

MONIVAIHEINEN TUNNISTAUTUMINEN



WINNOVA
LÄNSIRANNIKON KOULUTUS OY

Sisällys

Kuvaus.....	2
Miten monivaiheinen tunnistautuminen toimii käytännössä?.....	2
Monivaiheisen tunnistautumisen pika-ohje	2
Yksityiskohtaiset ohjeet	3
Ensikirjautuminen ja puhelinnumeron rekisteröinti.....	3
Tunnistautuminen tekstiviestillä.....	6
Turvatiedon lisääminen	7
Turvatieto - Microsoft Authenticator sovellus.....	7
Turvatieto - Muut sisäänkirjautumismenetelmät.....	11
Oletusarvon mukainen sisäänkirjautumismenetelmä	11
Intune - Salli organisaationi hallinta laitettani	13
Usein kysytyt kysymykset	14
Miksi minua pyydetään antamaan puhelinnumeroni uudelleen?.....	14
Puhelinnumeron vaihtuminen	14
Puhelimeni ei ole käytettävissä	14
Voinko käyttää monivaiheista tunnistautumista usealla puhelimella?	14
Oman puhelimen tietoturva – Lukitusnäyttö	14
Itslearning ympäristön ongelmat.....	14
PowerAutomate työkulun ongelmat	15
Puhelulla tunnistautuminen	15

Kuvaus

Monivaiheisen tunnistautumisen tarkoitus on varmentaa henkilön identiteetti käyttämällä monta eri tunnistautumismenetelmää. Tällä tavalla pyritään estämään käyttäjätilin luvaton käyttäminen.

Miten monivaiheinen tunnistautuminen toimii käytännössä?

Monivaiheista tunnistautumista käytetään silloin, kun verkkoyhteys muodostetaan WinNovan ulkopuolisesta verkosta käsin (esim. omasta puhelimesta, kotiverkosta, hotellista yms.) WinNovan pilvipalveluihin, kuten Teams, Sharepoint, OneDrive ja Outlook.

WinNovan toimipaikoissa eli ns. sisäverkossa vahvistusta ei pyydetä.

Tunnistautuminen voidaan tehdä esim. puhelun kautta, tekstiviestikoodilla tai vaikka puhelimeen asennettavan Microsoft Authenticator -apin kautta.

Monivaiheisen tunnistautumisen pika-ohje

- Lisätäksesi uuden kirjautumismenetelmän, siirry selaimella Oma tili sivulle: <https://myaccount.microsoft.com/> ja kirjaudu sisään WinNovan tunnuksilla.
- Lisää pyydettäessä puhelinnumerosi.
- **Oma tili** sivulta etsi kohta **Turvatieto** ja klikkaa joko siitä tai kohdasta **päivitä tiedot**.
- Täältä voit lisätä uuden kirjautumismenetelmän, klikkaamalla **+ Lisää kirjautumismenetelmä** kohtaa.
- Valitse haluamasi kirjautumismenetelmä, (esim. Authenticator-sovellus) ja paina **Lisää**.
- Seuraa ohjeita ja viimeistele kirjautumismenetelmä.
- Samalta sivulta voit muokata kirjautumismenetelmiä, esim. puhelinnumeron vaihtuessa.

- **HUOM!** On suositeltavaa, että on käytössä kaksi kirjautumistapaa (esim. puhelinnumero ja Authenticator). Vaikka numerosi olisi jo vaihtunut, pystyt vielä tällä tavalla vahvistamaan tunnistautumisen Authenticator sovelluksella ja käydä lisäämässä uuden numeron jälkikäteen.

Katso myös kohta:

- [Voinko käyttää monivaiheista tunnistautumista usealla puhelimella?](#)
- Saatat myös nähdä koneellasi ilmoituksen, jossa pyyntö **Salli organisaationi hallita laitettani**. Tästä lisätietoja kohdassa [Intune - Salli organisaationi hallinta laitettani](#)

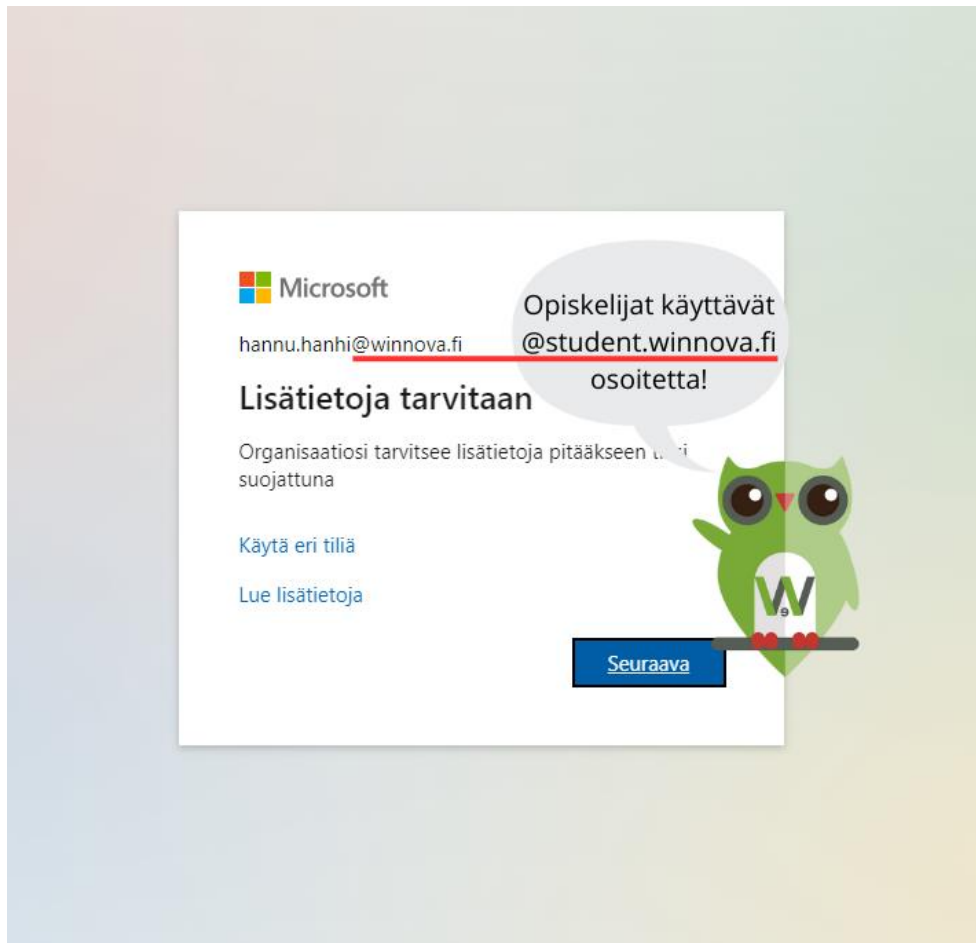
Jos kaipaat lisätietoja ja yksityiskohtaisemmat ohjeet jatka tämän dokumentin lukemista.

