

WithSecure Elements Mobile Protection for Android

Administrator's guide

Sisällys

Luku 1. Johdanto.....	4
1.1 Miksi WithSecure Elements Mobile Protection?.....	5
1.2 Tärkeimmät ominaisuudet.....	5
1.3 Järjestelmävaatimukset.....	6
1.4 Aloittaminen.....	7
Luku 2. Haitallisen sisällön etsiminen.....	9
2.1 Manuaalinen tarkistus.....	10
2.2 Automaattinen tarkistus.....	10
Luku 3. Internet-liikenteen suojaaminen.....	11
3.1 Verkon suojauksen käyttöönotto.....	12
3.2 Tekstiviestisuojauksen käyttöönotto.....	12
3.3 Mainepohjaisen selauksen ottaminen käyttöön.....	12
3.4 Sallitaan liikenteen reititys etävalityspalvelimen kautta.....	12
3.5 Sallii diagnostisten tiedostojen etäkeräyksen.....	12
3.6 Sovelluspoikkeuksien valitseminen.....	13
3.7 Suojaustilastojen katsominen.....	13
Luku 4. Tuki.....	14
Liite A. Lokitiedostojen vienti.....	16
A.1 Kuinka viedä lokitiedostoja.....	17
Liite B. MDM:n käyttö.....	18
B.1 Ennen kuin aloitat.....	19
B.2 Käyttöönotto Google Workspace MDM:llä.....	19
B.2.1 Android-sovelluksen lisääminen Google Workspace Endpoint Managementiin.....	19
B.2.2 Chromebookin rekisteröinti.....	20
B.3 Käyttöönotto VMware Workspace ONE MDM:llä.....	21
B.3.1 Android-sovelluksen lisääminen VMware Workspace ONE:n MDM:ään.....	21
B.3.2 Hallittujen sovellusten tarkasteleminen.....	22
B.3.3 Android Enterprise -käyttöönotto VMware Workspace ONE:n kanssa.....	22
B.4 Käyttöönotto Microsoft Intunella MDM:llä.....	24
B.4.1 Android-sovelluksen käyttöönotto Microsoft Intunen MDM:ssä.....	24
B.5 Käyttöönotto IBM MaaS360 MDM:llä.....	27
B.5.1 Android Enterprise -käyttöönotto IBM MaaS360:n MDM:ssä.....	27
B.6 Käyttöönotto Ivanti Endpoint Managementin avulla.....	28

B.6.1 Android-sovelluksen ottaminen käyttöön Ivanti Endpoint Managementin avulla.....	28
B.6.2 Android Enterprise -käyttöönotto Ivanti Endpoint Managementin kanssa.....	30
B.7 Käyttöönotto Miradore MDM:llä.....	30
B.7.1 Android-sovelluksen lisääminen Miradoren MDM:ään.....	30
B.8 Käyttöönotto Samsung Knoxin avulla.....	31
B.8.1 Android-sovelluksen käyttöönotto Samsung Knoxin kanssa.....	31

Luku 1

Johdanto

- [Miksi WithSecure Elements Mobile Protection?](#)
- [Tärkeimmät ominaisuudet](#)
- [Järjestelmävaatimukset](#)
- [Aloittaminen](#)

Tämä opas sisältää yleistä tietoa WithSecure Elements Mobile Protection -sovelluksesta ja sen tärkeimmistä ominaisuuksista.

Se antaa ohjeita sovelluksen aktivoimiseen ja hallintaan sekä sen käyttöönottoon MDM-ratkaisun kanssa.

Seurustelemme ja työskentelemme mobiililaitteillamme – missä ja milloin tahansa. Raja työn ja henkilökohtaisten laitteiden välillä on epäselvä. Käytämme mobiililaitteitamme päivittäiseen liiketoimintaan ja henkilökohtaisten asioiden hoitamiseen. Mobiililaitteet ovat myös jatkuvasti yhteydessä Internetiin, mikä tekee niistä houkuttelevan hyökkäysvektorin kyberrikollisille

WithSecure (aiemmin F-Secure Business) Elements Mobile Protection on ennakoiva, virtaviivainen suojausratkaisu mobiililaitteillesi. Voit estää kyberhyökkäykset ja puolustautua mobiiliuhkia vastaan käyttämällä viimeisimpiä mobiilitietoturvateknologiamme innovaatioita. Ratkaisun avulla voit torjua erilaisten sosiaalisten sovellusten ja tekstiviestilinkkien kautta tulevia tietojenkalasteluyrityksiä, suojata työntekijöitäsi haitallisilta verkkosivustoilta, estää haittaohjelmia ja pitää liiketoimintakriittiset tietosi turvassa.

WithSecure Elements Endpoint Protection on WithSecure Elements -kyberturvaalustan moduuli. Pilvipohjainen alusta tarjoaa tehokkaan suojan lunnasohjelmia ja edistyneitä hyökkäyksiä vastaan. Elements yhdistää haavoittuvuuksien hallinnan, automatisoidun korjaustiedostojen hallinnan, dynaamisen uhkien tiedustelupalvelun, jatkuvan käyttäytymisanalytiikan ja tietoturvan pilviyhteistyöpalveluillesi ja -infrastruktuurillesi. Voit käyttää yksittäisiä ratkaisuja tiettyihin tarpeisiin tai yhdistää ne kaikki saumattomasti maksimaalisen suojan saavuttamiseksi.

1.1 Miksi WithSecure Elements Mobile Protection?

Suojaus nykyaikaisia mobiiliuhkia vastaan

Elements Mobile Protection avulla voit estää työntekijöitä käyttämästä haitallisia verkkosivustoja ja käyttämästä riskialttiita sovelluksia reaaliaikaisen uhkatiedon ja tietoturva-analytiikan avulla. Se tarjoaa edistyneen suojan haittaohjelmia, tietojenkalasteluhyökkäyksiä ja muita haitallisia uhkia vastaan. Järjestelmänvalvojana voit estää tai sallia tiettyjä verkkosivustoja ja saada yksityiskohtaisia raportteja estetyistä URL-osoitteista.

Yhtenäinen kokemus kaikilla laitteillasi

Uusittu sovellus tukee uusimpia Android-versioita. Network Gateway avulla voit kuroa umpeen erilaisten mobiilialustojen välistä kuilua ja varmistaa, että kaikki käyttäjät hyötyvät vankasta tietoturvakehyksestä, edistyneistä ohjauksistamme ja parannetusta verkon suorituskyvystä. Lisäksi kaikki resurssiintensiiviset toiminnot on siirretty pilveen, mikä pidentää laitteidesi akun kestoa.

Yksinkertainen ja tehokas hallinta

WithSecure Elements Security Center tai MDM-ratkaisusi kautta voit ottaa Elements Mobile Protection käyttöön ja hallita sitä helposti. Se on helppo asentaa ja käyttää käyttäjäystävällisellä käyttöliittymällä. Sinulla on täysi näkyvyys ja hallinta, kun otat sovellusta käyttöön ja hallitset suojausasetuksia. Ratkaisu tarjoaa sinulle keskitetyn näkyvyyden haavoittuvien ja käyttöiän lopussa olevien käyttöjärjestelmien tunnistamiseen. Saat yksityiskohtaiset tietoturvatapahtumaraportit, joiden avulla voit nopeasti tunnistaa mahdolliset uhat ja puuttua niihin.

1.2 Tärkeimmät ominaisuudet

Tässä osiossa kuvataan WithSecure Elements Mobile Protection tärkeimmät ominaisuudet.

Selauksen suojaus

Browsing Protection on keskeinen suojakerros, joka estää ennakoivasti loppukäyttäjää vieraillemasta tietojenkalastelu- ja haitallisilla sivustoilla. Tämä varhainen puuttuminen vähentää huomattavasti yleistä altistumista haitalliselle sisällölle ja siten hyökkäyksille.

It on täysin selaimen agnostikko, koska se toimii verkkotasolla. Tämä varmistaa, että se tarjoaa suojan, vaikka loppukäyttäjä ei käyttäisi yrityksen hyväksymiä selaimia. Se suojaa loppukäyttäjää, jotka huijataan pääsemään näennäisesti laillisille tietojenkalastelusivustoille, pääsemään haitallisille sivustoille sähköpostilinkin kautta tai saamaan tartunnan muutoin laillisilla sivustoilla olevilla haitallisilla kolmannen osapuolen mainoksilla.

Browsing Protection hyödyntää reaaliaikaista uhkatietoa ja hakee verkkosivustojen ja niiden tiedostojen uusimmat mainetarkistukset WithSecure Security Cloudista useiden tietopisteiden, kuten IP-osoitteiden, URL-avainsanojen ja sivuston käyttäytymisen, perusteella.

SMS-suojaus

Tekstiviestisuojaus tarkistaa saapuvat tekstiviestit automaattisesti vaarallisten linkkien tai haitallisten QR-koodien varalta. Vaaralliseksi tunnistetut viestit siirretään roskapostikansioon, jolloin laitteesi ja henkilökohtaiset tietosi pysyvät turvassa.

Virusten ja uhkien suojaus

Network Gateway avulla mobiililaitteet suojataan automaattisesti haittaohjelmia ja haitallista sisältöä vastaan. Network Gateway yhdessä Security Cloud -pilvimme kanssa skannaa liikennettä verkkotasolla hyödyntäen koko tietoturva-analytiikkamme. Tämän ansiosta voimme tarjota parempaa tietoturvaa kuin perinteiset mobiilitietoturvaratkaisut seuraavista syistä:

- Mobiililaitteiden rajalliset resurssit eivät vaaranna suojaustasoa.
- Resurssiintensiiviset toiminnot käsitellään pilvessä.

