13. Systeminställningar

Under SYSTEMINSTÄLLNINGAR/SERVER samlas information och inställningar för serverdelen av Web Port. Vilka inställningar som är nödvändiga beror på hur Web Port skall användas.

Under generella inställningar (se kapitel 13.3) anges diverse information om den aktuella Web Port installationen.

Om Web Port skall göras tillgängligt via internet rekommenderas att HTTPS (SSL) används vilket beskrivs i kapitel 13.4.

Om e-post larm skall användas måste SMTP konfigureras, detta beskrivs under kapitel 13.9.

Om ett GSM modem finns tillgängligt måste COM-port och kommunikationshastighet anges, detta beskrivs under kapitel 13.10.

Web Port kan kopplas mot ett befintligt Active Directory (AD), vilket antingen kan göras via NTLM (se kapitel 13.5) eller via LDAP (se kapitel 13.6).

Databastyp och lagringsinställningar beskrivs i kapitel 13.12.

13.1 Serverstatus

Här visas information om aktuell status för Web Port servern.

Följande information finns att utläsa:

Serverstatus	
Version	Version av Web Port Server
Anslutna klienter	Antalet anslutna klienter
Ledigt lagringsutrymme	Ledigt utrymme på den hårddisk Web Ports datamapp finns.
Antal pågående frågor	Antalet samtidiga frågor från noder och klienter.
Taggar	
Totalt antal taggar	Antalet inlästa taggar
Totalt antal larmtaggar	Antalet larmtaggar
Totalt antal trendtaggar	Antalet trendtaggar
Lokala sidor	Antalet lokala sidor
Nod-sidor	Antalet sidor från noder
Trådar	
ALARM senaste cykel	Senaste cykel för larmkontroll
TREND senaste cykel	Senaste cykel för trendkontroll
TASK senaste cykel	Senaste cykel för uppgiftskontroll

” OBS:

Om någon av tidsstämplarna för Trådar inte är aktuell och inte uppdateras då dialogrutan för Serverstatus öppnas upprepade gånger är något troligen fel.

Kontrollera felloggar både i Web Port och i Windows för fortsatt felsökning.

13.2 Licensinformation

Under licensinformation finns information om eventuell aktiv licens. Här visas även versionsnummer för tillgängliga drivrutiner och funktionstillägg.

” Information:

(Gäller endast vid mjukvarulicens)

Dator-ID används vid generering av mjukvarulicenser. Denna skall alltid skickas med då en licens skall utökas eller skapas.

Om en mjukvarulicens skall genereras var noga med att det står (SOFTKEY) efter Dator-ID. Om så ej är fallet sitter antagligen ett hårdvarulås eller utvecklingslicens i datorn. Ta då bort denna och starta om Web Port.

*Var även noga med att datorn är ansluten till nätverket på det sätt som den kommer vara under drift, annars finns risk att Dator-ID kan ändras. Välj även **primärt nätverkskort** för att säkerställa att dator-ID inte ändras om VPN eller annat nätverk ansluts.*

13.3 Allmänna inställningar

Allmänna inställningar styr framförallt informationen vid inloggningsrutan. Här anges även URL-adressen till Web Port servern vilken bland annat används vid e-postlarm för att hänvisa till larmande sida.

Följande inställningar kan göras:

Anläggning	Text som beskriver anläggningen som Web Port visualiserar.
Företagsnamn	Eventuell företagsinformation
Hemsida företag	Länkadress till hemsida. Länkar företagsnamnet (öppnas i nytt fönster).
E-post företag	Eventuell e-postadress till företag
Supportinformation	Text som beskriver vem som skall kontaktas då support önskas.
WebPort-url	URL-adress till Web Port server (skall även innehålla port).
Bakgrundsfärg logotyp	Eventuell bakgrundsfärg bakom logotyp.

” Information:

En URL-adress anges med följande format:

http://adress:port ***exempel1:*** http://192.168.1.10:8090 ***exempel2:*** http://exempel.se:8090

*Om port 80 används behövs ej **:port** anges.*
*Om SSL används anges **https** i stället för **http**.*

” Information:

*Logotyp sätts genom att placera en fil med namn **logo.png** i katalogen **/assets/theme/***

*Bilden skall ha höjden **40px** och en brädd som bibehåller proportionerna för logotypen.*

*Det finns möjlighet att använda olika logotyper för olika användare och grupper. För att lägga in flera filer än standard, namnge dem **logo***.png**.*

13.4 SSL Certifikat

För att kryptera förbindelsen mot Web Port servern används Secure Socket Layer (SSL). För att detta skall fungera krävs att ett certifikat utfärdas. Detta kan göras från SYSTEMINSTÄLLNINGAR/SERVER/SSL Certifikat.