Yksityiskohtaiset ohjeet

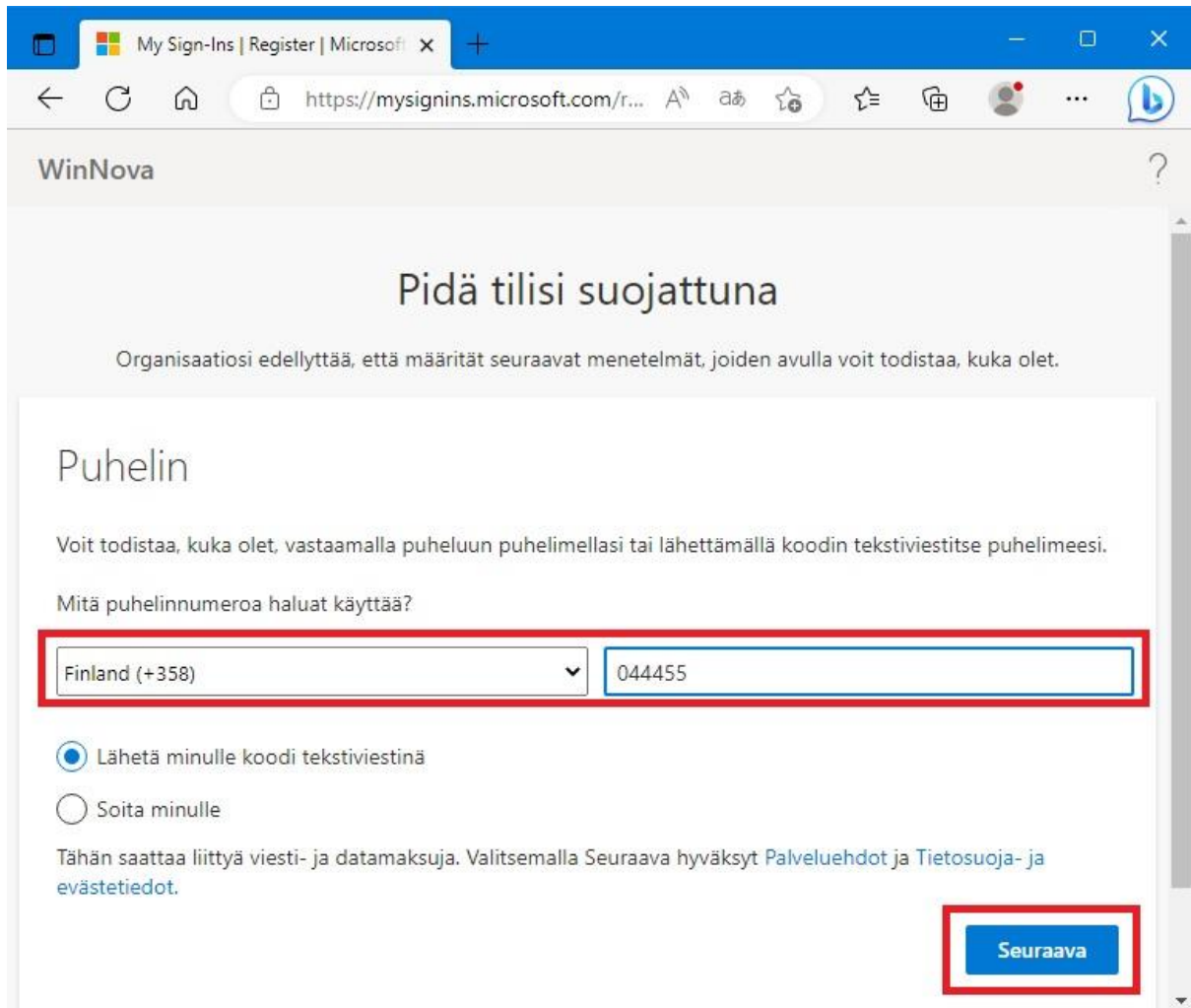
Ensikirjautuminen ja puhelinnumeron rekisteröinti

Ensimmäisen kirjautumisen yhteydessä sinua pyydetään rekisteröimään puhelinnumerosi, jota voidaan käyttää monivaiheiseen tunnistautumiseen. Jos olet tehnyt jo tämän voit siirtyä kohtaan [Turvatiedon lisääminen](#).