- Verkkotason tarkistus estää ennakoivasti kosketuksen haitalliseen sisältöön ja varmistaa, että järjestelmäsi pysyy suojattuna alusta alkaen
- Sovellukset ja tiedostot tarkistetaan käyttämällä reaaliaikaista uhkatietoa ja tietoturva-analytiikkaa.

Verkkoyhdyskäytävä

Network Gateway avulla Elements Mobile Protection voi tarkistaa jokaisen vieraillun verkkosivuston, ja käyttämällä WithSecure Security Cloud se voi rajoittaa pääsyä kyseisille sivustoille. Security Cloud tarjoaa koneoppimiseen perustuvan URL-mainepalvelun, joka analysoi miljoonia URL-osoitteita tarkistaakseen, millaista sisältöä ne tarjoavat. Verkkoyhdyskäytävää käytetään sitten URL-osoitteiden maineen arvioimiseen ennen niiden lataamista.

- Haitalliset sivustot on kokonaan estetty.
- Sivustot, jotka sisältävät tiettyjä sisältöluokkia, kuten aikuisille suunnattua sisältöä tai uhkapelisisältöä, voidaan haluttaessa estää. Nämä sivustot raportoidaan WithSecure Elements Security Center, jotta järjestelmänvalvoja voi päättää, tarvitaanko lisätoimenpiteitä.

Huomautus: URL-osoitteen näkyvyys voi olla rajoitettu tietoturvakeskuksessa työntekijöiden yksityisyyteen liittyvän paikallisen lainsäädännön vuoksi. Vastuullasi on organisaatiosi järjestelmänvalvojana varmistaa paikallisen lainsäädännön noudattaminen.

- Network Gateway innovatiivinen arkkitehtuuri eliminoi latenssin ja puskuroinnin, mikä varmistaa saumattoman selauskokemuksen.
- Network Gateway tarjoaa parannetun suojauksen ja edistyneen hallinnan tarjoamalla erilaisia ominaisuuksia, jotka suojaavat laitteita haitallisilta verkkosivustoilta ja sisällöltä.

SMS-suojaus

Tekstiviestisuojaus tarkistaa saapuvat tekstiviestit automaattisesti vaarallisten linkkien tai haitallisten QR-koodien varalta. Vaaralliseksi tunnistetut viestit siirretään roskapostikansioon, jolloin laitteesi ja henkilökohtaiset tietosi pysyvät turvassa.

Yksinkertaistettu hallinta

Kevyt ratkaisumme on yksinkertainen ja helppo hallita pilvessä. Sen avulla voit hallita suojausasetuksia ja profileja, ja se tarjoaa myös näkyvyyttä käyttöönoton aikana:

- Lähettämäsi kutsut ovat näkyvissä, kunnes asennus on valmis.
- Jokainen sähköpostilinkki on ainutlaatuinen ja mahdollistaa yhden asennuksen seuraavien 30 päivän aikana.
- Käyttöliittymän avulla voit helposti lähettää kutsun uudelleen tai luoda uuden päivitetyllä linkillä, kun edellinen vanhenee.

Joustavat käyttöönototavat

WithSecure Elements Mobile Protection integroituu saumattomasti kaikkiin suosittuihin Mobile Device Management (MDM) -ratkaisuihin, mikä mahdollistaa kattavan käytäntöjen hallinnan, kuten käyttöjärjestelmän vähimmäisversioiden pakottamisen ja laitteen salauksen.

1.3 Järjestelmävaatimukset

Tämä osio sisältää tärkeitä tietoja WithSecure Elements Mobile Protection -tuotteesta. Suosittelemme vahvasti, että luet koko asiakirjan ennen tuotteen käytön aloittamista.

Tuetut käyttöjärjestelmät

Android 12 ja uudemmat

Tuetut kielet

WithSecure Elements Mobile Protection -sovellus ja dokumentaatio on lokalisoitu seuraaville kielille:

Kiina (Taiwan), suomi, ranska, saksa, italia, japani, puola, portugali (Brasilia), espanja (Latinalaisamerikkalainen) ja ruotsi

Tuetut MDM:t

VMware Workspace ONE, Google Workspace Endpoint Management, IBM Security MaaS360, Microsoft Intune, Miradore, Ivanti Endpoint Management, Samsung Knox

Huomautus: Käyttöliittymän optimointi on vireillä Android-tableteille.

1.4 Aloittaminen

Ohjeet WithSecure Elements Mobile Protectionin asentamiseen ja aktivoimiseen sekä käytön aloittamiseen.

Sovellus voidaan aktivoida Android-laitteissa WithSecure Elements -portaalin kautta tai MDM:n avulla.

Huomautus: Katso tarkemmat ohjeet tuotteen käyttöönottoon kolmannen osapuolen MDM:n avulla liitteestä. [MDM:n käyttö](#) sivulla 18.

Tarvitset WithSecure Business -tilin käyttäaksesi WithSecure Elements Security Centeriä, joka on kaikkien WithSecure Elements -tuotteiden hallintaan tarkoitettu yhtenäinen hallinta-alusta. On olemassa kaksi mahdollista tilannetta:

- Kun ostat tuotteen WithSecure -kumppanilta, kumppani luo yleensä yritystilin organisaatiosi ensimmäiselle järjestelmänvalvojalle. Jos tämä koskee sinua, olet saanut WithSecurelta sähköpostiviestin, jossa on väliaikainen salasana ja linkki Elements Security Centeriin kirjautumiseen.
- Jos tiliäsi ei ole vielä luotu, mutta olet saanut tilausavaimen kumppaniltasi, voit käyttää tilausavainta luodaksesi WithSecure- yritystilin organisaatiosi ensimmäiselle järjestelmänvalvojalle. Voit tehdä sen käyttämällä yrityksen itserekisteröintilinkkiä. <https://elements.withsecure.com/self-register>.

1. Kirjaudu sisään WithSecure Elements Security Centeriin osoitteessa <https://elements.withsecure.com/> yritystilin tunnuksilla.

2. Sinun on lisättävä uudet laitteet lähettämällä sähköpostikutsu manuaalista asennusta varten:

Huomautus: Portaalissa näkyy etu- ja sukunimet, jos ne on lisätty. Jos niitä ei ole lisätty, järjestelmä tarkastaa, ovatko sähköpostiosoite ja aliasnimi tiedossa. Jos mitään näistä tiedoista ei ole saatavana, portaalissa näkyy UUID-tunnus.

- a) Valitse Elements Security Centerissä **Ympäristö**- kohdasta **Laitteet** > **Mobiililaitteet**.
- b) Valitse  ja valitse sitten **Lisää uusi laite**.
- c) Valitse käytettävä tilaus ja valitse **Seuraava**.
- d) Noudata ohjatun toiminnon ohjeita ja lähetä sähköpostikutsu yhdelle tai useammalle käyttäjälle, joka sisältää latauslinkin asennusohjelmaan.

3. Saat järjestelmänvalvojalta sähköpostiviestin, jossa sinua pyydetään asentamaan sovellus. Sähköpostiviesti sisältää linkin sovelluksen asentamiseen yhdelle laitteelle ja linkin lisenssin aktivoimiseksi. Sovelluksen asentaminen mobiililaitteellesi:

Huomautus: "Sinä" viittaa loppukäyttäjiiin.

- a) Avaa asennussähköposti.
- b) Valitse Android-kohdan vieressä oleva linkki.
Sinut ohjataan Google Play Kauppaan, josta voit ladata ja asentaa WithSecure Mobile Protection -sovelluksen.
- c) Kun olet asentanut sovelluksen laitteeseesi, aktivoi tilauksesi siirtymällä takaisin asennussähköpostiin ja valitsemalla **Aktivoi Androidille**.

Huomautus: Aktivointilinkki on voimassa 29 päivän ajan, mutta voit käyttää linkkiä vain kerran. Jos kirjaudut sovellukseen sähköpostissa olevilla käyttäjänimellä ja salasanalla, mutta et saa aktivoitua lisenssiä, voit kokeilla aktivointilinkkiä. Mutta jos kokeilet aktivointilinkkiä ensin eikä se jostain syystä toimi, ilmoitetut tunnistetiedot eivät enää toimi.

WithSecure Mobile Protection -sovellus avautuu.

- d) Valitse kysyttäessä **Salli**, niin sovellus saa tarvittavat käyttöoikeudet.

Huomautus: Sovellus tarvitsee luvan valokuvien, mediasisällön ja tiedoston käyttöön, jotta se voi etsiä haitallisia kohteita.

4. Käyttäjätietojen tarkasteleminen ja muokkaaminen:

- a) Napauta päänäkylässä  .
Valikkonäkymä avautuu.
- b) Napauta **Käyttäjätiedot**.
- c) **Käyttäjätietojen** näkymässä voit tarkastella ja muokata seuraavia tietoja:
- Sähköpostiosoite.
- Huomautus:** Et voi muokata rekisteröityä sähköpostiosoitetta.
- Etunimi
 - Sukunimi
 - Alias

Muutokset tallennetaan sekä paikalliseen sovellukseesi avainnippuun että Elements Security Centeriin.

Haitallisen sisällön etsiminen

- [Manuaalinen tarkistus](#)
- [Automaattinen tarkistus](#)

Tuote tarkistaa laitteesi ja etsii haitallista sisältöä ja muita laitteeseesi ja dataasi kohdistuvia uhkia.

2.1 Manuaalinen tarkistus

Voit tarkistaa laitteesi virusten ja muiden uhkien varalta milloin vain.