Det finns två typ av certifikat, egensignerade samt signerade av en betrodd tredje part. Då signerade certifikat används indikeras detta genom ett grönmarkerat adressfält i de flesta webbläsare. Självsignerade certifikat genererar en varning i de flesta webbläsare såvida inte den egna datorn kan verifiera certifikatet. Detta kan göras genom att det självsignerade certifikatet installeras i förväg på samtliga datorer som kommer ansluta mot Web Port servern.

Följande information fylls i för att generera ett certifikat, alternativt CSR.

Common Name (CN)	Den IP-adress eller det domännamn certifikatet skall utfärdas till.
Organisation	Organisationsnamn, exempelvis företagsnamn.
Avdelning	Eventuell avdelning inom företaget.
Stad	Stad där företaget har sin verksamhet.
Region / Landskap	Region i landet där företaget har sin verksamhet.
Land	Land där företaget har sin verksamhet.
Alternativa namn	Används om flera domännamn eller IP-adresser skall skyddas.
Nyckeltyp	Antal bitars kryptering i nyckeln
Lösenord	Lösenord för certifikatet
Självsignera	Markeras om ett själv-signerat certifikat skall genereras.

” Information:

Status ger information om aktuell status för certifikatet.

13.4.1 Självsignerade certifikat

Självsignerade certifikat kan utfärdas direkt av Web Port servern. Detta görs genom att följa instruktionen nedan:

1. Fylla i informationen som beskrivs under **13.4**
2. Markera rutan **Självsignera.**
3. Tryck på knappen SPARA
4. Tryck på knappen SKAPA CERT (till höger om SPARA)
5. Vänta tills en popupruta kommer fram där det framgår att certifikatet har genererats. Detta kan ta någon minut.
6. Stoppa Web Port servern
7. Gå till datakatalogen för Web Port.
8. Dubbelklicka på filen webport.p12 och installera certifikatet på lokal dator. Följ instruktionerna i Windows. Observera att välja **lokal dator** och **INTE** aktuell användare. Lösenordet som efterfrågas är det som angavs vid genereringen av certifikatet.
9. Starta upp Web Port server.
10. Uppdatera adressfältet i webbläsaren till **https** och återanslut till Web Port.

För att se information om aktuellt certifikat gå till SYSTEMINSTÄLLNINGAR/SERVER/SSL Certifikat

> ***” Information:***
>
> *För att undvika varningar på klienter som ansluter mot Web Port servern kan webport.p12 installeras på samtliga klienter som skall ha åtkomst till Web Port. För att göra detta kopiera filen till klienten och utför steg 8 enligt ovan.*

13.4.2 Signerade certifikat

Signerade certifikat utfärdas av en betrodd 3:e part. Det finns flera tjänster som kan göra detta. Enklast är att söka på nätet efter SSL certifikat. Då ett certifikat skall beställas krävs något som kallas Certificate Signing Request (CSR), vilket skapas direkt i Web Port. För att generera en CSR följ stegen nedan:

1. Fyll i informationen som beskrivs under **13.4**
2. Se till att rutan självsignera EJ är markerad
3. Tryck på knappen SPARA
4. Tryck på knappen SKAPA CSR
5. Vänta tills en popupruta indikerar att CSR har skapats
6. Ladda ner och spara **Privat Nyckel** på säkert ställe
7. Följ instruktioner hos utfärdaren av certifikatet och bifoga **CSR-fil**
8. Ange informationen om certifikatet som erhålls från utfärdaren i de tre rutorna: **Domäncertifikat**, **CA Intermediate-certifikat** samt **CA Root-certifikat**.
9. Tyck på knappen SPARA
10. Tryck på knappen SKAPA CERT
11. Vänta tills en popupruta kommer fram där det framgår att certifikatet har genererats. Detta kan ta någon minut.
12. Stoppa Web Port server
13. Gå till datakatalogen för Web Port.
14. Dubbelklicka på filen webport.p12 och installera certifikatet på lokal dator. Följ instruktionerna i Windows. Observera att välja **lokal dator** och **INTE** aktuell användare. Lösenordet som efterfrågas är det som angavs vid genereringen av certifikatet.
15. Starta upp Web Port server.
16. Uppdatera adressfältet i webbläsaren till **https** och återanslut till Web Port.
17. Kontrollera informationen om certifikatet under SYSTEMINSTÄLLNINGAR/SERVER/SSL Certifikat

13.4.3 Ta bort certifikat

För att ta bort ett aktivt certifikat gå till SYSTEMINSTÄLLNINGAR/SERVER/SSL Certifikat. Klicka sedan på knappen TA BORT CERT och starta sedan om Web Port.

” Information:

För att ta bort certifikatet från Windows öppna Certificate Manager (Klicka på Windows Start och skriv sedan certmgr.msc och ENTER). Sök och ta bort alla Certifikat som heter något mer webport.