Kun kirjaudut sisään esim. <https://myaccount.microsoft.com/> osoitteeseen sinua pyydetään syöttämään käyttäjätunnukseksi. Kun olet kirjautunut näet tämän ikkunan, jossa sinulta pyydetään lisätietoja. Paina **Seuraava** painiketta:



Valitse **Maa tai alue** kohdasta **Finland (+358)** ja lisää työpuhelinnumerosi. Tämän jälkeen valitse kohta **Lähetä minulle koodi tekstiviestinä** ja paina **Seuraava**:



The screenshot shows a web browser window with the URL <https://mysignins.microsoft.com/r...>. The page title is "WinNova" and the main heading is "Pidä tilisi suojattuna". Below the heading, it says "Organisaatiosi edellyttää, että määrität seuraavat menetelmät, joiden avulla voit todistaa, kuka olet." The section is titled "Puhelin" and contains the text "Voit todistaa, kuka olet, vastaamalla puheluun puhelimellasi tai lähettämällä koodin tekstiviestitse puhelimeesi." and "Mitä puhelinnumeroa haluat käyttää?". There is a dropdown menu showing "Finland (+358)" and a text input field containing "044455". Below these are two radio buttons: "Lähetä minulle koodi tekstiviestinä" (selected) and "Soita minulle". At the bottom right, there is a blue button labeled "Seuraava".

Lisää tekstiviestinä saatu koodi kenttään ja paina **Seuraava**:



The screenshot shows the same "Puhelin" section. It now displays "Lähetimme juuri kuusinumeroisen koodin numeroon +358 044455" and ". Anna alla oleva koodi." Below this is a text input field containing "999999". There is a link "Lähetä koodi uudelleen" below the input field. At the bottom right, there are two buttons: "Edellinen" and "Seuraava".

Saat vielä vahvistuksen, kun tekstiviesti on vahvistettu ja puhelin on rekisteröity onnistuneesti. Paina **Seuraava**:

Puhelin

 Tekstiviesti vahvistettiin. Puhelimesi rekisteröinti onnistui.


[Seuraava](#)

Ja viimeiseksi paina **Valmis** painiketta:

Onnistui!

Hyvää työtä! Olet määrittänyt suojaustietosi onnistuneesti. Jatka sisäänkirjautumista valitsemalla Valmis.

Oletusarvon mukainen sisäänkirjautumismenetelmä:

 Puhelin
+358 044455

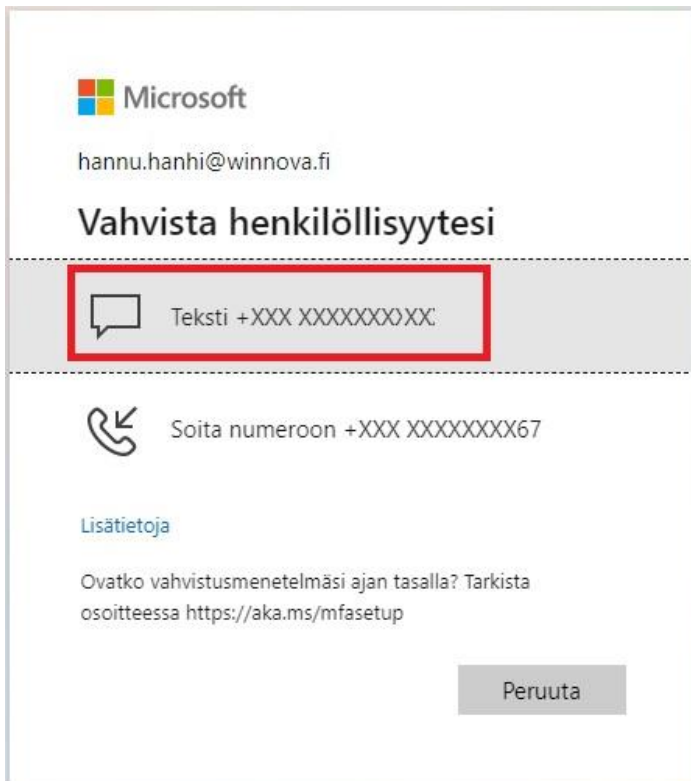
[Valmis](#)

Nyt kirjautuminen toimii käyttämällä tekstiviestiä tai puhelua monivaiheisessa tunnistautumisessa.

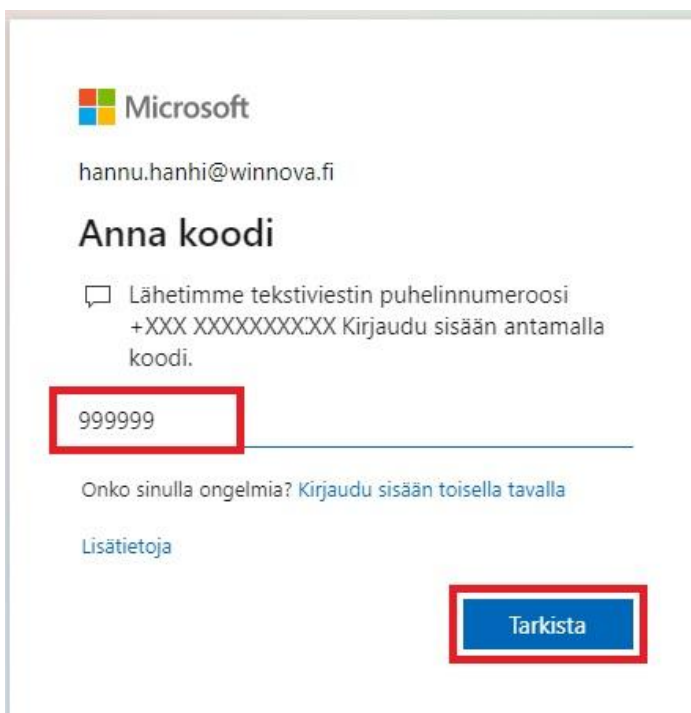
Alempana vielä esimerkki miten tunnistaudutaan tekstiviestillä.

