AnnTac

Uplink Server

Handleiding voor systeembeheerders

Installatie, drie inrichtingsscenario's, accounts, mappen, SMTP, SNMP, rapportage en dagelijks beheer.

Deze uitgaven zijn inhoudelijk gelijk opgebouwd. Schermafbeeldingen tonen de echte applicatie met uitsluitend synthetische demogegevens. Geen klantgegevens of werkende wachtwoorden zijn afgebeeld.

Inhoudsopgave

Basis en installatie

Architectuur en verantwoordelijkheden 3
Voorbereiding en rechten 4
Installeren of een oude omgeving bijwerken 5
Het clientoverzicht lezen 6

Scenario 1 - één account

Scenario 1: één account en één archief 7
Scenario 1: eerste levering controleren 8

Scenario 2 - gedeeld beheer

Scenario 2: meerdere archieven, gedeeld beheer 9
Scenario 2: overerving beheren 10

Scenario 3 - gescheiden omgevingen

Scenario 3: drie volledig gescheiden omgevingen 11
Scenario 3: eigen clientidentiteit als alternatief 12

Mappen en integraties

Extra bronmappen koppelen 13
Uploadmappen centraal publiceren 14
Lege importmappen en herstel 15

SMTP en dagrapporten

SMTP: algemene foutmeldingen 16
SMTP: testen en verzending beoordelen 17
Dagrapport en eigen klantmeldingen 18

SNMP en Zabbix

SNMPv3 veilig inrichten 19
SNMP: numerieke OIDs 20
SNMP: status, activatie en beperkingen 21
Zabbix: items en triggers 22

Ondersteuning en herstel

Ondersteuning en beheerafspraken 23
Windows-services beheren 24
Back-up, herstel en verwijderen 25
Storingen systematisch oplossen 26
Acceptatie en dagelijks beheer 27

Architectuur en verantwoordelijkheden

Server Manager is de beheerinterface. Elke client heeft een eigen Windows-service, AnnTac-aanmelding, uploadbasis, configuratie en status. Uploaden gaat door wanneer niemand bij Windows is aangemeld.

AnnTac Uplink Server Monitoring is een afzonderlijke service. Deze verzamelt fouten, verstuurt dagrapporten en publiceert centrale SNMP-gegevens. Zij blijft beschikbaar wanneer een clientservice stopt.

Het Windows-serviceaccount bepaalt toegang tot bestanden en shares. Het AnnTac-account bepaalt het ontvangende archief. SMTP- en SNMP-accounts zijn hiervan onafhankelijk. Verwar deze vier identiteiten niet.

De centrale monitoringservice draait als LocalSystem. Zij kan de beschermde clientstatus en rapporthistorie lezen. Verschillende clients op één host vormen daarom geen harde beveiligingsgrens tegenover de lokale beheerder of LocalSystem.

Voorbereiding en rechten

Installeer als lokale administrator. Gebruik een ondersteunde Windows x64-omgeving en test op de Windows Server-versie die bij de klant draait. De installer bevat de applicatie; klanten hebben Python, Inno Setup of SafeNet niet nodig.

Het upload-serviceaccount heeft Aanmelden als service nodig. Uplink kent dit lokaal toe bij accountconfiguratie; domeinbeleid kan dit overschrijven. Geef NTFS Wijzigen op uploadbasis, bronmappen en submappen: lezen, schrijven, hernoemen en verwijderen zijn nodig.

Voor netwerkbronnen zijn zowel share- als NTFS-rechten nodig. Gebruik UNC-paden, bijvoorbeeld \\fileserver\exports\client-a. Gebruik geen gebruikersgebonden Z:-schijf. LocalSystem gebruikt bij netwerktoegang doorgaans de computeridentiteit; een domeinserviceaccount of gMSA is vaak beter geschikt.

Sta uitgaand HTTPS naar de AnnTac-uploadserver en downloads.anntac.eu toe. Sta de gekozen SMTP-poort toe. Open inkomend SNMP-UDP uitsluitend vanaf de monitoringserver. Controleer DNS, proxy en certificaatvertrouwen onder de werkelijke service-identiteit.

Installeren of een oude omgeving bijwerken

1. Bewaar de vorige installer en maak een back-up van instellingen en documentmappen. Stop de oude uploader, ook als dit een desktopapp of geplande taak is.

2. Start de ondertekende installer als administrator. De wizard volgt de Windows-interfacetaal. Kies de applicatietaal op de pagina Taal / Language; er is geen afzonderlijk taalvenster meer.

3. Selecteer bij een upgrade de bestaande AnnTac-map, bijvoorbeeld D:\AnnTac. Bestaande Upload Folders, FTPS\Out-categorieën en back-ups worden op dezelfde locatie hergebruikt. Kies geen nieuwe lege map wanneer bestaande documenten moeten worden meegenomen.

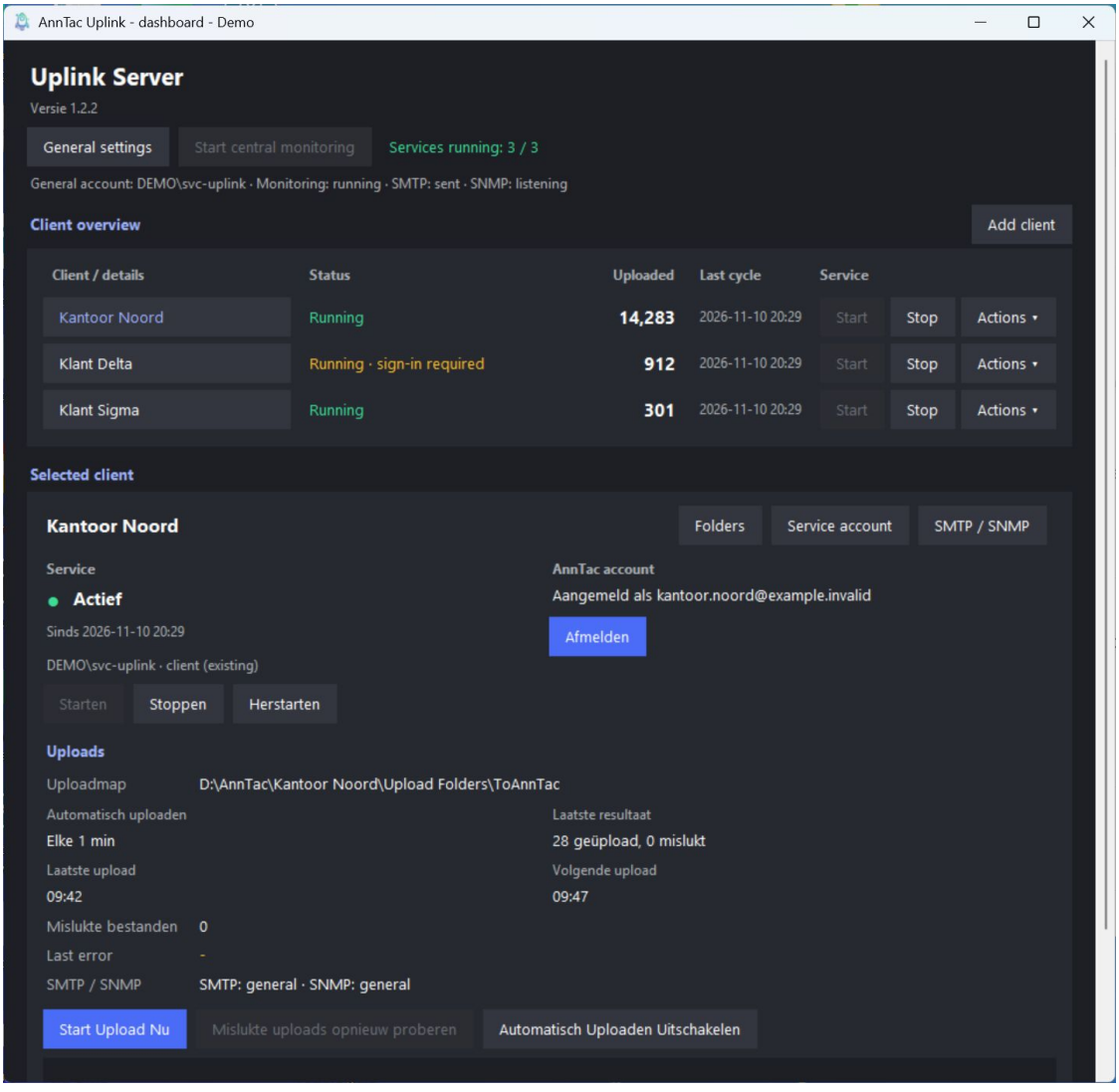
4. Setup stopt services en achtergebleven Uplink-processen. De VCRUNTIME-DLL's worden versiebewust vervangen. Herstart wanneer Setup daarom vraagt; kies niet Overslaan als oplossing voor een onvolledige installatie. Controleer daarna alle services en een proefupload.

