Skicka larm till SOS Alarm AB med SOS Access v.4

Nimbus kan skicka larm till SOS Alarm AB (SOSAB) med protokollet *SOS Access version 4*. Protokollet är XML-baserat och använder en TCP-förbindelse för att skicka larm. Förbindelsen kan också övervakas och har en primär- och en sekundärmottagare.

Detta dokument förutsätter Nimbus version 3.00.25 eller senare, där det finns stöd för *SOS Access v.4 specifikation 1.7*, inbyggt stöd för *pingrequest* (övervakning av förbindelsen) samt automatiskt byte från primär- till sekundärmottagaren om primärmottagaren inte svarar.

Servrar och portar

Kommunikationen går via en TCP förbindelse mot följande servrar och portar:

Mottagartyp i Nimbus (finns under Other\SOSAB)	***DNS namn [1]***	***IP [1]***	***Port [2]***	***Kommentar***
SOSAB (SOS Access) XML v4 (primary)	alarm1.sosalarm.se	194.14.58.9	19000	Primärmottagare Okrypterad trafik
SOSAB (SOS Access) XML v4 (secondary)	alarm2.sosalarm.se	194.14.60.9	19000	Sekundärmottagare Okrypterad trafik
SOSAB (SOS Access) XML v4 (encrypted/primary) - using NimbusTLSProxy	alarm1.sosalarm.se	194.14.58.9	19100	Primärmottagare Krypterad trafik [3]
SOSAB (SOS Access) XML v4 (encrypted/secondary) - using NimbusTLSProxy	alarm2.sosalarm.se	194.14.60.9	19100	Sekundärmottagare Krypterad trafik [3]

[1] Mottagartypsfilerna (RVC-filerna) har DNS-namnen specificerade och därför måste en fungerande DNS lookup finnas. Vill man istället använda sig av IP-adressen måste RCV-filerna redigeras (parameter URL). Detta gäller enbart okrypterad trafik.

[2] Ur brandväggssynvinkel är Nimbus alltid TCP socket klient.

[3] Ska man använda sig av kryptering så måste man också säkerställa att DNS lookup tillåter att certifikatkedjan kan valideras.

Redigera en mottagartypsfil (RCV-fil)

Enklaste sättet att redigera en RCV-fil är att högerklicka på mottagartypen i trädet och välja *Öppna RCV-filen i en texteditor*.

RCV-filerna ligger i *ReceiverTypes*-mappen som finns i *Project*-mappen. Sökvägen dit ser man längst ner till höger i Nimbus Explorer. Högerklickar man på sökvägen kan man direkt öppna Utforskaren i *Project*-mappen.

Information från SOS

SOS Alarm AB (SOSAB) har åtgärds- och installationsunderlag (*brand- inbrott- drift*) som man fyller i och skickar tillbaka. Kontakta *kundcenter@sosalarm.se* för att få underlagen.

Om man vill ha en övervakad förbindelse (ex 25 timmar) så kryssar man i det. Samma med krypterad/okrypterad förbindelse.

Utdrag ur installationsunderlaget:

Larmkoder/ingångar. *Ange vilka funktioner och larmkoder som installerats. Tekniskt fel samt Sabotage till nedan angivna funktioner ingår som standard.*							
Larmkod/Ingång		Larmbesked/Funktion		SIA- eller Contact ID-baserad sändare			
☐	01			☐	Inbrott	BA, BF, BG, BL, BM, BV, 130-136,139,146	
☐	02			☐	Brand	FA, FG, FM, 110-117	
☐	03			☐	Drift	GA, KA, QA, SA, WA, ZA.	
☐	04			☐	Brandindikering	FA, FG, FM, 110-117	
☐	05			☐	Överfallslarm	A, 120, 122-125	
☐	06			☐	Bråklarm	PA, 121	
☐	07			☐	Nödlarm	MA, 100-102	
☐	08			Ev. annan/ytterligare larmkod/ingång			Larmbesked/Funktion
				☒	IA		Driftlarm
Kommunikationsavbrott			Larmkod/Ingång	☐			
☐	Totalt kommunikationsavbrott			☐			
☐	Fel primärväg (IP)			☐			
☐	Fel sekundärväg (mobilt nät)			☐			
Reducering av korta störningar, genom att avvakta åtgärd på vissa larmhändelser som riskerar kortare störningar besparar vi kunden onödiga larmåtgärder. Om ni lägger in lokala fördröjningar meddela SOS Alarms kundcenter och ange detta under Övrigt.							