Tunnistautuminen tekstiviestillä

Kun kirjaudut sisään ulkoverkosta, sinua pyydetään vahvistamaan henkilöllisyytesi. Jos valitset Teksti +XXX XXXXXXXX kohdan sinulle lähetetään koodi tekstiviestinä. Alla on kuvia siitä miltä se näyttää selaimessa:



Syötä saamasi koodi ja paina **Tarkista** painiketta, jolloin pääset kirjautumaan:



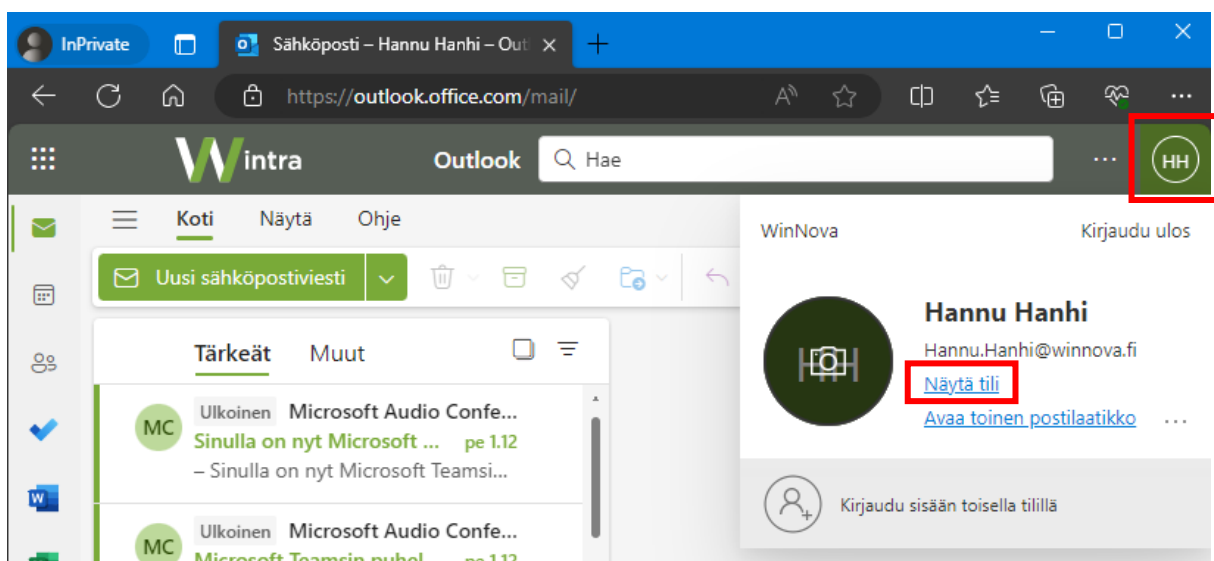
Turvätiedon lisääminen

Tekstiviestien käyttäminen monivaiheiseen tunnistautumiseen on toimiva ratkaisu, mutta sen lisäksi saattaa olla tarvetta lisätä muita numeroita tai käyttää Microsoft Authenticator sovellusta.

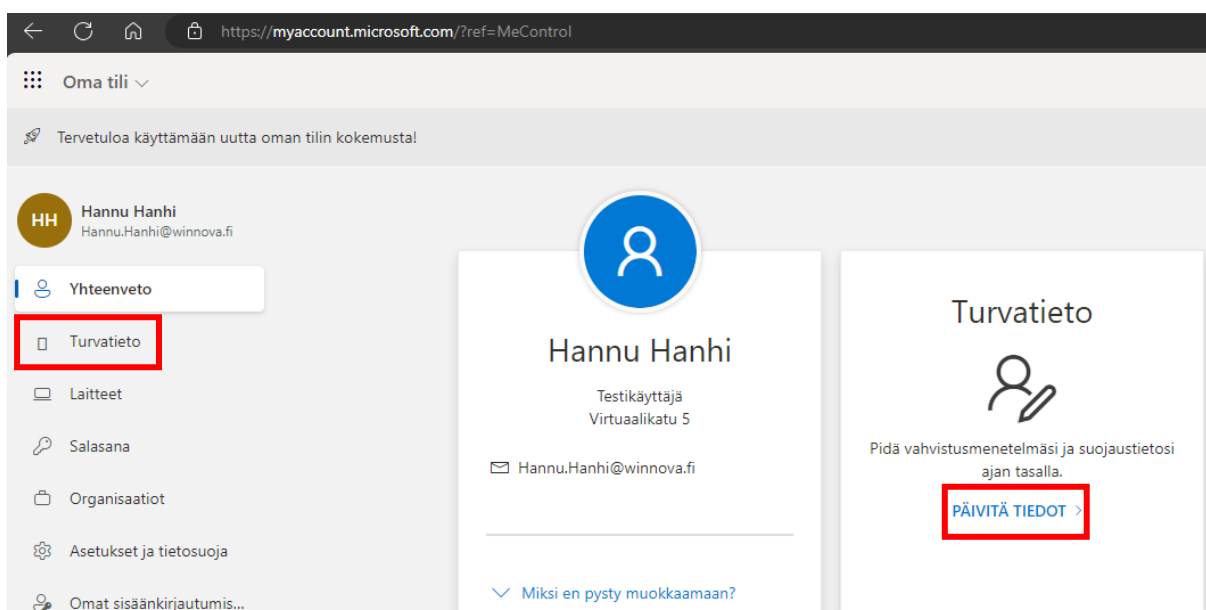
Turvatieto - Microsoft Authenticator sovellus

Microsoft Authenticator sovelluksen käyttöönottoa varten sinun täytyy mennä **Oman tili** -> **Turvatieto** sivuille. Pääset sinne menemällä osoitteeseen <https://myaccount.microsoft.com/> tai seuraamalla alla olevaa ohjetta.