Het clientoverzicht lezen

Elke rij toont een klant, actuele service-/uploadstatus, geregistreerde succesvolle documentleveringen, de laatste cyclus en aparte Start/Stop-knoppen. Selecteer de klantnaam voor de details.

Klik op een clientnaam: het paneel Selected client toont de service, het AnnTac-account en de uploads van die client bij elkaar. Folders, Service account en SMTP / SNMP gelden voor de getoonde klant. Actions in de clientregel selecteert die klant en bevat Rename client, Update folders en Remove client. Add client staat bij Client overview.

De teller is lokale uploadhistorie, geen live inventaris van het archief. .dx_-profielbestanden tellen niet als succesvol document. Een niet-leesbare teller hoort als onbekend te worden onderzocht, niet als nul te worden geïnterpreteerd.



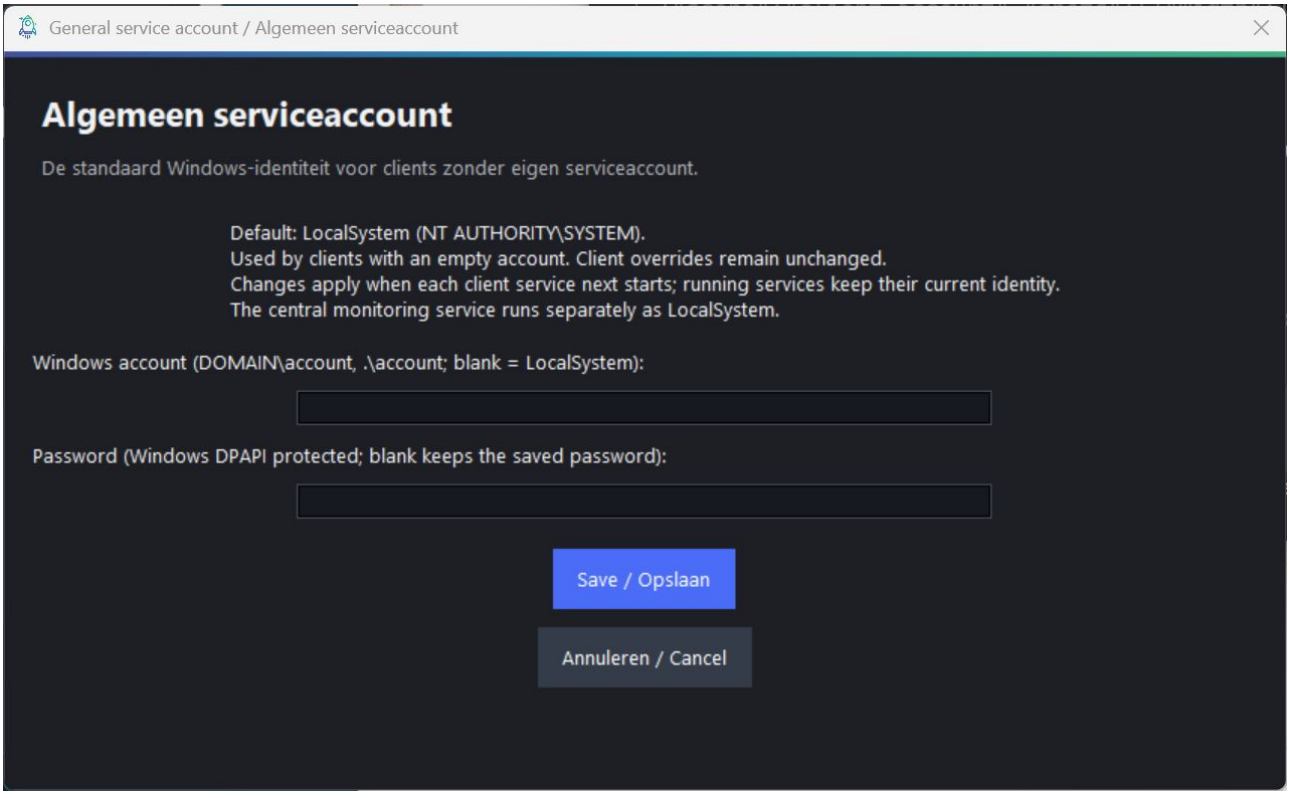
Applicatiescreenshot met demogegevens

Scenario 1: één account en één archief

Doel: één Windows-installatie, één AnnTac-aanmelding en één uploadbasis. Gebruik de oorspronkelijke client en geef deze een herkenbare klantnaam. Laat het client-serviceaccount leeg om de algemene instelling te gebruiken.

Zonder algemeen account is de standaard LocalSystem (NT AUTHORITY\SYSTEM). Dit werkt doorgaans voor lokale bestanden. Voor shares kan een apart domeinaccount nodig zijn. LocalSystem is niet de AnnTac-gebruiker en bepaalt niet in welk archief wordt geüpload.

Meld de client aan, bevestig de activatiemail, controleer het archief en upload één herkenbaar testdocument. Herstart de service en Windows om te controleren dat uploaden zonder interactieve login blijft werken.



