdaterat portbeskrivning
1.0	Marcus Tinnsten	Dokument färdigställt till systemversion 1.9
1.1	Marcus Tinnsten	Uppdaterat kapitlet ”systemkonfiguration”
1.11	Marcus Tinnsten	Nytt avsnitt i systemkonfiguration
1.2	Marcus Tinnsten	Dokumentet justerat för Lokala Säkerhetstjänster 2.0
1.3	Örjan Olofsson	Uppdaterat installationsguide samt kapitlet ”systemkonfiguration”
1.4	Roger Öberg	Uppdaterad
1.5	Daniel Fjällström	Uppdaterad

1 INLEDNING

1.1 Allmänt

Detta dokument beskriver installation för lokala Säkerhetstjänster vilket består av fyra stycken tjänster: Autentisering (IdP), Spärr, Samtycke och Patientrelation som kan installeras var och en för sig eller tillsammans på samma server. Färdigt installationspaket och operativsystemspecifika instruktioner gäller för Windows

Dokumentet beskriver i huvudsak fem områden:

1) Installation av databasserver
2) Installation av applikationsserver
3) Installation och konfiguration av lokala säkerhetstjänster på applikationsservern
4) Användning av lokala säkerhetstjänster
5) Administration, förvaltning och underhåll

Installationspaketet för lokala Säkerhetstjänster delar:

Sökväg	Beskrivning
db	Konfigurationsfiler och databasskript (MySQL).
doc	All dokumentation
example	Exempelkod för hur man kan ansluta en SP till IdP:n (lokal autentiseringstjänst)
install	Installationsskript och systemkomponenter.
Schema_wsdl	Tjänstekontrakten för lokala Säkerhetstjänster

1.2 Konventioner

I detta dokument finns vissa typografiska markeringar för att klargöra instruktioner. Dessa bör tolkas enligt följande:

Kursiv	Används vid hänvisning till ett specifikt namn, adress, eller annat värde som inte är löpande text.
[*Ref nr*]	Referensangivelse

1.3 Referenser

Referensnr	Namn	Adress
Ref 1	Inera AB	www.inera.se
Ref 2	Inera AB	Anvandarhandbok_Sakerhetstjanster.pdf

2 PLATTFORM OCH TREDJEPARTSPRODUKTER

Följande tredjepartsprodukter och infrastruktur måste installeras först och utgör "plattformen" för lokala Säkerhetstjänster.

2.1 Operativsystem

Lokala Säkerhetstjänster levereras med installationsanvisningar för *Windows Server 64bit*. Systemet fungerar även för andra operativsystem där Java och MySQL finns tillgängligt, men är kvalitetssäkrat på Windows Server 2008 R2 64bit varför detta operativsystem rekommenderas. Lokala Säkerhetstjänster bör driftsättas med minst två dedikerade maskiner, en applikationsserver och en databasserver.

2.2 Java

För att starta tjänsten krävs Oracle Java SE 6, JDK (senaste update), 64 bitar, som finns att hämta på: http://www.oracle.com/technetwork/java/javase/downloads/index.html. Systemet är kvalitetssäkrat med JDK 6 update 35.

2.2.1 JCE, Java Cryptography Extension

Det krävs även ett tillägg, http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html, som måste installeras för att kunna använda 256 bitars kryptering.

2.3 MySQL

Lokala Säkerhetstjänster kräver databasservern *MySQL Community Server 5.5* för Windows. Systemet är kvalitetssäkrat med *MySQL Community Server 5.5.27*.
Databasen bör ha redundant lagring och/eller en backup-rutin vid produktionssättning. Eftersom detta är en driftrelaterad fråga som kan lösas på en mängd olika sätt så beskrivs det inte mer här.

2.4 Lastbalanserare

En lastbalanserare som klarar HTTPS krävs för att köra lokala Säkerhetstjänster med skalskydd och/eller trafikdirigering. Anvisningar för lastbalanserare ingår inte i detta dokument. Läs även *kapitel 3.1* som beskriver infrastrukturen.

Lastbalansering till applikationsserver kan ske med round-robin då all sessionsdata delas mellan applikationsservrarna. Hur övervakning av applikationsservern kan ske finns beskrivet i *kapitel 10.2*. Men som ett minimum bör de externa https portarna som används tcp monitoreras innan lastbalansering sker till applikationsservern.

2.5 Tidssynkronisering

Operativsystemen för lokala Säkerhetstjänster skall vara tidssynkroniserade för att systemet skall fungera korrekt. Felaktigt inställd tid kan få till följd att autentisering av klienter misslyckas samt att systemet lagrar och/eller uppger felaktiga tidpunkter för verksamhetsdata. Detta säkerställs på operativsystemnivå och är inte en del av produkten. För att synkronisera tiden kan t.ex. *NTP* användas.

2.6 Certifikat

Innan installation av lokala Säkerhetstjänster påbörjas så måste två SITHS-tjänstecertifikat (funktionscertifikat) för legitimering **och** signering införskaffas, utfärdade för lokala Säkerhetstjänster applikationsserver. Certifikat används för att identifiera applikationsservern vid all sorts kommunikation. Certifikaten skall vara utfärdade till det värdnamn som skall användas för applikationsservern. Var god kontakta Inera för information kring SITHS-certifikat [*Ref 1*].

2.6.1 Ytterligare certifikat

Om lokala Säkerhetstjänster ska nyttjas tillsammans med andra IdP:er i en federation krävs ytterligare ett SITHS-tjänstecertifikat(legitimering) som är utfärdat till applikationsservern på den gemensamma domänen inom federationen. Dvs. om den gemensamma domänen i federationen är commondomain.example.com så behöver denna applikationsserver ha ett certifikat där också, t.ex. applikationsserver.commondomain.example.com

2.7 CSP, Cryptographic Service Provider

För att slutanvändare skall kunna använda ”hårda certifikat” (t.ex. SITHS-certifikat) för att autentisera sig och ansluta sig till administrationsgränssnittet för lokala Säkerhetstjänster via webbläsare krävs tillgång till en CSP på användarens dator. T.ex. kan Net iD användas. Var god kontakta Inera för information kring SITHS och Net iD [*Ref 1*].

2.8 Delad diskyta

För att kunna köra systemet med flera servrar i en HA-lösning krävs att samtliga noder har tillgång till en delade diskyta där bl.a. systemets gemensamma konfiguration finns lagrat. Den delade diskytan kan t.ex. sättas upp med hjälp av en samba-share eller microsoft cluster disk.

2.9 Terracotta

Om man kör systemet på flera servrar, kommer Terracotta installeras också på nod1 och nod2 i klustret. Terracotta kommer köras som egen process på noderna och är en form av databas där bl.a. sessionsdata och information om systemet lagas. Installation av terracotta görs i samband med installation av applikationsservern nedan.

2.10 Beroenden till externa system

2.10.1 HSA-WS

HSA-WS är en webtjänsteanslutning till underliggande HSA-katalog. Lokala Säkerhetsjänster använder HSA-WS version 2.19 eller senare. Applikationsserverns tjänstecertifikat för legitimering måste också läggas in i HSA-strukturen. Certifikatet behöver ha tillstånd att anropa följande operationer:

- *GetCareUnit*
- *GetCareUnitList*
- *GetHsaPerson*
- *GetHsaUnit*
- *GetMiuForPerson*
- *Ping*

Lokala Säkerhetstjänster använder HSA-WS för att hämta information om användare, användares medarbetaruppdrag, vilka vårdenheter som tillhör en vårdgivare, namn på vårdenheter m.m.
För att en användare ska kunna autentisera sig krävs det att användaren finns upplagd i HSA. Det finns dock inget krav på att användaren måste ha ett medarbetaruppdrag. Ifall användaren saknar medarbetaruppdrag kommer en ”tom” SAML-biljett att skapas utan egenskaper för användaren och det är upp till konsumenten av SAML-biljetten, SP:n, att avgöra vad som skall ske då (t.ex. visa ett felmeddelande).
HSA-WS ingår inte i produkten Lokala Säkerhetstjänster.

Adresser som kan användas för att nyttja HSA-WS:
Test: https://testhotell2.carelink.sjunet.org/svr-hsaws2/hsaws
Produktion: https://hsahotell.carelink.sjunet.org/svr-hsaws2/hsaws

2.10.2 Revokeringskontroll av certifikat

Applikationsservern för lokala Säkerhetstjänster använder i första hand OCSP och i andra hand CRL för att kontrollera ifall ett klientcertifikat är spärrat och därmed inte godkänt för autentisering. Adressen till servrarna som används för OCSP och CRL hämtas från certifikaten och kan därför variera beroende på vilka certifikatet som används. Dessa servrar måste kunna anropas från applikationsservern över HTTP (default port 80).

Exempel på adresser till crl och ocsp (Produktion):

Certifikat	Crl adress	Ocsp adress
SITHS Type 1 CA v1	http://crl1.siths.se/sithsrootcav1.crl http://crl2.siths.sjunet.org/sithsrootcav1.crl	http://ocsp1.siths.se http://ocsp2.siths.sjunet.org
SITHS CA v3 SITHS CA v4	http://www.carelink.se/siths-ca/ca003.crl	http://sithsocsp.trust.telia.com

Exempel på adresser till crl och ocsp (Test):

Certifikat	Crl adress	Ocsp adress
SITHS_Type_1_CA_v1_PP	http://crl1pp.siths.se/sithsrootcav1pp.crl http://crl2pp.siths.sjunet.org/sithsrootcav1pp.crl	http://ocsp1pp.siths.se http://ocsp2pp.siths.sjunet.org
SITHS CA TEST v3 SITHS CA TEST v4	http://www.carelink.se/siths-ca/test-crl0003.crl	http://sithsocsp.preprod.trust.telia.com

2.10.3 SPAR-tjänsten*

SPAR-tjänsten är en tjänst som innehåller personuppgifter. Lokala Säkerhetstjänster använder SPAR för att hämta patientens namn i användargränssnittet.

Adresser som kan användas för att nyttja SPAR:
Test: https://tgptest.npo.sjunet.org/PU/PUServiceCacheOnly.svc
Produktion: https://tgp.npo.sjunet.org/PU/PUServiceCacheOnly.svc

*SPAR-tjänsten används enbart ifall man installerar någon av tjänsterna: Samtycke, Patientrelation och Spärr

2.10.4 Nationell Spärrtjänst*

Den lokala spärrtjänsten har inbyggd funktionalitet för synkronisering av spärrdata mot den nationella spärrtjänsten. Innan replikeringen aktiveras måste förvaltningsorganisationen för nationell spärrtjänst kontaktas för att öppna upp access till tjänsten samt konfigurera vilka vårdgivare som denna lokala spärrtjänst tillåts hantera nationellt. Hur detta görs beskrivs senare i dokumentet. Kontakta Ineras förvaltning i god tid före driftstart [*Ref 1*].

Adresser som kan användas för att nyttja Nationell Spärrtjänst:
Test:
https://acctest.sparr.sakerhetstjanst.sjunet.org:8644

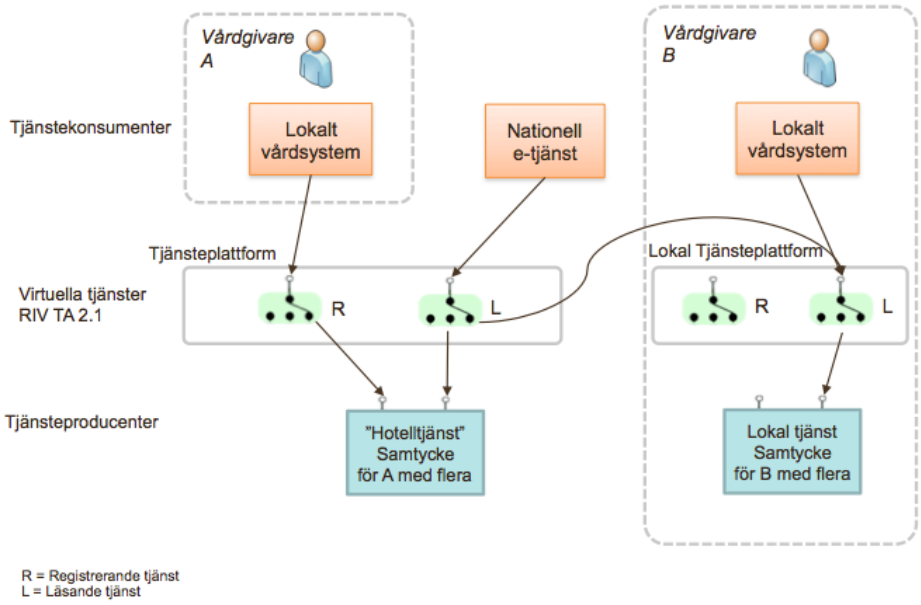
https://utvtest.sparr.sakerhetstjanst.sjunet.org:8644
https://prodtest.sparr.sakerhetstjanst.sjunet.org:8644

Produktion:
https://sparr.sakerhetstjanst.sjunet.org:8644

*Nationell Spärrtjänst används enbart ifall man installerar tjänsten Spärr
(Inom kort kommer synkroniseringen av spärrdata att kunna ske via tjänsteplattformen också)

2.10.5 Tjänsteplattformen*

Installerar man samtyckestjänsten och/eller patientrelationstjänsten måste man registrera dessa som producenter i tjänsteplattformen. Detta för att samverkan ska kunna ske med de nationella tjänsterna. Där t.ex. en nationell tjänst vill läsa ifrån denna lokala instans om ett samtycke finns registrerat. Figuren nedan illustrerar hur en läsande nationelltjänst routas via den nationella tjänsteplattformen, genom en lokal tjänsteplattform(optionell) för att till sist hamna i den lokala samtyckestjänsten.



Figur 1: Principer för samverkande tjänster för hantering av samtycke

Kontakta Ineras förvaltning i god tid före driftstart för att registrera tjänsterna i tjänsteplattformen [*Ref 1*].

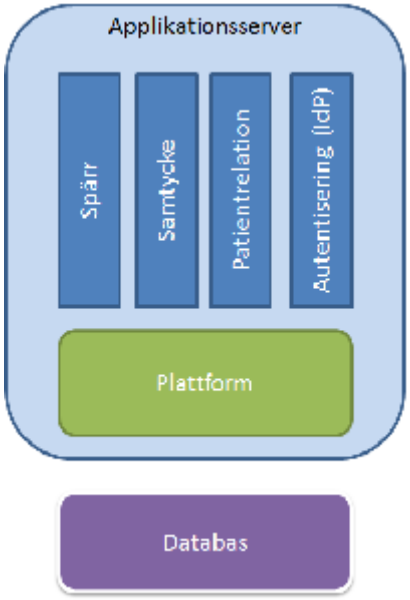
*Tjänsteplattformen används enbart ifall man installerar någon av tjänsterna: Samtycke och patientrelation.

3 SYSTEMÖVERSIKT

Detta kapitel beskriver hur systemet sätts upp med maskiner och nätverksstruktur.

3.1 Ingående servrar

Lokala Säkerhetstjänster består av en applikationsserver och en databasserver. På applikationsservern installeras en gemensam plattform. På plattformen kan man välja vilken/vilka utav de fristående tjänsterna Spärr, Samtycke, Patientrelation och Autentisering (IdP) man vill installera.

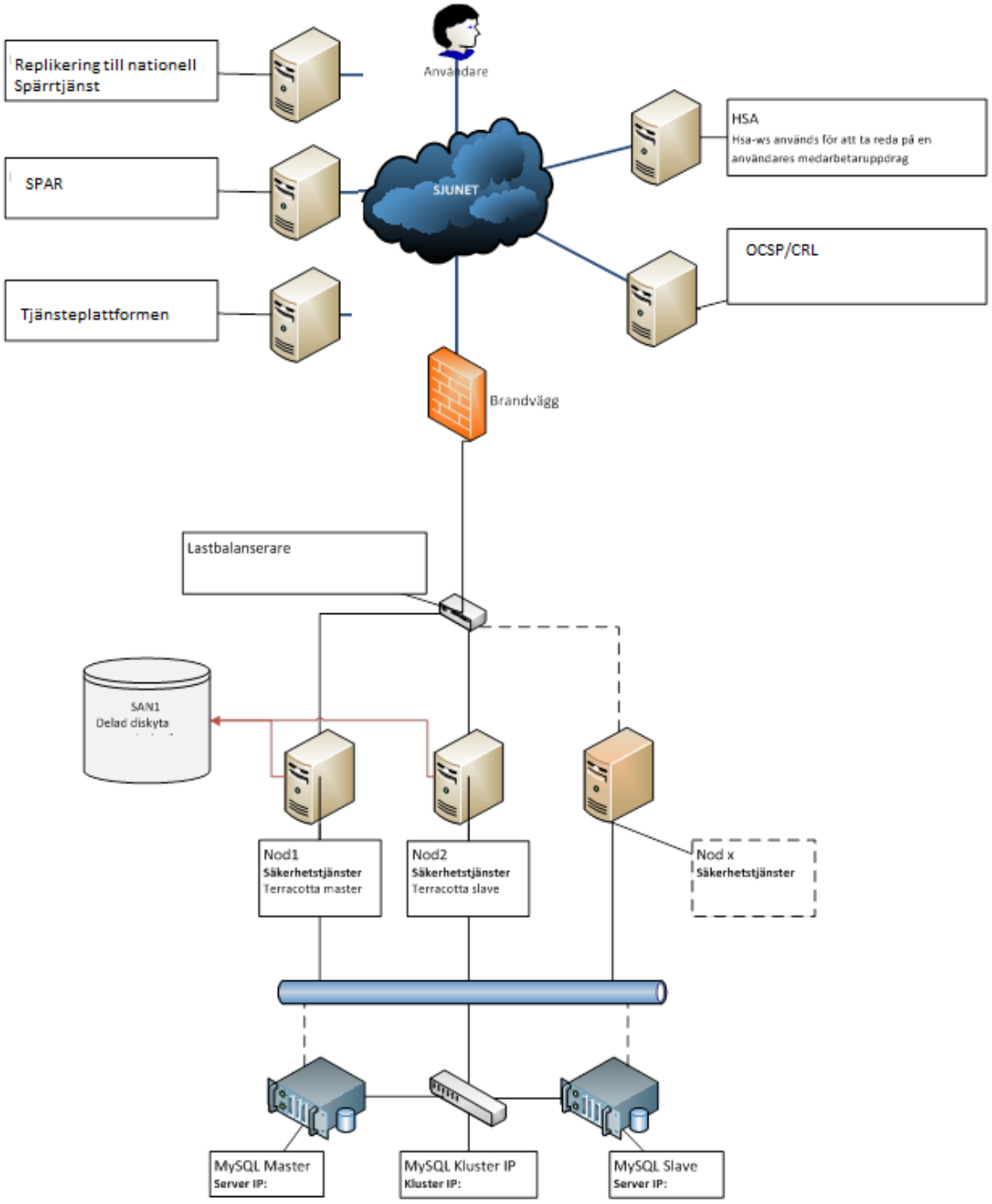


Figur 2: Översikt applikationsserver.

Lokala Säkerhetstjänster kan konfigureras på två grundläggade sätt, med eller utan så kallad "fail-over". Med fail-over avses en eller flera maskiner/servrar som används tillsammans med den primära servern för att höja tillgängligheten på systemet och öka kapaciteten på systemet. För att kunna köra med en eller flera fail-over servrar krävs att alla noder har en delad diskyta.

En lastbalanserare (omnämns inte i detalj här) används för att dirigera trafiken till alla applikationsservrar (genom t.ex. round-robin). Och om fel uppstår på någon av applikationsservrarna tas dirigeringen bort till den felaktiga servern. Fail-over-maskinerna bör vara identiska med ordinarie maskiner.

Singelserverlösning består av en (1) applikationsserver och en (1) databasserver, total två stycken maskiner. För fail-over tillkommer alltså ytterligare två maskiner. *figur 3* nedan visar ett exempel med fail-over.



Figur 3: Systemöversikt

3.2 Portöversikt

Denna tabell visar vilka portöppningar som krävs för att lokala Säkerhetstjänster skall fungera. Standardport avser föreslagen standardport, men dessa konfigureras manuellt vid installationen. *In* betyder inkommande trafik och *Ut* utgående trafik).

Server	Standardport	Beskrivning
Applikationsserver		
	8443 (in)	Extern HTTPS (envägs-SSL, generellt administrationsgränssnitt)
	8444 (in)	Extern HTTPS (tvåvägs-SSL, IdP webbgränssnitt för identifiera användare med certifikat t.ex. SITHS) *Används endast vid installation av lokal IdP
	8445 (in)	Extern HTTPS (envägs-SSL, IdP webbgränssnitt med bla.val av identifikationsmetod och SSO) *Används endast vid installation av lokal IdP
	8446 (in)	Extern HTTPS (envägs-SSL, IdP webbgränssnitt för CDC hantering)
	8080 (in)	Extern HTTPS (tvåvägs-SSL, WebServices, t.ex.CheckBlocks)
	8004 (in)	Java JMX-övervakning, behöver ej öppnas om inte övervakning används. Bör ej vara extern utanför DMZ.
	1111 (in)	Telnet-port för systemkonsol. Bör ej öppnas externt.
	9510 (in/ut)	Interna portar som används av terracotta-tjänsten då man använder fail-over. Ska ej öppnas externt utan endast vara öppen internt för de andra noderna.
	9520 (in/ut)	
	9530 (in/ut)	
	443 (ut)	HTTPS-anrop till HSA-WS. SPAR-tjänsten
	80 (ut)	Porten används av systemet för slagningar mot OCSP och CRL kontroll för verifiering av certifikat på exempelvis SITHS-kort. Använder man andra certifikat än SITHS kan andra portar vara aktuella för OCSP/CRL.
	8644 (ut)	Replikering till nationell spärrtjänst *Används endast vid installation av lokal spärrtjänst
	3306 (ut)	Anrop till databasservern.
Databasserver		
	3306 (in)	Anslutningsport till MySQL-databas. Används av applikationsservern. Bör ej vara extern utanför DMZ.

En användare som nyttjar lokala Säkerhetstjänster kommer att behöva nyttja portar 8443-8446. Externa system som ska använda tjänsten ansluter mot port 8080.

3.3 Adressöversikt gränssnitt

Denna tabell visar adresser/URL:er till de webbgränssnitt som kan användas av användare av den lokala Säkerhetstjänsten. Se tjänstekontraktsbeskrivningen för detaljerad beskrivning av tjänsterna och dess användning.