Laitteen tiedostojen manuaalinen skannaus:

1. Napauta päänäkylässä **Haittaohjelasuojaus**.
2. Napauta **Aloita skannaus**.
Tarkistus alkaa.
3. Kun skannaus on valmis, sovellus näyttää seuraavat tiedot:
 - Viimeisimmän täyden skannauksen päivämäärä ja aika
 - Tarkistetut tiedostot - tarkistettujen tiedostojen määrä
 - Tarkistetut sovellukset – tarkistettujen sovellusten määrä
 - Havaitut uhat – niiden uhkien määrä, jotka sovellus havaitsi tarkistuksen aikana

Huomautus: Valitsemalla **Näytä koko tarkistushistoria** voit nähdä manuaalisten ja automaattisten tarkistusten päivämäärät ja kellonajat. Valitsemalla **Manuaalinen tarkistus** -kohdan vieressä olevan nuolen voit tarkastella tarkistuksen tietoja.

2.2 Automaattinen tarkistus

Oletusarvoisesti sovellus tarkistaa laitteesi automaattisesti virusten ja muiden uhkien varalta.

Kun **virustorjunta** on käytössä, sovellus tarkistaa laitteen automaattisesti esimerkiksi aina, kun asennettu sovellus päivitetään, kun laite käynnistetään uudelleen tai kun SD-kortti asennetaan.

Laitteen tiedostojen tarkistaminen automaattisesti:

1. Napauta päänäkylässä .
Valikkonäkymä avautuu.
2. Napauta **Asetukset**.
3. Ota **virustorjunta** käyttöön.
Sovellus tarkistaa automaattisesti uudet sovellukset ja tiedostot.
4. Ota käyttöön **Mittausperusteinen tarkistus**, jos haluat sovelluksen tarkistavan laitteesi, vaikka laite olisi käytössä käytön mukaan laskutettavassa verkkoyhteydessä.

Huomautus: Tämän valinnan käyttöönotto voi kasvattaa dataliikennettä.

Internet-liikenteen suojaaminen

- Verkon suojauksen käyttöönotto
- Tekstiviestisuojauksen käyttöönotto
- Mainepohjaisen selauksen ottaminen käyttöön
- Sallitaan liikenteen reititys etävälityspalvelimen kautta
- Sallii diagnostisten tiedostojen etäkeräyksen
- Sovelluspoikkeuksien valitseminen
- Suojaustilastojen katsominen

Network Gateway käytetään URL-osoitteiden maineen arvioimiseen ennen niiden lataamista.

Käyttämällä WithSecure Security Cloud se voi rajoittaa pääsyä kyseisille sivustoille. Security Cloud tarjoaa koneoppimiseen perustuvan URL-mainepalvelun, joka analysoi miljoonia URL-osoitteita tarkistaakseen, millaista sisältöä ne tarjoavat.

Network Gateway antaa sinulle edistyneen hallinnan URL-osoitteiden estoon ja sallittujen luetteloon. Voit estää kokonaisia sivustoluokkia estääksesi pääsyn tiettyntyyppiseen sisältöön, kuten aikuisille suunnatuille, uhkapelisivustoille tai sosiaalisen median sivustoille. Lisäksi voit sallia tiettyjä URL-osoitteita, jolloin käyttäjät voivat käyttää hyväksytyjä verkkosivustoja, jotka voivat olla oletuksena estetty.

Network Gateway avulla kaikki käyttäjät laitteestaan ja mobiilialustastaan riippumatta hyötyvät tietoturvakäytännöistämme ja verkon suorituskyvystä. Käytänpä sitten Network Gateway -yhdyskäytävääme suoraan tai kolmannen osapuolen palveluun, se tarjoaa yhtenäisen suojan ja nopeutetun suorituskyvyn. Kaikki käyttäjät on suojattu haitallisilta verkkosivustoilta, ja heillä on edistynyt verkkokokemusten hallinta.

Lisäksi Network Gateway tarjoaa parannetun suojauksen ja edistyneen hallinnan Android-laitteille. Se tarjoaa useita ominaisuuksia, jotka suojaavat laitteita haitallisilta verkkosivustoilta ja sisällöltä.

3.1 Verkon suojauksen käyttöönotto

Kun otat suojauksen käyttöön, Elements Mobile Protection arvioi URL-osoitteiden maineen ennen verkkosivustojen lataamista.

Verkkosuojauksen ottaminen käyttöön:

Napauta päänäköymän **Verkon suojaus** -kohdassa **Suojaus: POIS** aktivoidaksesi suojauksen.

Verkkosi on nyt suojattu.

3.2 Tekstiviestisuojauksen käyttöönotto

Kun otat tekstiviestisuojauksen käyttöön, Elements Mobile Protection suojaa laitteitasi tekstiviestillä tehtäviltä tietojenkalasteluyrityksiltä.

SMS-suojauksen ottaminen käyttöön:

Aktivoi **tekstiviestisuojaus** napauttamalla päänäköymässä kohdassa Tekstiviestisuojaus kohtaa **Suojaus: POIS PÄÄLTÄ**.

3.3 Mainepohjaisen selauksen ottaminen käyttöön

Maineeseen perustuva selaus estää epäilyttävät tai haitallisiksi tiedetyt verkkosivustot.

Huomautus: Maineeseen perustuvan selaamisen käyttämiseksi verkon suojauksen on oltava käytössä.

Maineeseen perustuvan selaamisen ottaminen käyttöön:

1. Napauta päänäköymässä .
Valikkonäkymä avautuu.
2. Napauta **Asetukset**.
3. Ota **maineeseen perustuva selaus** käyttöön.
4. **Maineperusteinen selaus** -kohdassa voit ottaa käyttöön seuraavat:
 - **Estä pääsy haitallisiksi arvioiduille verkkosivustoille**
 - **Estä pääsy epäilyttäviksi luokitelluille verkkosivustoille**
 - **Estä pääsy kielletyiksi luokitelluille verkkosivustoille**
 - **Estä verkkosivuilta löytyvät seurantalaitteet**
 - **Estä pääsy äskettäin luotuihin verkkotunnuksiin**

3.4 Sallitaan liikenteen reititys etävälityspalvelimen kautta

Voit sallia verkkoyhdyskäytävän reitittää liikennettä etävälityspalvelimen kautta.

Huomautus: Voit määrittää tämän iOS-laitteesi Wi-Fi-asetuksista.

Etävälityspalvelimen asetusten salliminen:

1. Napauta päänäköymässä .
Valikkonäkymä avautuu.
2. Napauta **Asetukset** > **Verkon suojaus**.
3. Ota käyttöön **Salli etävälityspalvelimet**.

3.5 Sallii diagnostisten tiedostojen etäkeräyksen

Kun otat tämän asetuksen käyttöön, järjestelmänvalvojat voivat kerätä diagnostiikkatiedoston etänä laitteeltasi.

Ota asetus käyttöön seuraavasti:

1. Napauta päänäkyymässä .
Valikkonäkymä avautuu.
2. Napauta **Asetukset**.
3. Valitse **Lisää** -kohdasta **Hyväksy diagnostiikkatiedoston etäkokoelma**.

3.6 Sovelluspoikkeuksien valitseminen

Ohjeet sovellusten valitsemiseen, jotka haluat muodostaa Internet-yhteyden suoraan verkkoyhdyskäytävän suojauksen ohittamiseen.

Sovellusten valitseminen:

1. Napauta päänäkyymässä .
Asetukset- näkymä avautuu.
2. Napauta **Verkon suojaus** -kohdassa **Sovelluspoikkeukset**
3. Napauta avautuvassa näkyymässä sovellusluettelosta niitä, jotka haluat muodostaa Internet-yhteyden suoraan.

Valitsemasi sovellukset muodostavat yhteyden suoraan internetiin ohittaen Network Gateway suojauksen.

3.7 Suojaustilastojen katsominen

Päänäkymästä näet, kuinka monta uhkia sovellus on estänyt.

Huomautus: Estettyjen seurantayritysten ja haitallisten verkkosivustojen määrä näytetään vain, jos maineeseen perustuva selaus on päällä. Se, onko tämä ominaisuus käytössä vai pois päältä, riippuu laitteelle määritetystä profilista.

Tilastotietojen katsominen:

1. Päänäkymässä **Verkon suojaus** -kohdassa näet seuraavat tilastot:
 - Internet-liikenne suojattu – näytä sovelluksen suojaaman liikenteen määrä (Mt).
 - Tarkistettujen sivustojen kokonaismäärä – sovelluksen tarkistamien verkkosivustojen määrä
 - Estetyt haitalliset sivustot – sovelluksen estämien haitallisten verkkosivustojen määrä
 - Seurantayritykset estetty – sovelluksen estämien seurantayritysten määrä
2. Voit tarkastella viimeaikaista toimintaa seuraavasti:
 - a) Napauta **Viimeaikainen toiminta** -linkkiä.
 - b) Napauta **Viimeaikainen toiminta** -näkyymässä .
 - c) Ota käyttöön **Näytä kaikki tallennetut URL-osoitteet**.
 - d) Valitse **URL-kategoriassa** luokat, jotka haluat suodattaa, ja napauta **Tallenna**. Voit valita ne yksitellen tai kaikki kerralla.

Näyttöön tulee luettelo, jossa näkyvät kaikki URL-osoitteet – sallitut ja estetyt – jotka sovellus on tallentanut.

Luku 4

Tuki

Odotamme innolla kommentteja ja palautetta tuotteen toimivuudesta, käytettävyydestä ja suorituskyvystä.

Voit ilmoittaa kaikista teknisistä ongelmista WithSecure tukisivuston kautta [täällä](#).

Liite A

Lokitiedostojen vienti

- [Kuinka viedä lokitiedostoja](#)

Jos sinulla on tekninen ongelma, tekninen tuki voi pyytää sinua viemään ja lähettämään lokitiedostoja tutkittavaksi.

Tässä osiossa kerrotaan, kuinka lokitiedostoja viedään mobiililaitteiden aktivoituihin ja aktivoimattomiin sovelluksiin.

A.1 Kuinka viedä lokitiedostoja

Ohjeet lokitiedoston viemiseen Android-laitteiden aktivoituun tai ei-aktivoituun sovellukseen.

