Näin Secapp toimii: Secapp API:t

Käyttötavat · https://www.secapp.fi/fi/docs/muu-dokumentaatio/kayttotavat/nain-secapp-toimii-secapp-apit/

Johdanto

Sovellusrajapinnat (application programming interfaces, API:t) ovat tapa, jolla tietojärjestelmät voivat "keskustella" keskenään. Niiden avulla tieto ja tapahtumat välittyvät järjestelmästä toiseen, tai yksi järjestelmä voi kysyä toiselta tietoja, jolloin toinen järjestelmä voi reagoida, vastata tai jatkokäsitellä toisen järjestelmän havaitsemia tapahtumia sekä keräämää tai tuottamaa dataa.

Rajapintojen ensisijainen tarkoitus on purkaa siiloja ja mahdollistaa muuten erillisten järjestelmien saumaton integrointi. Tällaiset integraatiot vähentävät merkittävästi manuaalista työtä, tehostavat ja automatisoivat keskeisiä prosesseja, minimoivat inhimillisiä virheitä ja parantavat kokonaisreaktiokykyä.

Secapp-rajapinnat pähkinänkuoressa

Secappin rajapinnat perustuvat REST-periaatteisiin. Rajapintakutsu tehdään (tai vastaanotetaan – tästä lisää myöhemmin) HTTP-pyynnöllä tiettyyn URL-osoitteeseen. Vastauksena saat (tai lähetät) HTTP-vastauksen, jonka JSON-payloadissa kulkee tarvittava tieto.

Tietoturvasyistä käytössä on aina HTTPS, jotta yhteyden yli kulkeva data on salattua siirron aikana.

JSONista lyhyesti: JSON (JavaScript Object Notation) on kevyt, tekstiin perustuva formaatti, jota käytetään datan tallentamiseen ja vaihtamiseen järjestelmien välillä tavalla, joka on helposti luettavissa sekä ihmisille että koneille.

Autentikointia varten rajapinnat käyttävät API-avaimia, jotka välitetään pyyntöjen otsikkotiedoissa (request headers).

Tässä dokumentissa esitellään lyhyesti tällä hetkellä saatavilla olevat rajapinnat. Mikäli mikään näistä ei vastaa tarpeitasi, on mahdollista kehittää myös lisärajapintoja.

Viestintä

Rajapintojen viestintäominaisuuksien avulla ulkoiset sovellukset voivat lähettää ja vastaanottaa viestejä sekä seurata niihin tulevia vastauksia. Kun lähetät tai vastaanotat viestin/viestejä, saat jokaisesta viestistä yksilöllisen tunnisteen (ID). Näiden ID:iden avulla voit pyytää järjestelmää palauttamaan ajantasaiset vastausmäärät tai täydelliset vastaustiedot (vastaajan käyttäjänimi, OK/NOK, vastaushetken aikaleima jne.).

API:n kautta lähetetyt viestit toimitetaan ensin Secappin niin sanottuun reititysmoottoriin (routing engine). Tämä moottori tarkistaa (tarvittaessa), onko lähettäjä oikeutettu lähettämään viestejä. Se voi myös tarkistaa viestin sisällöstä tiettyjen avainsanojen esiintymisen ja, jos vastaavuuksia löytyy, laukaista viestin, joka perustuu kyseisille avainsanoille määriteltyyn viestipohjaan. Luotu viesti voi sisältää API:n kautta tulleen alkuperäisen viestisisällön, ja pohjassa voidaan määritellä lisäsisältöä (tekstiä, liitetiedostoja). Pohja määrittelee myös viestin jakelun: kenelle se lähetetään ja mitä kanavia pitkin. Tämä on erityisen kätevää, jos mahdollisuutesi tai oikeutesi muokata lähettävän järjestelmän toimintaa ovat rajalliset: kaikki jakelun muutokset, eskalointisäännöt jne. voidaan tehdä Secappin käyttöliittymässä ilman muutoksia lähettävän järjestelmän koodiin tai konfiguraatioon.

