ELISA VPN SSL ASENNUSOHJE

Versio 1.0

Asiakasohje

Elisa VPN SSL palvelu Pulse Secure-sovelluksen asennus ja käyttö

Sisällys

Pulse Secure vpn-sovelluksen asennus Windows

(työasemille joilla on Java asennettuna)

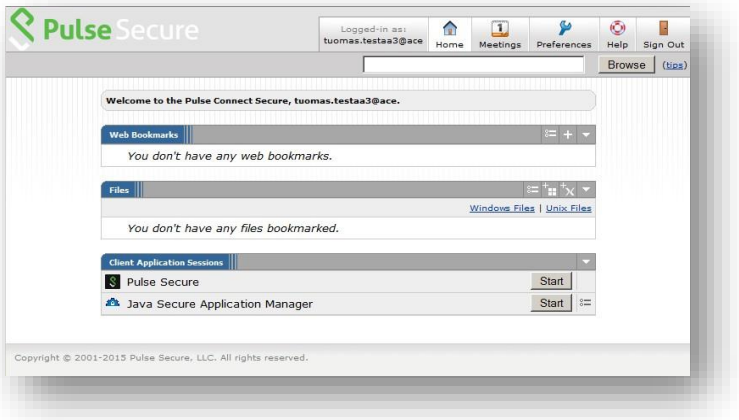
Vanhan asennuksen poisto

Organisaatiosi kanssa sovittuna uuteen vpn-sovellukseen siirtymisen ajankohtana voit seuraavien ohjeiden mukaisesti toimimalla ottaa käyttöösi Pulse Secure -sovelluksen. Aloita kirjautumalla palveluun tavalliseen tapaan Network Connect -sovelluksella. VPN-yhteyden muodostuttua pura yhteys tavalliseen tapaan. Network Connect poistetaan koneeltasi automaattisesti.

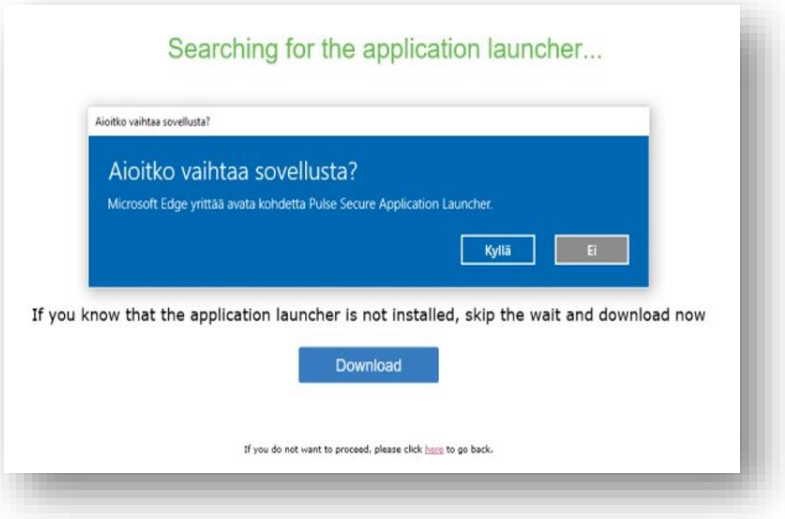
Seuraavissa vaiheissa kirjaudut organisaatiosi Pulse Secure vpn-portaaliin www-selaimella ja käynnistät uuden vpn-sovelluksen asennuksen.

Uuden sovelluksen asennus

Kirjaudutaan käyttäjätunnuksilla asiakaskohtaiseen portaaliin
Sisäänkirjautumisen jälkeen klikataan hiirellä Client Application Session -kohdassa, rivillä Pulse Secure Start-painiketta

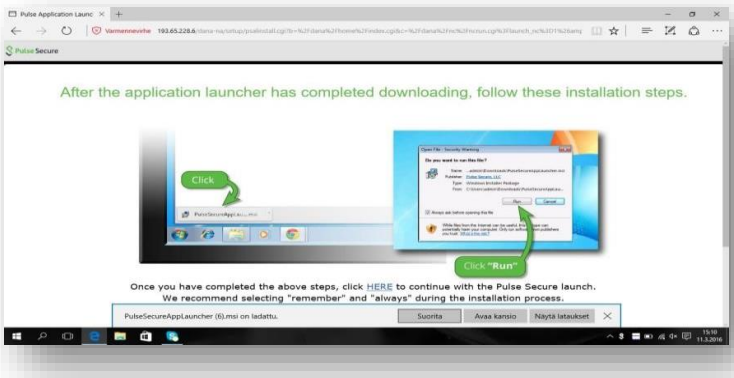


Jos koneelle ei ole asennettu ennestään Juniper/Pulse Application Launcher komponenttia, se asennetaan ensiksi.