Alla adresser för webbgränssnitt har följande prefix:
https://<Hostnamn-Applikationsserver>:8443/

Adress	Beskrivning
blockservice	Den lokala säkerhetstjänstens administrations guit. Där sidor för bl.a. spärr, samtyck och patientrelation finns.
consentpdlservice	
Patientrelationservice	
spadmin	Webbsida för adminstration
monitor	Webbsida för att övervaka systemet.
com.logica.se.bif.externalpages.web	Samtyckes-dialog som externa tjänster kan nyttja

Alla adresser för webbgränssnitt för idp har följande prefix:
https://<Hostnamn-Applikationsserver>:8445/

Adress	Beskrivning
idp	Autentiseringstjänst (IdP)

Alla adresser för webbtjänstegränssnitt har följande prefix:
https://<Hostnamn-Applikationsserver>:8080/

Spärr Rivta 2.0
services/CancelTemporaryExtendedRevokeResponderService
services/CheckBlocksResponderService
services/DeleteExtendedBlockResponderService
services/GetAllBlocksResponderService
services/GetBlocksForPatientResponderService
services/GetExtendedBlocksForPatientResponderService
services/RegisterExtendedBlockResponderService
services/RegisterTemporaryExtendedRevokeResponderService
services/RevokeExtendedBlockResponderService

Spärr Rivta 2.1
blockingLocalService/CancelTemporaryExtendedRevoke/2/rivtabp21
blockingLocalService/CheckBlocks/2/rivtabp21
blockingLocalService/DeleteExtendedBlock/2/rivtabp21
blockingLocalService/GetBlocks/2/rivtabp21
blockingLocalService/GetBlocksForPatient/2/rivtabp21
blockingLocalService/GetExtendedBlocksForPatient/2/rivtabp21
blockingLocalService/GetPatientIds/2/rivtabp21
blockingLocalService/PingForConfiguration/1/rivtab21
blockingLocalService/RegisterExtendedBlock/2/rivtabp21
blockingLocalService/RegisterTemporaryExtendedRevoke/2/rivtabp21
blockingLocalService/RevokeExtendedBlock/2/rivtabp21

Samtycke Rivta 2.1
consentService/CancelExtendedConsent/1/rivtabp21
consentService/CheckConsent/1/rivtabp21
consentService/DeleteExtendedConsent/1/rivtabp21
consentService/GetConsentsForCareProvider/1/rivtabp21
consentService/GetConsentsForPatient/1/rivtabp21
consentService/GetExtendedConsentsForPatient/1/rivtabp21
consentService/PingForConfiguration/1/rivtab21
consentService/RegisterExtendedConsent/1/rivtabp21
Patientrelation Rivta 2.1
blockingLocalService/CancelTemporaryExtendedRevoke/2/rivtabp21
blockingLocalService/CheckBlocks/2/rivtabp21
blockingLocalService/DeleteExtendedBlock/2/rivtabp21
blockingLocalService/GetBlocks/2/rivtabp21
blockingLocalService/GetBlocksForPatient/2/rivtabp21
blockingLocalService/GetExtendedBlocksForPatient/2/rivtabp21
blockingLocalService/GetPatientIds/2/rivtabp21
blockingLocalService/PingForConfiguration/1/rivtab21
blockingLocalService/RegisterExtendedBlock/2/rivtabp21
blockingLocalService/RegisterTemporaryExtendedRevoke/2/rivtabp21
blockingLocalService/RevokeExtendedBlock/2/rivtabp21

3.4 Flera instanser

Man kan låta flera vårdgivare använda samma enskilda installation av lokala säkerhetstjänster eftersom åtkomstkontroll sker på vårdgivarnivå i systemet. Slutanvändare av adminstrationen av t.ex. spärr tillåts bara hantera spärrar på sin egen vårdgivare och kommer aldrig åt spärrar för andra vårdgivare.

4 INSTALLATION AV DATABASSERVER

Det är av prestandaskäl rekommenderat att tilldela lokala Säkerhetstjänsters databasserver en egen fysisk maskin. Servern bör vara multikärning med minst 8 GB RAM. För utökad support och funktionalitet såsom online-backup så finns samma version i *Enterprise Edition*-utförande som dock inte är kostnadsfri.
Mer information om detta finns här: http://www.mysql.com/products/enterprise

För att nyttja automatisk fail-over samt databasreplikering med MySQL så rekommenderas DRBD. Mer information om detta finns här: http://downloads.mysql.com/docs/mysql-ha-drbd-en.a4.pdf

Den MySQL-användare som används kräver behörighet att kunna ändra, uppdatera och lägga till nya tabeller i de scheman som skapas för systemet, användaren behöver dock inte ha behörighet att kunna skapa nya scheman. Vid skapandet av scheman krävs en inloggning med en användare som har root-rättigheter.

4.1 Installationsanvisningar för MySQL

MySQL har officiella installationsanvisningar för Windows här:
http://dev.mysql.com/doc/mysql-windows-excerpt/5.5/en/index.html

4.1.1 Skapa ny användare.

Efter att MySQL är installerad så skall en användare skapas, som kräver behörighet att kunna ändra, uppdatera och lägga till nya tabeller i de scheman som skapas för systemet, användaren behöver dock inte ha behörighet att kunna skapa nya scheman. Vid skapandet av scheman krävs en inloggning med en användare som har root-rättigheter, vilket skapas under installationen av MySQL.

1. Logga in i mysql-prompten, kommando: `mysql -u root -p`
   (Ange det lösenord som angetts)
2. Skapa ny användare (i detta exempel är användarnamnet *sak* vilket rekommenderas, samt ett lösenord) genom att skriva följande rader, varje rad avslutas med *enter*:

```
3. CREATE USER 'sak'@'localhost' IDENTIFIED BY 'password';
   GRANT CREATE, DROP, EVENT, DELETE, INDEX, INSERT, SELECT,
   UPDATE, CREATE TEMPORARY TABLES, LOCK TABLES, TRIGGER, CREATE
   VIEW, SHOW VIEW, EXECUTE ON  *.* TO 'sak'@'localhost';
4. FLUSH PRIVILEGES;
```

5. Avsluta prompten, kommando: `quit`

Nu behöver scheman för de olika tjänsterna skapas:
Logga in i mysql-prompten och skapa scheman enligt tabellen nedan,
använd kommandot:

```
CREATE schema accesscontrol CHARACTER SET utf8 COLLATE utf8_bin;
```

Kör därefter följande kommando från ett kommandofönster i samma katalog som sql-filerna:

```
mysql -u root -p accesscontrol < accesscontrol.sql
```

Upprepa för varje skriptfil i tabellen.

Skripten som skall köras för att skapa dom tabeller som krävs för respektive schema finns under katalogen:

db\mysql

De skript som tillhör respektive schema visas i den högra kolumnen nedan.

Schema	Skript
accesscontrol	*accesscontrol.sql*
audit	*audit.sql*
blkloc	*blkloc.sql*
blknat	*blknat.sql*
consent	*consent.sql*
idp	*idp.sql* *idp_data.sql*
inftyp	*inftyp.sql* *inftyp_data.sql*
logreport	*logreport.sql* *logreport_data.sql*
metadata	*metadata.sql*
patientrelation	*patientrelation.sql*
sp	*sp.sql*

5 INSTALLATION AV APPLIKATIONSSERVER

Det är av prestandaskäl rekommenderat att tilldela lokala Säkerhetstjänsters applikationsserver en egen fysisk maskin. Servern bör vara multikärning med minst 12 GB RAM. På applikationsservern exekverar IdPn Java-mjukvara. Java-processen är konfigurerad att tilldelas ca. 2 GB minne.

5.1 Installera Java och JCE

Installera java och tillägget JCE Java Cryptography Extension, enligt kapitel 2.2

6 INSTALLATION AV LOKALA SÄKERHETSTJÄNSTER

När databasserver och applikationsserver är förberedda kan programvaran för lokala Säkerhetstjänster installeras. Detta görs på applikationsservern.

6.1 Installera systemet på Windowsmiljö

Konfigurera brandväggen lokalt för windows servrarna (om man valt att att slå av den lokala brandväggen, gå till kapitel 6.1.1).
Konfigurera inställningarna för branväggen genom att starta verktyget *Windows Firewall with Advanced Security* som ligger under Adminstrative Tools.

Skapa en ny regel under *Inbound rules.*

Steg	Val	Beskrivning
Rule Type	Port	Regel som kotrollerar anslutningar för TCP eller UDP port
Protocol and Ports	TCP Specific local ports	Ange dom portar som beskrivs i tabellen under kapitel 3.2.
Action	Allow the connection	Inkluderar anslutningar som vare sig är skyddade eller ej utav IPsec
Profile	Domain, Private, Public	Regeln gäller för alla dessa val.
Name	Lokala säkerhetsjänster	Namn och beskrivning för regeln,

6.1.1 Installation

Installationsprogrammet ligger under katalogen *Lokal säkerhetstjänst (win)\install\setup.exe*. Starta installationen genom att exekvera **setup.exe**. Välj den sökväg där du vill att lokala Säkerhetstjänster ska installeras och gå vidare.

- För installation av en singleserver gå till kapitel SingleServer installation
- Är detta första noden i en fail-over lösning gå till första noden i en fail-over lösning
- Är detta andra noden i en fail-over lösning gå till andra noden i en fail-over lösning
- Är detta övriga noder i en fail-over lösning gå till övriga noder (nod3- nodx) i en fail-over lösning

6.1.2 Installation av SingleServer

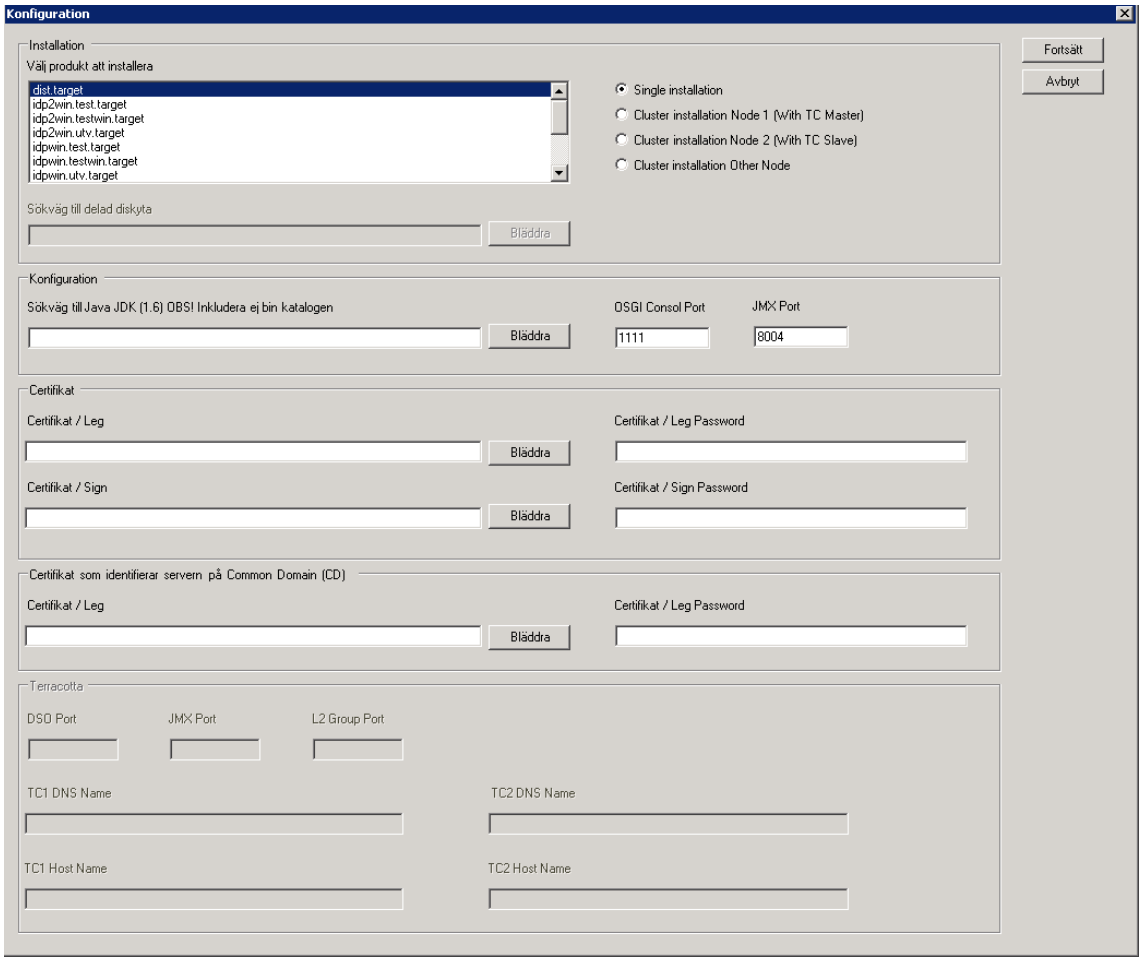
Denna installation kommer att kopiera in de filer som behövs för applikationsservern samt registrera en service ”Lokal Säkerhetstjänst”. Efter installationen är det rekommenderat att man byter servicekonto, se Appendix A Skapa separat servicekonto.

Ett konfigurationsfönster öppnas där man markerar produkten **dist.target**.

Välj *Single installation.*
Fyll i sökvägar för java och certifikat. Om man vill kan man ändra de defaultportar som används för OSGI-konsolen och JMX.

Certifikaten du anger måste vara ett *”Leg”* (legitimation) certifikat och ett *”Sign”* (signering) certifikat. De certifikaten du ska använda diskuteras i *kapitel2.6.* Ett legitimeringscertifikat måste anges som identiferar servern på *”Common Domain”.* Ange lösenord för respektive certifikat.

Klicka sedan på **Fortsätt**.



Figur 4: GUI för installation, singel installation.

Därefter öppnas ett kommandofönster där man fyller i värden för fortsatt installation. Konfiurationen är uppdelad under ett antal avsnitt, under varje avsnitt finns konfigurationsvärden som skall anges, vissa är förvalda som default värden. Fyll i de adresser och portar ni använder i respektive tillhörande kategori.

Http(s) setup
Idp Http(s) setup
Common Domain http(s) setup
HSA-WS setup
Database setup
Mongo db setup (detta avsnitt kan man ignorera under denna version, men kommer att nyttjas i senare versioner. Acceptera default värden och gå vidare)

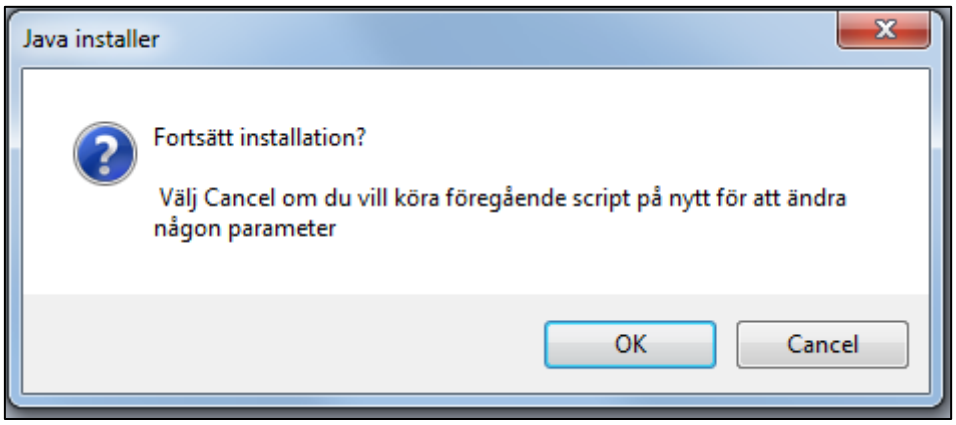
Efter varje satt värde så klickar man enter och går vidare, se *figur 3*, kommandofönster, nedan.

Figur 5: Kommandofönster

Det sista som sker är att allt kopieras ned till den förvalda installationskatalogen, sedan om allt gått bra så visas meddelandet #### Installation completed! ####

Avsluta kommandofönstret genom att skriva **exit** och trycka på **Enter**.

Klicka **Yes** på det lilla *Java installer* fönstret om ni är nöjd med konfigurationerna som angivits. (se *figur 4* nedan - observera att fönstret kan gömma sig bakom andra installationsfönster!). Klicka på **Cancel** om ni önskar att återgå till GUI:t för installationen och göra om Java konfigurationen (eller för att avrbyta installationen).



Figur 6: Java installer bekräftelsefönster

Ett bekräftelsefönster visas följande. Klicka **Close**. Gå in i verktyget *Server Manager* och *Services* och verifiera att servicen för lokala Säkerhetstjänster (LokalSakerhetstjanstService) startar upp automatiskt. Notera att uppstarten kan ta någon minut.

6.1.3 Installation på första noden i en fail-over lösning

Denna installation kommer att kopiera in de filer som behövs för applikationsservern samt kopiera de gemensamma filerna som används till den delade diskytan sam registrera två stycken servicar: ”Lokal Säkerhetstjänst” och ”Lokal Säkerhetstjänst Terracotta”. Efter installationen är det rekommenderat att man byter servicekonto, se Appendix A Skapa separat servicekonto.

Ett konfigurationsfönster öppnas där man markerar produkten **dist.target**.
Välj Cluster installation Node 1 (With TC Master)

Fyll i sökvägar för:

- Delad diskyta (som är gemensam med de andra noderna)
- Java
- Certifikat

Certifikaten du anger måste vara ett *”Leg”* (legitimation) certifikat och ett *”Sign”* (signering) certifikat. De certifikaten du ska använda diskuteras i *kapitel2.7.* Ett legitimeringscertifikat måste anges som identiferar servern på *”Common Domain”.* Ange lösenord för respektive certifikat.

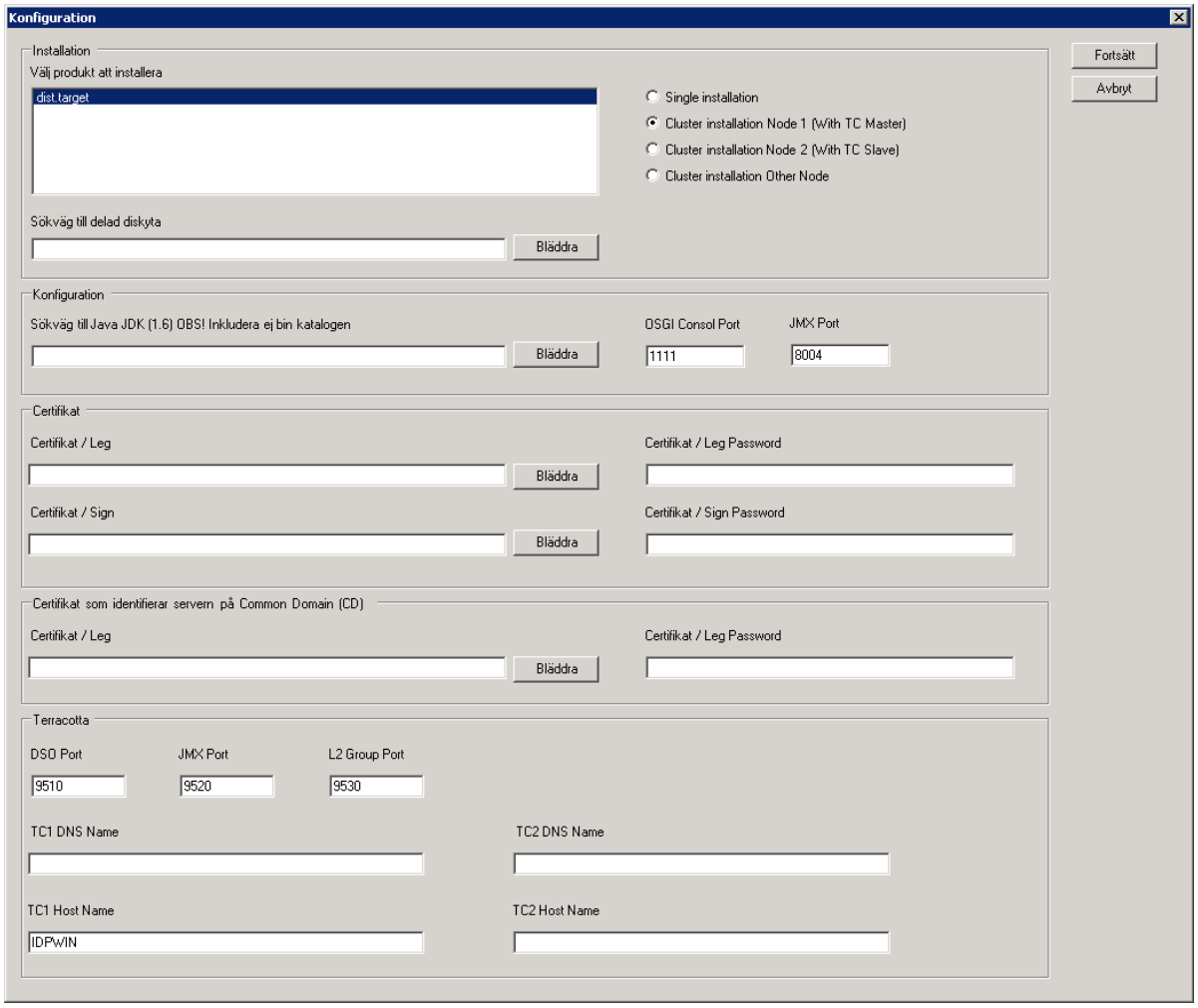
Fyll sedan i terracottaservrarnas DNS och Hostname i respektive fält och fortsätt installationen. Terracotta är en fristående applikation som kommer att installeras och köras på nod1 och nod2 (Master/Slave).
Ange därför nods 1 respektive nods2 hostname respektive DNS enligt fältena:

TC1 DNS Name = nod 1 DNS namn (t.ex. nod1.sakerhetstjanst.example.com)

TC1 Host Name = nod 1 Hostname (t.ex. nod1)

TC2 DNS Name = nod 2 DNS namn (t.ex. nod2.sakerhetstjanst.example.com)
TC2 Host Name = nod 2 Hostname (t.ex. nod2)

Klicka sedan på **Fortsätt**.



Figur 7: GUI för installation, kluster nod 1.

Därefter öppnas ett kommandofönster där man fyller i värden för fortsatt installation. Konfiurationen är uppdelad under ett antal avsnitt, under varje avsnitt finns konfigurationsvärden som skall anges, vissa är förvalda som default värden. Fyll i de adresser och portar ni använder i respektive tillhörande kategori.