Applicatiescreenshot met demogegevens

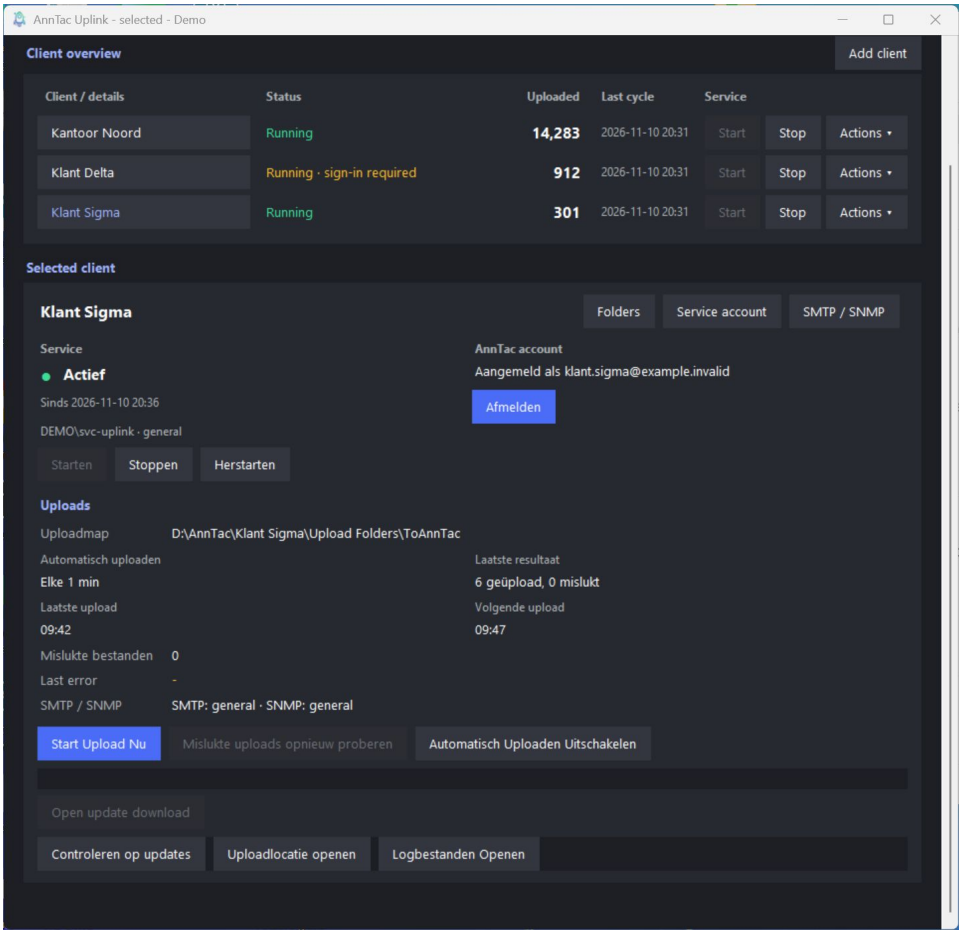
Scenario 1: eerste levering controleren

Plaats een voltooid testdocument in een aangemaakte hoofdcategorie, bijvoorbeeld Upload Folders\ToAnnTac. Laat de producer klaar zijn met schrijven. De automatische verwerking gebruikt een veiligheidsvertraging voor recente of vergrendelde bestanden.

Controleer achtereenvolgens: service Actief, server bereikbaar, account geactiveerd, planning aan, laatste resultaat en het document in het juiste AnnTac-archief. Test ook een onderliggende map en een document met profielbestand wanneer de integratie die gebruikt.

Een servicestop is geen afmelding. Gebruik Afmelden alleen wanneer de backend-sessie bewust moet worden gedeactiveerd. Bewaar bronbestanden en importjournalen bij een fout totdat de levering gecontroleerd is.

Bovenaan staan General settings, centrale monitoring en het aantal actieve clientservices. De geselecteerde klant blijft herkenbaar aan de naam boven het account- en uploadpaneel. Een client selecteren toont de bijbehorende uploadinstellingen; het start niet automatisch een upload.



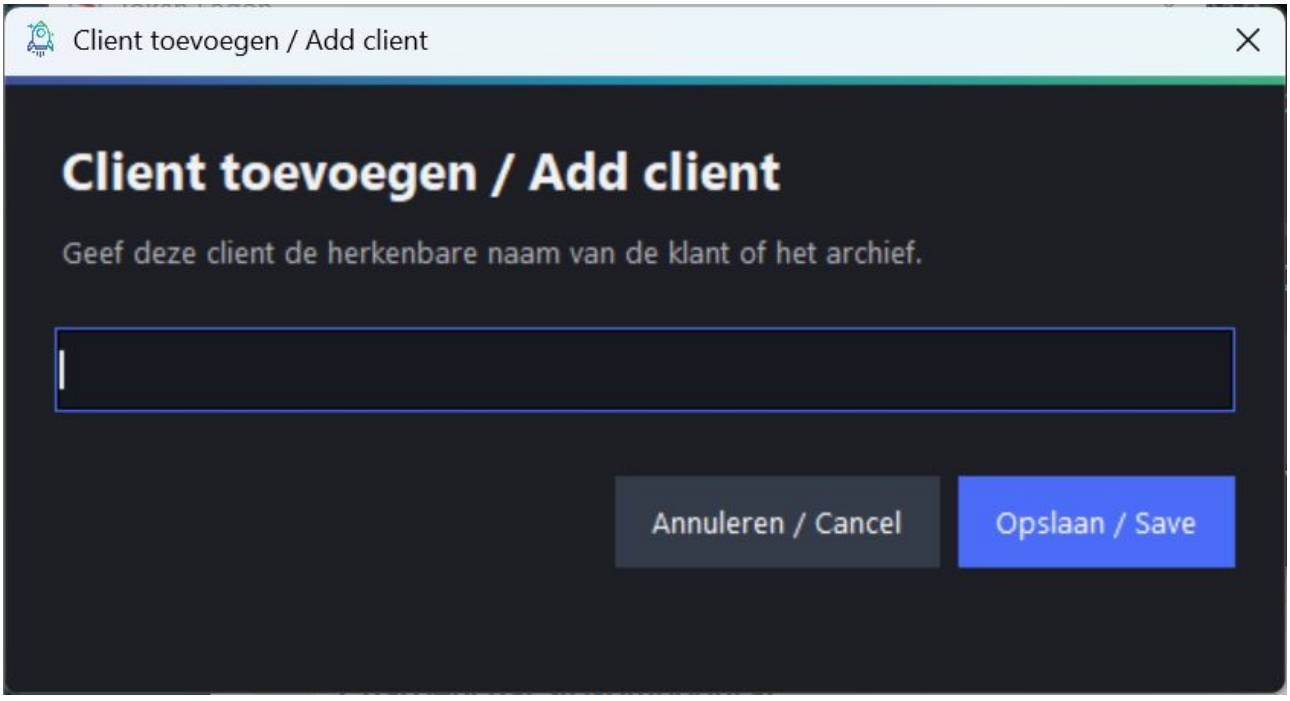
Applicatiescreenshot met demogegevens

Scenario 2: meerdere archieven, gedeeld beheer

Maak voor ieder klantarchief een eigen client. Iedere client krijgt een eigen AnnTac-aanmelding en een niet-overlappende uploadbasis. Gebruik bijvoorbeeld D:\AnnTac\KlantA en D:\AnnTac\KlantB; configureer nooit twee uploaders op dezelfde bron- of uploadmap.

Stel één algemeen Windows-serviceaccount in en laat de client-accountvelden leeg. Geef dat account alleen de vereiste rechten op alle bedoelde klantmappen. Configureer één algemene SMTP- en SNMP-instelling voor het IT-bedrijf.

De centrale monitoringservice verzamelt fouten van alle clients. Een client kan aanvullend eigen meldingen of rapportontvangers hebben. Test met verschillende documenten dat elke client uitsluitend naar het bedoelde archief levert.