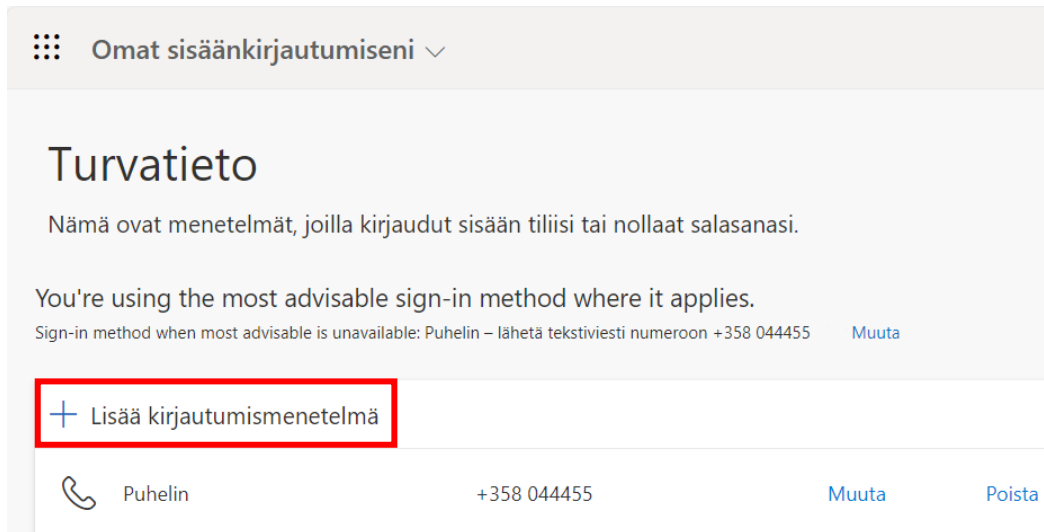
Kun olet kirjautunut mihin tahansa M365 palveluun, esim. Outlookiin (<https://outlook.office.com/mail/>) klikkaa oikeassa ylä laidassa olevia nimikirjaimia eli **Tilin hallinta** kuvaketta ja sitten valitse sieltä **Näytä tili**:



Täällä valitse **Turvatieto** tai **päivitä tiedot** kohta:



Nyt olet päässyt **Turvatieto** kohtaan, josta pystyt lisäämään itsellesi uusia kirjautumismenetelmiä. Klikkaa + **Lisää kirjautumismenetelmä** kohtaa:



Omat sisäänkirjautumiseni ▾

Turvatieto

Nämä ovat menetelmät, joilla kirjaudut sisään tiliisi tai nollaat salasanasasi.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Puhelin – lähetä tekstiviesti numeroon +358 044455 [Muuta](#)

+ Lisää kirjautumismenetelmä

Puhelin +358 044455 [Muuta](#) [Poista](#)

Valitse alasvetovalikosta **Authenticator-sovellus** ja paina **Lisää** painiketta:



Lisää menetelmä

Minkä menetelmän haluat lisätä?

Authenticator-sovellus ▾

[Peruuta](#) [Lisää](#)

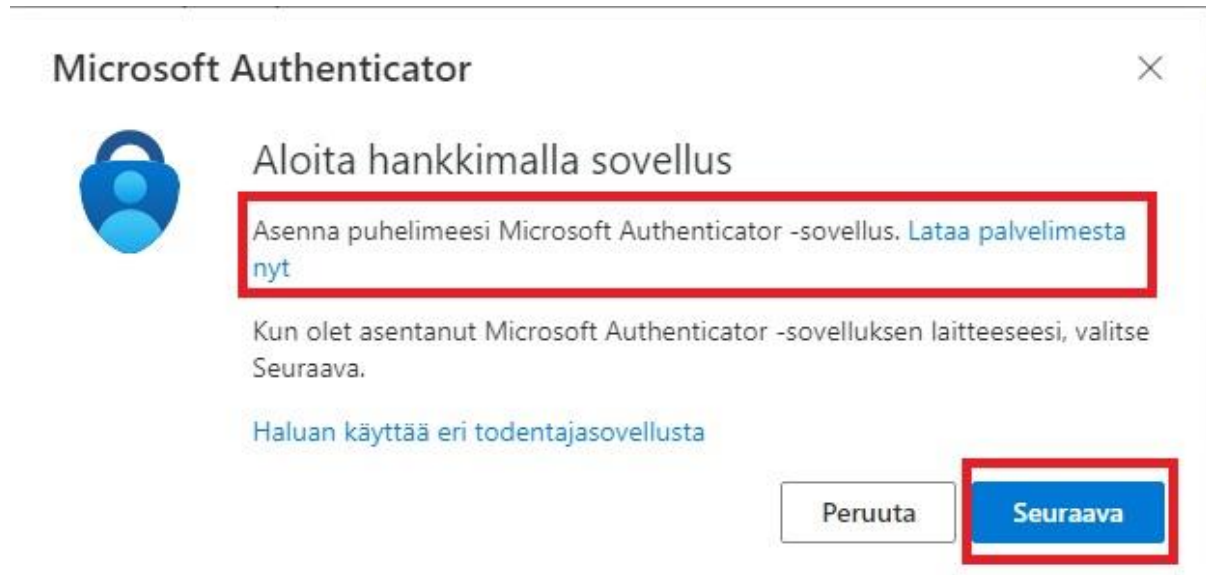
Tässä vaiheessa sinua pyydetään asentamaan Microsoft Authenticator -sovellus puhelimeesi. Ohjeet on jaoteltu siihen mitä tehdään puhelimesta ja selaimessa.

Puhelimesta

Sinun tulee avata puhelimestasi sovelluskauppa (esim. Google Play tai App Store) ja sieltä etsit ja lataat **Microsoft Authenticator** sovelluksen. Kun ohjelma on asennettu, avaa se puhelimestasi.