Viestien vastaanottamista ulkoiseen järjestelmään varten Secapp tarjoaa ulos lähtevän webhookin, joka voidaan määritellä tekemään HTTP-pyyntö ulkoisen järjestelmän URL-osoitteeseen aina, kun tiettyyn viestipohjaan perustuva viesti lähetetään (ei rajoitu yhteen pohjaan – tarvittaessa webhook voidaan liittää mihin tahansa tai kaikkiin pohjiin). Yhdessä pohjassa voi olla useita webhoookeja, ja ne kaikki laukaistaan, kun viesti lähetetään. HTTP-pyynnön JSON-payload sisältää viestisisällön (kaikilla kielillä, jos niitä on tarjolla) sekä muita tietoja – kuten käytetyt kanavat ja lähetyksen aikaleimat – joita ulkoinen järjestelmä voi jatkokäsitellä.

Esimerkkejä käyttötapauksista

- IT- tai tietoturvajärjestelmän hälytykset: Kun valvontajärjestelmä havaitsee vikoja tai poikkeamia verkon tai IT-järjestelmän toiminnassa, se hälyttää vastaavan tiimin Secappin kautta. Jos kyseessä on vakava ongelma, Secapp välittää tiedon samanaikaisesti myös ylimmälle johdolle. Secapp-hälytykset ovat erityisen hyödyllisiä silloin, kun vakavia häiriöitä tapahtuu normaaliin työaikaan kuulumattomina aikoina ja vapaa-ajalla oleva henkilöstö täytyy hälyttää paikalle.
- Kiinteistöautomaation tai prosessinohjauksen hälytykset toimitetaan kenttätyöntekijöille.
- Hälytyksiä tai tilannetiedotteita julkaistaan Secappin kautta myös infonäyttöjärjestelmissä.

- Ulkoinen tilannekuvajärjestelmä vastaanottaa hälytyksiä ja hakee vastauksia Secappista täydentääkseen tilannekuvaa.

Käyttäjien hallinta

Käyttäjähallinnan API antaa täyden hallinnan järjestelmän käyttäjiin. Sen avulla voit hakea listan järjestelmän käyttäjistä, lisätä uusia käyttäjiä, päivittää olemassa olevien käyttäjien tietoja/asetuksia sekä poistaa käyttäjiä järjestelmästä. On myös mahdollista määritellä, mihin ryhmiin käyttäjä kuuluu ja poistaa käyttäjä yhdestä tai useammasta ryhmästä.

Esimerkkejä käyttötapauksista

- Luo Secapp-käyttäjät HR- tai IT-järjestelmän tiedoista, synkronoi muutokset, jotta tiedot pysyvät ajan tasalla ja poista käyttäjät, jotka ovat lähteneet organisaatiosta.
- Teollisuusalueen vierailijahallintajärjestelmä rekisteröi vieraat Secappiin ja tiettyihin ryhmiin, jotta he saavat paikalliset hälytykset. Rekisteröinnit poistetaan, kun vieraat poistuvat alueelta.

Secappin oman käyttäjähallinnan API:n lisäksi Secapp tukee myös SCIM 2.0 -rajapintaa käyttäjähallintaan. Se on ensisijaisesti tarkoitettu käytettäväksi Microsoft Entra ID:n kanssa käyttäjätietojen synkronoimiseen Entra ID:n ja Secappin välillä, mutta se voidaan ottaa käyttöön myös muissa järjestelmissä käyttäjätietojen hallintaa varten. SCIM pohjautuu REST-periaatteisiin samalla tavalla kuin Secappin oma rajapinta.

Secappin oma API tarjoaa kuitenkin tarkemman ja laajemman pääsyn käyttäjäasetuksiin ja niiden hallintaan, kun taas SCIM tukee suppeampaa joukkoa käyttäjän asetuksia.

Ryhmien hallinta

Ryhmähallinnan API tarjoaa pääsyn järjestelmän ryhmiin. Rajapinnan kautta on mahdollista selvittää, mitä ryhmiä järjestelmässä on, ketkä (käyttäjät tai ryhmät) kuuluvat kuhunkin ryhmään, lisätä ja poistaa käyttäjiä ja ryhmiä ryhmistä sekä poistaa kokonaisia ryhmiä. Huomaa, että rajapinta operoi vain ryhmillä: jos poistat ryhmän, ainoastaan ryhmä poistuu järjestelmästä. Ryhmän jäseninä olleet käyttäjät säilyvät järjestelmässä.