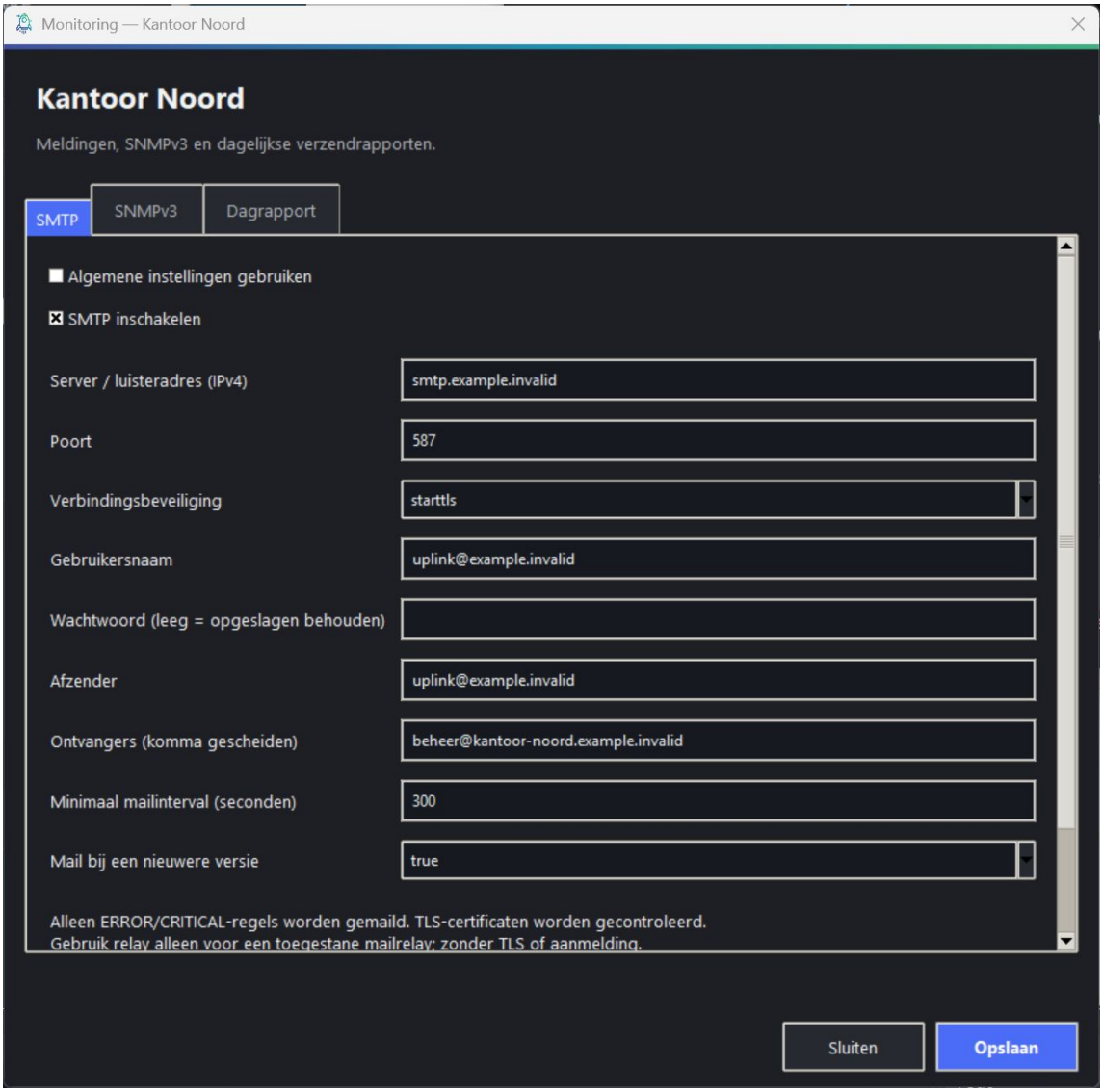
Applicatiescreenshot met demogegevens

Scenario 2: overerving beheren

Algemene instellingen vormen de standaard. Bij SMTP, SNMP en dagrapporten schakelt Algemene instellingen gebruiken de overerving per onderdeel in. Uitschakelen maakt een expliciete clientafwijking mogelijk.

Een leeg serviceaccount erft het algemene account. Een ingevuld clientaccount heeft voorrang. Bestaande expliciete accounts uit oudere installaties blijven behouden. Het opslaan van een algemeen account werkt de Windows-configuratie voor de volgende start bij; een draaiend proces wisselt pas na stop/start van identiteit.

De Manager toont de werkelijke identiteit van een actieve service en zo nodig de volgende identiteit. De centrale monitoringservice blijft afzonderlijk als LocalSystem draaien.



Applicatiescreenshot met demogegevens

Scenario 3: drie volledig gescheiden omgevingen

Voor volledige scheiding gebruikt u drie aparte Windows-instanties: bijvoorbeeld VM-A, VM-B en VM-C. Installeer Uplink afzonderlijk op iedere VM, met eigen service-identiteit, AnnTac-aanmelding, documentopslag en lokale instellingen.

Gebruik per omgeving eigen SMTP/SNMP-credentials en firewallregels. Geef geen serviceaccount toegang tot de document- of instellingenmappen van een andere omgeving. Back-ups en herstelprocedures moeten eveneens gescheiden zijn.

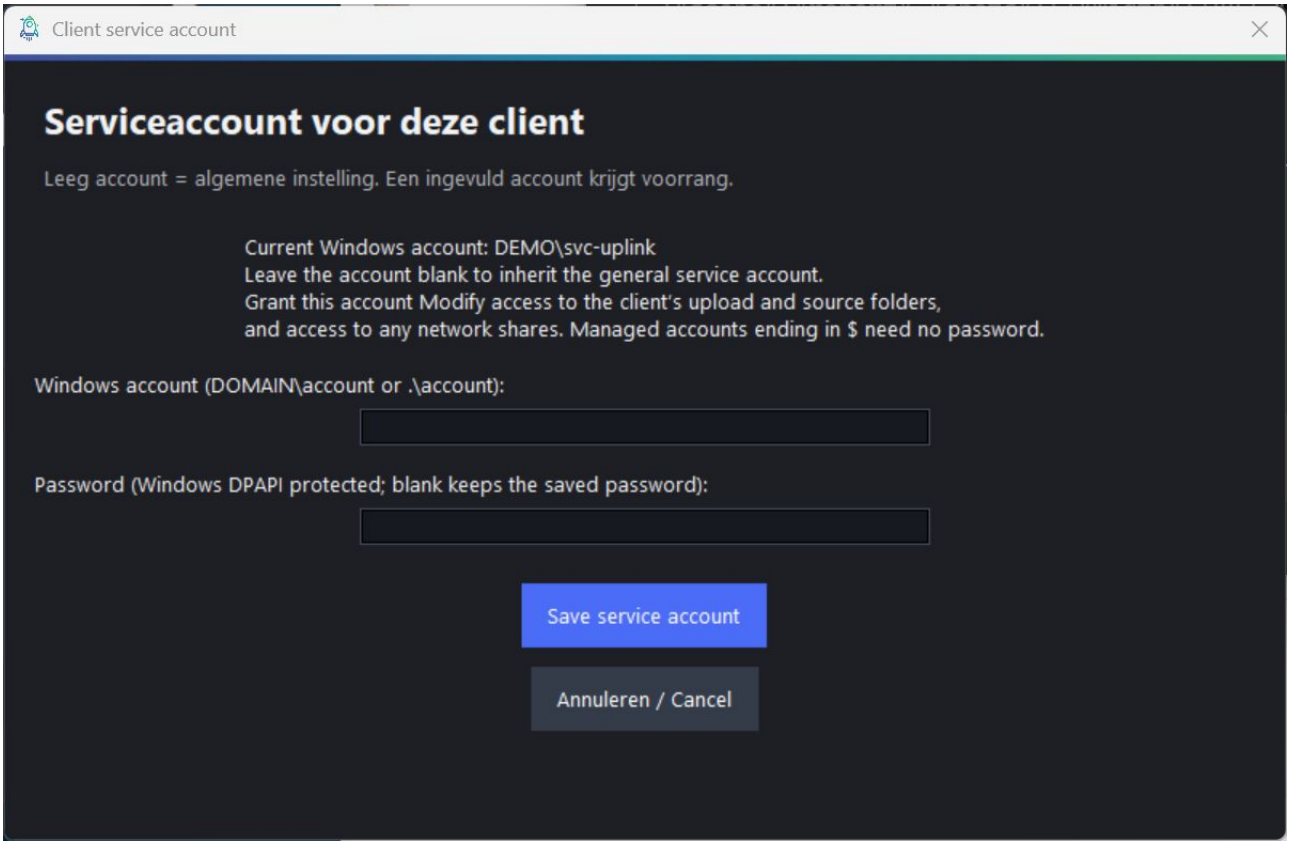
Eén extern Zabbix-systeem kan de drie servers bewaken via drie afzonderlijke SNMP-interfaces. Dit deelt monitoring, niet de uploadprocessen of aanmeldtokens.