Efter varje satt värde så klickar man enter och går vidare, se tabell nedan

Parameter	Defaultvärde	Info
(BIF http(s) setup)		
Host adress	--	Säkerhetstjänstens publika adress.
Path to server Identity PKCS#12 certificate	--	Sökväg till legitimeringscertifkatet(.p12-fil) för Säkerhetstjänsten.
Identity PKCS#12 certificate password	--	Lösenord till legitimeringscertifikatet.
Path to server Signature PKCS#12 certificate	--	Sökväg till signeringscertifikatet (.p12-fil) för Säkerhetstjänsten.
Ws port	8080	Port som Säkerhetstjänsten kommer att publiceras på.
Https port	8443	Https port för Säkerhetstjänstens administrationsgränssnitt.
Https mutual authenticated port	8444	Https port för Säkerhetstjänstens autentisering.
(Database setup)		
Host Address	--	Address till databas(mysql)-servern.
Port	3306	Port till mysql.
User name	sak	Den användare som Säkerhetstjänstens skall använda för att kopppla upp sig mot databasen.
Password	--	Lösenord för databasanvändaren.
(Common Domain http(s) setup)		
Https port	8446	Https port för Säkerhetstjänstens Idp webgränssnitt för CommonDomainCookie hantering
Host Address on Common Domain	--	Säkerhetstjänsten publika Common Domain adress.
Host Address on Common Domain address	--	Säkerhetstjänstens Common Domain adress.

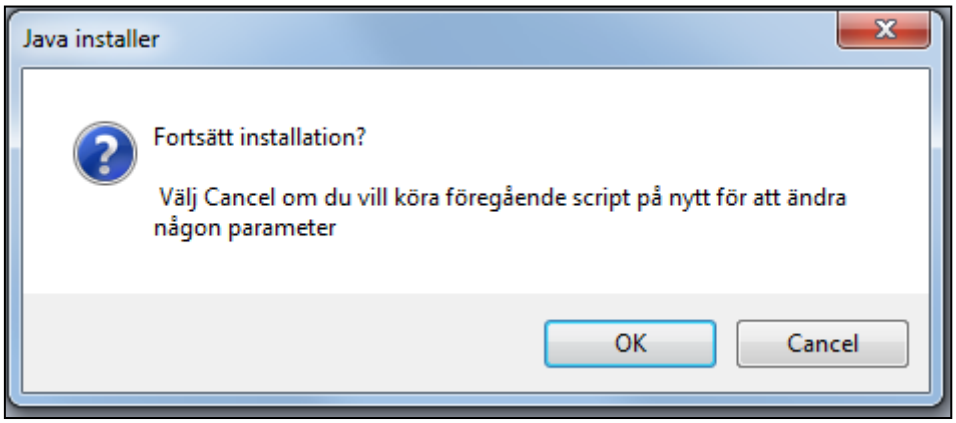
(Idp http(s) setup)		
Https port,Two-way SSL	8444	IdP Web gränssnitt för identifiera/autentisers certifikats användare (SITHS)
Https port,One-way SSL	8445	IdP Web gränssnitt som används av SSO-service
(HSA-WS setup)		
Host name	hsahotell.carelink.sjunet.org	Address till hsa-ws tjänsten
Port	443	Port för hsa-ws tjänsten
Search base	c=SE	Sökbas för has-ws
Context	/svr-hsaws2/hsaws	Context path för hsa-ws
(BIF mongo db setup)		
Address	--	Address till mongo-db.
Port	27017	Mongo-db port.
Username	sak	Mongo-db användare.
Password	--	Mongo-db lösenord.

Figur 8: Konfigurationsvärden

Det sista som sker är att allt kopieras ned till den förvalda installationskatalogen, sedan om allt gått bra så visas meddelandet #### Installation completed! ####

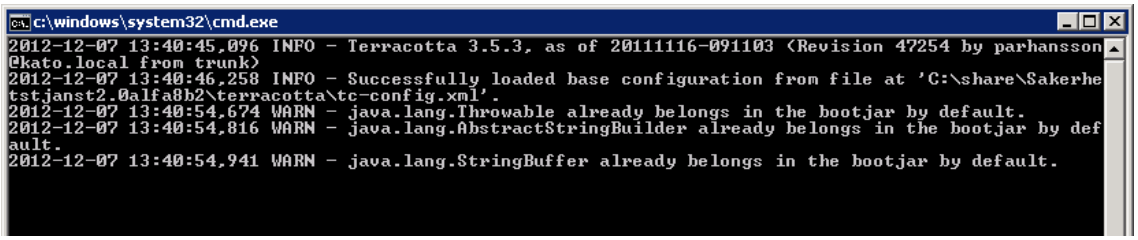
Avsluta kommandofönstret genom att skriva **exit** och trycka på **Enter**.

Klicka **Yes** på det lilla *Java installer* fönstret om ni är nöjd med konfigurationerna som angivits. (se *figur 4* nedan - observera att fönstret kan gömma sig bakom andra installationsfönster!). Klicka på **Cancel** om ni önskar att återgå till GUI:t för installationen och göra om Java konfigurationen (eller för att avrbyta installationen).



Figur 9: Java installer bekräftelsefönster

Sista steget är installationen av Terracotta som sker automatiskt (det visas ”WARN”, i texten, se bild nedan, vilket i det här fallet är ok)



Figur 10: Installation av Terracotta nod 1

Ett bekräftelsefönster visas följande. Klicka **Close**.

6.1.4 Installation på andra noden i en fail-over lösning

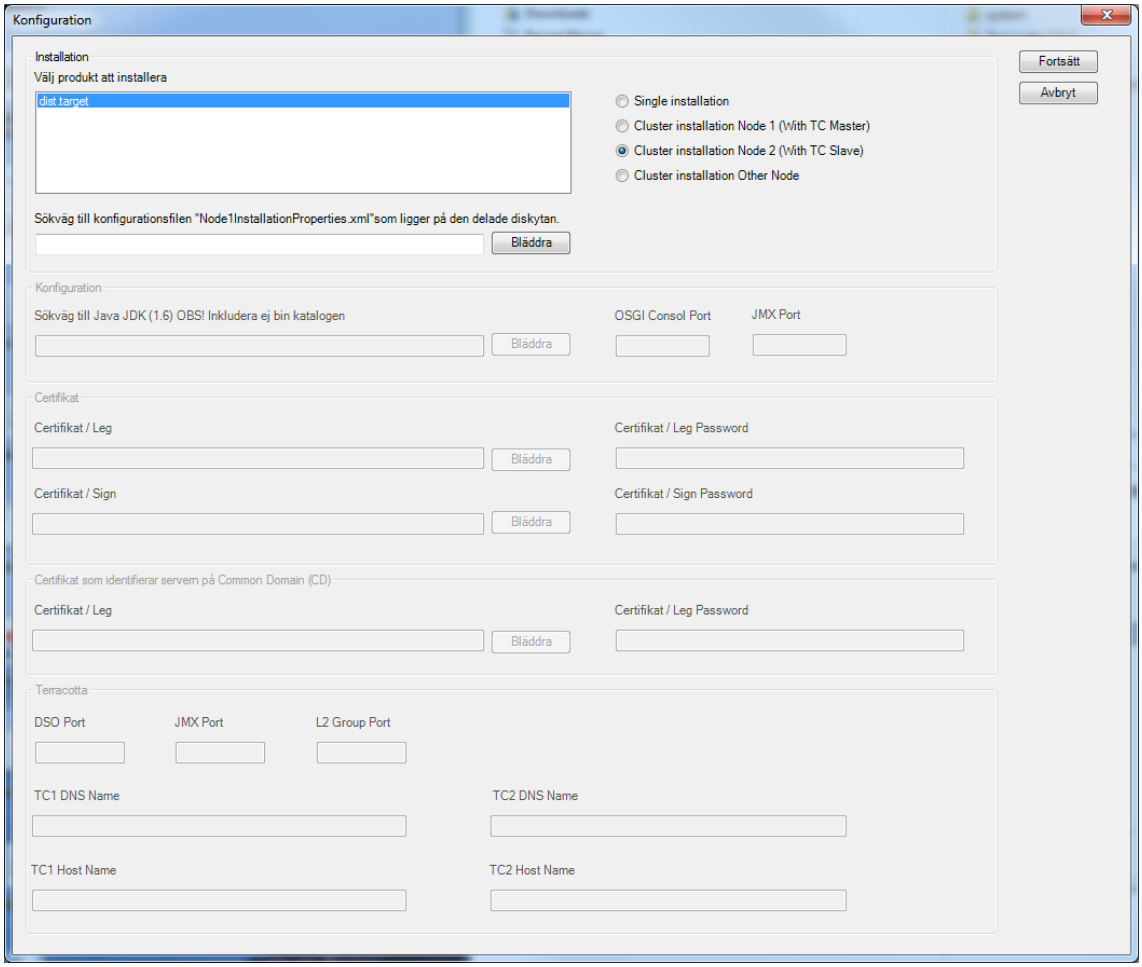
Denna installation kommer att registrera två stycken servicar: ”Lokal Säkerhetstjänst” och ”Lokal Säkerhetstjänst Terracotta”. Efter installationen är det rekommenderat att man byter servicekonto, se Appendix A Skapa separat servicekonto.

Ett konfigurationsfönster öppnas där man markerar produkten **dist.target**.

Välj ”*Cluster installation Node2 (with TC Slave)”*

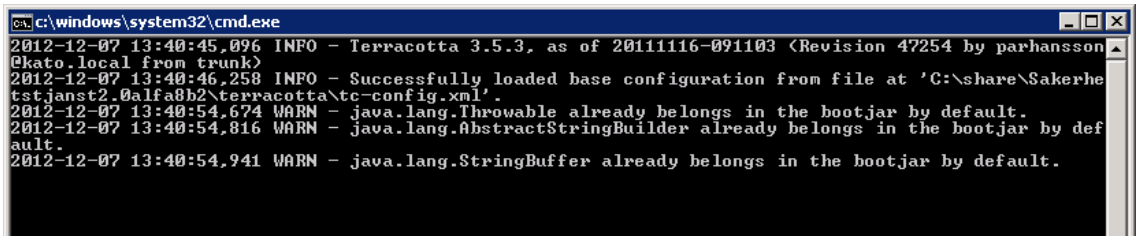
Ange sökväg till den delade diskytan och peka ut konfigirationsfilen ”Node1InstallationProperties.xml” som skapades vid installationen på den första noden.

Klicka sedan på **Fortsätt**



Figur 11: GUI för installation, kluster nod 2

Sista steget är installationen av Terracotta som sker automatiskt (det visas ”WARN”, i texten, se bild nedan, vilket i det här fallet är ok)



Figur 12: Installation av Terracotta nod 2

Ett bekräftelsefönster visas följande. Klicka **Close**.

6.1.5 Installation på övriga noder (nod3- nodx) i en fail-over lösning

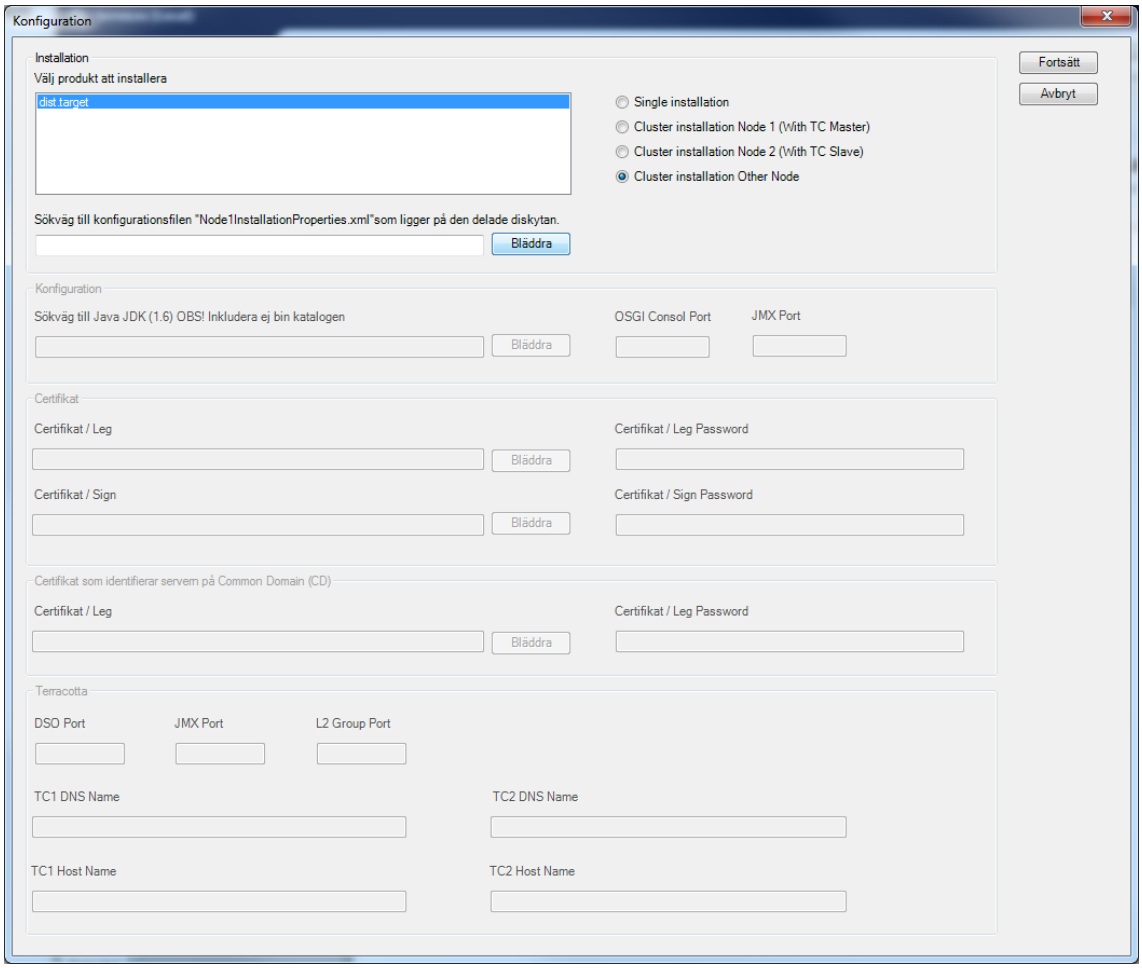
Denna installation kommer att registrera en service: ”Lokal Säkerhetstjänst”
Efter installationen är det rekommenderat att man byter servicekonto, se Appendix A Skapa separat servicekonto.

Ett konfigurationsfönster öppnas där man markerar produkten **dist.target**.

Välj ”*Cluster installation Other Node”*

Ange sökväg till den delade diskytan och peka ut konfigirationsfilen ”Node1InstallationProperties.xml” som skapades vid installationen på den första noden.

Klicka sedan på **Fortsätt**



Figur 13 GUI för installation, kluster nod 3 - nod x

7 Uppstart av server

NOTERA: Har man valt att installera singleserver installation (alternativ 1), så kan man hoppa direkt till kapitel 7.2
Vid uppstart kommer först Terracotta-servrarna att startas och därefter startas den första noden för säkerhetstjänsterna.
Den första noden kommer då att ansluta till Terracotta-klustret som dock i det här läget inte innehåller något data (*bundle states*, om bundlarna är startade, stoppade, installerade, etc). Installerar sedan de valda komponenterna för säkerhetstjänsterna i Terracotta-klustret och startar dessa.
När sedan de övriga servrarna startas och ansluter till klustret, t.ex. när -nod 2 i Bild 1 startas, så hämtar de all information om *bundle states* etc, dvs. övriga servrar kommer att bli en ”spegling” av den första servern i klustret.

7.1 Uppstart av Terracotta

Nod1:

1. Starta Terracotta servern på första noden, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters Terracotta service (Lokal Säkerhetstjänst Terracotta) och klicka på **Start**.

Nod2:

2. Starta igång Terracotta servern på andra noden, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters Terracotta service (Lokal Säkerhetstjänst Terracotta) och klicka på **Start**.

7.2 Uppstart av Lokal säkerhetstjänst på första noden

Nod1:

1. För att **starta** systemet, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters service (Lokal Säkerhetstjänst) och klicka på **Start**.

2. Logga in till osgi konsolen:
   ```
   telnet localhost 1111
   ```

   NOTERA: Det kan ta ca en minut innan servern har startat och det går att logga in till osgi konsolen.
   NOTERA: Har en annan port än defaultport 1111 angetts i installationen anger man denna istället.

3. I osgi konsolen verifiera att systembundlen med id 0 har startat, dvs har statusen ACTIVE, genom att exekvera osgi kommadot ss:

```
osgi> ss
```

Utskriftsexempel:

```
Framework is launched.

id State Bundle
0 ACTIVE org.eclipse.osgi_1.0.3
```

Statusförklaring för utskriften för fältet ”State”:

INSTALLED
Bundeln finns i systemet men ej startad.

STARTED
Bundeln startad men ännu inte aktiv.

ACTIVE
Bundeln startad.

RESOLVED
Bundeln stoppad efter start.

4. När ni har kommit in i osgi konsollen så är det dags att installera de komponenter man vill ha. För att lista de komponenter som finns skriv: *pkg list*

osgi> pkg list

Id	Name	Description
1	Local server	Includes all below services
2	Consent component	Bundles for consent installation
3	Common archive component	Bundles for common archive
4	IDP component	Bundles for IDP
5	Block local component	Bundles for local block installation
6	Patient/Consent dialog	Bundles for Patient/Consent dialog
7	Patientrelation component	Bundles for patientrelation installation

osgi>

5. Välj en eller flera komponenter du vill installera.

    - Alla lokala tjänster, välj alternativ 1 *Local server*.
    - Spärr, alternativ 5 Block component.
    - Samtycke, alternativ 2 Consent component.
    - Patientrelation, 6 Patientrelation component.
        - Samtyckesdialogen, 6 (kräver både samtycke och patientrelation)
    - Autentiseringstjänst, 4 IdP component

    Det är alltså möjligt att installera enbart en av tjänsterna, t.ex. Spärr. Dock så kräver tjänsterna Spärr, Samtycke och Patientrelation tillgång till en autentiseringstjänst för att man som användare ska kunna logga in och komma åt webbtjänsterna. Det kan t.ex. vara en annan lokal autentiseringstjänst eller den nationella autentiseringstjänsten eller så installerar man autentiseringstjänsten tillsammans med den/de lokala tjänsterna man vill installera.

    För att installera komponent 1: *pkg install –package 1*.
    För att installera komponent 5: *pkg install –package 5*.

6. Sedan är det dags att starta: *pkg start*.
```
osgi> pkg start
```

    Vänta ett tag på att bundlarna startar upp, ca 2 min.

7. Verifiera att samtliga bundlar är uppstartade med kommandot dep. Det kommandot listar alla bundlar som **inte** startat ännu. Exekvera kommandot:
```
osgi> dep
```

    Utskriftsexempel:

```
osgi> dep
id Bundle State Unsatisfied dependencies
```

    Förklaring: Listas inte någon bundle här så är samtliga bundlar startade, i annat fall vänta tills kommandot inte listar någon bundle.

8. Verifiera att alla beroenden är uppfyllda med kommandot:
```
osgi> context state
```

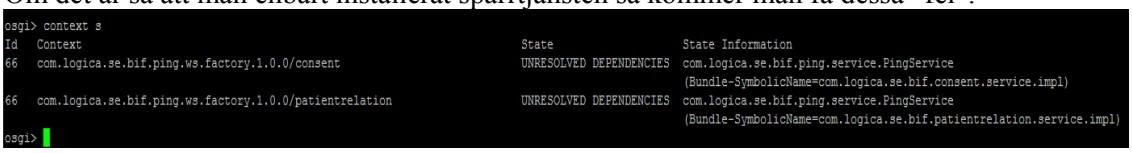
    Utskriftsexempel:

```
osgi> context state
```

```
id    Context
State                    State Information
```

Förklaring: Listas inte någon bundle här så är samtliga bundlar startade, i annat fall vänta tills kommandot inte listar någon bundle.

9. Om det är så att man enbart installerat spärrtjänsten så kommer man få dessa ”fel”.



Figur 14: Context state, unresolved dependencies exempel.

com.logica.se.bif.ping.ws.factory väntar på en samtyckestjänst och en patientrelationstjänst.
För att få bort felet så får man gå in i konfigurationskatalogen för com.logica.se.bif.ping.ws.factory och ta bort samtycke och paientrelation.
Om man enbart installerat samtycke så får man ta bort spärr och patientrelation osv.

Gå till katalogen:
<installationskatalog>\sakerhetstjansten\config\com.logica.se.bif.ping.ws.factory.1.0.0\
Ta bort *consent.xml* och *patientrelation.xml*.

Uppdatera com.logica.se.bif.ping.ws.factory i osgi konsollen: *update 66* (siffran till vänster om com.logica.se.bif.ping.ws.factory i bilden ovan).
Då ska dessa försvinna.

10. Koppla ned från osgi konsolen med kommandot:
```
osgi> disconnect
```

7.3 Anslut till webbgränssnittet

Verifiera att det går att ansluta till webbgränssnittet på den första noden.

1. Om serverns adress inte finns i DNS-servern måste den lokala host-filen temporärt uppdateras på den klientdator som används för att ansluta till webgränssnittet. Lägg till följande i lokala host-filen:
   - <server ip-adress nod1> nod1

2. Anslut med SITHS-kort.

3. Verifiera att det går att ansluta till webbgränssnittet ex.
   ex. **https://[servernamn]:8443/spadmin**

4. Välj ”continue to this website” när frågan om att servern inte har ett giligt certifikat visas.

7.4 Uppstart av Lokal säkerhetstjänst på övriga noder

1. För att **starta** systemet, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters service (Lokal Säkerhetstjänst) och klicka på **Start**.

2. Vänta en stund, ca 5 min, på att systemet startar upp.

3. Logga in till osgi> konsolen:
   ```
   telnet localhost 1111
   ```

4. Verifiera att samtliga bundlar är uppstartade med kommandot dep. Det kommandot listar alla bundlar som **inte** startat ännu. Exekvera kommandot:
   ```
   osgi> dep
   ```

   Utskriftsexempel:

   ```
   osgi> dep
   id  Bundle                    State              Unsatisfied
   dependencies
   ```

   Förklaring: Listas inte någon bundle här så är samtliga bundlar startade, i annat fall vänta tills kommandot inte listar någon bundle.