” Tips:

Det går även att tillfälligt inaktivera certifikatet genom att döpa om filen webport.p12 och sedan starta om Web Port server.

Kom ihåg att ändra till http istället för https då detta görs.

För att återaktivera certifikatet är det bara att döpa om filen igen så att den heter webport.p12 och sedan starta om Web Port server.

13.5 Inloggnings-inställningar

Under inloggningsinställningar ställer man in hur användaren skall logga in. Som standard används inloggning via HTML-formulär med en automatisk utloggning efter 10 minuter.

Här kan även väljas om användaren skall kunna se sin profil samt byta språk.

Obligatorisk grupp anger om en användare måste tillhöra en viss grupp för att överhuvudtaget kunna logga in i Web Port.

Följande inloggningsmöjligheter finns:

FORM	Inloggning via HTML formulär (standard)
BASIC	Inloggning via Basic Authentication, kräver att Aktivera BASIC har valts.
NTLM	Inloggning via NTLM, kräver att Aktivera NTLM har valts.

Det går även att använda en typ av inloggning som standard och via URL styra inloggningen till en annan typ. Detta görs enligt följande URL:er.

FORM	http://serveradress/access/login
BASIC	http://serveradress/access/loginbasic
NTLM	http://serveradress/access/loginntlm

” Information:

*För att använda BASIC authentication krävs att bockrutan **Aktivera BASIC** markeras.*

” Information:

*För att använda NTLM krävs att bockrutan **Aktivera NTLM** markeras.*

” Information:

Då NTLM används utnyttjas användare som finns definierade i AD. Åtkomst till Web Port styrs då genom att skapa matchande grupper i AD och Web Port, och sedan anges rättigheter på respektive grupp i Web Port.

” Tips:

NTLM kan med fördel användas för Single-Sign-On (SSO) då både klient och server är anslutna mot samma AD. Kontrollera inställningar i aktuell Webbläsare så att den är den för vidare uppgifter om inloggad användare till webbservern.

13.6 LDAP-inställningar

På motsvarande sätt som för NTLM kan inloggning via FORM användas för att verifiera användare mot ett AD. Detta görs genom att konfigurera en koppling via LDAP mellan Web Port och upp till två stycken AD-servrar. Web Port kommer då först försöka verifiera användaren mot AD, misslyckas det kommer en lokal verifiering att göras.

Då LDAP används måste matchande grupper skapas i AD och Web Port. Rättigheterna för Web Port sätts på respektive grupp under SYSTEMINSTÄLLNINGAR/ÅTKOMST/GRUPPER.

Följande inställningar kan anges för LDAP:

Aktivera LDAP	Aktiverar funktionen för LDAP uppslagning.
Active Directory Host	Adress till AD-server
Base DN	Plats att påbörja AD-sökning
User Filter	Sökuttryck. {0} byts ut mot användarnamn vid sökning.
Domain	Används för att rikta sökningen mot en viss server.
Auth-typ	Inloggningstyp mot AD.
Användarnamn	Användarnamn för anslutning mot AD.
Lösenord	Lösenord för anslutning mot AD.

” Information:

Uppgifterna ovan tillhandahålls av den IT-avdelning som administrerar AD-servrar.

” Tips:

För att verifiera att LDAP informationen är korrekt och att en koppling finns mot AD utför en testinloggning.

Inloggningen måste göras med en användare som finns i AD och resultatet skall vara en uppsättning med grupper användaren är medlem i.

13.7 Tillägg

Under tillägg kan olika tilläggsfunktioner aktiveras i Web Port. Som standard finns endast objektsamlingar (se kapitel 12). Om något Addon installerats i Web Port kan detta erbjuda tilläggsfunktioner som utökar antalet val.

För att aktivera en tilläggsfunktion markera respektive bockruta och tryck sedan SPARA.

13.8 Tidkanaler

Web Ports tidkanalhantering är som standard inaktiverade. För att aktivera denna markera bockrutan **Aktivera Tidkanaler** och tryck SPARA. För att läsa mer om tidkanaler se kapitel 10.

13.9 Epost-inställningar

För att skicka e-post från Web Port krävs åtkomst till en SMTP-server. Information om vilken SMTP-server som skall användas kan ges av den IT-avdelning eller Internet Service Provider (ISP) som tillhandahåller nätverket.

Följande inställningar kan göras för e-post:

SMTP-server	IP-adress eller hostnamn till SMTP-servern
SMTP-port	Den port som används för att ansluta till servern
Sändande e-postadress	Den e-postadress som kommer stå som avsändare
Användarnamn	Eventuellt användarnamn för att ansluta till SMTP-servern
Lösenord	Eventuellt lösenord för att ansluta till SMTP-servern
Använd SSL	Markera om SMTP-servern kräver anslutning via SSL
Teckenformat	Det teckenformat e-post skall sändas med.