Drie clients met verschillende accounts op één host bieden logische scheiding, geen volledige hostisolatie. De lokale administrator en centrale LocalSystem-service kunnen daar nog steeds alle clientinstellingen benaderen.

Scenario 3: eigen clientidentiteit als alternatief

Als één host bewust wordt gedeeld, configureer per client een apart serviceaccount en aparte bron-/uploadmappen. Stop de client voordat u de identiteit wijzigt. Voer DOMAIN\account, .\account of een ingerichte gMSA in.

Geef Wijzigen op de eigen documentmappen en, bij netwerkbronnen, de juiste share-rechten. Uplink kent toegang tot de eigen beschermde instellingen toe. Een gMSA moet vooraf op de host zijn ingericht; een naam eindigend op $ alleen maakt nog geen werkende gMSA.



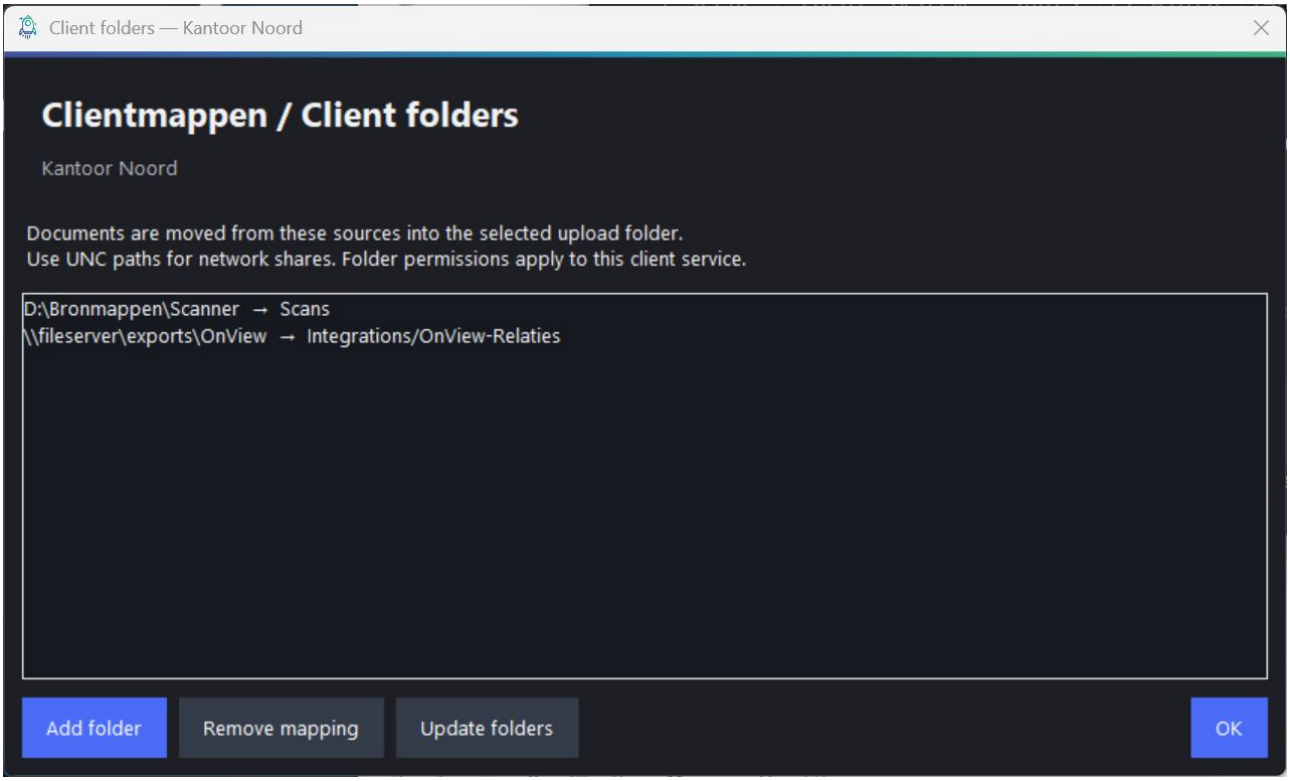
Applicatiescreenshot met demogegevens

Extra bronmappen koppelen

Open de bedoelde client en kies Folders. Add folder vraagt een bestaande bronmap en vervolgens een uploadcategorie of integratie. Gebruik een UNC-pad voor een share. Controleer de gekozen client voordat u opslaat.

Documenten worden naar een Imported-<mapping-id>-submap binnen de doelcategorie overgebracht. Een kopie wordt gecontroleerd voordat het origineel wordt verwijderd. Verwijderen van een koppeling stopt toekomstige scans; reeds gepubliceerde of gejournaliseerde overdrachten blijven herstelbaar.

De OK-knop sluit het dialoog. De externe bronmap wordt niet verwijderd door de opruimfunctie.



Applicatiescreenshot met demogegevens

Uploadmappen centraal publiceren

AnnTac beheert de centrale uploadmappencatalogus. Met Update folders haalt Uplink de actuele mappenstructuur op. De beheerder hoeft hiervoor geen intern adres te configureren.

Voorbeelden: Upload Folders\Scans; Upload Folders\ToAnnTac; Upload Folders\Integrations\Stratech; Upload Folders\Integrations\AnnTac_List_Converter. De lijst bepaalt de mappenstructuur; het aanmaken van een map implementeert geen nieuwe conversie- of productlogica.

Update folders haalt de lijst op, voegt ontbrekende mappen toe en verwijdert vervallen mappen uitsluitend wanneer ze leeg zijn. Actieve koppelingen en onvoltooide importjournalen worden beschermd. Niet-lege oude categorieën blijven beschikbaar voor verwerking.

Bij een onbereikbare of ongeldige lijst blijft de laatste goede configuratie behouden. Een nieuwe installatie heeft een ingebouwde basislijst. Paden buiten Upload Folders, onveilige namen en padtraversal worden geweigerd.

Lege importmappen en herstel

Na uploadcycli verwijdert Uplink lege onderliggende mappen, inclusief Imported-...-mappen. Hoofdcategorieën en expliciete integratiepaden uit de catalogus blijven bestaan, ook wanneer ze leeg zijn.