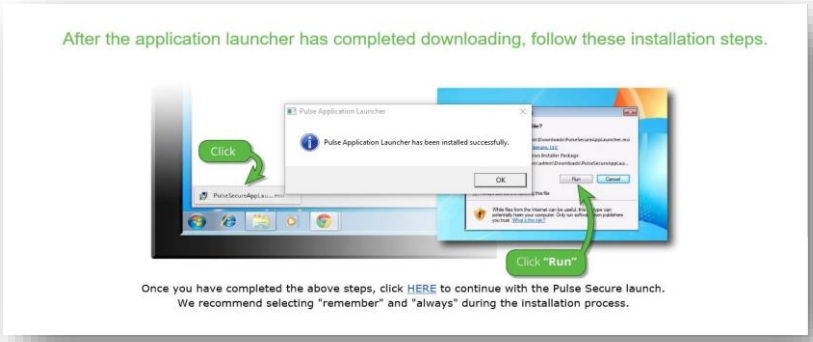


Windows-käyttöjärjestelmä saattaa kysyä lupaa Application Launcerin käynnistämiseen, vastataan klikkaamalla Kyllä / Ok / Yes. Sen jälkeen klikataan sivun keskellä näkyvää download-painiketta.

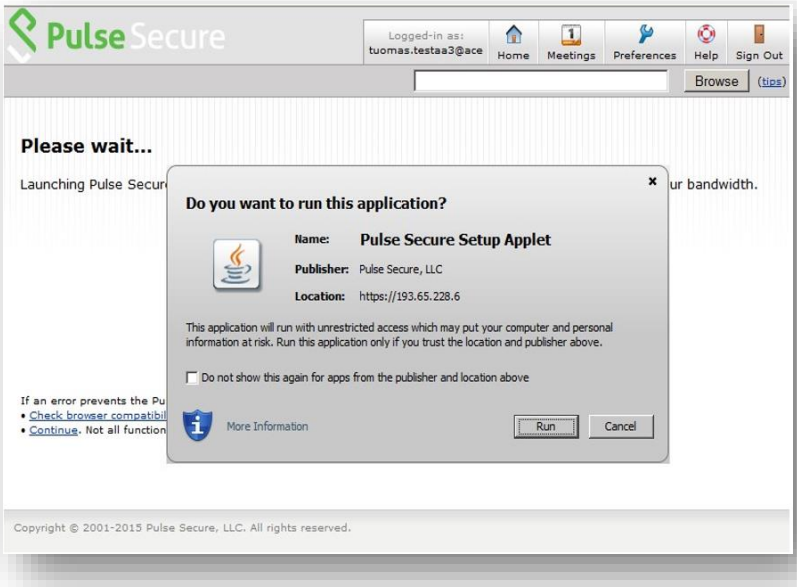
Kun Application Launcherin asennusohjelma on ladattu, ajetaan valitsemalla Suorita / Run.



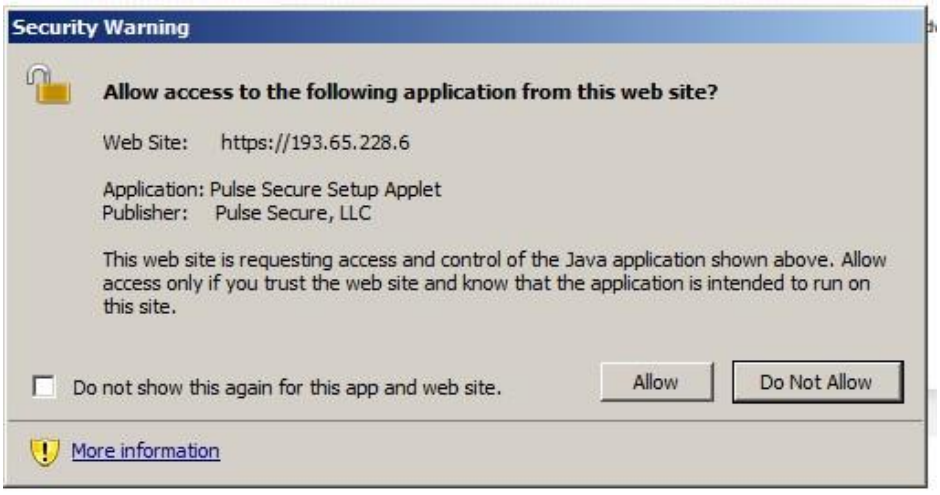
Windows ilmoittaa Application Launcherin asennuksen valmistuneen, kuitataan ilmoitus ok-painikkeella. ja klikataan selainikkunan alalaidassa HERE-sanaan liitettyä linkkiä.