Esimerkkejä käyttötapauksista

- Käytä HR-/vuorohallintajärjestelmää päivittämään ryhmiä vuoronvaihtojen yhteydessä. Esimerkiksi päivystyksen trauma-tiimi saa hälytykset aina EMG–Trauma-ryhmän kautta, mutta ryhmään kuuluvat henkilöt vaihtuvat jokaisen vuoronvaihdon yhteydessä.

- Lisää ja poista henkilöstöä ryhmistä automaattisesti, kun he aloittavat tai lopettavat työsuhteen.

Tilastot

Järjestelmä tallentaa ajanjaksot, jolloin yksintyöskentelyominaisuus on ollut käytössä, eli jaksot, jolloin laskuri on käynnissä tai pysäytetty.

Nämä tilastot ovat saatavilla myös rajapinnan kautta, ja niitä käytetään usein osoittamaan työturvallisuuteen liittyvien säädösten noudattamista.

Tiedot säilytetään Secappissa oletuksena 60 päivän ajan, minkä jälkeen ne poistetaan. Jos tarvitset tietojen säilytystä lyhyemmäksi tai pidemmäksi aikaa, ole yhteydessä Secappin tukeen.

Raportointi ja dokumentointi

Secappin raportointi- ja dokumentointiominaisuuksilla voidaan:u

- hallita ja seurata työtä/tehtäviä sekä niihin liittyviä tilauksia/laskutusta
- tarjota tarkistuslistoja (checklist) tiettyihin tehtäviin tai menettelyihin
- kerätä tietoa raporttien ja kyselyjen avulla mihin tahansa tarkoitukseen
- hallita kohteita (sites) ja niissä olevia assetteja
- ja paljon muuta…

Lisätietoja löydät osoitteesta: https://www.secapp.fi/fi/tuote/tehtavalistat-ja-raportointi/

Rajapintojen kautta ulkoiset järjestelmät voivat kysellä ja noutaa työpaketteja/työtilauksia niiden tilatietoineen, niihin liittyviä laskutettavia eriä (työ tai materiaali) sekä kohde- ja laitetietoja. Ulkoiset järjestelmät voivat tämän jälkeen jatkokäsitellä dataa esimerkiksi taloushallinto- tai kunnossapitojärjestelmien syötteeksi.

Tiedostot

Secappin mobiilisovelluksessa on myös Tiedostot-osa, jonka avulla käyttäjille voidaan jakaa tiedostoja niin, että ne ovat käytettävissä myös offline-tilassa. Tyypillisesti tällaisia tiedostoja ovat sellaiset dokumentit, joiden on oltava saatavilla kaikissa tilanteissa – joskus erityisesti suurten häiriöiden ja kriisien aikana: evakuointiohjeet, hätätoimintaohjeet, pelastautumisreittien kartat, kokoontumispaikkojen kuvat jne.

Jos käytössäsi on niin sanottu single source of truth, eli paikka, jossa "aina saatavilla" -dokumenttien viimeisimmät versiot säilytetään, Secapp voi nyt synkronoida tiedostot automaattisesti tästä lähteestä.

Synkronointia varten tarvitset SFTP-yhteyden tiedostoihisi. Secapp voidaan konfiguroida noutamaan tiedostot SFTP-palvelimeltasi.

Kun rajapinta on otettu käyttöön, voit määritellä palvelinosoitteen ja siirrossa käytettävät avaimet Secappissa. Siirto ajetaan automaattisesti kerran vuorokaudessa ja se synkronoi tiedostot ja kansiorakenteen Secappin Tiedostot-osioon.

Käytön aloittaminen

Rajapintojen käytön aloittamiseksi suosittelemme olemaan yhteydessä myyntitiimiimme ja keskustelemaan tarkemmin integraatiotarpeistasi.

Secapp toimittaa tarvittavat käyttöoikeustiedot (credentials), ja tarkka toimitustapa sovitaan tapauskohtaisesti, toivottujen viestintäkanavien mukaisesti. Koska tunnisteet ovat turvallisuuskriittisiä, niitä tulee aina käsitellä asianmukaisella huolellisuudella ja luottamuksellisesti.