Som larmkod anger man *IA (Driftlarm)*

Från SOSAB kommer då information som ska fyllas i Nimbus Explorer. Informationen som man får kan se ut såhär:

Larmcentral: Nationell
Protokoll: SOS Access V4 okrypterad (Nationell)
Primärt Nr: 194.14.58.9 (alarm1.sosalarm.se)
Sekundärt Nr: 194.14.60.9 (alarm2.sosalarm.se)
Sändare: IO971234
Instansnamn: SV300
Port: 19000
Distribution: 10
Lösenord: gxkopje13s9rw

Konfiguration i Nimbus

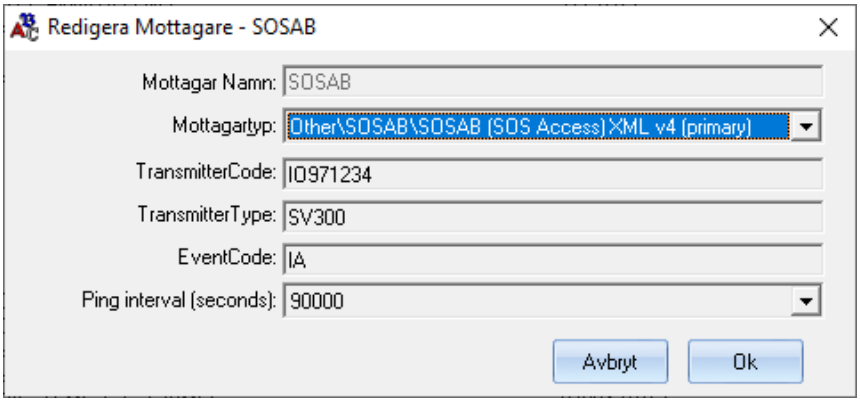
Nimbus har fyra mottagartyper för SOS Access v.4. Vanligtvis lägger man bara upp en enda mottagare och använder sig av en av följande mottagartyper beroende på om förbindelsen ska vara krypterad eller ej:

Other\SOSAB\SOSAB (SOS Access) XML v4 (primary)
Other\SOSAB\SOSAB (SOS Access) XML v4 (encrypted/primary) - using NimbusTLSProxy