Jos ilmoitat teknisestä ongelmasta, liitä palautteeseen lokitiedosto seuraavasti:

1. Avaa Elements Mobile Protection -sovellus.
2. Napauta päänäköymässä .
Valikkonäkymä avautuu.
3. Napauta **Tietoja sovelluksesta**.
4. Napauta **Mobiilisuojaus** -kohdassa versionumeroa seitsemän kertaa.
Lähetä loki -painike tulee näkyviin.
5. Noudata näyttöön tulevia ohjeita.

MDM:n käyttö

- [Ennen kuin aloitat](#)
- [Käyttöönotto Google Workspace MDM:llä](#)
- [Käyttöönotto VMware Workspace ONE MDM:llä](#)
- [Käyttöönotto Microsoft Intunella MDM:llä](#)
- [Käyttöönotto IBM MaaS360 MDM:llä](#)
- [Käyttöönotto Ivanti Endpoint Managementin avulla](#)
- [Käyttöönotto Miradore MDM:llä](#)
- [Käyttöönotto Samsung Knoxin avulla](#)

Tässä osiossa kuvataan, kuinka WithSecure Elements Mobile Protection -sovellus voidaan integroida MDM:ään.

WithSecure Elements Mobile Protection on ihanteellinen ratkaisu organisaatioille, jotka haluavat lisäsuojasta mobiililaitteilleen niiden perusturvaominaisuuksien lisäksi, jotka nykyinen MDM-ratkaisu jo sisältää. Ratkaisu parantaa huomattavasti tietoturvaa mm. haittaohjelmia, tietojenkalastelua ja tietovarkauksia vastaan.

WithSecure Elements Mobile Protection voidaan integroida seuraaviin MDM:eihin: Google Workspace Endpoint Management, VMware Workspace ONE, Microsoft Intune, IBM Security MaaS360, Ivanti Endpoint Management (aiemmin MobileIron Cloud), Miradore ja Samsung Knox.

WithSecure Elements Mobile Protectionin voi ottaa käyttöön profiilirekisteröintikohtaisesti. Eli jos päätelaitteessa käytetään sekä henkilökohtaista että työprofiilia, sovellus on asennettava molempiin profiileihin.

Vihje: Suosittelemme testaamaan rekisteröitymisprosessin ensin yhdellä laitteella.

Huomautus: Muuttujat määritetään yleensä, kun WithSecure Elements Mobile Protection määritetään MDM-alustaa varten. Muuttujien avulla määritetään, rekisteröidäänkö sovellus sähköpostiosoitetta, käyttäjänimeä vai UUID-tunnusta käyttämällä. Esimerkki:

- Jos sovellusta ei määritetä, se käyttää UUID-tunnusta, joka näkyy WithSecure Elements -portaalissa laitteen nimen alla.
- Jos sähköpostiosoitteet määritetään, ne näkyvät portaalissa laitteen nimen alla.

Kun sovellus on määritetty MDM-alustalle, sitä ei pitäisi enää muuttaa. Jos päätät tehdä muutoksia, laitteet on poistettava ensin WithSecure Elements -portaalista ja sovellus on lisäksi poistettava MDM-agentista, koska muutoin muutosten tekeminen tuottaa kaksoiskappaleita.

B.1 Ennen kuin aloitat

Sovellus voidaan aktivoida mobiililaitteissa MDM:n avulla tai WithSecure Elements -portaalin kautta kutsumalla käyttäjiä.

B.2 Käyttöönotto Google Workspace MDM:llä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android-laitteissa Google Workspace MDM:n avulla.

B.2.1 Android-sovelluksen lisääminen Google Workspace Endpoint Managementiin

Ohjeet WithSecure Elements Mobile Protection -sovelluksen lisäämiseen sallituksi Android-laitteissa Google Workspace MDM:n avulla.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
- Määritä sovellus ja määritä se WithSecuren tarjoamalla tilausavaimella.

Voit lisätä tuotteen Google Workspacen MDM:ään seuraavasti:

1. Kirjautu sisään Google Workspacen hallintakonsoliin.
2. Valitse hallintapaneelissa **Apps > Web and mobile apps**.
3. Valitse **Web and mobile apps** -sivulla **Add App > Add private Android app**.
4. Valitse **Managed Android apps** -sivulla **Search Play Store** ja kirjoita hakuruutuun **mobile protection elements**.
5. Valitse sovellus ja valitse sitten **Approve > Select**.
6. Valitse haluamasi vaihtoehto **User access** -kohdassa ja valitse **Continue**.
7. Valitse haluamasi vaihtoehdot **Access method** -kohdassa ja valitse **Finish**.

Android-sovellus lisätään Google Workspacen MDM:ään.

Android-sovelluksen määrittäminen

Ohjeet Android-sovelluksen määrittämiseen.

Huomautus: Google Workspace ei tue muuttujia. Rekisteröintiavain-kenttä hyväksyy kuitenkin tilausavaimen muuttujana vakiomuodossa. Kirjoita siksi tilausavain sellaisenaan, mutta älä kirjoita sähköpostiosoitetta. Jos teet niin, kaikilla laitteillasi näytetään sama sähköpostiosoite WithSecure Elements Security Center. Kun jätät sähköpostiosoitteen tyhjäksi, laitteet, joihin on asennettu WithSecure Elements Mobile Protection näytetään laitteen UUID-tunnuksella.

1. Valitse **Hallintakonsoli**-sivulla **Hallitut kokoonpanot** -kohdassa **Lisää hallittu kokoonpano**.
2. Kirjoita kokoonpanon nimi Hallittu kokoonpano -sivulle ja tee seuraavaa:
 - a) Kirjoita tuotteen tilauskoodi Rekisteröintiavain-kenttään.
Löydät tilausavaimen WithSecure Elements Security Center **kohdasta > Hallintatilaukset > .**
 - b) Kirjoita etu- ja sukunimesi niitä vastaaviin kenttiin (valinnainen).
 - c) Kirjoita Valenimi-kenttään (valinnainen) vaihtoehtoinen nimi.

- d) Kirjoita sähköpostiosoitteesi Sähköpostiosoite-kenttään (valinnainen).
- e) Kirjoita Ympäristö-kenttään (valinnainen) 2.

3. Valitse **Tallenna**.

B.2.2 Chromebookin rekisteröinti

Ohjeet Chromebookin rekisteröimiseen Google Workspace MDM:ään ja WithSecure Elements Mobile Protection -sovelluksen ja WithSecure Browsing Protection -laajennuksen asentamiseen hallitulle Chromebookille.

Chromebook-yhteensopivuus

Yleiskatsaus WithSecure -tuotteen yhteensopivuuteen Chrome OS:n kanssa.

Seuraavat WithSecure -tuotteet ovat yhteensopivia Chrome OS:n kanssa:

- Selauksen suojauslaajennus - saatavilla **Chrome Web Storen** kautta
- Elements Mobile Protection – saatavilla Android-sovelluksena **Google Play Kaupasta** Chromebookkeille, jotka tukevat Android-sovelluksia

Chromebookin rekisteröinti Google Workspace MDM:ään

Ohjeet Chromebookin rekisteröimiseen Google Admin Consolen avulla keskitettyä hallintaa varten.

Ennen kuin aloitat, varmista, että sinulla on seuraavat:

- Google Workspace -järjestelmänvalvojan tili
- Chrome Enterprise -päivityslisenssi
- Chromebook, jonka tehdasasetukset on palautettu

Chromebookin rekisteröiminen:

1. Kirjaudu sisään **Google-hallintakonsoliin**.
2. Siirry kohtaan **Laitteet > Chromen > asetukset > Laittehallinta**.
3. Tarkista, että ilmoittautumisasetukset ja organisaatioyksiköt ovat oikein.
4. Käynnistä Chromebook ja aloita rekisteröinti painamalla **Ctrl + Alt + E**.
5. Anna järjestelmänvalvojan käyttäjätunnus ja salasana.
6. Varmista, että Chromebook näkyy hallintakonsolin **Laitteet > Chrome- > laitteet** -kohdassa.

WithSecure Elements Mobile Protectionin asentaminen

Ohjeet sovelluksen asentamiseen hallitulle Chromebookille.

Varmista, että seuraavat vaatimukset täyttyvät:

- Chromebook on rekisteröity Google Mobile Device Managementiin (MDM)
- Sinulla on aktiivinen WithSecure Elements Mobile Protection -tilaus
- Google Play Kauppa on otettu käyttöön organisaatiollesi hallintakonsolissa.
- Chromebookit tukevat Android-sovelluksia (useimmat nykymallit)

Sovelluksen asentaminen:

1. Kirjaudu sisään **Google-hallintakonsoliin**.
2. Siirry kohtaan **Laitteet > Chrome > -asetukset > Käyttäjä- ja selainasetukset**.
3. Vieritä **Android-** sovellusosiointiin ja valitse sopiva organisaatioyksikkö.
4. Määritä **Chrome-laitteiden Android-sovellusten** asetukseksi **Salli käyttäjien asentaa Android-sovelluksia Chrome-laitteille** ja valitse **Tallenna**.
5. Aktivoi Android Enterprise -tilaus **kohdassa > Laskutustilaukset** ja hyväksy Google Playn käyttöehdot.

WithSecure-selaussuojauslaajennuksen asentaminen

Ohjeet WithSecure Browsing Protection -laajennuksen asentamiseen hallitulle Chromebookille.

Varmista, että seuraavat vaatimukset täyttyvät:

- Chromebook on rekisteröity Google Mobile Device Managementiin (MDM)
- Google Play Kauppa on otettu käyttöön organisaatiollesi hallintakonsolissa.