Selaimessa

Paina selaimessa **Seuraava** painiketta:



Microsoft Authenticator

Aloita hankkimalla sovellus

Asenna puhelimeesi Microsoft Authenticator -sovellus. Lataa palvelimesta nyt

Kun olet asentanut Microsoft Authenticator -sovelluksen laitteeseesi, valitse Seuraava.

Haluan käyttää eri todentajasovellusta

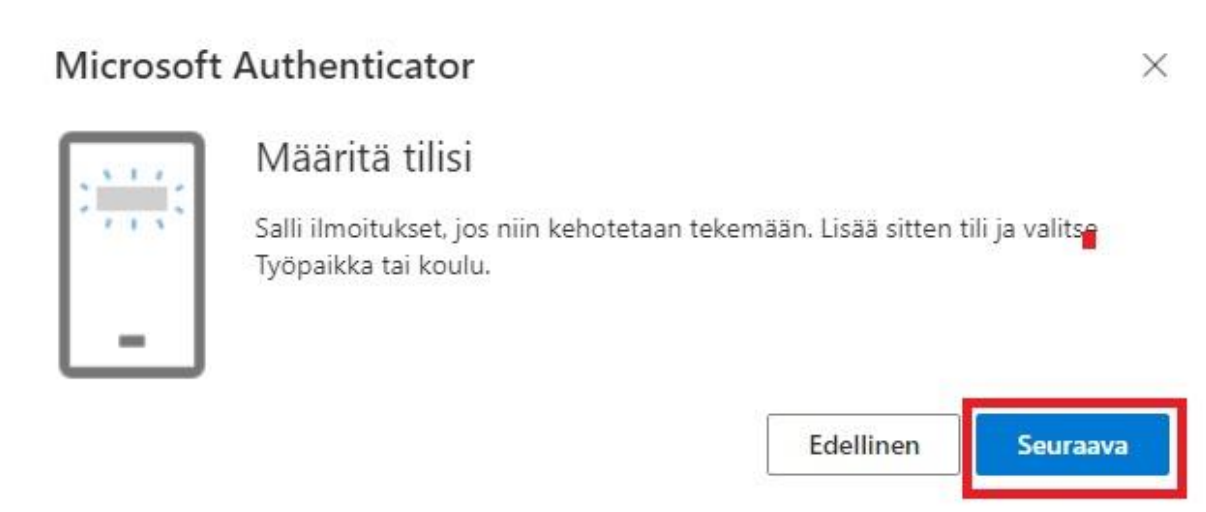
Peruuta Seuraava

Puhelimessa

Kun sinulla on puhelimesa Authenticator sovellus auki klikkaa ylhäällä olevaa + Kuvaketta, josta lisätään tili. Valitse sieltä kohta **Työ- tai koulutili**.

Selaimessa

Nyt voit painaa selaimessa **Seuraava** painiketta:



Microsoft Authenticator

Määritä tilisi

Salli ilmoitukset, jos niin kehoitetaan tekemään. Lisää sitten tili ja valitse Työpaikka tai koulu.

Edellinen Seuraava

Puhelimessa

Nyt puhelimen Authenticatorissa valitse **Skanna QR-koodi** ja skanna selaimessa näkyvä QR-koodi. Mikäli puhelin pyytää lupaa käyttää sovellusta tms. salli ne.

Selaimessa

Paina **seuraava** painiketta.

Microsoft Authenticator



Skannaa QR-koodi

Skannaa QR-koodi Microsoft Authenticator -sovelluksen avulla. Tämä yhdistää Microsoft Authenticator -sovelluksen tiliisi.

Kun olet skannannut QR-koodin, valitse Seuraava.



Eikö kuvaa voi skannata?

Edellinen

Seuraava

Puhelimessa

Sovellus lähettää tässä vaiheessa hyväksyntäilmoituksen puhelimeesi. Jos sovellus on auki, se näkyy suoraan näytöllä tai sitten mahdollisesti puhelimen ylälaidassa push ilmoituksena tai puhelimen ilmoituksissa. Klikkaa sitä ja hyväksy kirjautuminen.

Selaimessa

Kun kirjautuminen on hyväksytty paina **Seuraava**:

Microsoft Authenticator



Kokeillaan sitä

Hyväksy ilmoitus, jonka lähetämme sovellukseesi.

Edellinen

Seuraava

Nyt kirjautuminen onnistuu myös Authenticator sovelluksen avulla. Seuraavan kerran kirjaudut ja sinua pyydetään tunnistautumaan, voit valita Authenticator sovelluksen.

Turvatieto - Muut sisäänkirjautumismenetelmät

Voit lisätä myös muita kirjautumismenetelmiä, mikäli niin haluat. Oletuksena lisättävissä on Authenticator sovellus, Vaihtoehtoinen puhelinnumero ja Toimiston puhelinnumero:

Lisää menetelmä ×

Minkä menetelmän haluat lisätä?

Valitse menetelmä ∨

- Authenticator-sovellus
- Vaihtoehtoinen puhelinnumero
- Toimiston puhelinnumero

Oletusarvon mukainen sisäänkirjautumismenetelmä

Voit vaihtaa oletusarvoisen sisäänkirjautumismenetelmän, jota käytetään, *mikäli turvallisin kirjautumistapa ei ole mahdollinen.*

Microsoftin [lista turvallisimmista kirjautumistavoista.](#)

Turvatieto sivulla valitse kohta **Muuta**:

☰ Omat sisäänkirjautumiseni ∨


Turvatieto

Nämä ovat menetelmät, joilla kirjaudut sisään tiliisi tai nollaat salasanasi.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Puhelin – lähetä tekstiviesti numeroon +358 044455 Muuta

+ Lisää kirjautumismenetelmä

 Puhelin	+358 044455	Muuta	Poista
---	-------------	--------------------	---------------------

Sitten valitse haluamasi tapa esim. **Sovelluspohjainen todentaminen – ilmoitus** (puhelimesi Authenticator sovellukseen lähetetään push viesti) tai **Sovelluspohjainen todentaminen – koodi** (Sinun täytyy syöttää puhelimen Authenticator sovelluksessa oleva koodi). Esimerkissä on valittuna koodi menetelmä.