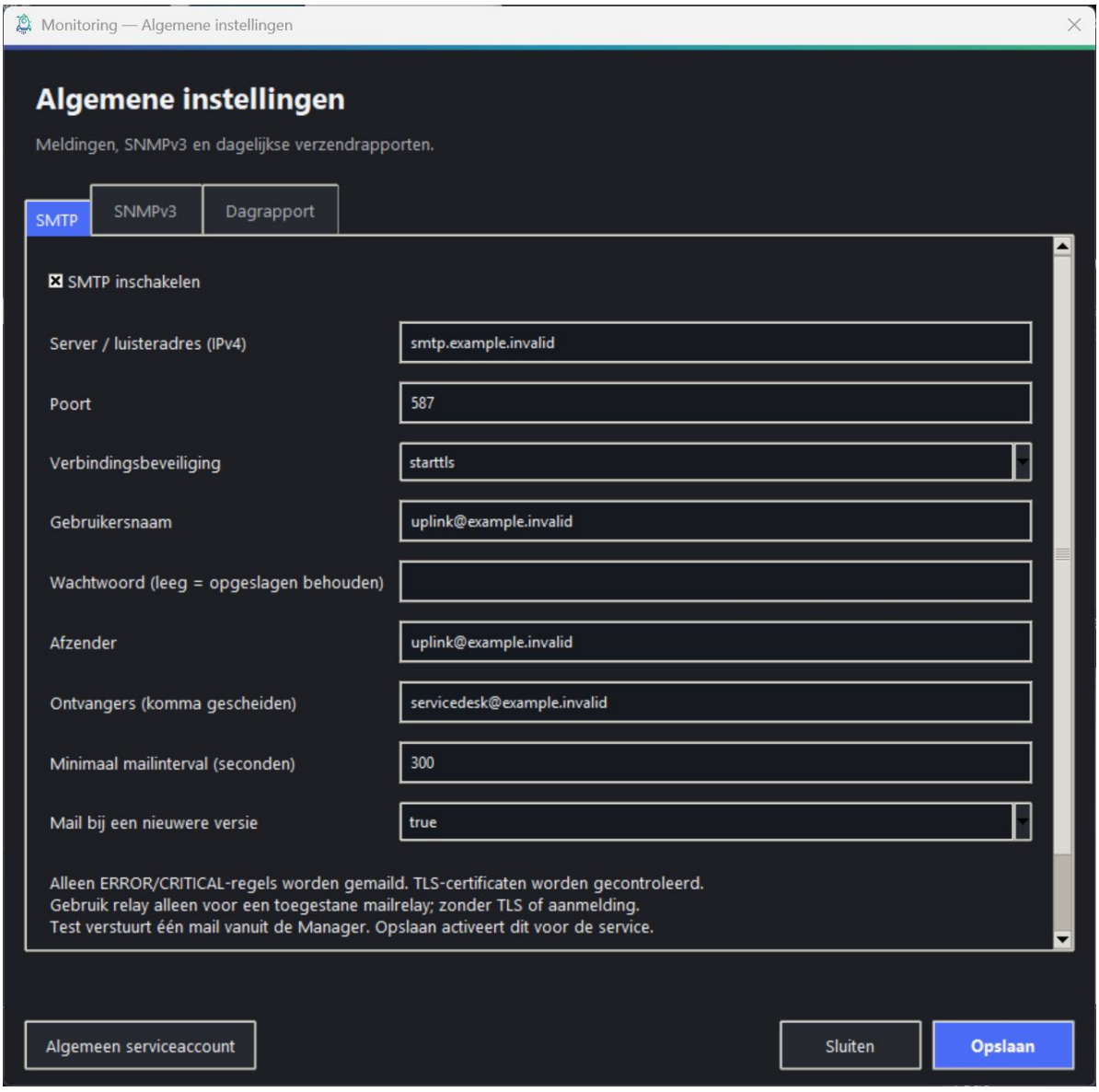
Een door Explorer of een ander proces geopende map kan nog vergrendeld zijn. De opruiming slaat die over en probeert het bij een volgende cyclus opnieuw. Bestanden worden hiervoor nooit verwijderd en symbolische links/junctions worden niet gevolgd.

Bij een fout: controleer bron, bestemming en imports.json voordat u handmatig iets verwijdert. Een bestaande bestemming wordt niet overschreven. Herstel rechten of de naamconflictsituatie en laat de volgende cyclus opnieuw proberen.

SMTP: algemene foutmeldingen

Open General settings, tab SMTP. Vul host, poort, beveiliging, afzender en ontvangers in. Meerdere ontvangers worden gescheiden door komma's. STARTTLS gebruikt meestal poort 587; directe TLS meestal 465.

Relay is uitsluitend bedoeld voor een bewust toegestane mailrelay zonder TLS of login. Authenticatie met gebruikersnaam/wachtwoord vereist TLS. Certificaatvalidatie wordt niet uitgezet.



Applicatiescreenshot met demogegevens

SMTP: testen en verzending beoordelen

Testmail versturen verzendt één herkenbare mail vanuit de Manager. Opslaan laat de service de configuratie inlezen. Controleer ook een echte foutmelding: Manager en LocalSystem/serviceaccount kunnen verschillende netwerk-, proxy- of relayrechten hebben.

Normale foutmail bevat ERROR/CRITICAL-records; succesvolle uploads en gewone waarschuwingen worden niet gemaild. De centrale verzending bundelt fouten en bevestigt journalen pas na acceptatie door SMTP. Het standaardminimuminterval is 300 seconden.

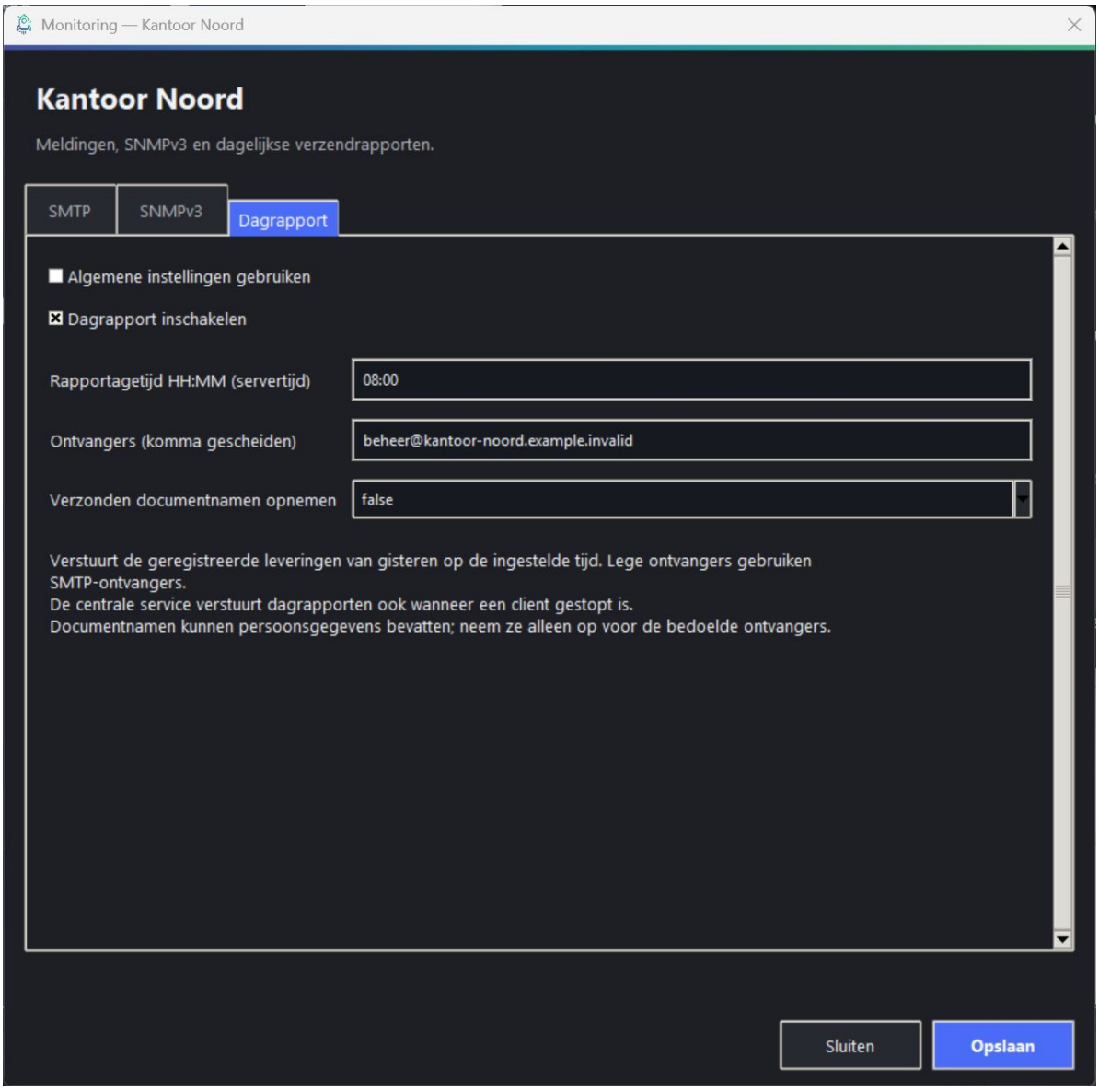
Acceptatie door SMTP bewijst niet dat de mailbox het bericht uiteindelijk ontving. Controleer bij ontbreken ook quarantaine, spamfilter en bounces. Een crash tussen mailacceptatie en lokale bevestiging kan een dubbel bericht veroorzaken.