Laajennuksen asentaminen:

1. Kirjaudu sisään [Google-hallintakonsoliin](#).
2. Siirry kohtaan [Laitteet](#) > [Chrome](#) > [-sovellukset ja -laajennukset](#) > [Käyttäjät ja selaimet](#).
3. Valitse kohdeorganisaatioyksikkö, johon haluat ottaa laajennuksen käyttöön, ja valitse [Lisää](#) > [Chrome Web Storesta](#).
4. Etsi [WithSecuren selaamisen suojaus](#) ja valitse se.
5. Valitse [Asennuskäytäntö](#)-kohdasta [Pakota asennus](#) ja valitse sitten [Tallenna](#).

Laajennus asennetaan automaattisesti kaikkiin kohdeorganisaatioyksikön rekisteröityihin Chromebookeihin.

Kirjaudu sisään hallitulla Chromebookilla ja avaa `chrome://extensions` varmistaaksesi, että laajennus on asennettu ja aktiivinen.

B.3 Käyttöönotto VMware Workspace ONE MDM:llä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon VMware Workspace ONE (aiemmin AirWatch) MDM:n avulla Android- ja iOS-laitteissa.

Huomautus: Nämä ohjeet eivät sisällä käyttäjien ja laitteiden luomista ja määrittämistä koskevia tietoja.

B.3.1 Android-sovelluksen lisääminen VMware Workspace ONE:n MDM:ään

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen VMware Workspace ONE MDM:ään.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
 - Määritä sovellus ja määritä se WithSecureen tarjoamalla tilausavaimella.
1. Siirry VMware Workspace ONE -hallintaportalissa kohtaan [Apps and Books](#) ja valitse [Native](#).
 2. Valitse seuraavaksi Julkinen-välilehdellä [Lisää sovellus](#).
 3. Toimi sovelluksen lisäyssivulla seuraavasti:
 - a) Valitse avattavasta [Alusta](#)-valikosta [Android](#).
 - b) Valitse [Lähde](#)-kentästä [Hae App Storesta](#).
 - c) Kirjoita [Nimi](#)-kenttään WithSecure Elements Mobile Protection.
 - d) Valitse [Seuraava](#).
 4. Valitse Sovellukset-näkymästä [WithSecure Elements Mobile Protection](#).
 5. Valitse [WithSecure Elements Mobile Protection](#) -näkymässä [Hyväksy](#) > [Valitse](#).
 6. Valitse Muokkaa sovellusta -näkymässä [Käyttöehdot](#)-välilehti.
 7. Valitse avattavasta [SDK](#) -valikosta [MP strings@ WithSecure](#).
 8. Valitse [Tallenna ja määritä](#).

B.3.2 Hallittujen sovellusten tarkasteleminen

Ohjeet hallittujen sovellusten tarkastelemiseen VMware Workspace ONE MDM:ssä.

1. Valitse VMware Workspace ONE -konsoliikkunassa [Sovellukset ja kirjat](#) ja valitse sitten [Sovellukset](#) -kohdasta [Luettelonäkymä](#).
Luettelonäkymä-sivu tulee näkyviin
2. Valitse [Public](#)-välilehti.

WithSecure Elements Mobile Protection -sovellus näkyy VMware Workspace ONE -hallintaportaalin sovellusluettelossa.

B.3.3 Android Enterprise -käyttöönotto VMware Workspace ONE:n kanssa

Tässä luvussa on ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android Enterprise -kontekstissa VMware Workspace ONE:n avulla.

Android Enterprisen määrittäminen VMware Workspace ONE:n MDM:ssä

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen asetusten määrittämiseen Android Enterprise -kontekstissa.

Jotta sovellus voidaan ottaa käyttöön Android Enterprise -kontekstissa, yrityksellä on oltava Google-järjestelmänvalvojan tili. Kaikilla käyttäjillä on oltava tilit, joko ennalta määritettyinä tai rekisteröinnin aikana luotuin.

Toimialueen järjestelmänvalvojan on luotava EMM-tunnus ja sitova VMware Workspace ONE EMM-palveluntarjoajaksi.

Voit määrittää Android Enterprisen seuraavasti:

1. Kirjaudu VMware Workspace ONE -hallintaportaaliin.
2. Siirry kohtaan [Groups and Settings](#) ja valitse [All Settings](#).
3. Valitse Asetukset-näkymässä [Laitteet ja käyttäjät](#) -kohdassa [Android](#).
4. Valitse [Android](#)-kohdassa [Android EMM Registration](#).
5. Valitse tilikuvake oikeasta yläkulmasta ja sitten [Manage your Google Account](#).
6. Kirjaudu sisään sähköpostiosoitteellasi ja salasasanallasi.
7. Valitse Tuo Android töihin -sivulla [Aloita](#).
Android EMM Registration -sivu tulee näkyviin.
8. Kun palvelutili on määritetty, hyväksy [Rekisteröintiasetukset](#) - ja [Ilmoittautumisrajoitukset](#) -välilehtien asetukset ja valitse [Tallenna](#).
Asetukset tallennetaan.

Profiilien lisääminen VMware Workspace ONEen

Ohjeet profiilien lisäämiseen.

1. Siirry VMware Workspace ONE -hallintaportaaliin kohtaan [Apps & Books](#) > [All Apps & Books Settings](#).
Settings-sivu tulee näkyviin.
2. Valitse siirtymisruudussa [Settings and Policies](#) > [Profiles](#).
Profiilit-näkymä tulee näkyviin.
3. Valitse [Add Profile](#) > [SDK Profile](#) > [Android](#).
Add a New Android Profile -sivu tulee näkyviin.
4. Valitse [General](#), kirjoita uuden profiilin nimi ja kuvaus ja valitse [Save](#).

Android-sovelluksen lisääminen

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen VMware Workspace ONE MDM:ään Android Enterprise -kontekstissa.

1. Siirry VMware Workspace ONE -hallintaportalissa kohtaan **Apps & Books > Applications > Native**. Luettelonäkymä tulee näkyviin.
2. Valitse **Public**-välilehti ja sitten **Add application**.
3. Toimi Add Application -näkyvässä seuraavasti:
 - a) Valitse avattavasta **Alusta**-valikosta **Android**.
 - b) Kirjoita sovelluksen nimi: mobile protection elements.
 - c) Valitse **Seuraava**. **Sovellukset**-sivu tulee näkyviin.
4. Valitse WithSecure Elements Mobile Protection.
5. Valitse WithSecure Elements Mobile Protection -näkyvässä **Hyväksy > Valitse**. Muokkaa sovellusta -näkyvä tulee näkyviin.
6. Valitse **SDK**- välilehti ja valitse avattavasta **Sovellusprofiili** -valikosta **MP strings @ WithSecure**.
7. Valitse **Tallenna ja määritä**. **WithSecure Elements Mobile Protection - Tehtävä** -sivu avautuu.
8. Valitse **Jakelu** ja toimi seuraavasti:
 - a) Kirjoita Nimi-kenttään jakelun nimi, kuten kaikki laitteet.
 - b) Valitse Tehtävä-ryhmistä haluamasi laitteen jakeluryhmä.
9. Valitse seuraavaksi **Sovelluskokoonpano** ja toimi seuraavasti:
 - a) Kirjoita tuotteen tilauskoodi **Rekisteröintiavain**-kenttään.
Huomautus: Löydät WithSecure Elements Mobile Protection -tilausavaimen WithSecure Elements Security Center kohdasta **Endpoint Protection > Subscriptions**.
 - b) Kirjoita Etunimi (valinnainen) -kenttään **{FirstName}**
 - c) Kirjoita Sukunimi (valinnainen) -kenttään **{LastName}**
 - d) Kirjoita Valenimi (valinnainen) -kenttään **{EnrollmentUser}**
 - e) Kirjoita Sähköposti (valinnainen) -kenttään **{EmailAddress}**
 - f) Valitse **Luo**.**Määrittelykset**-välilehti tulee näkyviin.
10. Valitse **Tallenna**. **Esikatsele määritettyjä laitteita** -sivu avautuu.
11. Valitse **Julkaise**.

Android-sovelluksen määrittäminen

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen VMware Workspace ONE MDM:ään Android Enterprise -kontekstissa.

Voit määrittää Android-sovelluksen seuraavasti:

1. Valitse VMware Workspace ONE -hallintaportalissa **Edit Application** -sivu.
2. Valitse **Määrittely**-välilehti ja määritä määrittelyryhmä.
3. Valitse **Lähetä sovelluskokoonpano**.
4. Lisää **Kokoonpanoavain**-kohdassa arvot seuraaviin kokoonpanomerkintöihin:

Huomautus: Jälleenmyyjä toimittaa arvot sinulle.

- fate_registration_key - lisenssiavain
- etunimi (valinnainen) – nimi, joka helpottaa käyttäjän tunnistamista WithSecure Elements Security Center
- sukunimi (valinnainen) – nimi, joka helpottaa käyttäjän tunnistamista WithSecure Elements Security Center

Lisää lisämäärytykset valitsemalla **Lisää hakuarvo** -kohdan vieressä oleva kuvake ja valitsemalla vastaavat muuttujat. Kentät täytetään automaattisesti, kun sovellus otetaan käyttöön käyttäjän laitteissa.

5. Täytä loput sovelluksen asetuksista kohdassa **Tiedot ja määrittäminen** ja valitse **Tallenna ja julkaise**, jotta sovellus lisätään **luettelonäkymään**.

B.4 Käyttöönotto Microsoft Intunella MDM:llä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android- ja iOS-laitteissa Microsoft Intune MDM:n avulla.

B.4.1 Android-sovelluksen käyttöönotto Microsoft Intunen MDM:ssä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Microsoft Intune MDM:n avulla.