Det är enbart en del av informationen som ska fyllas i enligt följande

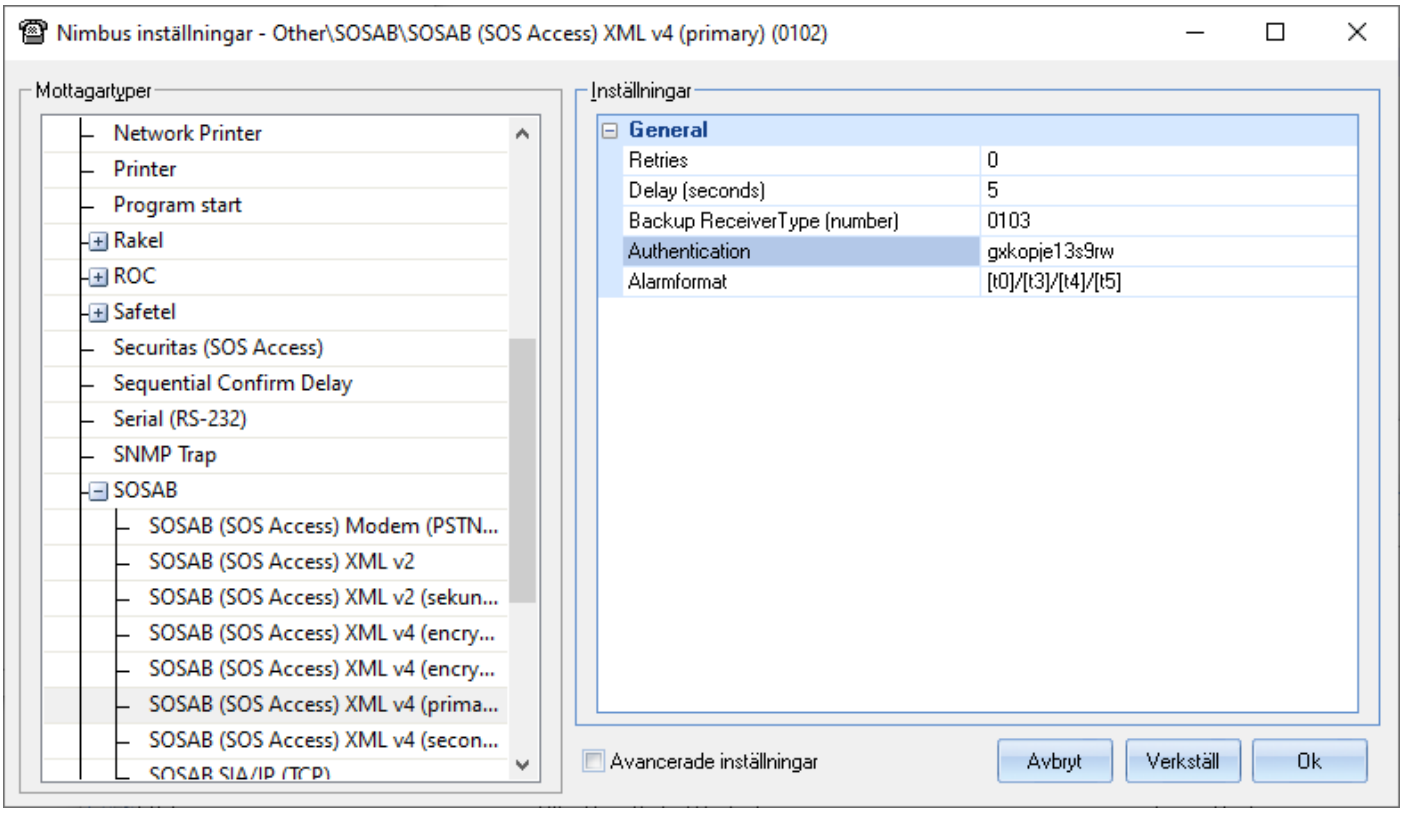
Nimbus benämning (samma som i XML)	***SOS benämning***	***Exempel***	***Kommentar***
Authentication	Lösenord	gxkopje13s9rw	Lösenord som validerar att avsändaren är giltig
TransmitterCode	Sändare	IO971234	Avsändarens identitet
TransmitterType	Instansnamn	SV300	Typ av sändare
EventCode	Larmkod	IA	IA betyder 'Driftlarm' och kommer från SIA-specen

Så här konfigureras en mottagare i Nimbus Explorer (okrypterad trafik):



Observera att i exemplet ovan så är abonnemanget beställt som okrypterat och med övervakning (25 timmar, dvs 90000 sekunder). Om abonnemanget inte är beställt med övervakning så måste detta fält vara tomt eller *Disabled* vara valt.

Så här konfigureras mottagartypen i Nimbus Explorer:



Observera att *Authentication* ska fyllas i både *Primary* och *Secondary* mottagartypen. Samma om man ändrar *Alarmformat*, glöm inte ändra också på *Secondary*.

Backup ReceiverType är förifyllt och ska finnas enbart på *Primary*. Vill man inte att Nimbus automatiskt provar med *Secondary* så ska fältet vara tomt på båda.