Vastataan avautuvan ikkunan kysymykseen "Do you want to run this application?" klikkaamalla Run.



Jos Windows esittää seuraavan valintaikkunan, klikataan "Allow".



Pulse Secure -client asennus valmistuu hetken kuluttua ja vpn-yhteys muodostuu.

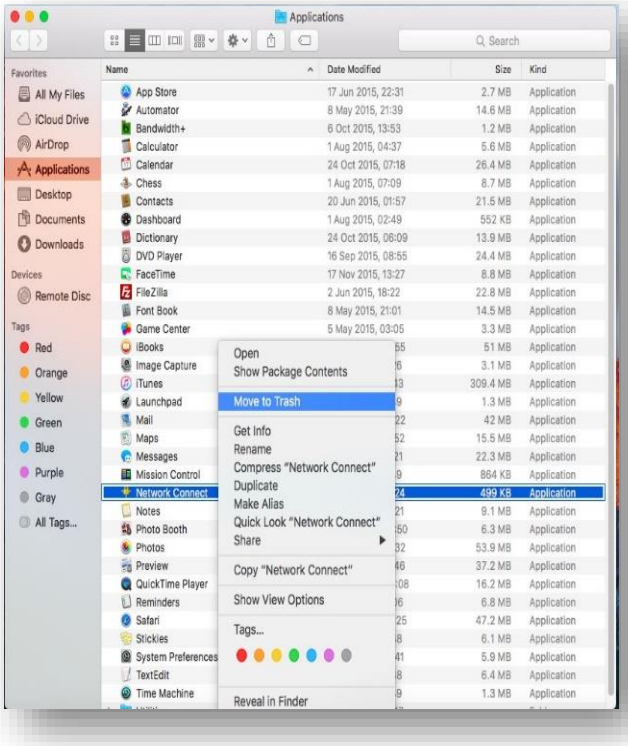
Pulse Secure vpn-sovelluksen asennus Mac OS X (työasemille joilla on Java asennettuna)

Vanhan asennuksen poisto

Organisaatiosi kanssa sovittuna uuteen vpn-sovellukseen siirtymisen ajankohtana voit seuraavien ohjeiden mukaisesti toimimalla ottaa käyttöösi Pulse Secure -sovelluksen. Aloita kirjautumalla palveluun tavalliseen tapaan Network Connect -sovelluksella. VPN-yhteyden muodostuttua pura yhteys tavalliseen tapaan. Network Connect poistetaan koneeltasi automaattisesti.

Mac OS X versiolla El Capitan varustetuissa työasemissa saatat joutua poistamaan Network Connect -sovelluksen manuaalisesti Finderin Applications -näkymässä

Seuraavissa vaiheissa kirjaudut organisaatiosi Pulse Secure vpn-portaaliin wwwselaimella ja käynnistät uuden vpn-sovelluksen asennuksen.

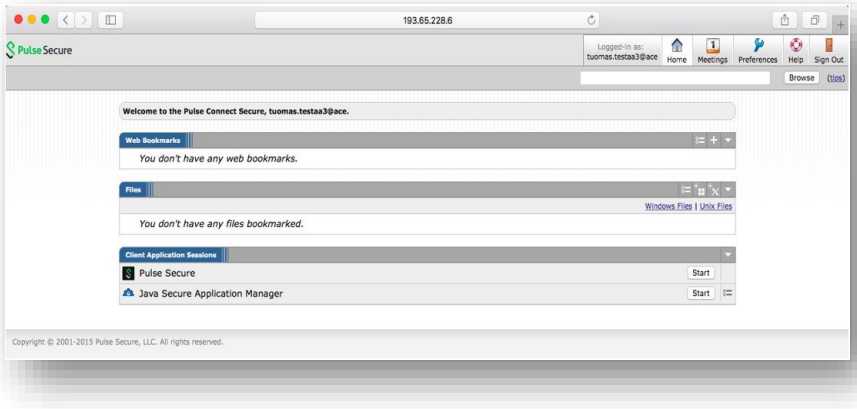


Seuraavissa vaiheissa kirjaudut organisaatiosi Pulse Secure vpn-portaaliin wwwselaimella ja käynnistät uuden vpn-sovelluksen asennuksen.