5. Verifiera att alla beroenden är uppfyllda med kommandot:
   ```
   osgi> context state
   ```

   Utskriftsexempel:

   ```
   osgi> context state
   id    Context
   State                    State Information
   ```

   Förklaring: Listas inte någon bundle här så är samtliga bundlar startade, i annat fall vänta tills kommandot inte listar någon bundle.

5. Koppla ned från osgi konsolen med kommandot:
   ```
   osgi> disconnect
   ```

6. Verifiera att det går att ansluta till webbgränssnittet ex.
   https://[servernamn]:8443/spadmin

8 SYSTEMKONFIGURATION

Efter den lokala säkerhetstjänsten har installerats och startats, kan slutligen en **systemkonfiguration** genomföras. Observera att filtret måste vara avstängt när användaren ska göra den första IdP/SP konfigurationen.

Stäng av filtret:

1. Gå in i systemkonsolen (OSGI).
2. Skriv efter osgi>: `sys spfilter –off.`
3. Filtret är nu avstängt. Fortsätt konfigurationen efter anvisningar i avsnitt 8.1.

När konfigurationen av systemet (som beskrivs nedan) är genomförd kan nu användaren aktivera SAML filtret (OSGI kommando: `sys spfilter –on`) och börja använda systemet.

Efter den lokala säkerhetstjänsten har installerats och startats, kan slutligen en **systemkonfiguration** genomföras. Observera att systemets ”filter” (det som tvingar att en användare gör en autentisering innan man får åtkomst till webbsidan) måste vara avstängt för att man ska kunna göra den initiala konfigurationen.

Stäng av filtret:

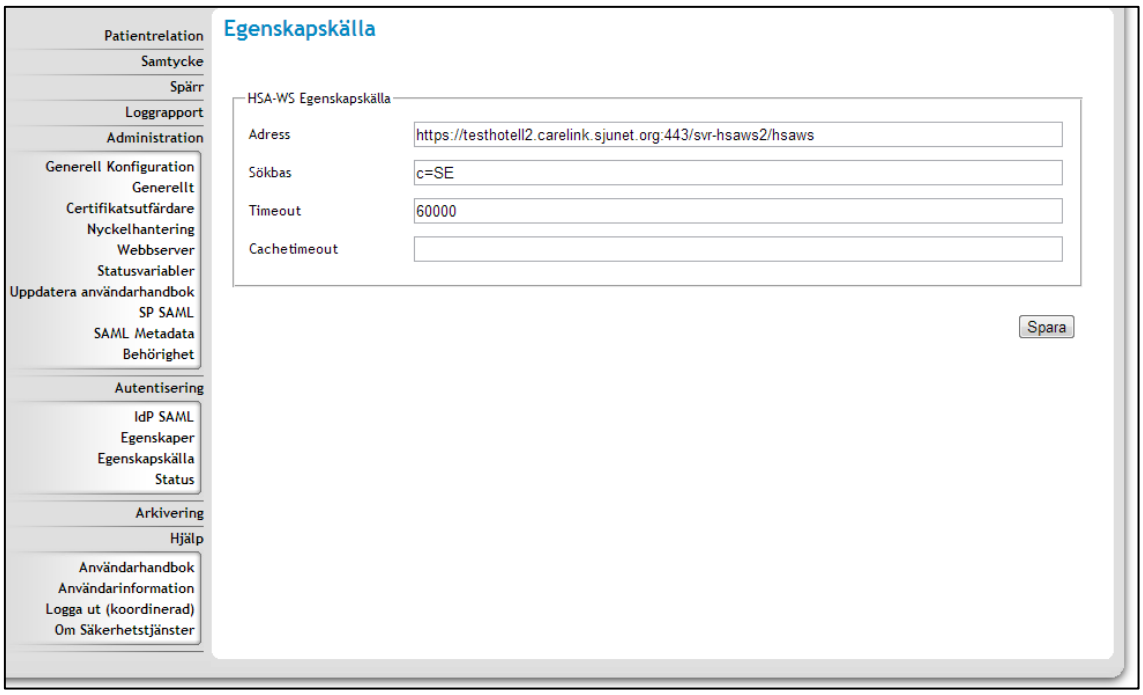
4. Gå in i systemkonsolen (OSGI).
5. Skriv efter osgi>: `sys spfilter –off.`
6. Filtret är nu avstängt. Fortsätt konfigurationen efter anvisningar i avsnitt 8.1.

Anslut till webbgränssnittet på **https://[servernamn]:8443/spadmin**

8.1 Kopplingar mot externa system

8.1.1 HSA-WS

Vid installationen anger man adressen till HSA-WS så denna ska man normalt inte behöva konfigurera. Har man dock angivit fel adress eller vill ändra denna kan man göra det på menyn **Autentisering->Egenskapskälla**

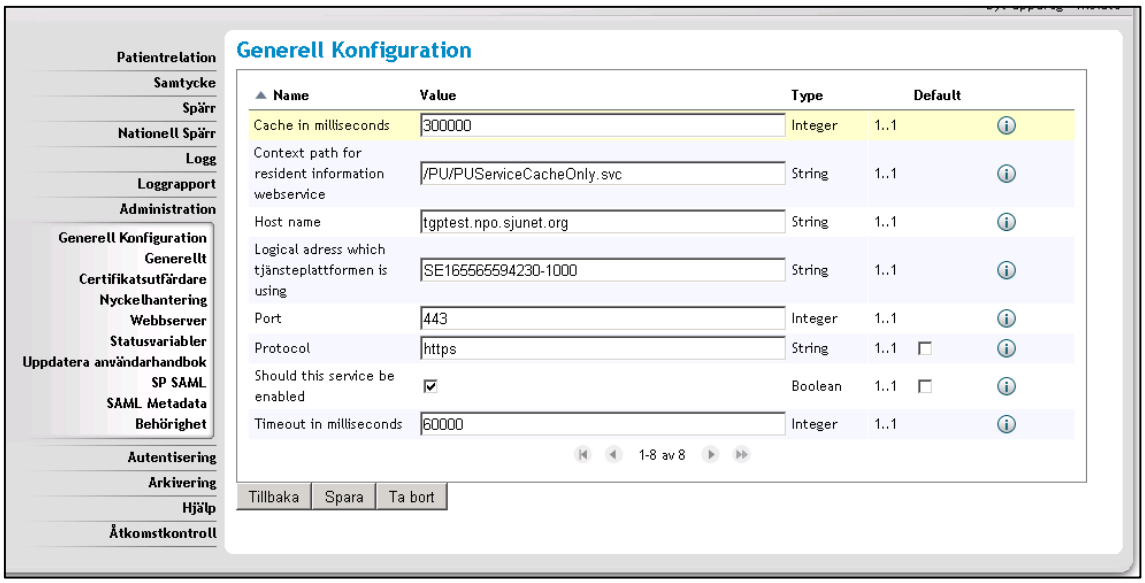


Figur 15: Gui för Egenskapskälla

Ange adress och/eller ny sökbas och klicka spara. Timeout och cachetimeout ska man normal inte behöva ändra på

8.1.2 Spar-tjänsten*

För att konfigurera SPAR så går man in i menyn **Administration->Generell konfiguration**, Sedan väljer man konfiguration `Resident Information Lookup Service Impl 1.0.0`



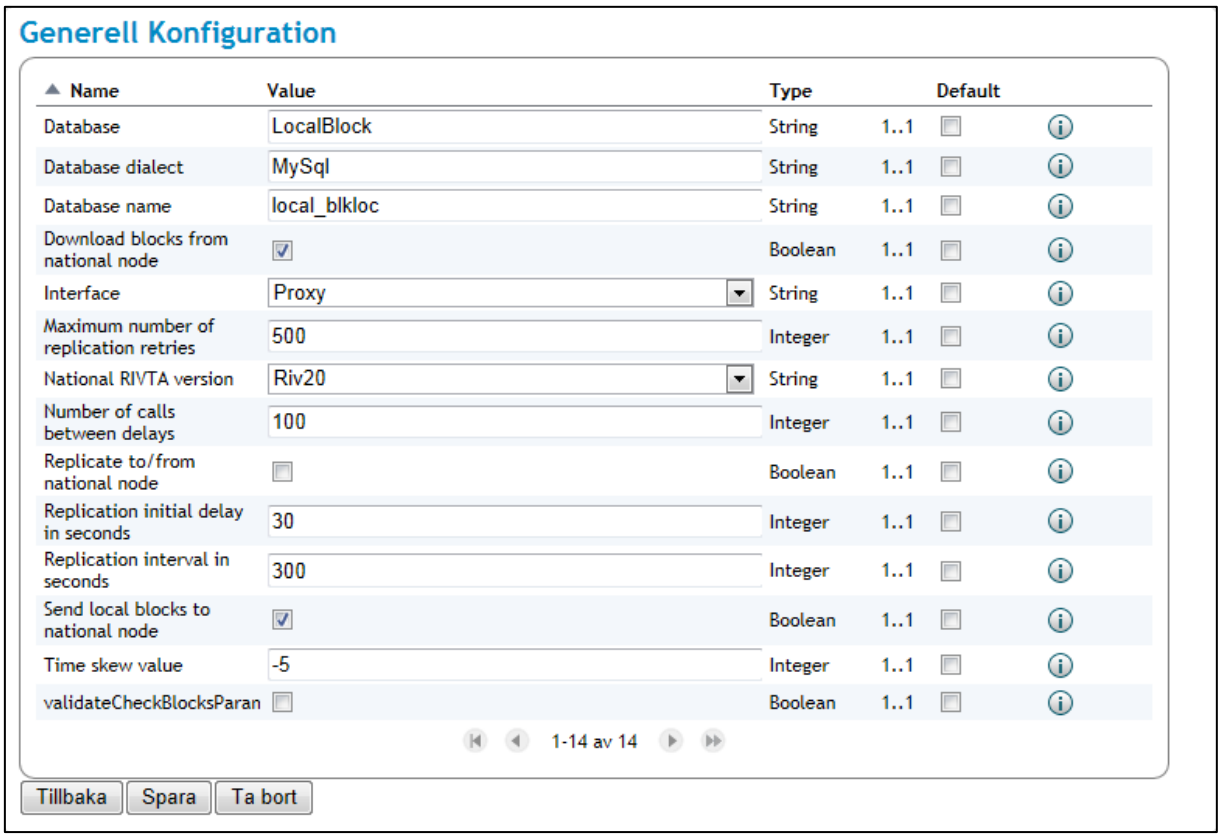
Figur 16: Gui för konfiguration av SPAR tjänsten.

Ange adress till spartjänsten, vilken port och vilket protokoll man ska använda. Här kan man även ange om SPAR-tjänsten ska användas (enabled). När man är klar trycker man på spara och sedan tillbaka.

*SPAR-tjänsten behöver enbart konfigureras ifall man installerat någon av tjänsterna: Samtycke, Patientrelation och Spärr

8.1.3 Synkronisering till nationell spärrtjänst*

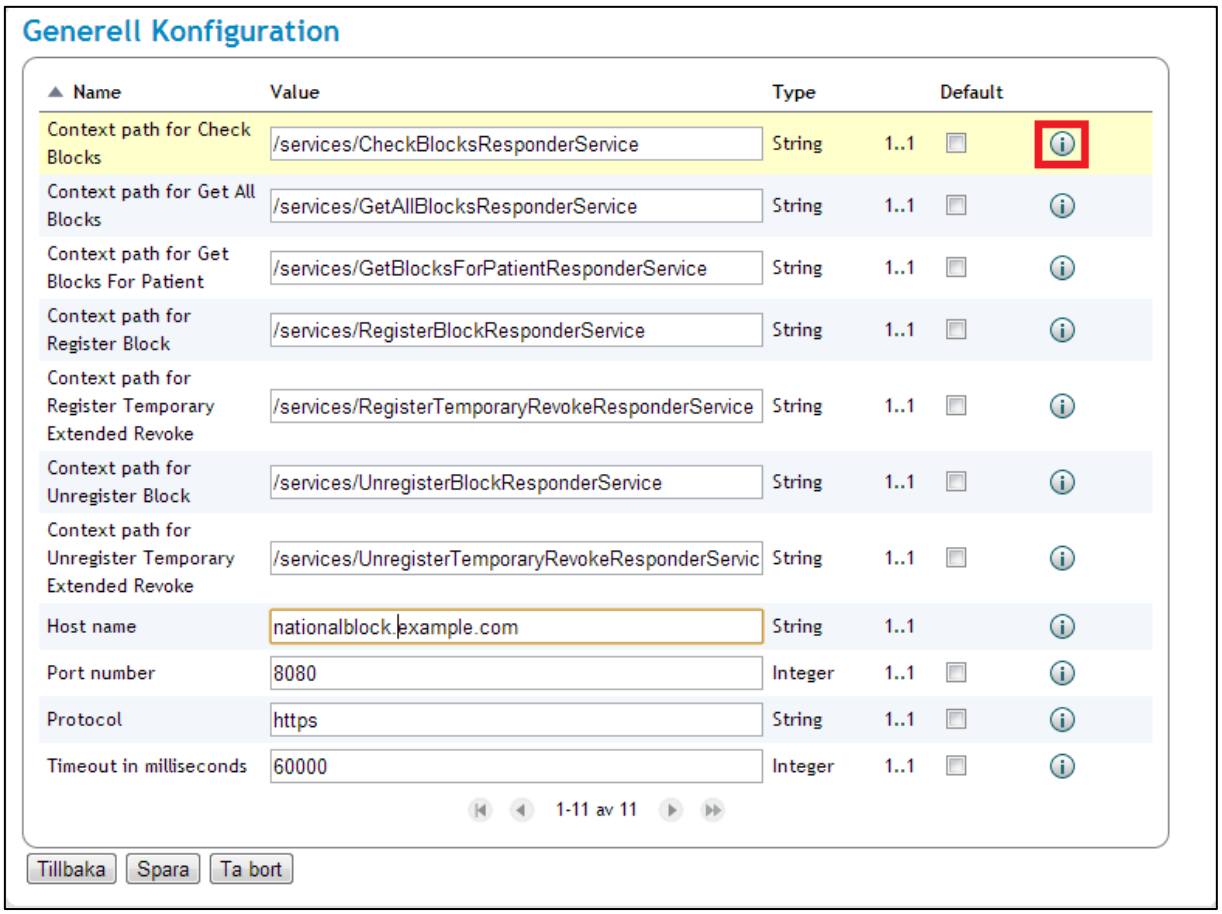
För att konfigurera synkronisering till nationell spärrtjänst, använd menyn **Administration->Generell konfiguration.** Därefter väljer man konfiguration *Block Local Service 2.0.0.*



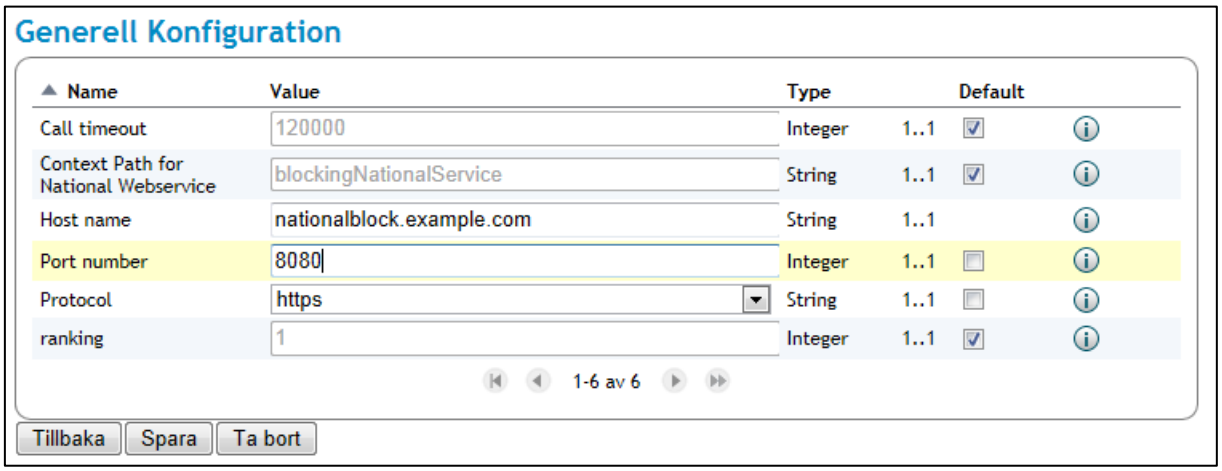
Figur 17: Gui för konfiguration av Block Local Service

Här ska man ställa in om synkroniseringen ska mot Riv20 eller Riv21 gränssnitten på den nationella spärrtjänsten. För att skicka spärrar till nationell spärrtjänst ska *Send local block to national node* vara i bockad.
För att aktivera Synkroniseringen till nationell spärrtjänst, så skall ”*Replicate to/from national node*” vara ibockad.
Klicka på spara och sedan tillbaka när konfigurering är klar.

Gå sedan på *Block National Webservice Proxy for RIV 2.0 1.0.0* (för Riv20 replikering) eller *Block National Webservice Proxy 1.0.0* (för Riv21 replikering).



Figur 18: Gui för konfiguration av *Block National Webservice Proxy for RIV 2.0*



Figur 19: Block National Webservice Proxy

Där ska Host name och Port number konfigureras. För att veta vart ni ska replikera kontakta Inera.

Kontakta Inera för att ta reda på vilken man ska använda. Ni kommer även att behöva kontakta dem för att få behörighet att replikera.

*Nationell Spärrtjänst behöver enbart konfigureras ifall man installerat lokal spärrtjänst.

8.2 Sätta upp behörighet för användare

8.2.1 Allmänt

I leveransen ingår en mall för de behörighetsregler som en lokal installation behöver (ligger under katalogen install\install files). Behörighetsreglerna uppdateras med vårdgivarinformation innan de läsas in i systemet,
Behörighetsreglerna är uppdelade på resursnivå och även på systemnivå. Behörigheten styrs av de egenskaper som en aktör eller ett system har tilldelats. En aktör får sina egenskaper från HSA katalogen medans ett system får de egenskaper som anges i den metadata-fil som importeras i systemet. Anropande vårdsystem måste läggas till i systemet för att de skall få behörighet via en metadata-fil.
Behörighetsreglerna är uppdelade på aktör, externt system och internt system, d v s systemet i sig självt.

8.2.1.1 Anpassa behörighetsregler

Behörighetsreglerna som levereras med systemet måste anpassat till den eller de vårdgivare som systemet skall hantera. Enklast är att öppna filen regler_default_lokal.xml och byta ut värdet ”`${replace_this_careprovider}`” med HSA-id värdet på den vårdgivare som systemet skall hantera.
Om systemet skall hantera fler än en vårdgivare måste ytterligare en rad per ny vårdgivare läggas till i filen:

```
<attribute name="urn:sambi:names:attribute:careProviderHsaId"
value="${replace_this_careprovider}"/>
```

Ange följande kommando för att läsa in reglerna:

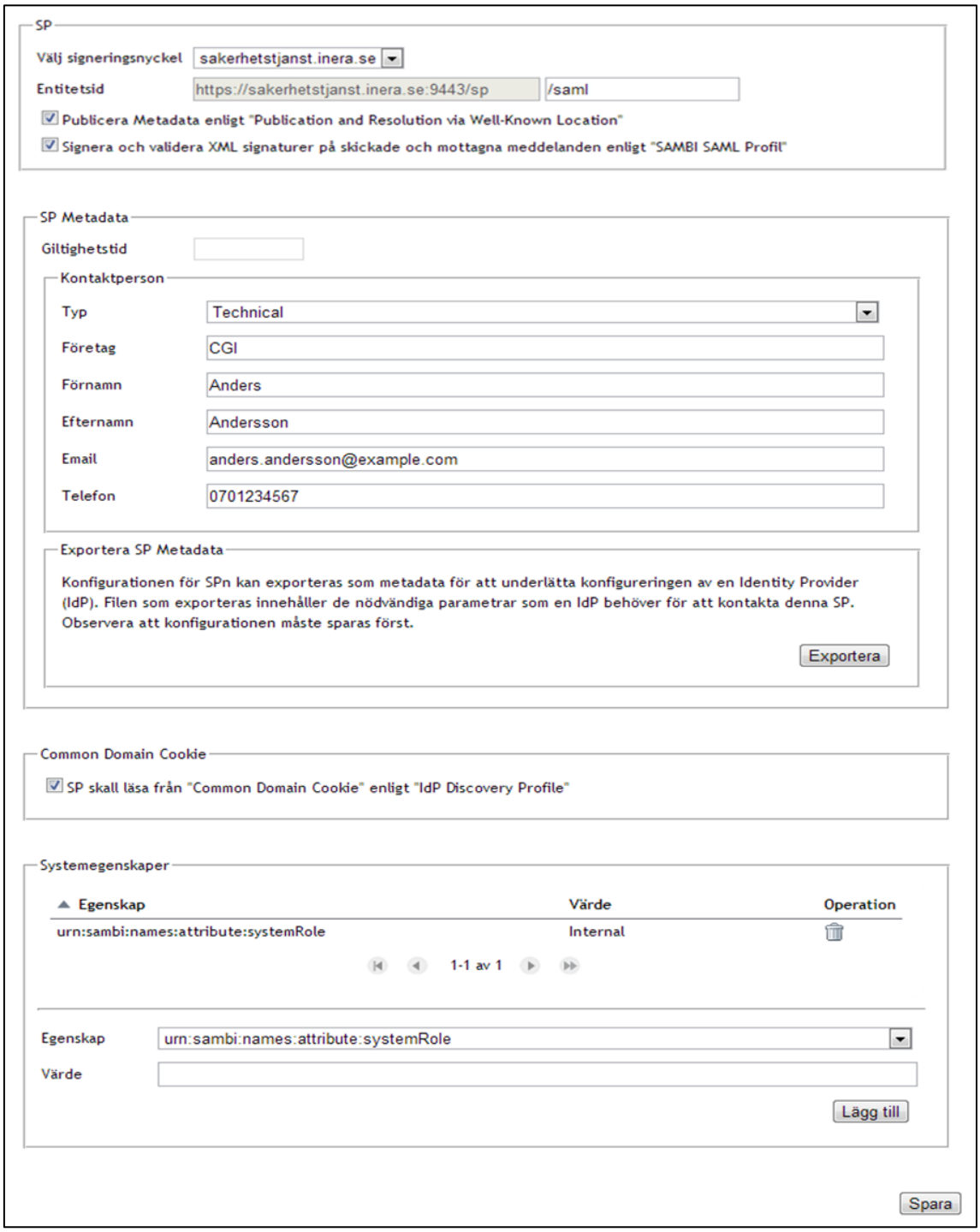
```
osgi> sys acc –import file:///c:\regler_default_lokal.xml
```

8.2.1.2 Tilldela systembehörighet

Systemet i sig själv måste ges behörighet. Detta görs genom att lägga till egenskaper via menyn *Administration->SP SAML*. Systemets egenskaper skall vara:

```
urn:sambi:names:attribute:systemRole = Internal
urn:sambi:names:attribute:careProviderHsaId = <Vårdgivar Id>
```

i <Vårdgivar Id> ska det stå ert vårdgivar id.