MDM-hallituissa laitteissa WithSecure Elements Mobile Protection tukee hiljaista aktivointia, myöntää automaattisesti kaikki tarvittavat järjestelmä- ja ominaisuusoikeudet ja ottaa VPN-profiilin käyttöön ilman käyttäjän toimia. Tämä tarjoaa aidosti itsepalveluperiaatteella toimivan käyttöönottokokemuksen, toisin kuin tavallisissa käyttöönottoissa, joissa käyttäjien on hyväksyttävä manuaalisesti jokainen lupapyyntö ja asennettava VPN-profiili.

Android-sovelluksen lisääminen Microsoft Intunen MDM:ään

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen Microsoft Intunen MDM:ään.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
- Määritä sovellus ja määritä se WithSecuren tarjoamalla tilausavaimella.

1. Kirjaudu Microsoft Intune -portaaliin.
2. Valitse **Sovellukset > Android > Lisää**.
Valitse sovellustyyppi -ruutu tulee näkyviin.
3. Valitse avattavasta **Sovelluksen tyyppi** -valikosta **Hallinnoitu Google Play -sovellus** ja valitse sitten **Valitse**.
4. Kirjoita **Hallinnoitu Google Play** -näkyvässä Haku-kenttään WithSecure Elements.
Sovellukset -näkyvä tulee näkyviin.
5. Valitse **WithSecure Elements Mobile Protection**.
6. Valitse näkyviin tulevasta näkymästä **Hyväksy > Hyväksy**.
7. Valitse **Hyväksymisasetukset** -välilehdessä **Pidä hyväksyntä, kun sovellus pyytää uusia käyttöoikeuksia** ja valitse sitten **Valmis**.
Hallinnoitu Google Play -näkyvä tulee näkyviin.
8. Valitse **Synkronoi** vasemmasta yläkulmasta.
Android-sovellukset -näkyvä tulee näkyviin.
9. Valitse **Päivitä** ja valitse sitten **WithSecure Elements Mobile Protection**.
WithSecure Elements Mobile Protection -näkyvä tulee näkyviin.
10. Valitse **Hallinta** -kohdasta **Ominaisuudet**.

WithSecure Elements Mobile Protection -näkymä tulee näkyviin.

11. Valitse **Määritykset**-kohdassa **Muokkaa**.
Muokkaa sovellusta -näkymä tulee näkyviin.
12. Tee **Määritykset**-välilehdessä seuraavaa:
 - a) Valitse **Pakollinen**-kohdassa **Lisää kaikki käyttäjät**.
 - b) Valitse **Tarkista + tallenna**.
 - c) Valitse **Tarkista + tallenna** -välilehdessä **Tallenna**.

WithSecure Elements Mobile Protection -sovellus on lisätty Microsoft Intunen MDM:ään.

Lisää seuraavaksi sovelluksen kokoonpanokäytännöt.

Android-sovelluksen kokoonpanokäytäntöjen lisääminen

Ohjeet WithSecure Elements Mobile Protection -määrityskäytäntöjen lisäämiseen hallituille Android-laitteille.

1. Valitse **Sovellukset**.
Sovellusten yleiskuvaus -ruutu tulee näkyviin.
2. Valitse **Käytäntö**-kohdasta **Sovelluksen kokoonpanokäytännöt**.
3. Valitse **Lisää > Hallinnoidut laitteet**
Luo sovelluksen kokoonpanokäytäntö -ruutu tulee näkyviin.
4. Tee **Perusasetukset**-välilehdessä seuraavaa:
 - a) Kirjoita **Nimi**- kenttään WithSecure Mobile Protection.
 - b) Valitse avattavasta Alusta-valikosta **Android Enterprise**.
 - c) Valitse Profiilityyppi-pudotusvalikosta joko **Vain henkilökohtaisesti omistettu työprofiili** tai **Täysin hallinnoitu, oma ja yrityksen omistama työprofiili**.
 - d) Valitse **Kohdistettu sovellus** -kohdassa **Valitse sovellus**.
Liitetty sovellus -ruutu tulee näkyviin.
 - e) Valitse **WithSecure Elements Mobile Protection** ja valitse sitten **OK > Seuraava**.
Asetukset-välilehti tulee näkyviin.
5. Toimi seuraavasti:
 - a) Valitse avattavasta Kokoonpanoasetusten muoto -valikon **Kokoonpanoasetukset**-kohdasta **Käytä kokoonpanon suunnittelutoimintoa**.
 - b) Valitse **+Lisää**.
 - c) Valitse oikealle avautuvasta ruudusta seuraavaa:
 - Rekisteröintiavain
 - Valenimi (valinnainen)
 - Sähköpostiosoite (valinnainen)
 - Ympäristö (valinnainen)
 - d) Valitse **OK**.
 - e) Valitse arvotyytit ja syötä kokoonpanoarvot seuraaville kokoonpanoavaimille:
 - fate_registration_key: arvontyyppi: **Merkkijono** ; kokoonpanon arvo: [WithSecure Elements Mobile Protection -tilausavain].

Huomautus: Löydät WithSecure Elements Mobile Protection -tilausavaimen WithSecure Elements Security Centeristä **kohdasta > Hallintatilaukset**.

 - alias: arvotyyppi: **String** ; määritysarvo: {{käyttäjänimi}}
 - sähköposti: arvotyyppi: **String** ; määritysarvo: {{mail}}
 - env: arvotyyppi: **Kokonaisluku**; kokoonpanoarvo:2

Huomautus: Kokoonpanoavain env ja sen arvo määrittävät, mihin VPN-päätelaite muodostaa yhteyden.
 - f) Valitse **Seuraava**.
Määritykset-välilehti tulee näkyviin.
 - g) Valitse **Sisällytetyt ryhmät** -kohdasta **Lisää kaikki käyttäjät** ja sitten **Seuraava**.

Tarkista + luo -välilehti tulee näkyviin.

h) Valitse **Luo**.

Sovelluksen kokoonpanokäytäntö on luotu ja määritetty.

Sinun on asennettava sovellus Android-laitteeseen.

Android-laitteen määrittäiskäytäntöjen lisääminen

Ohjeet laitemäärittäiskäytäntöjen lisäämiseen hallituille Android-laitteille.

1. Valitse **Laitteet**.
Laitteiden yleiskatsausruutu avautuu.
2. Valitse **Laitteiden hallinta-kohdasta Määrittäiset**.
3. Valitse **Käytännöt** -välilehdeltä **Luo > uusi käytäntö**.
Luo **profiili** -ruutu avautuu.
4. Valitse **Alusta** -pudotusvalikosta **Android Enterprise**.
5. Valitse **Profiilityyppi** -pudotusvalikosta **Mallit**.
6. Valitse joko **Täysin hallinnoitu, Dedikoitu ja Yrityksen omistama työprofiili** tai **Vain henkilökohtaisen omistajan työprofiili** -kohdasta **Laiterajoitukset > Luo**.
Laiterajoitukset -ruutu avautuu.
7. Tee **Perusteet** -välilehdellä seuraavat toimenpiteet:
 - a) Kirjoita **Nimi** -kenttään WithSecure Mobile Protection.
 - b) Kirjoita **Kuvaus** -kenttään käytännön kuvaus.
 - c) Valitse **Seuraava**.
8. Valitse **Määrittäasetukset** -välilehden Yhteydet-kohdasta seuraavat:
 - a) Valitse Aina päällä oleva VPN -kohdasta **Ota käyttöön**.
 - b) Valitse VPN-asiakasohjelman kohdalla avattavasta valikosta **Mukautettu**.
 - c) Kirjoita pakettitunnukseksi com.fsecure.mp.ucf.
 - d) Pidä Lukitustilan asetuksena oletusarvo: **Ei määritetty**.
 - e) Valitse **Seuraava**.
9. Valitse **Tehtävät-välilehden** Sisällytetyt **ryhmät** -kohdasta **Lisää kaikki käyttäjät** ja valitse **Seuraava**.
Tarkista + luo -välilehti avautuu.
10. Tarkista tiedot ja valitse **Luo**.

Laitemäärittäiskäytäntö luotiin ja määritettiin.

Seuraavaksi sinun on asennettava sovellus Android-laitteelle.

Käyttöoikeuksien myöntäminen sovellukselle

Ohjeet luvan myöntämiseen sovellukselle hiljaiseen aktivointiin.

1. Kirjaudu sisään Microsoft Endpoint Manager järjestelmänvalvojakeskukseen.
2. Valitse **Sovellukset > Sovelluksen määrittäiskäytännöt > Lisää > hallittuja laitteita**.

Huomautus: Voit lisätä joko hallinnoituja laitteita tai hallinnoituja sovelluksia. Lisätietoja on kohdassa **Sovellukset, jotka tukevat sovellusmäärittäisiä**.

3. Kirjoita **Perustiedot** -sivulle seuraavat tiedot:
 - Nimi - portaalissa näkyvän profiilin nimi
 - Kuvaus - profiilin kuvaus, joka näytetään portaalissa
 - Laitteen rekisteröintityyppi - oletusvaihtoehto on **Hallitut laitteet**
4. Valitse **Alustat** -kohdasta **Android Enterprises**.
5. Valitse **Kohdistettu sovellus** -kohdan vierestä **Valitse sovellus**.
Liitetty sovellus -ruutu tulee näkyviin.
6. Valitse **Liitetty sovellus** -ruudusta hallittu sovellus, jonka haluat liittää määrittäiskäytäntöön, ja valitse **OK**.

7. Valitse **Seuraava** > **Lisää**.

Lisää käyttöoikeudet -ruutu avautuu.

8. Valitse käyttöoikeudet, jotka haluat ohittaa.

Huomautus: Myönnetyt käyttöoikeudet ohittavat valittujen sovellusten oletusarvoisen sovelluksen käyttöoikeuskäytännön.