Vaihda oletusmenetelmä



Mitä menetelmää haluat käyttää sisäänkirjautumiseen?

Puhelin – lähetä tekstiviesti numeroon +358 044455



Puhelu – soita numeroon +358 044455

Puhelin – lähetä tekstiviesti numeroon +358 044455

Sovelluspohjainen todentaminen – ilmoitus

Sovelluspohjainen todentaminen tai laitteistotunnus – koodi

Vahvista muutos:

Vaihda oletusmenetelmä



Mitä menetelmää haluat käyttää sisäänkirjautumiseen?

Sovelluspohjainen todentaminen tai laitteistotunnus – k... ▾

Edellinen

Vahvista

Muutos on valmis ja näet sen Turvatieto sivulla:

Turvatieto

Nämä ovat menetelmät, joilla kirjaudut sisään tiliisi tai nollaat salasanasasi.

Oletusarvon mukainen sisäänkirjautumismenetelmä: Authenticator-sovellus tai laitteistotunnus – koodi [Muuta](#)

+ Lisää kirjautumismenetelmä



Puhelin

+358 0444557567

[Muuta](#)

[Poista](#)



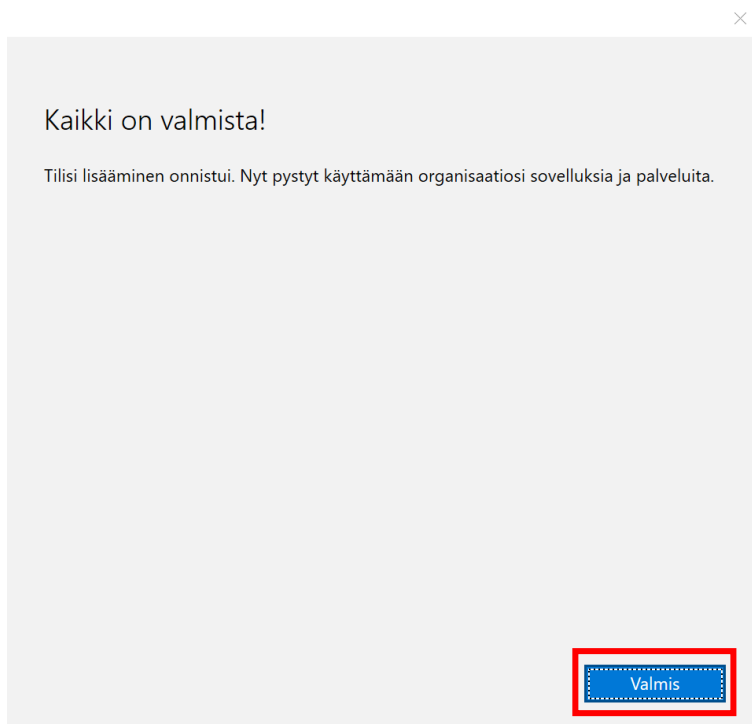
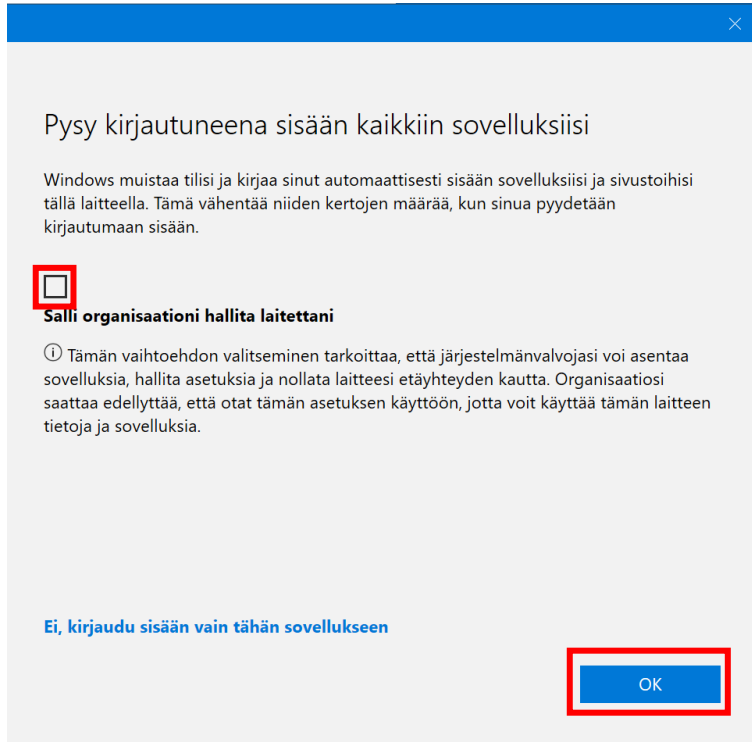
Microsoft Authenticator

[Poista](#)

Intune - Salli organisaationi hallinta laitettani

Kun kirjaudut sisään koneellesi ja avaat Teamsin tai Outlookiin saatat nähdä tämän alla olevan pop-up ikkunan. Ota rasti pois ruudusta **Salli organisaationi hallita laitetta** ja paina **OK**.

Jos valitset **Ei, kirjaudu sisään vain tähän sovellukseen** sinua pyydetään vahvistamaan kirjautuminen jokaiseen sovellukseen erikseen.



Usein kysytyt kysymykset

Miksi minua pyydetään antamaan puhelinnumeroni uudelleen?