Figur 20: SP SAML webbgränssnitt

8.3 Ge externa vårdsystem behörighet

Vårdsystem som skall ges behörighet till systemet måste beskrivas i en metadata-fil där dess egenskaper anges.
Följande exempel visar en metadata-fil för ett vårdsystem som har HSA-id SE12345678-1234 och som ges behörighet till information gällande vårdgivare med HSA-ID SE12345678-1234. Om systemet hanterar flera vårdgivare kan ett vårdsystem får tillgång till fler vårdgivare genom att ange flera vårdgivarid i metadata-filen.

```
<?xml version='1.0' encoding='UTF-8'?>
<md:EntityDescriptor xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="SE12345678-1234"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
   <md:Extensions>
      <mdattr:EntityAttributes>
         <saml:Attribute Name="urn:sambi:names:attribute:systemRole">
            <saml:AttributeValue>System</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="urn:sambi:names:attribute:careProviderHsaId">
            <saml:AttributeValue>SE12345678-1234</saml:AttributeValue>
         </saml:Attribute>
      </mdattr:EntityAttributes>
   </md:Extensions>
   <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:AssertionConsumerService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dummy/HTTP-POST"
          index="1" isDefault="true" />
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Inläsning av metadata-filen sker i menyn *Administration/SAML Metadata*.

Figur 21: Importera metadata

8.4 Ta bort root-certifikat för test vid en produktionssättning

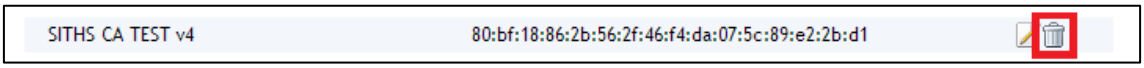
I och med produktionssättning av systemet bör alla CA rotcertifikat för test **tas bort** ur listan med konfigurerade certifikatsutfärdare. Detta skall göras i syftet att utesluta att certifikat för tessyften kan ges någon form av åtkomst till systemet. Säkerställ att inga tester skall genomföras i systemet innan de tas bort.

En eller flera förtroendekällor kan ha certifikatutfärdaren under användning. För att ta bort en certifikatutfärdare måste därför först den webbserver som kopplingen går mot avmarkeras i Webbserveradministrationen.

Observera att när en webbserver skall tas bort så måste först de konnektorer som är kopplade till denna att tas bort.

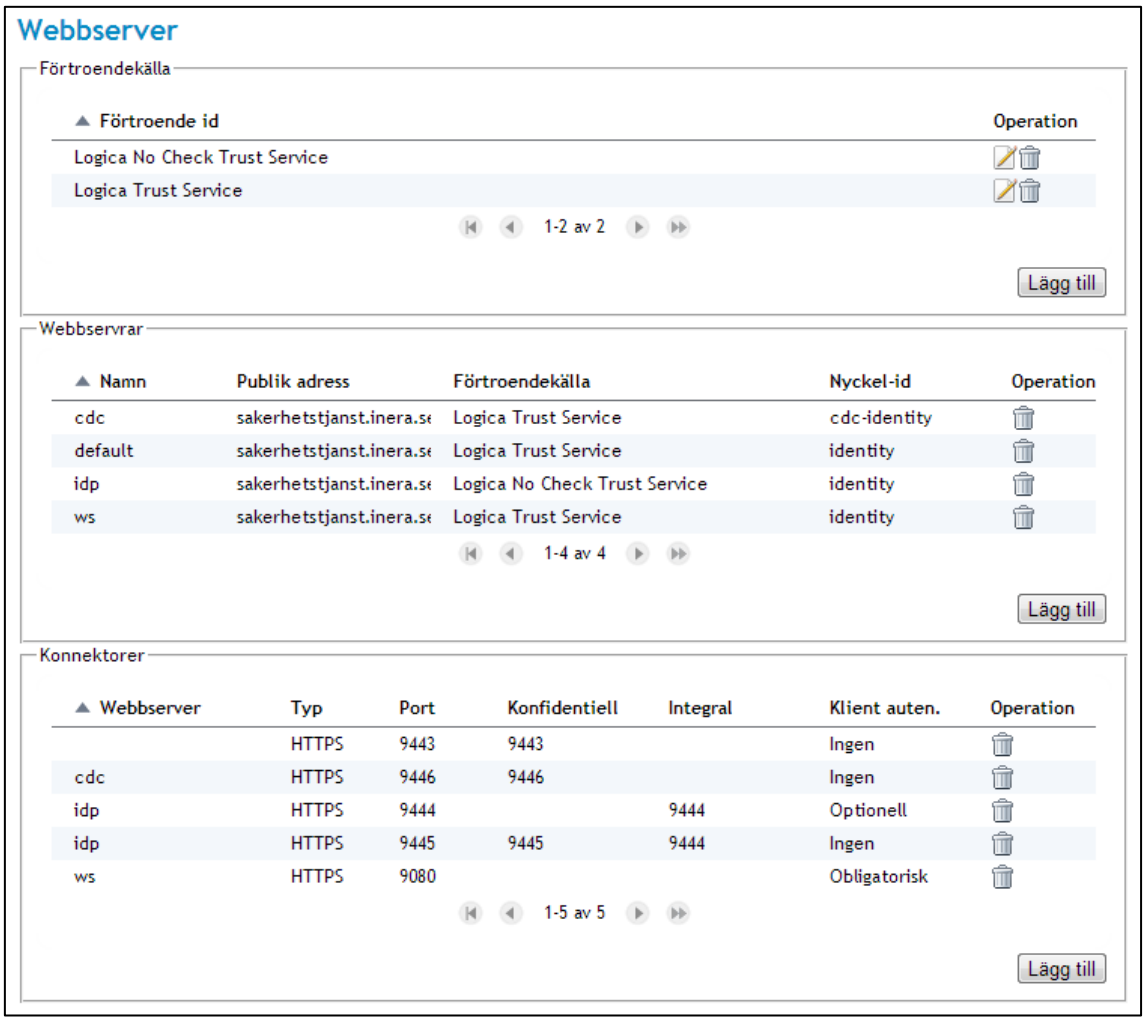
Kontrollera att inga förtroendekällor använder certifikatutfärdaren ni vill ta bort, genom följande anvisningar:

1. Klicka på **soptunnan** som tillhör den certifikatutfärdaren ni vill ta bort. Se bilden nedan (https://[servernamn]:[port]/ sysadmin/#page=certAuthority).



Figur 22: Gui för borttagning av certifikatsutfärdare

2. Navigera till menyvalet *Webbserver* (https://[servernamn]:[port]/ sysadmin/#page=httpService) om meddelandet *”En eller flera förtroendekällor använder denna certifikatsutfärdare. För att kunna ta bort denna certifkatsutfärdare måste den avmarkeras i Webbserveradministrationen”* visas.



Figur 23: Menyvalet "Webbserver"

Börja med att ta bort den konnektor som är kopplad till webbservern.
Gör så här:

1. Identifiera under avsnittet *"Konnektorer"* vilken konnektor som skall tas bort.
2. Klicka på ikonen **soptunnan** längst till höger på den valda raden. Bilden ovan illustrerar vyn.

Fortsätt sedan med att ta bort den berörda webbservern:

1. Klicka på ikonen **soptunnan** under menyn *"Webbservrar"*.

Notera att det inte går att ta bort en webbserver om en konnektor är kopplad till denna. Följande felmeddelande visas i ett sådant scenario: *"*[Webbserverns namn] *har en eller flera konnektorer kopplad*".

2. Bekräfta borttagningen genom att klicka på **Ja** eller avbryt genom att klicka på **Tillbaka.**

Återgå till menyn för *Certifikatutfärdare* (https://[servernamn]:[port]/ sysadmin/#page=certAuthority). Efter att kopplingarna nu är borttagna så kan certifikatutfärdarna dedikerade för testsyften tas bort. Upprepa stegen ovan tills alla certifikatutfärdare för testsyften är borttagna från systemet.

8.5 Konfigurera upp anslutning till autentiseringstjänst

Detta kapitel beskriver hur man konfigurerar upp anslutning till autentiseringstjänst. Detta kan göras på två olika sätt. Detta beror på om man installerat en egen autentiseringstjänst eller inte.

8.5.1 Extern autentiseringstjänst

Om ni inte installerar egen autentiseringstjänst måste man ansluta sig mot en extern autentiseringstjänst. Då måste man exportera sp metadata och skicka till de som tillhandahåller autentiseringstjänsten och ni måste ha deras IdP Metadata som ni sedan läser in i systemet. Hur man exporterar SP Metadata kan ni läsa i kapitel 8.5.3.2.

8.5.2 Lokal autentiseringstjänst

Om ni installerat en lokal autentiseringstjänst så måste man exportera och importera IdP/SP Metadata. Hur man gör detta kan man läsa i kapitel 8.5.3

8.5.3 Inläsning av IdP/SP Metadata

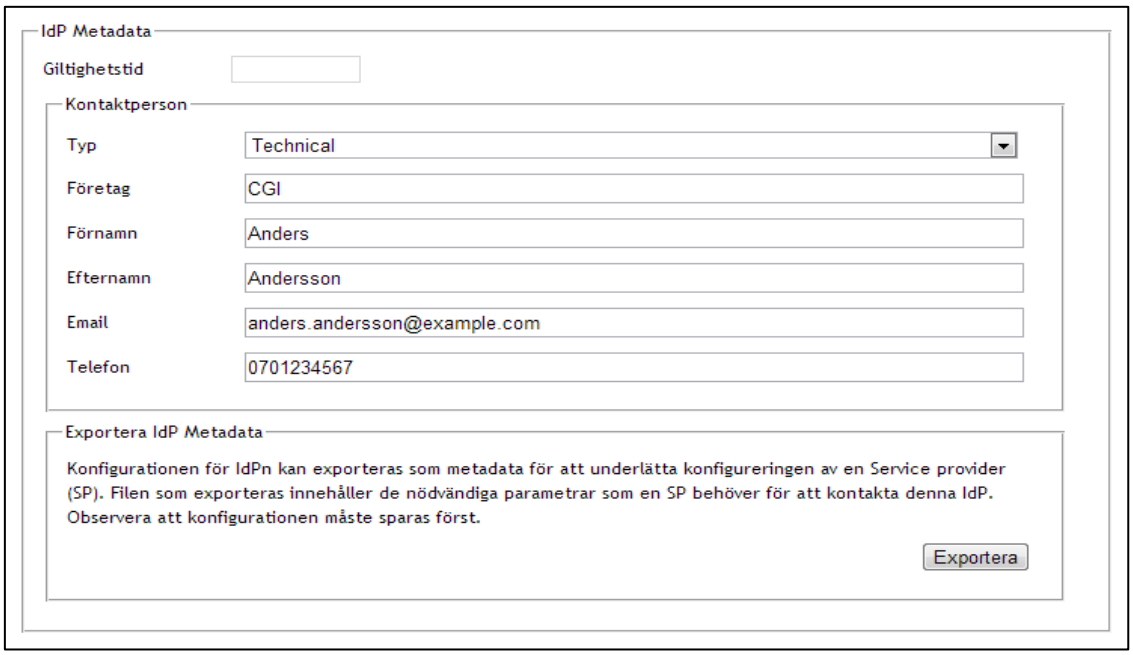
Denna del beskriver konfigureringen av IdP samt SPn via Metadata filer. Både IdPn samt SPn stödjer exportering och inläsning av varandras Metadata XML-filer för att underlätta konfigureringen av de båda. Inläsning av IdP/SP Metadata måste ske för varje SP som ska ingå i federationen.

8.5.3.1 Exportera och importera IdP Metadata

Öppna webbgränssnittet (**https:// [servernamn]:[port]/idpadmin**). Navigera till huvudmenyn för autentisering.

För att exportera IdP Metadata:

1. Välj hur länge IdP Metadatat ska vara giltigt under menyvalet *”IdP SAML”.*
2. Öppna menyvalet IdP Metadata under *Autentisering*.
   (https:// [servernamn]:[port]/idpadmin/#page=idpadministration)
   Se bildexemplet, *figur 24*, nedan hur vyn ser ut.



Figur 24: vy över menyvalet IdP Metadata

3. Klicka på knappen **Exportera** och spara IdP XML-filen.

Importera IdP Metadata:

1. Öppna menyvalet *”SAML Metadata”* under menyn *Administration.* (https:// [servernamn]:[port]/spadmin/#page=metadata)
2. Klicka på knappen **Välj fil** och välj den IdP Metadata XML-fil som du nyss exporterade.
3. Klicka avslutningsvis på knappen **Importera**.

8.5.3.2 Exportera och importera SP Metadata

För att exportera SP Metadata:

1. Välj hur länge SP Metadatat ska vara giltigt under menyvalet *”SP SAML”.*
2. Öppna menyvalet *”SP Metadata”* under menyn *Administration.* (https://[servernamn]:[port]/spadmin/#page=spadministration)
3. Klicka på knappen **Exportera** och spara SP XML-filen för att möjliggöra inläsning till IdPn.

För att importera SP Metadata:

1. Öppna menyvalet *”SAML Metadata”* under menyn *Administration.* (https:// [servernamn]:[port]/idpadmin/#page=metadata)

2. Klicka på knappen **Välj fil** och välj SP XML-filen som du i föregående rubrik exporterade.
3. Klicka avslutningsvis på knappen **Importera**. En bekräftelseruta kommer visas följande på sidan och meddela om processen lyckades eller inte.

8.6 Aktivering av filter och åtkomstkontroll

Avsluta konfigurationsavsnittet och aktivera SP filtret.

```
osgi> sp sysfilter –on
```

Aktivera åtkomstkontrollen genom kommandot

```
osgi> sys authz -on
```

Därefter kan man gå till det grafiska webbgränssnittet för lokala Säkerhetstjänster: **https://[servernamn]:[8443]/spadmin**.

Nu krävs inloggning (med certifikat) för att åtkomst ska ges.

9 ANVÄNDNING, START OCH STOPP

9.1 Logga in i lokala Säkerhetstjänster

När ni har installerat servern kan ni gå till det grafiska webbgränssnittet för lokala Säkerhetstjänster: **https://[servernamn]:[port]/spadmin**.

Denna testar inloggningsförfarandet, med val av certifikat, val av medarbetaruppdragsval.

9.2 Start och stopp

För att **starta** systemet, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters service (LokalSakerhetstjanstService) och klicka på **Start**.

För att **stoppa** systemet, gå in i verktyget Server Manager och services och gå till lokala Säkerhetstjänsters service (LokalSakerhetstjanstService) och klicka på **Stop**.

Tjänsten kan alternativt startas och stoppas genom att användaren trycker CTRL+ALT+DELETE, väljer *”Windows Task Manager”* och väljer tabben *”Services”.* När ni hittat tjänsten (LokalSakerhetstjanstService), högerklicka och välj att stoppa eller att starta tjänsten.

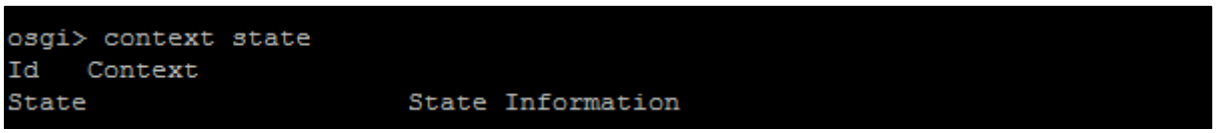
Man bör alltid säkerställa att systemet startat korrekt genom att kontrollera att systemloggen är fri från *Exception* (fel). Avvakta upp till en minut så att lokala Säkerhetstjänster har givits tid att starta upp och kontrollera därefter den senaste loggfilen (läs mer om loggning och felsökning i de avslutande *kapitlen*).

9.3 Hantera aktiviteter i OSGI

Systemet har en inbyggd systemkonsol (OSGi-konsol) som är åtkomlig via Telnet på port 1111 (om inget annat angavs under installationen). Systemkonsolen används endast vid produktsupport eller felsökning, samt av- och påslag av SAML filtret. För att filtret ska vara aktivt måste användaren ange kommandot *”sys spfilter –on”*. För att stänga av filtret används kommandot *”sys spfilter –off”*.

Verifiera att samtliga bundlar är uppstartade med kommandot context state. Det kommandot listar alla bundlar som inte startat ännu. Exekvera kommandot: osgi> context state.

Figur 5, utskriftsexempel av kommandot osgi>context state:



Figur 25: OSGI context state exempel

Förklaring: Listas inte någon bundle här så är samtliga bundlar startade, i annat fall vänta tills kommandot inte listar någon bundle. Kommandot *Context state* används för att verifiera att alla beroenden är uppfyllda.

Koppla ned från osgi konsolen med kommandot:

```
osgi> disconnect
```

9.3.1 Aktivering och avaktivering av SAML filter

Ange följande kommando för att **aktivera** filtret:

```
osgi> sys spfilter -on
```

Ange följande kommando för att **avaktivera** filtret:

```
osgi> sys spfilter -off
```

9.3.2 Inläsning av behörighetsregler

Ange följande kommando för att läsa in regler:

```
osgi> sys acc -import file:///c:\regler_default_lokal.xml
```

9.3.3 Aktivering och avaktivering av behörighet

Ange följande kommando för aktivera eller avaktivera behörighet:

```
osgi> sys authz -off
osgi> sys authz -on
```

9.4 Systemloggning

Lokala Säkerhetstjänster för Windows producerar en logg som avser teknisk förvaltning och felsökning, en så kallad systemlogg, eller audit-logg (benämnd som outputlog_service.txt). Loggen består av en textfil som lagras på filsystemet.
Systemlog lagras i följande katalog (enligt standardinstallationen för Windows):
<sökväg till installerad Säkerhetstjänst>\sakerhetstjansten\log\

9.4.1 Loggning via loggtjänsten

Logga in i osgi-prompten (telnet localhost 1111) och slå

audit search –level error	(Alla error loggar)
audit search –level error –time 1h	(Alla error loggar senaste timmen)
audit search –time 1h	(Alla loggar senaste timmen)
audit search –time 5m	(Alla loggar från de senaste 5 minuterna)

Loggning funkar som så att den börjar med fil-loggningen (så att man ska få med startuploggar), men när den interna loggtjänsten går igång tar den över loggningen och man söker i de genom ovan kommandon.

9.5 Felsökning

Om problem uppstår där lokala Säkerhetstjänster misstänks vara orsaken bör följande saker undersökas:

- Monitorera MySQL-processen och kontrollera att databasen svarar på enkla förfrågningar
- Monitorera Java-processen på applikationsserver och kontrollera att "monitor"-sidan svarar
- Vid akuta problem, starta om applikations- och/eller databasservern och kontrollera systemlogg

Om produktfelanmälan skall göras så måste alla systemloggar kring felet samt ett beskrivande scenario kring vad som föranledde felet bifogas.

10 FÖRVALTNING OCH UNDERHÅLL

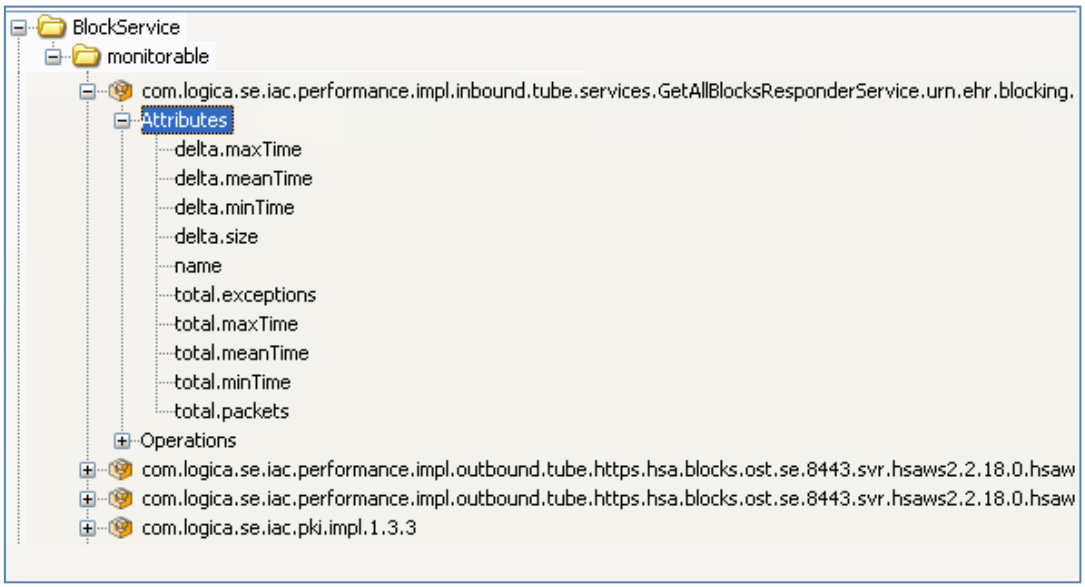
10.1 Periodiskt underhåll

Läs *kapitel 9.4* för information angående hur systemloggar lagras och hur de loggas med hjälp av *Loggtjänsten. Kapitel 9.3* beskriver hur systemet kan hanteras och kontrolleras i systemkonsolen (OSGI).

10.2 Övervakning

Applikationsserver publicerar en mängd systemmoduler som kan övervakas över JMX-protokollet som är Javas teknik för generell övervakning. Med valfritt JMX-verktyg kan applikationsserverns webbtjänster övervakas, se *kapitel 3.2* för gällande port. Observera att JMX-porten inte får tillgängliggöras för någon annan part annat än den maskin som skall sköta övervakningen. Standardinställningarna för JMX kan ändras i <installationskatalog>\LocalSakerhetstjanstConfig.xml

Alla systemkompomenter publiceras som monitorerbara JMX-bönor. Nedan visas en exempelbild från programmet *JConsole* som medföljer Java SE.



Figur 26: Exempelbild från programmet JConsole

Alla bönor med namn ***com.logica.se.iac.performance.impl.inbound*** respektive ***.outbound*** är övervakade webbtjänster som vid behov kan övervakas för att samla in statistik. *Inbound* avser

alla för servern inkommande anrop och *outbound* de utgående. Övriga bönor är interna systemkomponenter och innehåller ingen övervakningsbar information.

Varje webbtjänst har en uppsättning attribut med värden enligt följande lista:

Attribut	Beskrivning
delta.maxTime	Det anrop som tagit längst tid att exekvera (millisek.) inom aktuellt mätfönster/delta.
delta.meanTime	Snittid för alla anrop (millisekunder) inom aktuellt mätfönster/delta.
delta.minTime	Det anrop som tagit kortast tid att exekvera (millisek.) inom aktuellt mätfönster/delta.
delta.size	Antal paket/anrop som ingår i delta-beräkningarna, t.ex. "de 50 senaste".
name	Namn på webbtjänsten.
total.exceptions	Totalt antal exceptions/fel som inträffat för webbtjänsten sedan systemet startades.
total.maxTime	Det anrop som tagit längst tid att exekvera (millisek.) sedan systemet startades.
total.meanTime	Snittid för alla anrop (millisek.) sedan systemet startades.
total.minTime	Det anrop som tagit kortast tid att exekvera (millisek.) sedan systemet startades.
total.packets	Totalt antal paket/anrop som behandlats sedan systemet startades.

10.3 Uppgradering

Lokala Säkerhetstjänster kan mjukvaruuppgraderas då nyare versioner av produkten görs tillgängliga. Mer information om detta ges för respektive uppgradering. Var god kontakta Inera för information kring aktuella versioner [*Ref 1*].

11 HSA-WS

För att slutanvändare skall få tillgång till administrationssidan så krävs minst ett medarbetaruppdrag för de SITHS-kort som används. Var god kontakta Inera för mer information kring anslutning och dokumentation [*Ref 1*].

All autentisering och åtkomstkontroll till gränssnitttet för Systemadmin baserar sig på att användaren är inloggad i systemet på ett visst medarbetaruppdrag inom en viss vårdgivare. Medarbetaruppdragen lagras i HSA-katalogen och är kopplade till användarens SITHS-kort och HSA-id. Användaren kan när som helst logga ut från systemet och logga in igen för att välja ett annat uppdrag.