Kehitystyö aloitetaan tyypillisesti erillisessä testijärjestelmässä, jossa rajapintojen toiminnallisuutta voidaan kokeilla ja varmentaa turvallisesti ennen tuotantoympäristöön siirtymistä. Osana käyttöönottoa pyydämme keräämään ja jakamaan keskeiset tekniset tiedot, kuten niiden järjestelmien tai sovellusten IP-osoitteet, jotka tulevat kutsumaan rajapintaa. On myös tärkeää arvioida odotettu käyttömäärä – mukaan lukien API-kutsujen likimääräinen lukumäärä ja tiheys (myös mahdolliset piikit) – jotta voimme varmistaa optimaalisen suorituskyvyn, suunnitella kapasiteetin ja säätää kutsurajoittimet oikein liikennettäsi varten.

Vaikka API- ja testijärjestelmän käyttöoikeudet voidaan yleensä myöntää melko nopeasti, käytännön kokemus osoittaa, että koko päästä päähän -ratkaisun saaminen tuotantovalmiiksi vie usein pidempään. Secappin data tulee kyllä nopeasti saataville, mutta integraatiotyö, datan käsittely sekä tulosten vieminen kohdejärjestelmään niin, että niistä on todellista hyötyä, pidentävät kokonaisprojektin aikajännettä.

Vaihtoehtoiset integraatiotavat

Tässä dokumentissa ei käsitellä vaihtoehtoisia integraatiotapoja tarkemmin, mutta niitä on tarjolla siinä tapauksessa, ettei API-pohjainen lähestymistapa sovi käyttötapaukseesi.

Viestintä

- **SMS:** Lyhytviestejä (tekstiviestejä) voidaan lähettää Secappiin ja käyttää hälytyksen laukaisemiseen ennalta määritellyn pohjan perusteella. Secapp voidaan myös konfiguroida lähettämään tekstiviesti tiettyyn numeroon/numeroihin aina, kun hälytys lähetetään.
- **Sähköposti:** Sähköpostiviesti voidaan lähettää Secappiin, jolloin se laukaisee hälytyksen ennalta määritellyn pohjan perusteella. Secapp voidaan myös konfiguroida lähettämään sähköposti ulkoiseen osoitteeseen aina, kun hälytys/viesti lähetetään.

Molemmista edellä mainituista kanavista tulevat viestit toimitetaan samaan reititysmoottoriin, josta kerrottiin viestintä-API:n yhteydessä. Näin niissä voidaan hyödyntää samoja lähettäjä- ja avainsanapohjaisia suodatusominaisuuksia.

Muuten SMS- ja sähköpostipohjaisten integraatioiden kyvykkyys on melko rajallinen verrattuna viestintä-API:n tarjoamiin mahdollisuuksiin. Ne tarjoavat kuitenkin matalan kynnyksen vaihtoehdon integraatioon erityisesti silloin, kun lähettävä järjestelmä ei tue API-pohjaista toimintaa ja/tai sinulla ei ole pääsyä järjestelmään tai kykyä toteuttaa API-pohjaista integraatiota.

Käyttäjähallinta

- **MS Entra ID:** Saatavilla on myös MS Graph API -pohjainen toteutus käyttäjätietojen synkronointiin MS Entra ID:n ja Secappin välillä.

Suosittelemme kuitenkin käyttämään SCIMiä kaikkiin uusiin toteutuksiin, sillä se antaa asiakkaille paremman kontrollin integraation käytettävissä oleviin tietoihin.

Räätälöidyt integraatiot

Suosittelemme vahvasti hyödyntämään Secappin valmiita rajapintoja integraatioissa, sillä se on nopea ja kustannustehokas ratkaisu verrattuna täysin räätälöityjen rajapintojen tai integraatioiden kehittämiseen. Tiedämme kuitenkin, ettei tämä aina ole mahdollista monista eri syistä. Jos siis tarvitset jotain, mitä nykyiset rajapinnat eivät kata, ota silti yhteyttä. Secapp toteuttaa säännöllisesti räätälöityjä integraatioita – katsotaan yhdessä, miten voimme ratkaista juuri sinun

haasteesi.

Lopuksi

Toivomme, että tämä katsaus on tuonut esiin Secapp-rajapintojen tarjoamat mahdollisuudet tehostaa toimintaasi ja parantaa tiedonvaihtoa. Kannustamme ottamaan yhteyttä myyntitiimiimme ja ottamaan selvää, miten rajapintoja voidaan hyödyntää juuri sinun käyttötapauksessasi ja miten ne voivat auttaa avaamaan Secapp-palvelun ja siihen integroitujen järjestelmien koko potentiaalin.