Övervakning (option)

Övervakning måste beställas för att kunna användas och är också förbunden med en extra kostnad för abonnemanget.

Förbindelsen övervakas genom att Nimbus cykliskt skapar ett internt larm som skickas till SOSAB med pakettypen *pingrequest*. Intervallet mellan dessa larm räknas ut automatiskt och är en tredjedel av *Ping interval*. I exemplet ovan således drygt 8 timmar (30000 sekunder, dvs 500 minuter).

Om det inte kommer in en *pingrequest* inom den beställda övervakningstiden observeras det hos SOSAB som ett *ledningsfel* och de vidtar överenskommen åtgärd.

Det lägsta ping intervallet som kan väljas är 90 sekunder men det ska inte användas eftersom Nimbus servern hanterar alla larmsändningar i sekvens en i taget och om Nimbus är upptaget med att skicka exempelvis en skur av larm till andra typer av mottagare kan intervallet överstiga 90 sekunder och i så fall skapas ett *ledningsfel* hos SOSAB.

Det interna larmet som cykliskt skapas och skickas visas inte i Nimbus Explorer men loggas i systemloggen och syns givetvis i debuggern. Om man vill att dessa larm (heartbeats) ska synas i Nimbus Explorer så kan man ställa parametern *[General]HideHeartBeatAlarms=0* i Nimbus_Server.ini. Nimbus Server behöver startas om efter en ändring.

När Nimbus Servern startar upp så kommer servern således skicka den första pingrequest efter en tredjedel av ping interval.

Vill man att servern ska skicka ett första pingrequest snabbare så kan man ändra parametern *[Protocol]FirstPingRequestDelay* i respektive RCV-fil. Nimbus Server behöver startas om efter en ändring.

Tänk på att om man ställer tiden för kort och startar om Nimbus Server flera gånger efter varandra så kommer SOSABs server reagera på att man skickar *pingrequest* för ofta.

OBS! Om man av någon anledning skapar flera mottagare med samma *TransmitterCode* för en övervakad förbindelse så ska enbart en av dem ha ett *Ping interval*, övriga ska ställas på *Disabled*.

Avprovning

Prova att skicka ett vanligt textmeddelande till SOSAB. Om det ser ut att gå bra, kontakta kundcenter (0771-505 100) och meddela det och be dem titta om det kom in. Du behöver ange det lösenord som angavs i åtgärdsunderlaget.