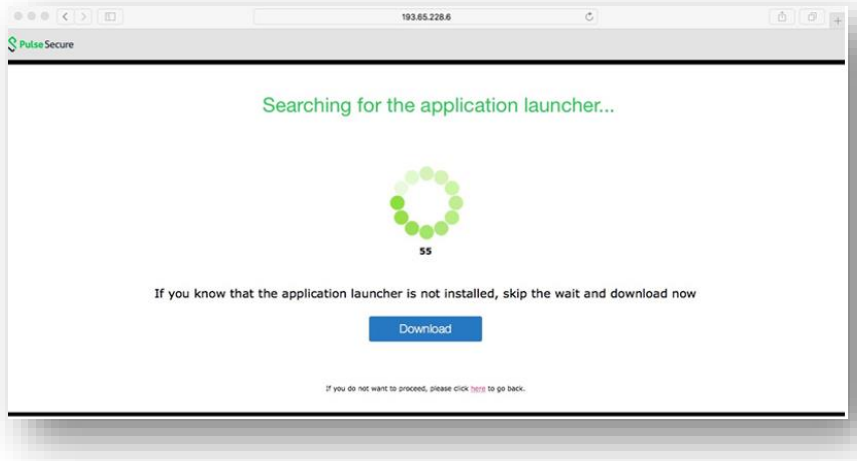
Uuden sovelluksen asennus

Kirjaudutaan käyttäjätunnuksilla asiakaskohtaiseen portaaliin

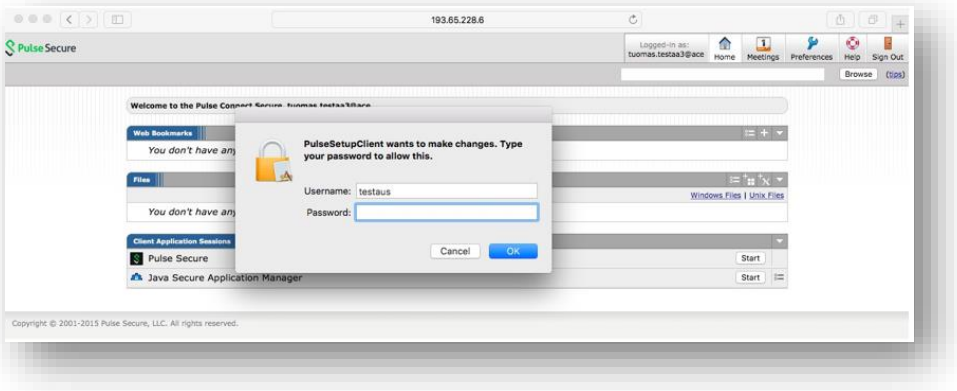
Sisäänkirjautumisen jälkeen klikataan hiirellä Client Application Session -kohdassa, rivillä Pulse Secure Start-painiketta



Pulse Application Launcher käynnistyy. Jos sitä ei löydy koneelta, se ladataan portaalista ja käynnistyy automaattisesti 60 sekunnin kuluttua. Tässä tapauksessa voit nopeuttaa käynnistymistä klikkaamalla selaimessa näkyvää Download-painiketta.



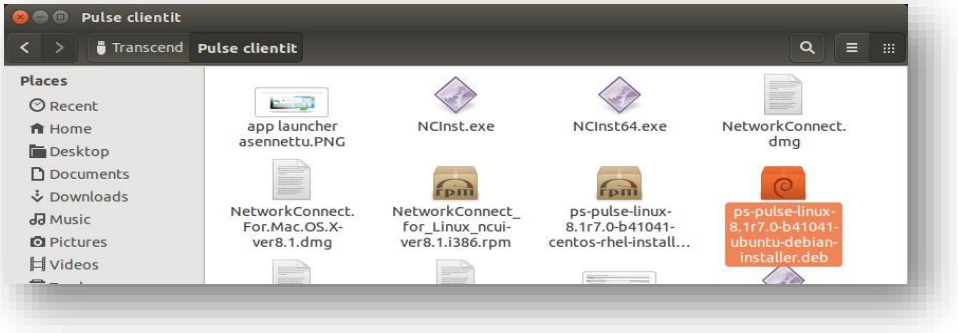
Anna järjestelmän ylläpito-oikeudellisen käyttäjän käyttäjätunnus ja salasana, jos niitä kysytään.