Wachtwoorden zijn met Windows DPAPI aan de computer gebonden. Een leeg wachtwoordveld behoudt de opgeslagen waarde. Voer monitoringwachtwoorden op een nieuwe server opnieuw in; deel nooit tokens, PIN's of wachtwoorden in tickets.

Dagrapport en eigen klantmeldingen

Kies op de client Monitoring, tab Dagrapport. Stel aan/uit, een lokaal servertijdstip en eventueel eigen ontvangers in. Lege ontvangers gebruiken de effectieve SMTP-ontvangers. De voorgaande kalenderdag wordt gerapporteerd.

Het rapport bevat geregistreerde succesvolle documenten, mislukte bestandspogingen en cycli. Documentnamen zijn optioneel en standaard uit. De historie begint bij deze functie, blijft 90 dagen bewaard en wordt niet uit het archief gereconstrueerd.

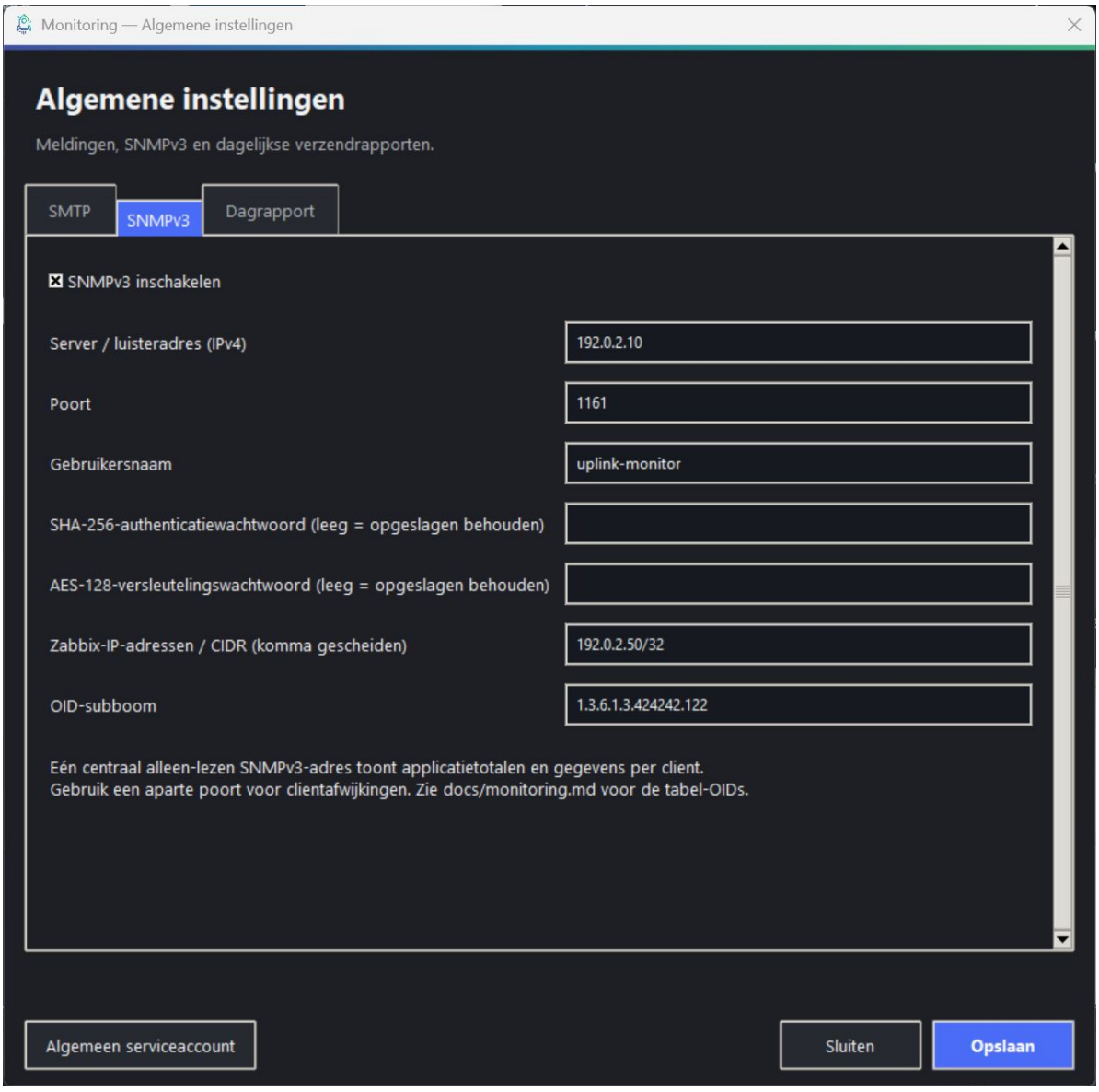


Applicatiescreenshot met demogegevens

SNMPv3 veilig inrichten

Schakel algemene SNMP in en kies het echte IPv4-luisteradres van de server. 127.0.0.1 is uitsluitend lokaal. Gebruik bijvoorbeeld UDP 1161 en beperk zowel de allowlist als de firewall tot de monitoringserver.

Gebruik SNMPv3 authPriv, SHA-256 en AES-128 met eigen gebruikersnaam en twee wachtwoorden van minimaal acht tekens. Er is geen onbeveiligde SNMPv1/v2c-community. Een eigen clientlistener vereist een andere poort.



Applicatiescreenshot met demogegevens

SNMP: numerieke OIDs

B is de ingestelde basis-OID. De ingebouwde basis 1.3.6.1.3.424242.122 is experimenteel, geen geregistreerde AnnTac-PEN. Gebruik voor een formele enterprise-MIB een aan uw organisatie toegewezen subtree.