Om det misslyckades, titta i *Log->Visa debugfönstret* vad Nimbus servern fick för svar av SOSABs server (raderna i debuggern är ihopskrivna). I följande exempel är någon av uppgifterna felaktig, exempelvis lösenordet:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<alarmresponse>
 <status>4</status>
 <info>NOT_AUTHORIZED</info>
 <reference>0141</reference>
 <arrivaltime>2021-07-07 12:54:24.341</arrivaltime>
</alarmresponse>
```

Om Nimbus servern inte fick något svar alls är sannolikt någon brandvägg felkonfigurerad eller så fungerar inte DNS-lookup.

Nimbus provar automatiskt sekundärservern om primärservern inte svarar.

Ställ upp antal *Retries* från 0 till 1 när konfigurationen är klar och fungerande (både på *Primary* och *Secondary*)

OBS! Oavsett om en förbindelse är övervakad eller ej är det lämpligt att enligt bestämt schema prova av att förbindelsen faktiskt fungerar, speciellt efter förändringar i IT-strukturen exempelvis vid byte av switchar eller brandväggar. Speciellt sekundärservern i en redundant konstellation då den i vanliga fall är inaktiv sällan kommer skicka pingrequests eller larm. Avprovning överenskommes och stäms av med SOSAB.

Redundans

I en redundant konfiguration säkerställer Nimbus att *pingrequests* enbart skickas ut av den aktiva servern. Om *pingrequests* skickas från båda servrarna så märker inte SOSAB om att den ena servern går ner samt att de då skickas för ofta.

Om man av någon anledning vill prova skicka från båda servrarna så sätter man *SendPingrequestsAlsoFromInactiveServer=0* i RCV-filerna och startar om Nimbus Server.

I en redundant konfiguration måste man konfigurera mottagartyperna likadant på båda servrarna och testa att skicka ett meddelande också från sekundärservern.

Kryptering

Nimbus servern är utvecklad med en äldre teknik som inte enkelt medger implementation av modern SSL/TLS kryptering och för att använda kryptering så finns det därför en proxyserver, *NimbusTLSProxy*. Det är ett program som installeras som tjänst i samma server som Nimbus servern.

Nimbus servern använder *NimbusTLSProxy* som mellansteg i trafiken till SOSAB. Trafiken mellan Nimbus servern och *NimbusTLSProxy* är en vanlig TCP-förbindelse där *NimbusTLSProxy* är socket server på portarna 19101 samt 19102. *NimbusTLSProxy* upprättar i sin tur en krypterad förbindelse till SOSABs server på TCP port 19100 varje gång Nimbus servern vill skicka något.

NimbusTLSProxy programmet kan vid behov installeras på en annan server om man ex vis av säkerhetsskäl behöver hoppa mellan servrar. Om NimbusTLSProxy installeras i en annan server än Nimbus Server så måste man ange ett undantag i Windows brandvägg i den servern för att tillåta trafik till dessa portar (eller till *NimbusTLSProxy*) från servern där Nimbus är installerat.

Installera *NimbusTLSProxy* med installationspacket. Programvaran kräver *.NET 4.6.1*.

Konfigurera i *NimbusTLSProxy.exe.config* om det skulle behövas. Varje parameter är beskriven i config-filen.

Kör till att börja med *NimbusTLSProxy* som en vanlig applikation. Den information som visas i fönstret sparas också i *SysLog*-mappen som skapas vid uppstart. De filerna, liksom filerna i *DebugFiles*-mappen, raderas automatiskt efter 90 dagar (default)

Behöver man felsöka applikationen så kan man avmarkera *<system.diagnostics>* sektionen i config-filen som är bortkommenterad med *<!--* samt *-->* och starta om programmet. Då skapas en *trace.log* där man kan följa validering av certifikat etc. Glöm inte kommentera sektionen igen efteråt eftersom *trace.log* kan växa sig stor - den raderas inte automatiskt.

För att ändringar i config-filen ska slå igenom behöver programmet startas om. Det avslutas genom att trycka *ESC* i fönstret.

För att kryptering ska fungera måste certifikatkedjan och SOSABs servernamn (*alarm1.sosalarm.se* samt *alarm2.sosalarm.se*) kunna lösas upp via DNS

Lägg till NimbusTLSProxy som tjänst

Avsluta programmet.

Starta en CMD-prompt som Administratör. CD:a ner i mappen *C:\Program Files\TroSoft\NimbusTLSProxy*

Kör foljande kommando:

NimbusTLSProxy /i

Programmet läggs nu till som tjänst och behöver startas manuellt via tjänstehanteraren första gången, det heter *Nimbus SSL/TLS service*.

Ta bort NimbusTLSProxy som tjänst

För att ta bort programmet från tjänster så stoppas det först via tjänstehanteraren och avinstalleras på samma sätt som det installerades men med kommandoradsparametern /u istället för /i

Konfigurera NimbusTLSProxy på en annan server

Redigera i RCV-filerna tillhörande mottagartyperna *SOSAB (SOS Access) XML v4 (encrypted/primary) - using NimbusTLSProxy* samt *SOSAB (SOS Access) XML v4 (encrypted/secondary) - using NimbusTLSProxy* och revidera URL så de pekar på den server där *NimbusTLSProxy* är installerad.

I *NimbusTLSProxy.exe.config* kan man konfigurera parametern *AllowedNimbusAddresses* för att begränsa vilka IP som får ansluta på portarna alternativt lösa det via brandväggsregler.