9. Aseta kullekin luvalla käyttöoikeustila. Voit valita seuraavista vaihtoehtoista:

- Kehote - Pyydä käyttäjää hyväksymään tai hylkäämään.
- Automaattinen myöntö - Hyväksyy automaattisesti ilmoittamatta käyttäjälle.
- Automaattinen hylkäys - Hylkää automaattisesti ilmoittamatta käyttäjälle.

10. Valitse **Tarkista + tallenna**.

Asetuksesi tallennetaan.

B.5 Käyttöönotto IBM MaaS360 MDM:llä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android- ja iOS-laitteissa IBM MaaS360:n avulla.

B.5.1 Android Enterprise -käyttöönotto IBM MaaS360:n MDM:ssä

Tässä luvussa on ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android Enterprise -kontekstissa IBM MaaS360 MDM:n avulla.

Android Enterprise -asetusten määrittäminen

Ohjeet Android Enterprise -asetusten määrittämiseen.

Huomautus: Ennen kuin rekisteröit laitteet, määritä Android Enterprise -asetukset.

1. Valitse IBM MaaS360 -hallintaportalissa **Asetukset** > **Palvelut**.
2. Valitse **Mobile Device Management**, **Enable Android Enterprise Solution Set Enable via Managed Google Play Accounts (no G-suite for business)** -kohdassa **tämä**.
Vahvista Androidin hallintoitujen Google Play -tilien käyttöönotto ikkuna.
3. Valitse **Ota käyttöön**.
4. Kirjoita salasanasasi **Turvataarkastus**-ikkunaan ja valitse **Vahvista**.
Google Play tulee näkyviin.
5. Valitse **Tuo Android to Work** -sivulla **Aloita** ja tee seuraavaa:
 - a) Kirjoita yrityksesi nimi ja valitse **Seuraava**.
 - b) Kirjoita yhteystietosivulle nimesi, sähköpostiosoitteesi ja puhelinnumerosi (valinnainen), valitse **Olen lukenut ja hyväksynyt Managed Google Play -sopimuksen** ja valitse sitten **Vahvista**.
6. Valitse **Viimeistelet rekisteröityminen**.
Asennus on valmis.

Seuraavaksi sinun on lisättävä WithSecure Elements Mobile Protection -sovellus.

WithSecure Elements Mobile Protection -sovelluksen lisääminen

Ohjeet WithSecure Elements Mobile Protection -sovelluksen lisäämiseen IBM MaaS360 MDM:ään.

1. Valitse IBM MaaS360 -hallintaportalissa **Sovellukset** > **Luettelo**.
2. Valitse Sovellusluettelo-sivulta **Lisää** > **Android** > **Google Play-sovellus**.
3. Kirjoita hakuruutuun WithSecure Elements Mobile Protection.
4. Valitse ensin **WithSecure Elements Mobile Protection** ja sitten **Valitse**.
5. Lisää sovellus valitsemalla Hyväksy lupa -ikkunassa **Hyväksy**.

Seuraavaksi sinun on määritettävä sovelluksen asetukset.

Sovelluksen määrittäminen

Ohjeet WithSecure Elements Mobile Protection -sovelluksen kokoonpanon määrittämiseen.

- Valitse Lisää Google Play -sovellus -ikkunan **Määitykset** -välilehdeltä Määritä **sovellusasetukset** ja toimi seuraavasti:
 - Kirjoita Rekisteröinti-kenttään tuotteen tilausavain.
Huomautus: Löydät WithSecure Elements Mobile Protection -tilausavaimen WithSecure Elements Security Center kohdasta **Endpoint Protection** > **Subscriptions**.
 - Kirjoita etu- ja sukunimesi niitä vastaaviin kenttiin (valinnainen).
 - Kirjoita Valenimi-kenttään (valinnainen) vaihtoehtoinen nimi.
 - Kirjoita sähköpostiosoitteesi Sähköpostiosoite-kenttään (valinnainen)
 - Kirjoita Ympäristö-kenttään (valinnainen) 2.
- Valitse **Lisää**.
Turvallisuustarkistus-ikkuna tulee näkyviin.
- Kirjoita salasanasasi ja valitse **Vahvista**.
Sovellus on lisätty.

Sovelluksen jakelu

Ohjeet sovelluksen jakamiseen valituille kohteille.

- Valitse Sovellusluettelo-sivun **WithSecure Elements Mobile Protection** -kohdassa **Näytä**.
- Valitse näkyviin tulevalta sivulta oikeasta yläkulmasta **Jaa**.
Jaa sovellus -ikkuna tulee näkyviin.
- Valitse avattavasta Kohde-valikosta jokin seuraavista vaihtoehdoista:
 - Määrätty laite
 - Ryhmä
 - Kaikki laitteet
- Valitse **Jaa**.

B.6 Käyttöönotto Ivanti Endpoint Managementin avulla

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Ivanti Endpoint Management (aiemmin MobileIron Cloud MDM) kanssa Android- ja iOS-laitteisiin.

B.6.1 Android-sovelluksen ottaminen käyttöön Ivanti Endpoint Managementin avulla

Ohjeet Android-sovelluksen ottamisesta käyttöön Ivanti Endpoint Managementin avulla.

Voit määrittää WithSecure Elements Mobile Protection -sovelluksen manuaalisesti lisäämällä tilausavaimen ja muut muuttujat Ivanti Endpoint Managementin avulla valitsemalla **Sovellusmääitykset Hallitut Android-määitykset**.

WithSecure Elements Mobile Protectionin Android-sovelluksen lisääminen Ivanti Endpoint Managementiin

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen Ivanti Endpoint Management MDM:ään.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
- Määritä sovellus ja määritä se WithSecuren tarjoamalla tilausavaimella.

Android-sovelluksen lisääminen Ivanti Endpoint Management:

1. Siirry Ivanti Endpoint Management MDM -hallintaportalissa **Apps**-sivulle ja valitse **Add**.
2. Valitse valikosta **Google Play**.
3. Etsi WithSecure Elements Mobile Protection.
4. Valitse sovellus ja napsauta sitten **Valitse**.
5. Tarkista, että sovellusluokka on oikea. Valinnaisesti voit lisätä sovelluksen tiedot Kuvaus-ruutuun.
6. Valitse **Seuraava**.
7. Valitse, haluatko delegoida sovelluksen kaikkiin tiloihin, ja valitse **Seuraava**.
8. Valitse haluamasi jakeluryhmä ja paina **Seuraava**.

Seuraavaksi sinun on määritettävä sovelluksen asetukset.

Android-sovellusten hallinnan määrittäminen manuaalisesti

Ohjeet Android-sovellusten hallinnan manuaaliseen määrittämiseen.

1. Valitse **App Configurations** > **Managed Configurations for Android** -kohdassa pluskuvake. **Kokoonpanon asetukset** -sivu tulee näkyviin.
2. Toimi seuraavasti:
 - a) Anna kokoonpanolle nimi.
 - b) Valitse **Managed Configurations** -kohdassa **Automaattinen käynnistys asennuksen yhteydessä**.
 - c) Varmista, että **Vain push-asetukset, joiden arvot on määritetty** on valittuna.
 - d) Kirjoita tilausavain **kohdan Rekisteröintiavain** viereen.

Huomautus: Löydät tilausavaimen WithSecure Elements Security Center.
 - e) Kirjoita Sähköpostiosoite-kenttään arvoksi \${userEmailAddress}.
 - f) Valitse **Hallinnoi käyttöoikeuksia**.
Valitse käyttöoikeudet -ikkuna avautuu.
 - g) Valitse kaikki vaihtoehdot ja napsauta sitten **Valitse**.
 - h) Selaa **Suorituksen aikaiset käyttöoikeudet** -kohdassa kaikki avattavat valikot, valitse **Automaattinen myöntäminen** ja valitse sitten **Seuraava**.
Sovelluskokoonpano -sivu tulee näkyviin
3. Valitse **Asenna laitteeseen -kohdan** vieressä pluskuvake ja toimi seuraavasti:
 - a) Anna nimi konfiguraatiolle.
 - b) Ota **Laitteen asennusasetukset** käyttöön.
 - c) Valitse **Sovelluspäivitystila** -vaihtoehto ja valitse avattavasta valikosta **Korkea prioriteetti**.
 - d) Valitse **Seuraava**.
Sovelluskokoonpano -sivu tulee näkyviin.
4. Valitse **Promootio** vierestä pluskuvake ja toimi seuraavasti:
 - a) Anna nimi konfiguraatiolle.
 - b) Valitse **Suosittelun luettelo**.
 - c) Valitse **Seuraava**.
5. Valitse **Delegated Device Permissions** -kohdan vieressä oleva pluskuvake ja toimi seuraavasti:
 - a) Anna nimi konfiguraatiolle.
 - b) Valitse **Hallinnoi sovellusmäärittämiä**.
 - c) Valitse **Seuraava**
6. Valitse **Valmis**.

WithSecure Elements Mobile Protection on lisätty sovellusluetteloon.

B.6.2 Android Enterprise -käyttöönotto Ivanti Endpoint Managementin kanssa

Tässä luvussa on ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android Enterprise -ympäristössä Ivanti Endpoint Management avulla.

WithSecure Elements Mobile Protection -sovelluksen lisääminen

Ohjeet WithSecure Elements Mobile Protection -sovelluksen lisäämiseen Ivanti Endpoint Managementiin.