B.M.0 is een scalar. Centrale clientrijen gebruiken B.100.I.M.0, met stabiele rij-index I en metricnummer M. Ontdek rijen via GETNEXT/GETBULK; metric 24 geeft de client-ID en 25 de klantnaam.

1 versie; 2 toestand; 3 heartbeatouderdom; 4 server bereikbaar; 5 authenticatie geldig; 6 planning aan; 7 failed files; 8 laatste cyclus succesvol; 9 laatste cyclus mislukt; 10 totaal succesvol; 11 totaal mislukte pogingen; 12 foutteller; 13 laatste fout; 14 fouttijd (Unix); 15 laatste actie; 16 actietijd (Unix).

SNMP: status, activatie en beperkingen

17 SMTP-status; 18 uptime; 19 update beschikbaar; 20 gezondheid (1 goed, 2 aandacht); 21 laatste cyclustijd; 22 statistieken geldig; 23 laatste foutmailtijd; 24 client-ID; 25 klantnaam; 26 Windows-opstarttype (2 automatisch, 3 handmatig, 4 uitgeschakeld, 0 onbekend).

Het endpoint is alleen-lezen: GET, GETNEXT en GETBULK. Geen SET, remote start/stop of traps. Bewaak ook no-data/timeouts: een gestopte monitoringservice kan zichzelf niet melden. Centrale totalen kunnen dalen wanneer een client wordt verwijderd; gebruik clientrijen voor historische rates.

Niet-toepasselijke centrale velden zijn 0 of leeg. Raadpleeg de clientrij voor laatste actie/cyclus. Heartbeats en tellers zijn de laatst gepubliceerde waarden, geen onafhankelijke probe van de AnnTac-server.

Zabbix: items en triggers

Maak een SNMP-interface aan met serveradres, UDP-poort, authPriv, SHA256 en AES128. Gebruik numerieke OIDs; kies Numeric unsigned voor status/tellers en Text voor tekstvelden. Benamingen verschillen per Zabbix-versie.

Aanbevolen triggers: geen gegevens gedurende 3 minuten; heartbeat ouder dan 60 seconden gedurende meerdere polls; server 5 minuten onbereikbaar; authenticatie ongeldig terwijl server bereikbaar is; failed files > 0; stijgende foutteller; SMTP-status begint met failed.

Gebruik B.100.I.26.0 om bewust uitgeschakelde klantservices te herkennen. Houd rekening met onderhoudsafspraken en tellerresets bij een herstart.

Voorbeeld: snmpget -v3 -l authPriv -u uplink-monitor -a SHA-256 -x AES -A <auth-key> -X <privacy-key> <server>:1161 1.3.6.1.3.424242.122.1.0. Bewaar echte secrets in de beveiligde monitoringconfiguratie, niet in tickets of gedeelde commandogeschiedenis.

Ondersteuning en beheerafspraken

AnnTac zorgt dat klanten de actuele versie ontvangen. Gebruik het installatiebestand dat AnnTac of je IT-beheerder verstrekt.

Neem bij een storing contact op met je IT-beheerder of AnnTac. Vermeld de clientnaam, het tijdstip en de zichtbare foutmelding. Deel geen wachtwoorden of toegangstokens.

Windows-services beheren

In services.msc heten klantservices AnnTac Uplink Server - Klantnaam. De interne ID blijft AnnTacUplink voor de oorspronkelijke client en AnnTacUplink-client-… voor extra clients. De centrale ID is AnnTacUplink-monitor. Hernoemen van een klant verandert de interne ID niet.

Een upgrade behoudt Uitgeschakeld. Zet het opstarttype weer op Handmatig of Automatisch voordat de client opnieuw moet starten. Stoppen van één klant stopt de andere klanten of de centrale bewaking niet.

Back-up, herstel en verwijderen

Bewaar de installer, clientlijst, uploadlocaties, service-identiteiten en een consistente back-up van %ProgramData%\AnnTac Uplink plus de document-/back-upmappen. Stop services of gebruik een consistente back-upmethode voordat instellingen en importjournalen worden gekopieerd.

Bescherm user.ini, accounts.json, global/settings.ini, importjournalen, monitoringstatus en rapporthistorie. Tokens en machinegebonden versleutelde secrets horen niet in een openbaar ticket. Voer monitoring- en accountwachtwoorden op een nieuwe machine opnieuw in.

Client verwijderen stopt en verwijdert de geselecteerde service en registratie. Documenten, bronnen, back-ups en opgeslagen instellingen blijven voor herstel staan. Controleer achtergebleven credentials volgens het bewaarbeleid.

De-installeren is anders: de bestaande de-installatie verwijdert services en beschermde instellingen. Documenten buiten die instellingenmap blijven staan. Controleer back-ups vóór de-installatie en voer na herstel altijd een proefupload naar het juiste archief uit.

Storingen systematisch oplossen

Geen uploads: controleer service, serverbereikbaarheid, accountactivatie, planning, bestandsgereedheid en folderrechten in die volgorde. Een lopende service bewijst niet dat er een geldige AnnTac-sessie of toegang tot de share is.

Toegang geweigerd: controleer de werkelijk gebruikte service-identiteit, NTFS- én share-rechten en Aanmelden als service. Test UNC-toegang onder die identiteit. Controleer ook domeinbeleid en een verlopen servicewachtwoord.

Geen mail: controleer host/poort, TLS, credentials, relayregels, firewall, quarantaine en spamfilter. Geen SNMP: controleer de centrale service, bind-adres, unieke poort, firewall, allowlist en exact dezelfde SHA256/AES128-keys.

Lege map blijft staan: sluit Explorer/producer en laat een volgende cyclus opruimen. Bestanden blijven achter: lees de clientlogs, last_error en het importjournaal. Verwijder geen bron of journaal voordat de bestemming gecontroleerd is.

Tekstlogs worden dagelijks op UTC-datum naar een nieuw bestand geschreven. Uplink controleert tijdens het draaien iedere minuut op logs die meer dan 90 dagen niet zijn gewijzigd en probeert oude bestanden te verwijderen. Een vergrendeld bestand wordt later opnieuw geprobeerd. Er is geen vaste maximale bestandsgrootte per dag. Foutjournalen hebben een bewaartermijn van 90 dagen; documentback-ups hebben een aparte instelbare termijn.

Acceptatie en dagelijks beheer

Voor uitrol: test een upgrade met oude AnnTac-map; een nieuwe installatie; de gemelde runtime-DLL-herinstallatie; lokale en UNC-bronnen; een profielsidecar; een vergrendeld bestand; netwerkuitval; herstart en reboot.

Scenario 1: controleer LocalSystem of het gekozen account en één correct archief. Scenario 2: test elke aanmelding en centrale/eigen meldingen. Scenario 3: bewijs dat identiteiten van VM-A geen toegang tot VM-B/VM-C hebben.

Test Update folders met een nieuwe integratiemap, een lege vervallen map en een niet-lege vervallen map. Test mapopruiming met een open map.

Dagelijks: controleer centrale gezondheid, niet-geactiveerde accounts, fouten, achterblijvende documenten, mailaflevering en back-upresultaat. Periodiek: voer een hersteltest uit, controleer rechten en serviceaccounts, en leg wijzigingen vast.

Deze handleiding beschrijft de Uplink Server-interface. De screenshots zijn echte renders met demodata. De regressietests en ondertekening vervangen geen acceptatietest op de klantserver.