Puhelinnumeroa kysytään uudelleen automaattisesti 180 päivän välein, jotta varmistetaan tiedon ajantasaisuus.

Puhelinnumeron vaihtuminen

Jos puhelinnumerosi vaihtuu se ei päivity automaattisesti monivaiheisen tunnistautumisen järjestelmään, vaan sinun on itse käytävä lisäämässä uusi numero ennen vaihtoa oma tili sivulla, jos se vain on mahdollista.

On suositeltavaa, että on käytössä kaksi kirjautumistapaa (esim. puhelinnumero ja Microsoft Authenticator). Vaikka numerosi olisi jo vaihtunut, pystyt vielä tällä tavalla vahvistamaan tunnistautumisen Authenticator sovelluksella ja käydä lisäämässä uuden numeron jälkikäteen.

Vaihdon jälkeen muista poistaa vanha numerosi.”

Puhelimeni ei ole käytettävissä

Mikäli puhelimesi on rikki, kadonnut tai puhelinnumero on vaihtunut, tulee opiskelijoiden ilmoittaa asiasta vastuukouluttajalleen ja henkilökunta tekee palvelupyynnön WinNovan asiointiportaaliin. Ilman puhelintasi et pysty tunnistautumaan, etkä pääse WinNovan pilvipalveluihin käsiksi.

Voinko käyttää monivaiheista tunnistautumista usealla puhelimella?

Monivaiheiseen tunnistautumiseen voi käyttää useita puhelinnumeroita ja Microsoft Authenticator sovelluksen voi lisätä useaan puhelimeen. Voit tehdä nämä lisäykset **Turvatieto** sivun kautta.

HUOM! Tietoturvariskien minimoimiseksi emme kuitenkaan suosittele asentamaan näitä kovin moneen puhelimeen! Varmista, aina että puhelimesiasi on käytössä lukitusnäyttö.

Oman puhelimen tietoturva – Lukitusnäyttö

On hyvä varmistaa, että omassa puhelimesta on näytön lukituskoodi käytössä. Se voi olla PIN-koodi, salasana, kuvio, kasvokuva tai vaikka sormenjälki. Tämä varmistaa sen, että vaikka puhelimesi saattaisi joutua väärin käsiin, ei siihen pääse sisälle.

Samsung puhelimesta lukitusnäytön saa päälle menemällä Asetukset -> Lukitusnäyttö -> Näytön lukituksen tyyppi. Valitse täältä haluamasi menetelmät tai useampi.

Itslearning ympäristön ongelmat

Jos yrität avata materiaaleja ItsLearning ympäristössä saatat nähdä virheilmoituksen ”Muodosta yhteys uudelleen”



Pahoittelut, tiedostojesi näyttäminen ei onnistunut. Voit korjata asian liittämällä uudelleen käyttäjätilin [redacted]@winnova.fi. Jos tili on edelleen liitetty, katkaise yhteys ja muodosta sitten yhteys uudelleen kohdassa "Omat asetukset > Liitetyt tilit".

Virheen saa korjattua näin:

Mene itslearningissa oikeasta ylänurkasta **omiin tietoihin**, sieltä avaa **Omat asetukset** → **Liitetyt tilit** → **VAIHDA TILIÄ**

Kirjaudu omalla salasanalla ja monivaiheisella tunnistautumisella.

Nyt yhteyden pitäisi toimia taas.

PowerAutomate työkulun ongelmat

Jos näet virheilmoituksen ”Muodosta yhteys uudelleen” se korjaantuu muodostamalla yhteys työkulun ja oman tilin välille uudestaan.

Puhelulla tunnistautuminen

Jos yritätte vahvistaa monivaiheisen tunnistautumisen (MFA) puhelulla on tärkeää, että teette oikeat valinnat, jotta vältymme ylimääräiseltä työltä koskien virheellisten ilmoitusten käsittelyä.

Puhelun aikana kerrotaan eri vaihtoehdot, joista tiedot alla sekä mitä tapahtuu kunkin valinnan jälkeen.

Äänite 1: Tämä on Microsoft. Jos yrität kirjautua sisään, viimeistele kirjautuminen painamalla ruutu näppäintä (#)

- Jos valitset tämän, niin tunnistautumien vahvistetaan.

Äänite 2: Jos et yritä kirjautua sisään paina nolla ja ruutu (0 #) (Tästä tulee tietohallintoon paljon ns. virheellisiä ilmoituksia, joita haluaisimme vähentää. Valitse tämä vain, jos et ole yrittänyt kirjautua.)

- Jos valitset tämän, niin tunnistautuminen keskeytetään ja siitä tulee ilmoitus tietohallintoon, mutta **käyttäjän MFA kirjautumista ei lukita**. Jos käyttäjä valitsee tämän, annetaan vielä yksi ilmoitusvaihtoehto, joka on alla.

Äänite 3: Jos et yrittänyt kirjautua sisään suojaat tilisi ilmoittamalla IT tiimillesi painamalla ensimmäinen (1).

- Jos valitset tämän, niin tunnistautumien keskeytetään, siitä tulee ilmoitus tietohallintoon ja **käyttäjän MFA kirjautuminen lukitaan**, eli hänet lisätään estolistalle 90 päivän ajaksi, tai kunnes tietohallinto vapauttaa käyttäjän tunnuksen. Tämä kannattaa valita silloin, jos uskot, että joku muu kuin sinä yrittää päästä kirjautumaan tilillesi.

Niissä tapauksissa, kun me saamme **Multi-Factor Authentication Fraud Alert** ilmoituksen, tarkastamme aina, onko käyttäjä lisätty estolistalle vai ei ja tarvittaessa otamme yhteyttä käyttäjään tai opiskelijan vastuukouluttajaan tilanteen tarkistamiseksi.