1. Valitse Ivanti Endpoint Management -hallintaportalissa **Admin > Google > Android Enterprise**. Android Enterprise -sivu tulee näkyviin.
2. Valitse **Aloita suositeltu asennus** -kohdassa **Valtuuta Google**.
3. Valitse **Viimeistele rekisteröityminen**.
4. Valitse **Sovellukset > Sovellusluettelo** ja sitten **+ Lisää**. Ohjattu sovelluksen lisäämistoiminto käynnistyy.
5. Valitse Valitse-näkymän avattavasta valikosta **Google Play**.
6. Kirjoita Search the Google Play store... -ruutuun WithSecure Elements Mobile Protection.
7. Valitse sovellus ja valitse sitten **Hyväksy > Hyväksy**.
8. Valitse **Valmis > Valitse > Seuraava**.
9. Valitse Kuvaus-näkymässä **Seuraava**.
10. Valitse Edustaja-näkymässä **Seuraava**.
11. Valitse jakelunäkymästä haluamasi vaihtoehto ja valitse **Seuraava**.
12. Valitse määrittämisnäkymässä **Managed Configurations for Android -kohdan** vieressä oleva pluskuvake. Kokoonpanon asetukset -sivu tulee näkyviin.
13. Kirjoita Nimi-kenttään nimi ja toimi kohdassa **Managed Configurations**:
 - a) Kirjoita tuotteen tilauskoodi Rekisteröintiavain-kenttään.
Huomautus: Löydät WithSecure Elements Mobile Protection -tilausavaimen WithSecure Elements Security Center **kohdasta > Hallintatilaukset**.
 - b) Kirjoita etu- ja sukunimesi niitä vastaaviin kenttiin (valinnainen).
 - c) Kirjoita Valenimi-kenttään (valinnainen) vaihtoehtoinen nimi.
 - d) Kirjoita sähköpostiosoitteesi Sähköpostiosoite-kenttään (valinnainen).
 - e) Kirjoita Ympäristö-kenttään (valinnainen) 2.
14. Valitse **Jaa tämä sovelluskokoonpano** -kohdassa **Kaikki, joilla on sovellus** ja valitse sitten **Seuraava**.
15. Valitse Sovelluskokoonpanot-sivulta **Valmis**.
WithSecure Elements Mobile Protection näkyy **sovellusluettelosivulla**.

B.7 Käyttöönotto Miradore MDM:llä

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android- ja iOS-laitteissa Miradore MDM:n avulla.

Huomautus: Nämä ohjeet eivät sisällä käyttäjien ja laitteiden luomista ja määrittämistä koskevia tietoja.

B.7.1 Android-sovelluksen lisääminen Miradoren MDM:ään

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen Miradore MDM:ään.

Miradoren MDM voi toimittaa lisenssitiedot sovellukseen joko XML-tiedostona tai Google Play -kaupan Install Referrer -palvelulla. Valitse haluamasi menetelmä, ennen kuin aloitat sovelluksen lisäämisen MDM:ään.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
- Määritä sovellus ja määritä se WithSecuren tarjoamalla tilausavaimella.

1. Valitse Miradore-hallintaportaalin vasemmassa ruudussa olevasta valikosta **Hallinta** > **Sovellukset**.

2. Valitse oikealla olevasta **Toiminnot**-valikosta **Lisää** > **Android-sovellus**.

Ohjattu Lisää sovellus -toiminto käynnistyy.

3. Tee ohjatussa Lisää sovellus -toiminnossa seuraavaa:

a) Valitse vaiheessa 1 **Google Play -kauppa** ja sitten **Seuraava**.

b) Anna vaiheessa 2 seuraavat tiedot:

- Nimi: WithSecure Elements Mobile Protection for Android
- Paketin nimi: com.fsecure.mp.ucf
- Kuvaus: Kirjoita kuvaus, jota haluat käyttää.
- Ilmoitus käyttäjälle: Anna kaikki tiedot, jotka haluat käyttäjien näkevän.
- Lisää pikakuvake aloitusnäyttöön: Luo pikakuvake sovellukseen valitsemalla tämä.

c) Lisää seuraavat tiedot **Asennusviittaaja**-kenttään:

- Jos haluat käyttää Install Referrer -palvelua lisenssitietojen toimittamiseen, käytä asennusviittausmerkkijonoa, joka löytyy WithSecure Elements -palvelusta. Etsi **Google Play -lataus-URL-osoite**, jossa on WithSecure Elements Mobile Protection -aktivointimerkkijono. Kopioi merkkijonon jälkimmäinen osa alkaen utm-mediumista. Jos haluat lähettää sovellukseen lisätietoja, voit lisätä aktivointimerkkijonoon ylimääräisiä elementtejä.

4. Valitse **Luo**.

5. Varmista vaiheessa 4, että tiedot ovat oikein, ja valitse **Sulje**.

B.8 Käyttöönotto Samsung Knoxin avulla

Ohjeet WithSecure Elements Mobile Protection -sovelluksen käyttöönottoon Android-laitteissa Samsung Knoxin avulla.

Huomautus: Ohjeet eivät sisällä käyttäjien ja laitteiden luomista ja määrittämistä koskevia tietoja.

B.8.1 Android-sovelluksen käyttöönotto Samsung Knoxin kanssa

Ohjeet Android-sovelluksen käyttöönottoon Samsung Knoxin avulla.

Android-sovelluksen lisääminen Samsung Knoxiin

Ohjeet WithSecure Elements Mobile Protectionin Android-sovelluksen lisäämiseen Samsung Knoxiin.

Ennen kuin integroit WithSecure Elements Mobile Protectionin MDM-järjestelmään, varmista, että seuraavat edellytykset täyttyvät:

- Olet rekisteröinyt päätelaitteesi
- Olet asettanut profiilille käytäntörajoituksia

Huomautus: WithSecure ei tarjoa profiilien ja käytäntöjen tukea tai ohjeita, ellei toisin mainita.

- Internet-yhteys VPN-yhteyden ja tiedostojen käyttöoikeuksien määrittämistä varten
- Voimassa oleva WithSecure Elements Mobile Protection -tilaus

Integraatio koostuu seuraavista:

- Lisää sovellus MDM:hen Google Play Kaupasta
- Määritä sovellus ja määritä se WithSecuren tarjoamalla tilausavaimella.

Android-sovelluksen lisääminen Samsung Knoxiin:

1. Kirjautu Samsung Knox -konsoliin.
2. Valitse **Sovellus**.
Sovellus-sivu tulee näkyviin.
3. Valitse **Lisää**.
4. Valitse Valitse sovellustyyppi -näytöstä **Android-alusta > julkinen Managed Google Play** ja valitse sitten **OK**.
5. Kirjoita Lisää sovellus -sivulle WithSecure Elements Mobile Protection ja etsi sovellus.

Huomautus: Jos haluat muuttaa valitun alustan maata, valitse **Aseta maa -kohdan** vieressä oleva valintaruutu ja valitse sitten maa.

6. Valitse hakutuloksista ensin sovellus, jonka haluat lisätä, ja **valitse** sitten .
7. Muokkaa tarvittaessa seuraavia tuotuja tietoja:
 - Nimi - kirjoita sovelluksen nimi
 - Luokka - valitse sovelluksen luokka. Valitsemalla **Hallinnoi luokkaa** voit lisätä tai muokata sovellusluokkia.
 - Kuvaus - anna sovelluksen kuvaus
8. Jatka valitsemalla jokin seuraavista vaihtoehdoista:
 - Tallenna tiedot valitsemalla **Tallenna ja määritä** ja jatka sovelluksen määrittämistä valitsemalla **Jatka**.
 - Tallenna tiedot ja palaa sovellusluetteloon valitsemalla **Tallenna**. Voit määrittää tämän sovelluksen myöhemmin.

Android-sovelluksen määrittäminen ja määrittäminen

Ohjeet Android-sovelluksen liittämiseen ja määrittämiseen.

Tärkeää: Kun määrität profiilin pääorganisaatiolle, sen aliorganisaatiot perivät profiilin. Alaorganisaatiot eivät kuitenkaan peri sovelluksia ja sisältöä.

Android-sovelluksen määrittäminen ja määrittäminen Samsung Knoxissa:

1. Valitse **Sovellus**.
Sovellus-sivu tulee näkyviin.
2. Valitse **WithSecure Elements Mobile Protection** ja valitse sitten **Liitä**.
Määritä sovellus -sivu tulee näkyviin.
3. Määritä seuraavat tehtäväasetukset:
 - Kohdelaite – voit valita yhden seuraavista vaihtoehdoista: **Android Enterprise**, **Android Legacy** tai **Android Enterprise + Legacy**.
 - Asennusalue – näyttää määritellyn asennusalueen
 - Asennustyyppi - valitse yksi käytettävissä olevista vaihtoehdoista:
 - **Manuaalinen** - laitteen käyttäjät voivat asentaa sovelluksen manuaalisesti
 - **Automaattinen (Removable)** - määrittää sovelluksen asennettavaksi automaattisesti. Laitteen käyttäjät voivat myös poistaa sovelluksen manuaalisesti.
 - **Automaattinen (ei irrotettava, vain Android Management API)**
 - Automaattinen käynnistys asennuksen jälkeen (ei-Android Management API) - voit määrittää sovelluksen käynnistymään heti asennuksen jälkeen.
 - Automaattinen päivitysmalli – käytettävissä olevat vaihtoehdot ovat **Oletuspäivitys**, **Korkea prioriteetti** ja **Lykätty (90 päivää)**.
4. Valitse Managed Configuration -kohdan vierestä **Aseta kokoonpano** ja toimi seuraavasti:
 - Kirjoita Managed configuration -kenttään kuvaava nimi, esimerkiksi Työ.

- Kirjoita Rekisteröintiavain-kenttään WithSecure Elements Mobile Protection -tilausavain.
- Kirjoita Alias-kenttään seuraava: \$käyttäjänimi\$.
- Kirjoita Sähköpostiosoite-kenttään \$emailaddress\$.
- Kirjoita Ympäristö-kenttään 2.

Huomautus: WithSecure Elementsiin rekisteröidyt laitteet näytetään sähköpostiosoitteella, kun määrität arvon \$ emailaddress\$.

5. Tallenna muutokset valitsemalla **Tallenna**.
6. Valitse Kohde-kohdassa ryhmä, jolle haluat määrittää sovelluksen.