" Tips:

Verifiera att anslutningen mot SMTP-servern är korrekt genom att skicka ett testmeddelande.

Ange rubrik, meddelande samt vilken e-post adress som skall vara mottagare och klicka sedan på Skicka.

13.10 SMS-inställningar

Web Port kan använda GSM-modem för att skicka SMS. För att detta skall fungera krävs ett GSM-modem som ansluter antingen mot en fysisk eller virtuell COM-port i Windows. Kommunikation mot modemet måste kunna ske via AT kommandon.

Följande inställningar kan göras:

COM-port	Anger numret på den COM-port där modemet sitter.
Kommunikationshastighet	Kommunikationshastighet för modemet i baud.

" Tips:

Verifiera att anslutningen mot GSM-modemet är korrekt genom att skicka ett testmeddelande.

Ange ett meddelande samt vilket telefonnummer SMSet skall skickas till och klicka sedan på Skicka.

" OBS:

GSM-modem kräver SIM-kort vilka är förknippade med löpande kostnader, antingen för ett kontantkort som måste fyllas på, eller för ett abonnemang. SIM-kort tillhandahålls av telefonoperatörer.

" Tips:

Det finns även tjänster som omvandlar e-post till SMS. På så sätt kan SMS skickas genom att endast använda e-post funktionen i Web Port. Detta gör att mängden hårdvara kan minskas samt att ett och samma abonnemang kan användas för många Web Port installationer.

13.11 Grafiska inställningar

Här ändras globala inställningar kopplade till grafik.

Följande inställningar kan göras:

Uppdateringsfrekvens	Anger hur ofta dynamiska värden på sidor skall uppdateras.
Maximal skalning	Anger om sidor även skall förstoras då skala har aktiverats.

13.12 Databasinställningar

Här görs inställningar för vilken databas Web Port skall använda för datalagring, hur ofta skrivning sker till databas samt hur länga data skall lagras.

Följande inställningar kan göras:

Databastyp	Anger vilken typ av databas som används (Standard är SQLite)
Anslutningssträng	Används vid anslutning till MSSQL, samt MySQL databaser.
Lågt utrymmeslarm	Gränsvärde för larm om lågt diskutrymme.
Skrivbuffert	Antalet sekunder värden buffras i minnet mellan skrivningar till databas.
Standard larmhistorik	Antalet dagar larmhistorik lagras i databasen
Standard trendhistorik	Antalet dagar trendhistorik lagras i databasen

” Information:

Om MSSQL eller MySQL används måste en databas upprättas samt anslutningssträng skapas. Anslutningssträngen anger vilken användare som skall användas och till vilken server och databas Web Port skall ansluta.

Web Port genererar sina egna tabeller vid anslutning till databasen vilket gör att användaren måste ha rättigheter för detta.

För att importera befintligt larm och trenddata från sqlite till ny SQL-server, klicka på knappen ***Dataimport*** *i menyn efter att databasanslutningen har verifierats.*

” Information:

SQLite databaser är av filtyp och kan precis som andra filer fragmenteras. Om stora mängder data skrivs och tas bort från en databas kan med tiden en komprimering behövas. Detta kan göras genom att klicka på knappen Komprimera.

” OBS:

En komprimering kräver ledigt diskutrymme motsvarande dubbla filstorleken för databasen som skall komprimeras.

En komprimering tar en stund, invänta därför popuprutan som meddelar när komprimeringen har slutförts.

13.13 Kö-fördelning

Här ges möjlighet att styra hur läs och skrivköer prioriteras i Web Port. Detta kan vara användbart för att optimera svarstiden vid stora anläggningar. Köerna är uppdelade enligt nedan:

Läsning (Standard)	Bakgrundsläsning av taggar vid uppdatering av bilder
Läsning (Prioriterad)	Initial läsning då en bild eller inställningsruta öppnas
Skriv	Kö för skrivningar
Larm	Kö för läsning av larmtaggar
Trend	Kö för läsning av trendtaggar

13.14 Web Port Gateway

Web Port Gateway ger möjlighet att ansluta till Web Port för att läsa och skriva taggar enligt ett enkelt protokoll där information utbyts via en TCP-socket. Gränssnittet används till exempel i Web Port-drivrutinen till Citect som ger möjlighet att använda drivrutiner i Web Port direkt till Citect.

Följande inställningar kan göras:

Aktivera	Aktiverar gateway-funktionen
Gateway port	Anger vilken port Web Port lyssnar efter anslutningar på.
Gateway cachetid	Cachetid för hur ofta Web Port frågar io-enheter efter nya värden

” Information:

Önskas mer information kring protokollet eller drivrutinen till Citect?
Besök vår hemsida på www.webport.se för kontaktuppgifter.