Användaren och medarbetaruppdraget måste innehålla minst följande:

Namn	**Beskrivning**
HSA Systemroll	Användarens systemroll(er). För åtkomst till spärrar krävs rollen: ***BIF;Spärradministratör*** För åtkomst till loggar krävs rollen: ***BIF;Loggadministratör***
Hsa-id för medarbetaren	Användarens personliga HSA-id.
HSA-id för medarbetaruppdrag	Det valda medarbetaruppdragets HSA-id.
Namn på medarbetaruppdrag	Det valda medarbetaruppdragets namn.
Hsa-id för vårdgivare	HSA-id för vårdgivaren som medarbetaruppdraget gäller inom.
Namn på vårdgivare	Namn på vårdgivaren som medarbetaruppdraget gäller inom.
Hsa-id för vårdenhet	HSA-id för vårdenheten som medarbetaruppdraget gäller inom.
Namn på vårdenhet	Namn på vårdenheten som medarbetaruppdraget gäller inom.

- Om användaren saknar något av ovanstående attribut så visar systemet ett felmeddelande då användaren försöker logga in i spärradministrationen.
- Om användaren innehar systemrollen Spärradministratör så ges tillgång till all funktionalitet rörande spärrar.
- Om användaren innehar systemrollen Loggadministratör så ges tillgång till funktionalitet för att söka fram loggar.
- Om användaren innehar både systemrollerna så ges tillgång till all funktionalitet. Om båda systemrollerna saknas så visas ett felmeddelande då användaren försöker logga in.

Läs användarhandboken *[Ref 2]* för mer detaljerad information om åtkomst och regler i spärradministrationen.

12 Avinstallation

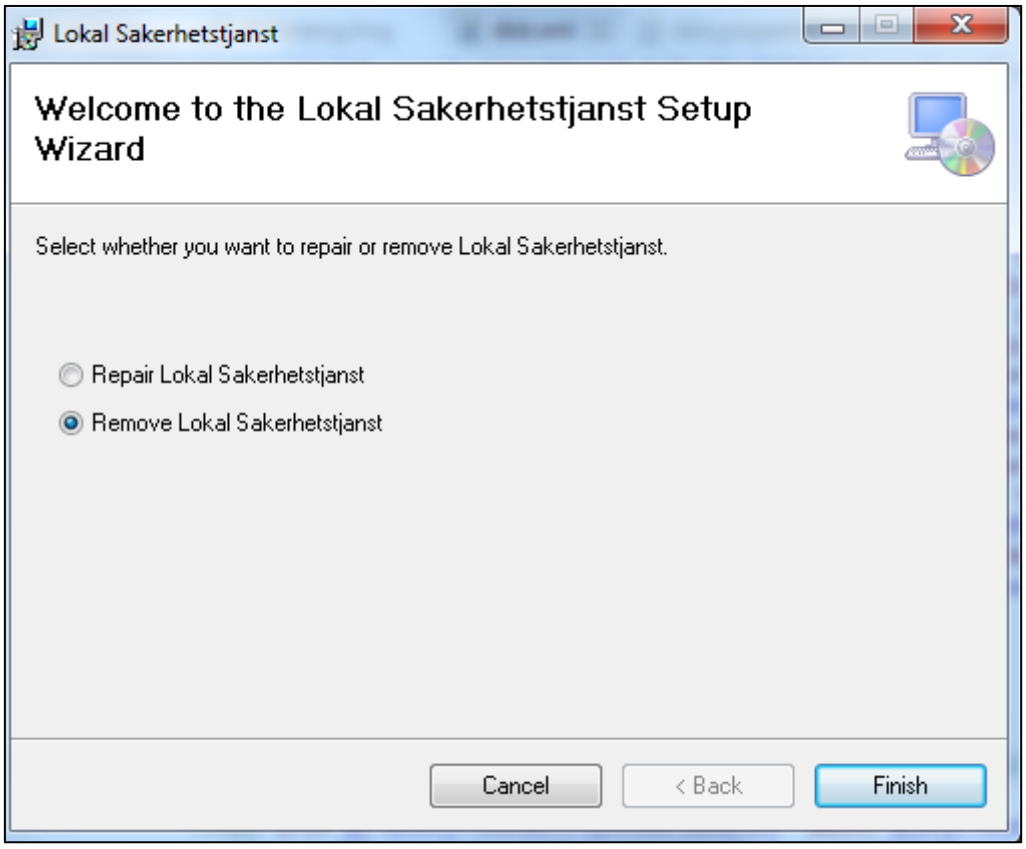
Avsnittet innehåller anvisningar för avinstallation av lokala Säkerhetstjänster genom två olika avinstallationsmetoder.

Avinstallationen avregistrerar service(ar), rensar upp i registret samt tar bort de flesta filer och kataloger som skapats. Dock kan det hända att någon enstaka fil i installationskatalogen blir kvar. Dessa kan manuellt tas bort i efterhand om så önskas.

Om installationen var en *Cluster node 1* installation så skapade den även en delad diskyta.

Kör installationsprogrammet *setup.exe*. Om tjänsten är igång när systemet avinstalleras kommer denna automatiskt stoppas. Följ anvisningarna nedan.

1. Dubbelklicka på **setup.exe** (som du hittar i katalogen där systemet är installerat, under *install*). Vyn *Avinstallera* visas.

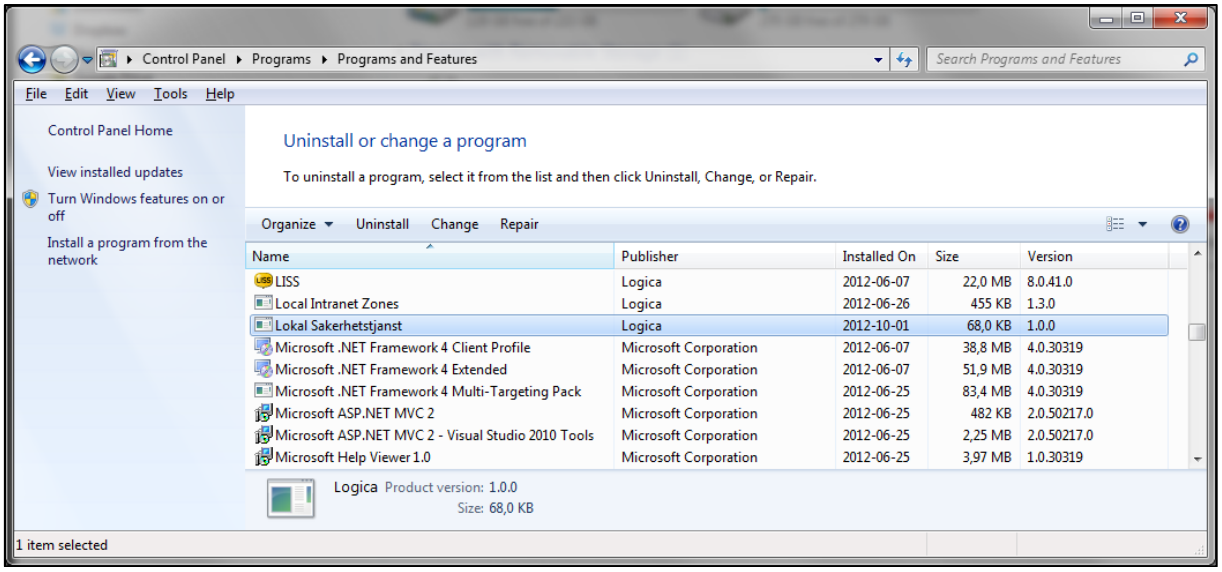


Figur 27: Avinstallera

1. Markera valet *”Remove Lokal Sakerhetstjanst”*.

2. Klicka på **Finish**.
3. En bekräftelse på att programmet har avinstallerats visas sedan.

Ni kan alternativt avinstallera systemet enligt standardiserat sätt i Windows kontrollpanel. Se *figur 8* nedan.



Figur 28: förtydligande bild över avinstallation av tjänsten

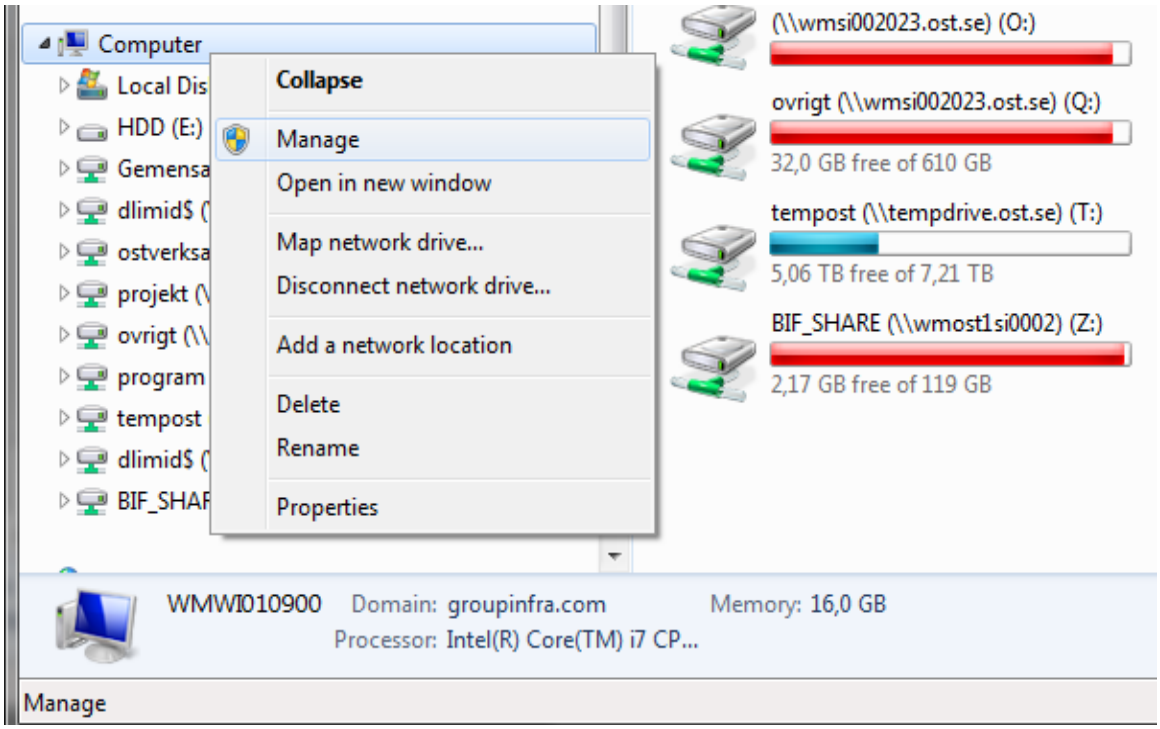
Gör så här:

1. Navigera till *Control Panel* i Windows.
2. Välj *”Uninstall a program”* under menyn *Programs*.
3. Dubbelklicka på **Lokal Sakerhetstjanst**. Lokala Säkerhetstjänster kommer nu avinstalleras.

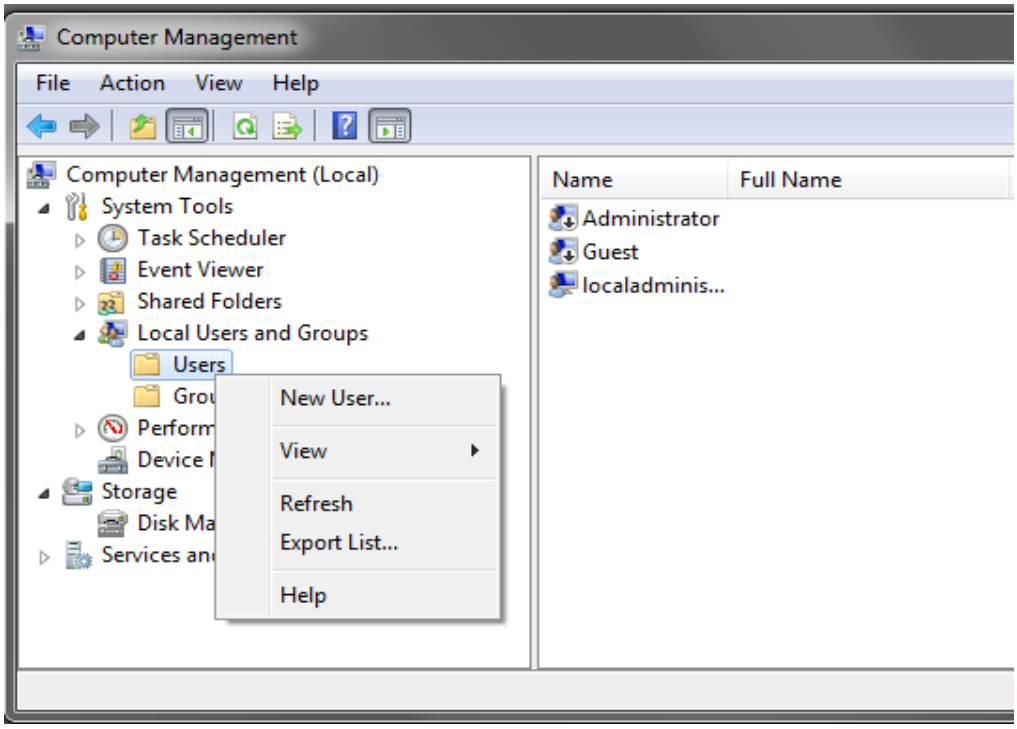
13 Appendix A Skapa separat servicekonto

Vid installation av servicarna ”Lokal Säkerhetstjänst” och ”Lokal Säkerhetstjänst Terracotta” installeras de och körs default som ”Local System”. Det är rekommenderat att man skapar ett separat servicekonto som servicen körs som i stället för detta.

För att skapa en ny användare finns ett par olika vägar att gå, vi väljer att gå via ”Computer Management” verktyget. Högerklicka på ”Computer” i utforskaren och välj ”Manage”.



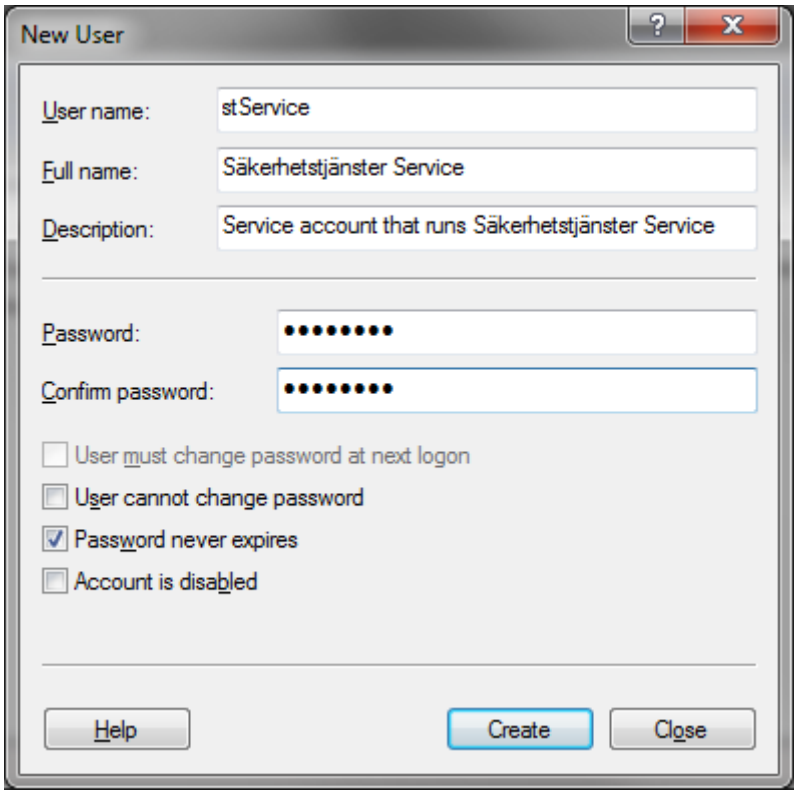
Figur 29: Gui för att komma till ”Computer Management”.



Figur 30: “Computer management” vyn.

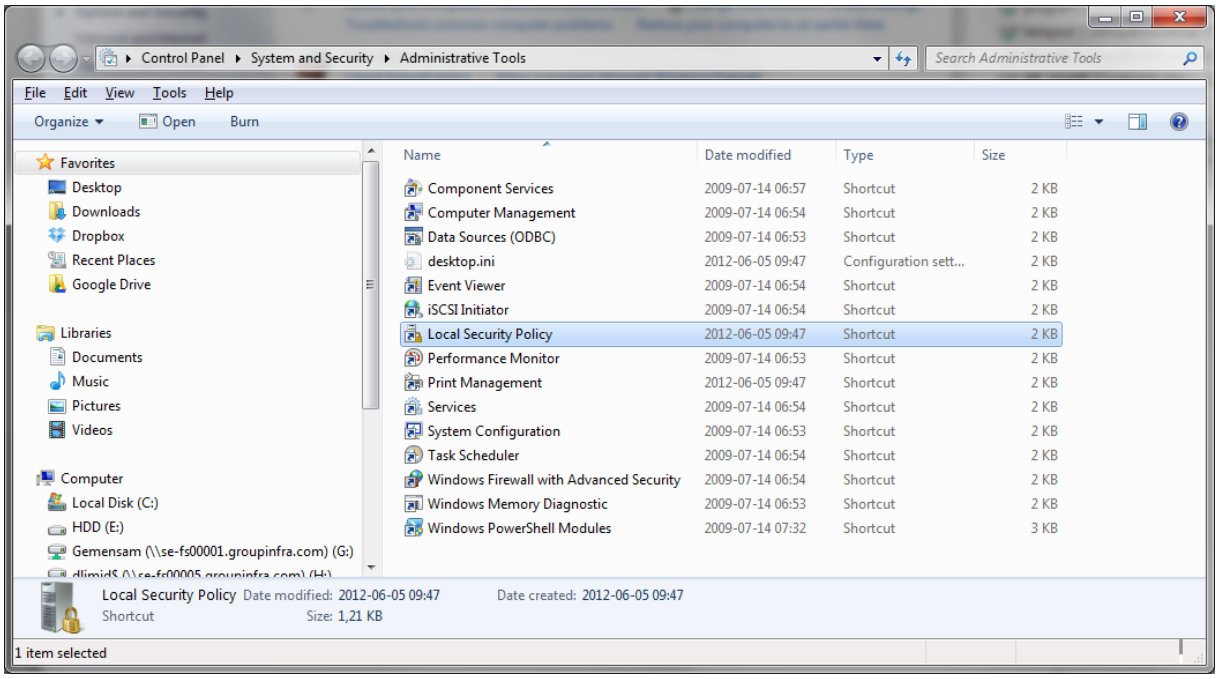
Välj ”Local Users and Groups” och högerklicka på ”Users” foldern och välj ”New User…”

Fyll i formuläret med önskade användaruppgifter samt se till att kryssrutorna är ikryssad enligt bilden nedan.



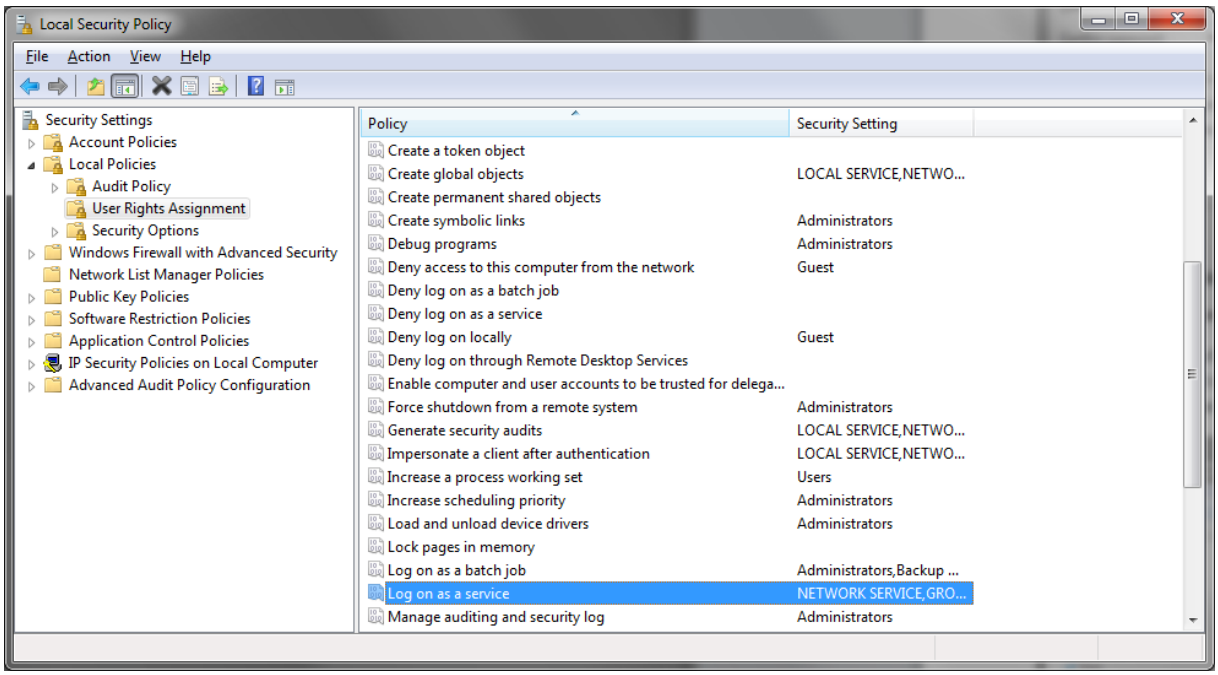
Figur 31: “New User” vyn.

Tryck sedan ”Create” samt ”Close” efter det.
För att användaren ska få behörighet att köra en service behöver den tilldelas en policy för detta och det gör man genom att starta ”Local Security Policy” som återfinns under ”Control Panel\System and Security\Administrative Tools”

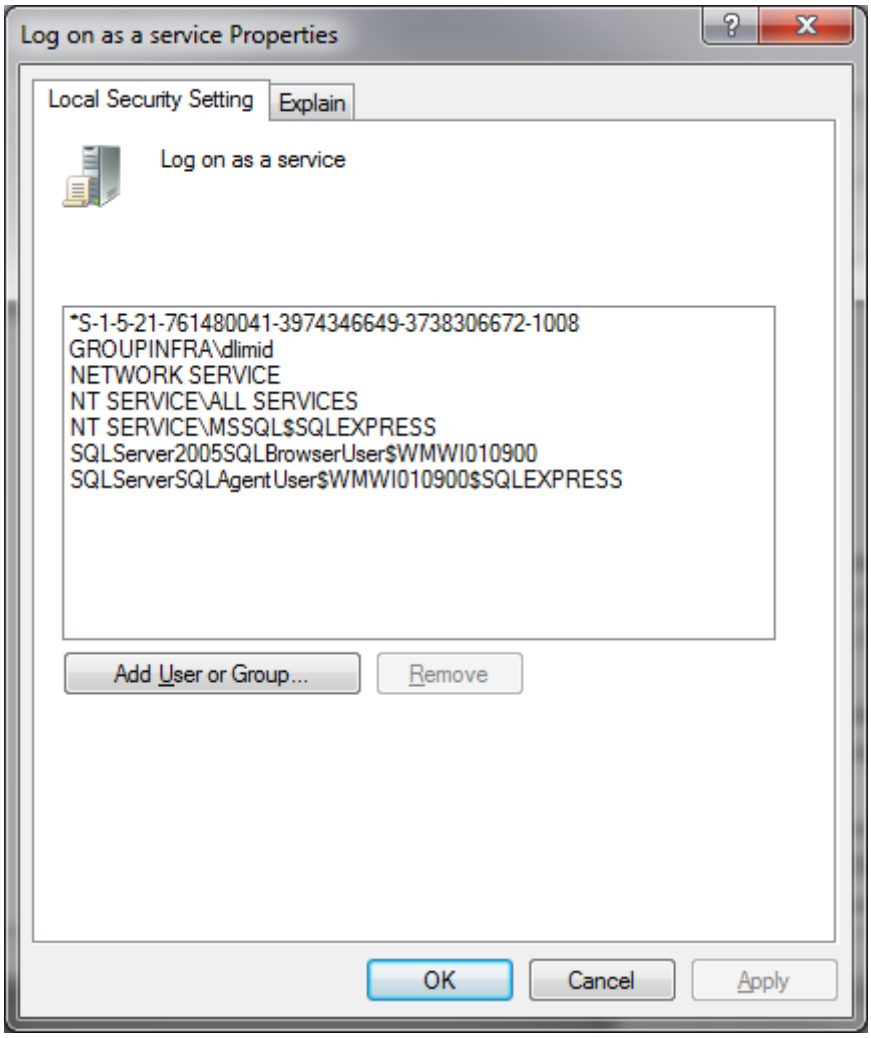


Figur 32: "Administrative Tools" vyn

Klicka på ”Local Policies” samt ”User Rights Assignment” i menyn till höger och lokalisera Policyn ”Log on as a service” i listan till höger och dubbelklicka på den.

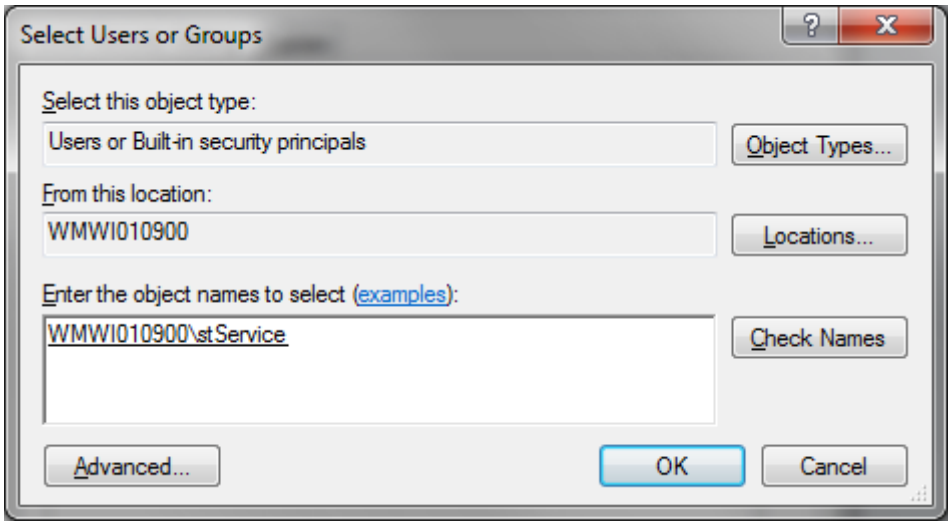


Figur 33: "Local Policies" vyn



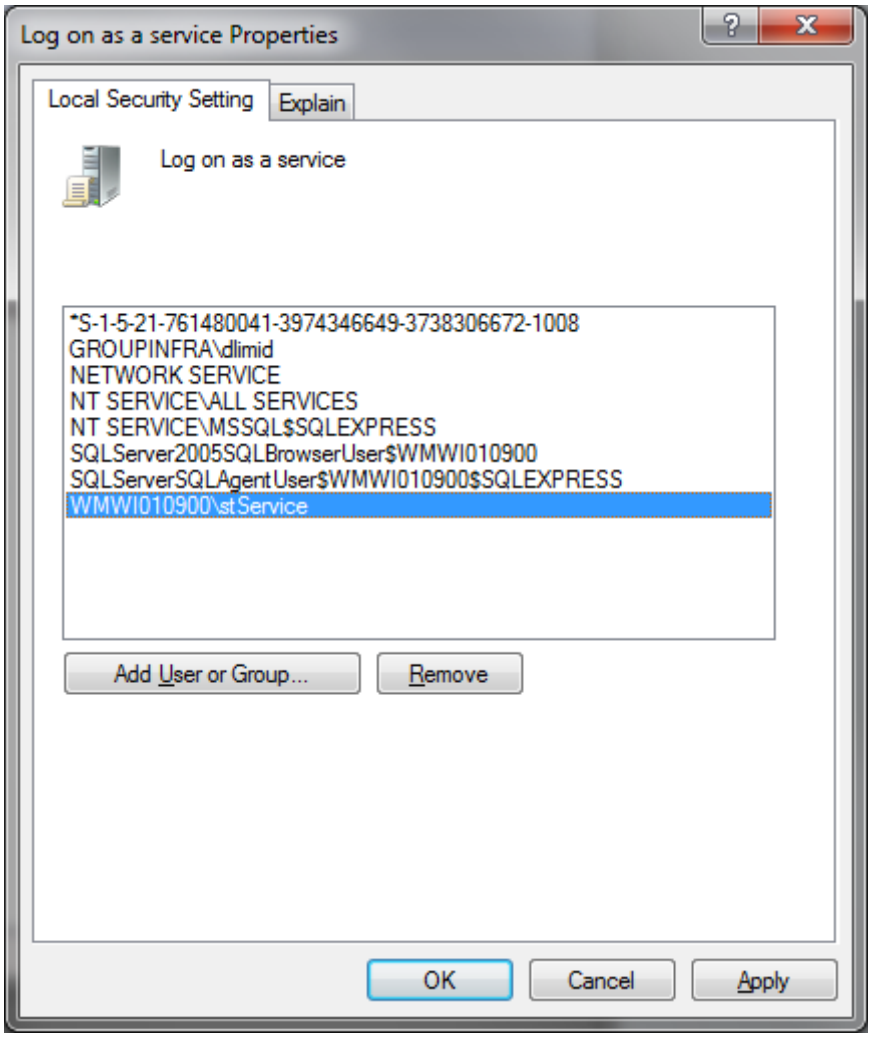
Figur 34: "Log in as a service" vyn

Välj ”Add User or Group” och peka ut den användare du vill servicen ska köras som. I exemplet är det den lokala användaren ”stService” som vi skapade i tidigare steg.



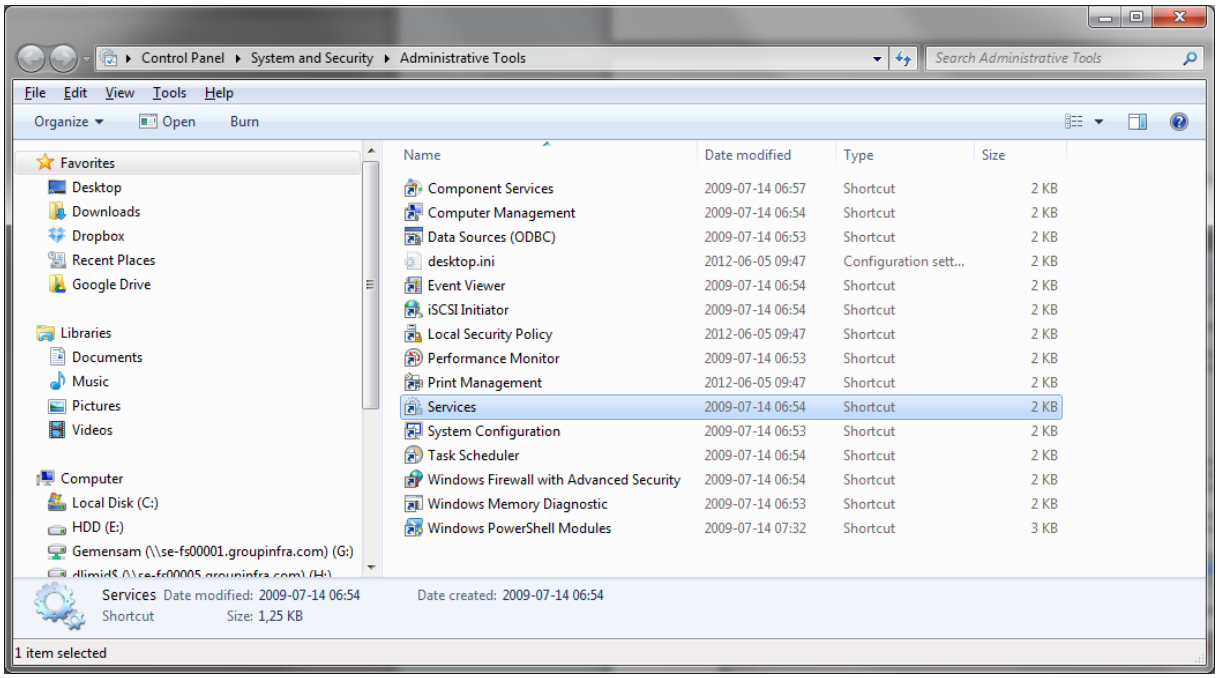
Figur 35: "Select users or group" vyn

Välj “Check Names” för att verifiera användaren du lagt till. Har du angivit en giltig användare som finns på den plats du pekat ut kommer användarnamnet i textboxen bli understruken som på bilden ovan.
Välj sedan OK.



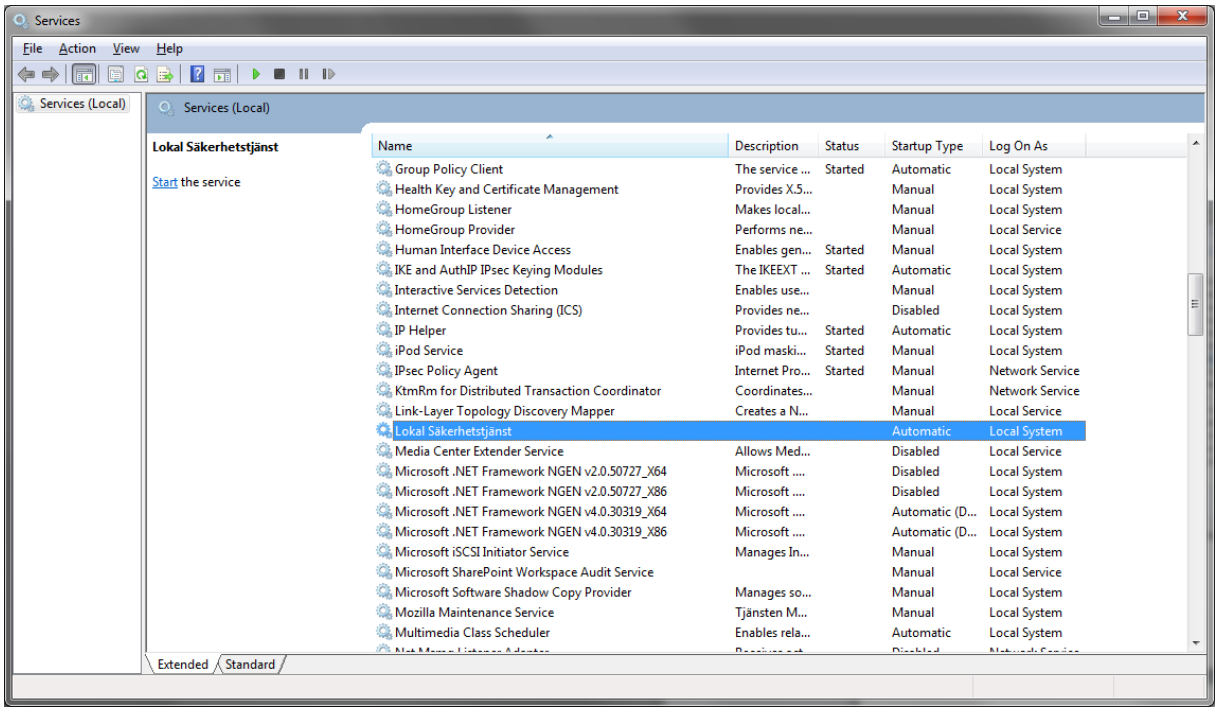
Figur 36: "Log in as a service" vyn

Verifiera att din användare nu ligger med i listan över användare som har ”Log on as a service”. Välj OK.



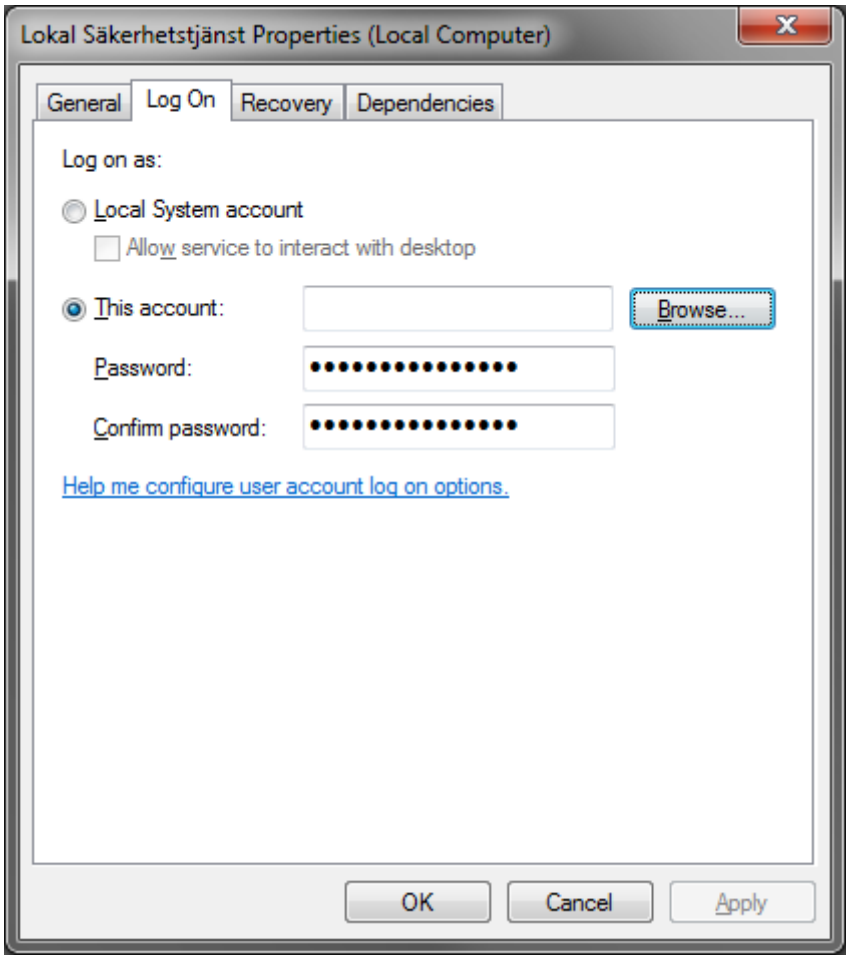
Figur 37: "Administrative tools" vyn

Nästa steg är att berätta för Servicen vilken användare den ska köras som. Detta gör du genom att gå till ”Services” som återfinns under ”Control Panel\System and Security\Administrative Tools”



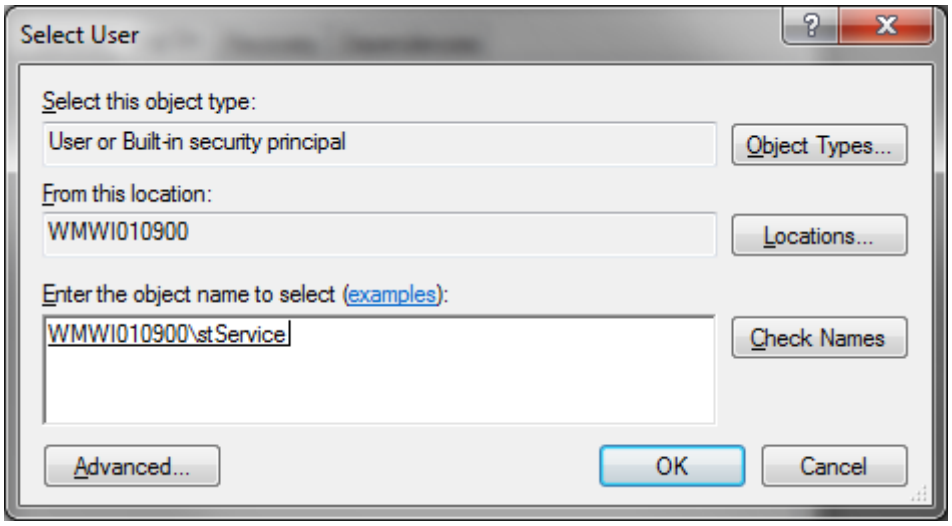
Figur 38: "Services" vyn

Leta rätt på servicen ”Lokal Säkerhetstjänst” i listan och dubbelklicka på den.



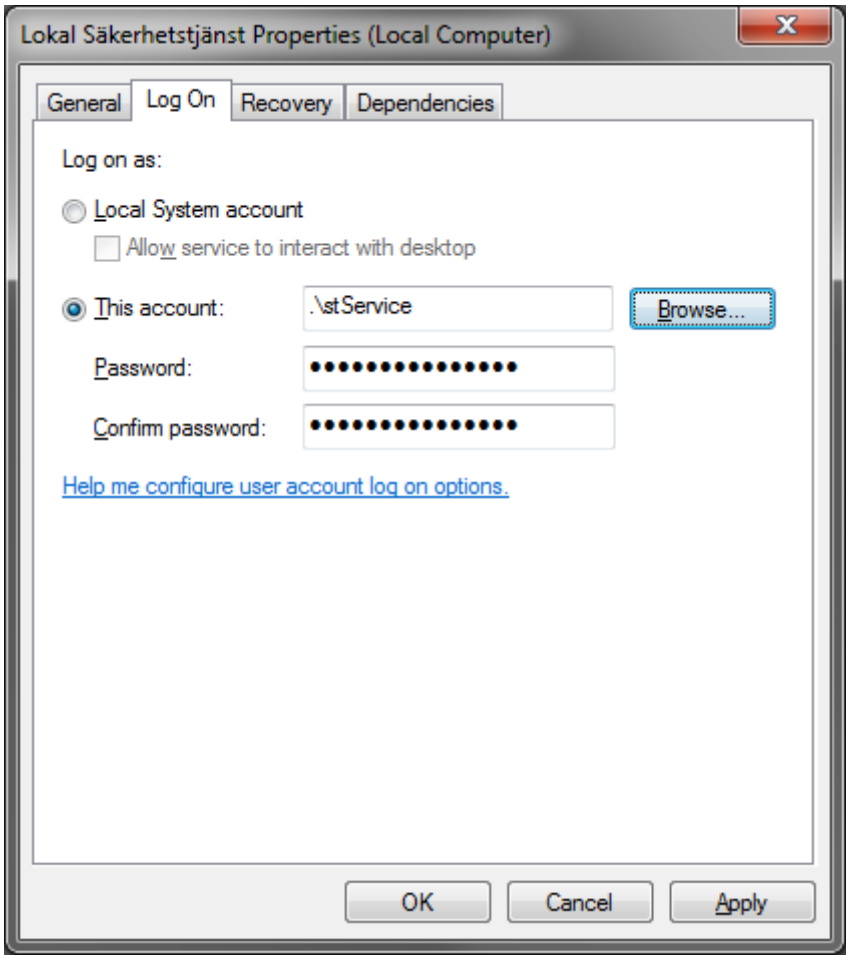
Figur 39: Lokal säkerhetstjänst inställningar

Välj sedan ”Log On” fliken i dialogen.
Default är värdet satt till ”Local Systen Account” men vi ska nu ange en specifik användare som ska köra servicen så välj istället ”This account” och välj ”Browse” för att peka ut den användare vi vill köra servicen som.



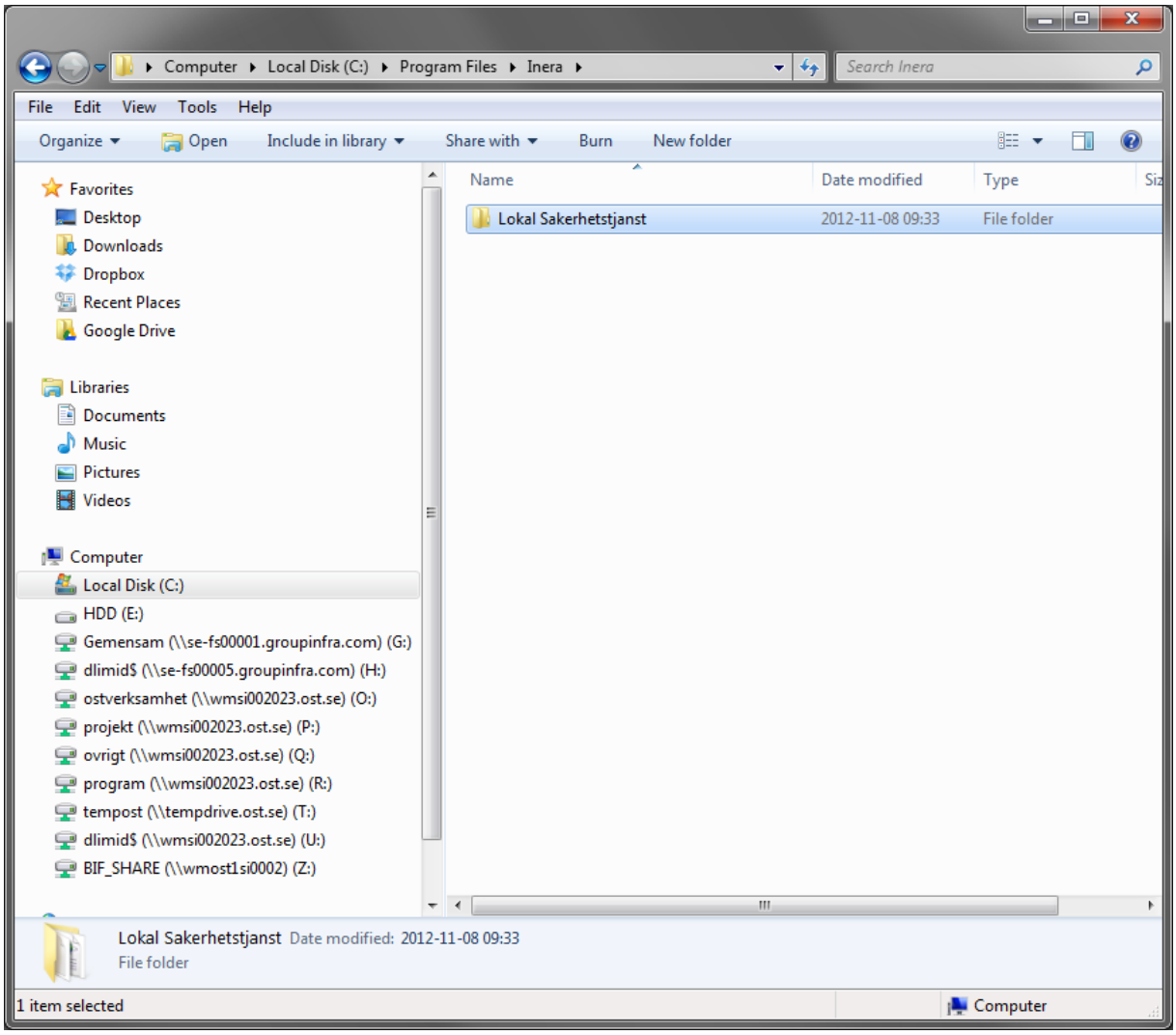
Figur 40: Val av användare som Lokala säkerhetstjänster ska köras som

Ange den användare du vill servicen ska köras som. I exemplet är det den lokala användaren ”stService” som vi skapade i tidigare steg.
Välj “Check Names” för att verifiera användaren du lagt till. Har du angivit en giltig användare som finns på den plats du pekat ut kommer användarnamnet i textboxen bli understruken som på bilden ovan.
Välj sedan OK.



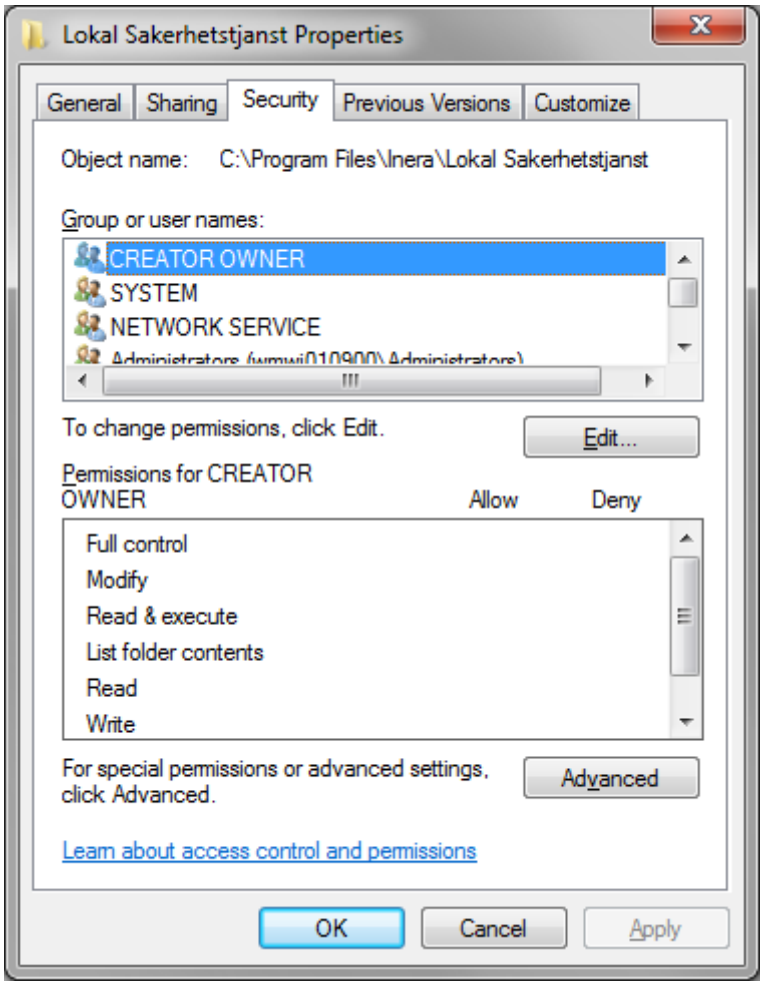
Figur 41: Lokal säkerhetstjänst inställningar

Ange lösenordet för användare och bekräfta det. Välj sedan på OK.
Nu när Säkerhetstjänster körs som en specifik använder så måste vi även ge denna användare behörighet till filerna och katalogerna som systemet ligger i.



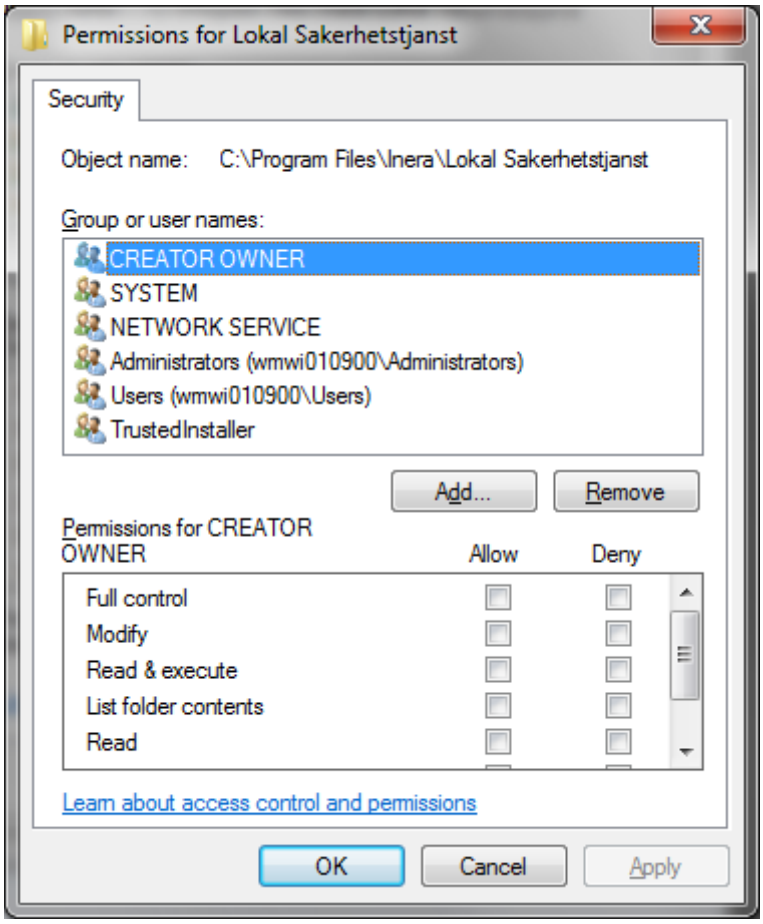
Figur 42: Lokal säkerhetstjänst installationskatalog

Välj utforskaren och bläddra fram dig till den katalog system är installerat i.
I exemplet ligger systemet installerat under ”C:\Program Files\Inera\Lokal Sakerhetstjanst”.
Höger klicka på katalogen ”Lokal Sakerhetstjanst” eller motsvarande katalog i er miljö och välj ”Properties” samt välj ”Security” fliken.



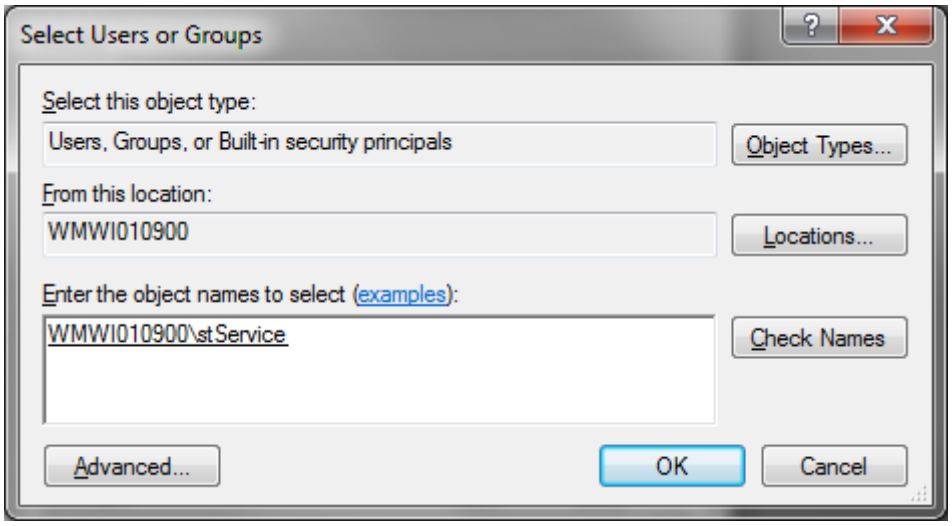
Figur 43: Security vyn

Välj ”Edit”.



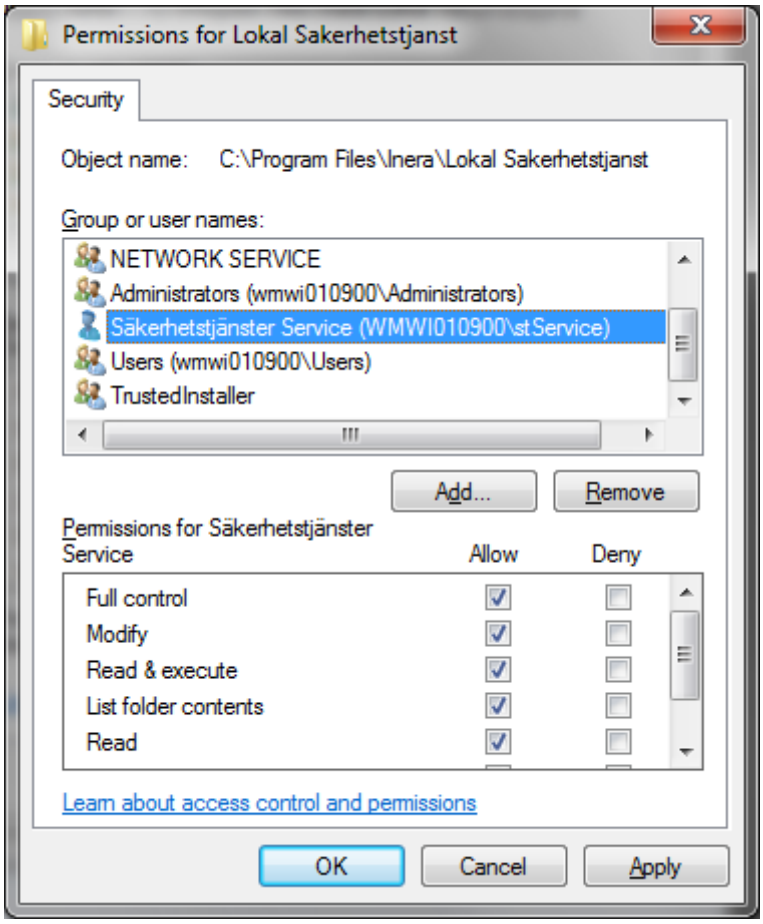
Figur 44: Behörighetsinstallningar

Välj ”Add”.



Figur 45: Lägg till användare

Peka ut användaren som vår service körs som och välj sedan OK.



Figur 46: Behörigheter för stService

Se till att vår nytillagda användare sedan är vald och kryssa i ”Full Control” och avsluta sedan genom att trycka OK och även OK i föregående dialog.

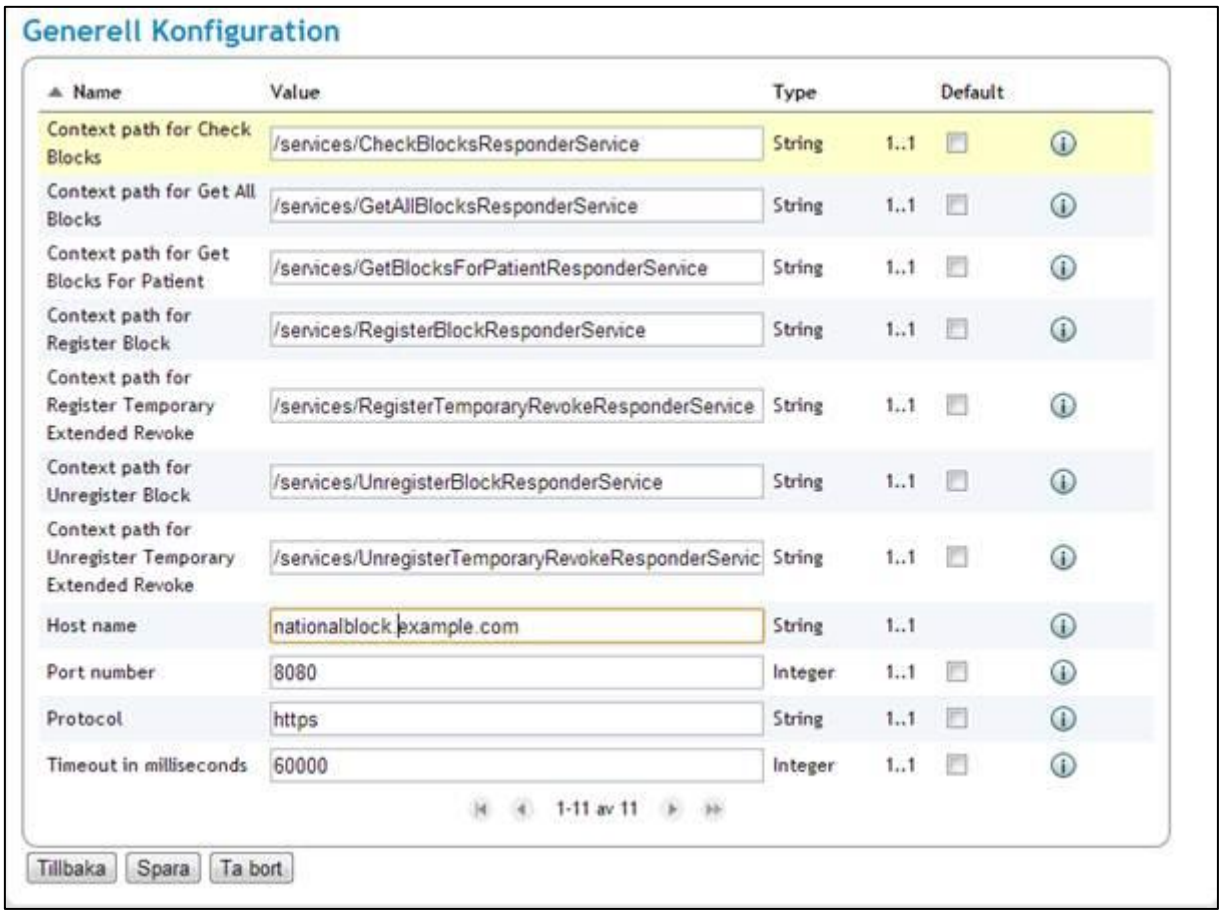
14 Appendix B Användning av generell konfiguration

I Generell konfiguration kan man ändra konfiguration för de olika tjänsterna. För att komma till generell konfiguration loggar du in i administrationsgränssnittet, läs mer om hur du gör det i kapitel 7.3. När du är i administrationsgränssnittet väljer du i vänstra menyn **Administration** -> **Generell konfiguration**.

Figur 47: Generell konfigurationssida.

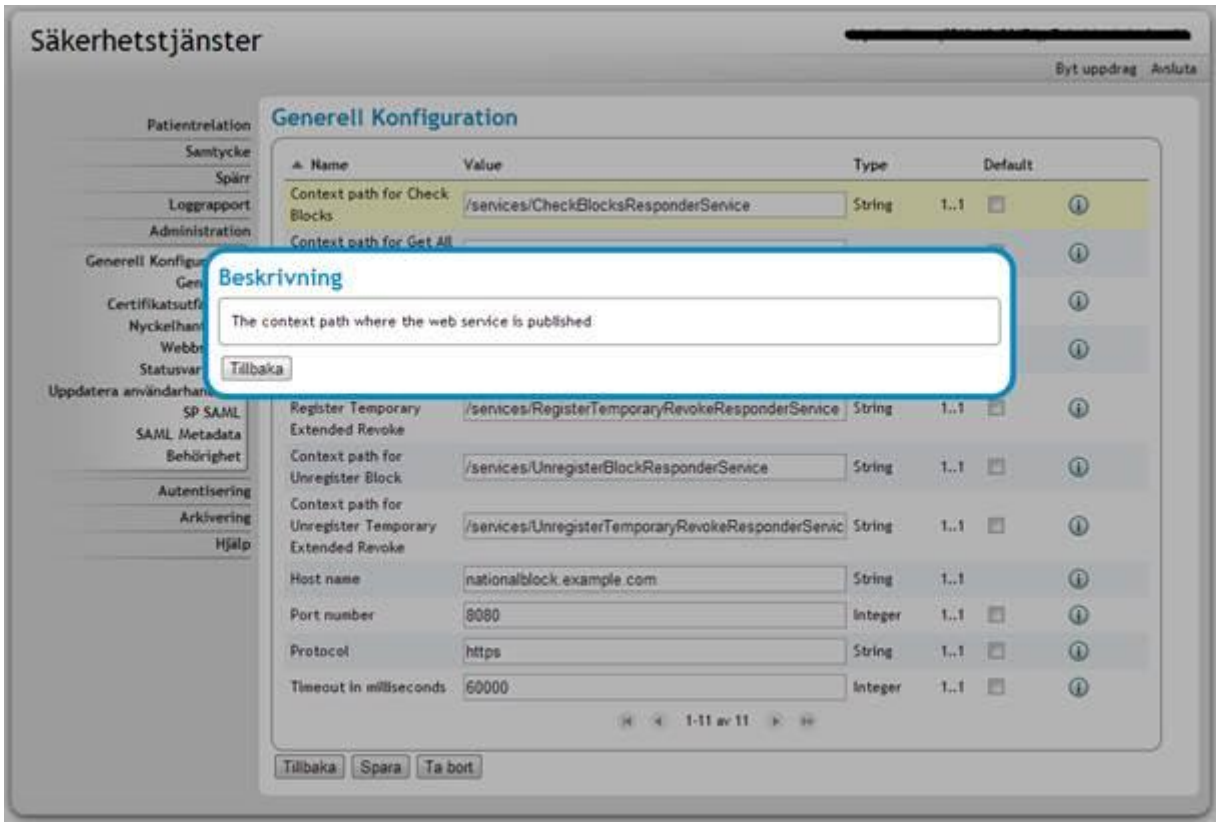
Då kommer du till Generell konfiguration. Där finns en lista på olika tjänster som kan konfigureras. För att välja en tjänst att konfigurera, klicka på pilen på den högra sidan.

Observera att Generell konfiguration enbart presenterar 20 tjänster per sida. Finns inte den tjänsten du vill konfigurera på den sidan kan du gå vidare till nästa sida, tills du hittat tjänsten. I nästa exempel kollar vi på konfigurationen för `Block National Webservice Proxy for RIV 2.0 1.0.0`



Figur 48: Nationell spärrtjänst konfigurationer

Här presenteras konfiguration för tjänsten. För att få mer information om varje konfiguration klickar i:et på den högra sidan.



Figur 49: Beskrivning generell konfiguration

När man ändrat konfiguration trycker man på spara, sedan tillbaka.