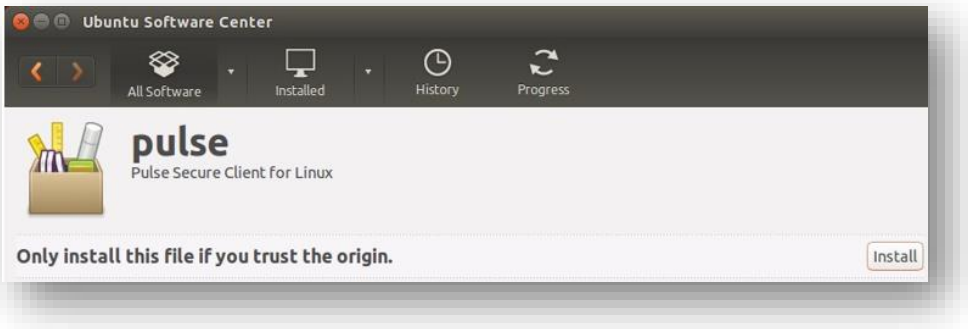
Pulse Secure -client asentuu ja vpn-yhteys muodostuu.

Pulse Secure vpn-sovelluksen asennus Linux (Ubuntu) työasemaan ja yhteyden muodostus

Käynnistä asennus kaksoisklikkaamalla asennuspakettia ja valitse sen avaaminen Ubuntu Software Centerissä

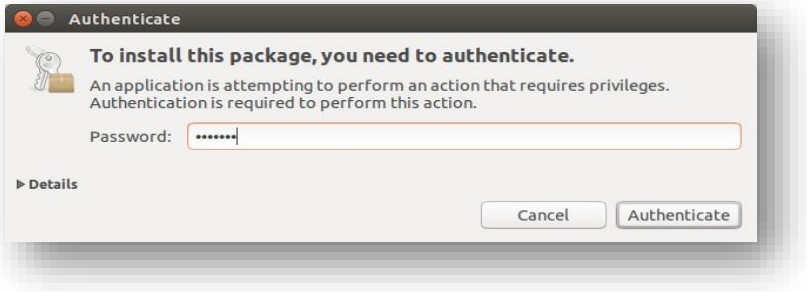


Klikkaa install



Kuittaa "The package is of bad quality" klikkaamalla Ignore and install.

Jos asennus pyytää antamaan pääkäyttäjän (root) salasanan, syötä se ja klikkaa Authenticate.



Asennus valmistuu. Sovelluksen asennushakemisto on /usr/local/pulse. Siirry kyseiseen hakemistoon ja anna komento

"./PulseClient.sh -h palvelimen_osoite -u käyttäjätunnuksesi -p salasana -f palvelimen_julkinen_sertifikaatti_tiedostossa"

Yhteys muodostuu. Yhteyden purkaminen onnistuu komennolla

"./PulseClient.sh -K"

Tarkempi englanninkielinen ohje löytyy Pulsen sivuilta osoitteesta
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40126

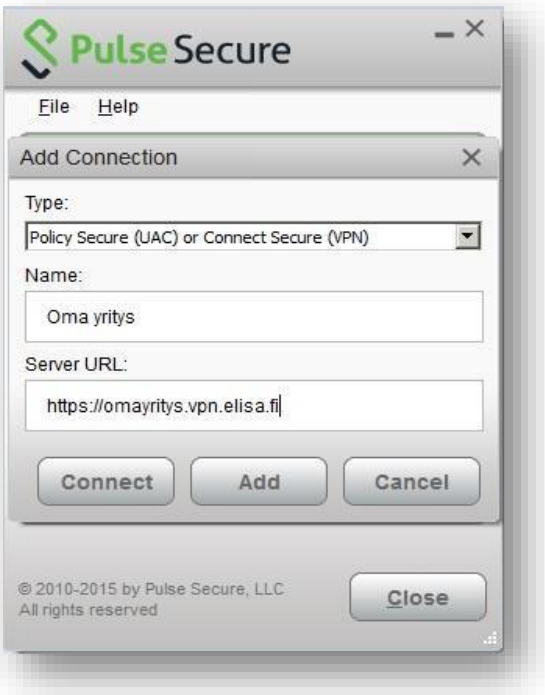
Pulse Secure client-sovelluksen peruskäyttö

Aloitusnäkymä ja yhteysosoitteen lisääminen

Lisätäkseni uuden vpn-yhteysosoitteen klikkaa Connections-palkin plus (+) merkkiä.

Kirjoita avautuneen Add Connection -ikkunan Name-kenttään yhteydelle nimi.

Kirjoita Server URL -kenttään organisaatiosi vpn-palvelun osoite ja klikkaa Add-painiketta.



Yhteyden muodostaminen

Valitse Connections-kohdan listasta se yhteys, jonka haluat avata ja klikkaa Connect.

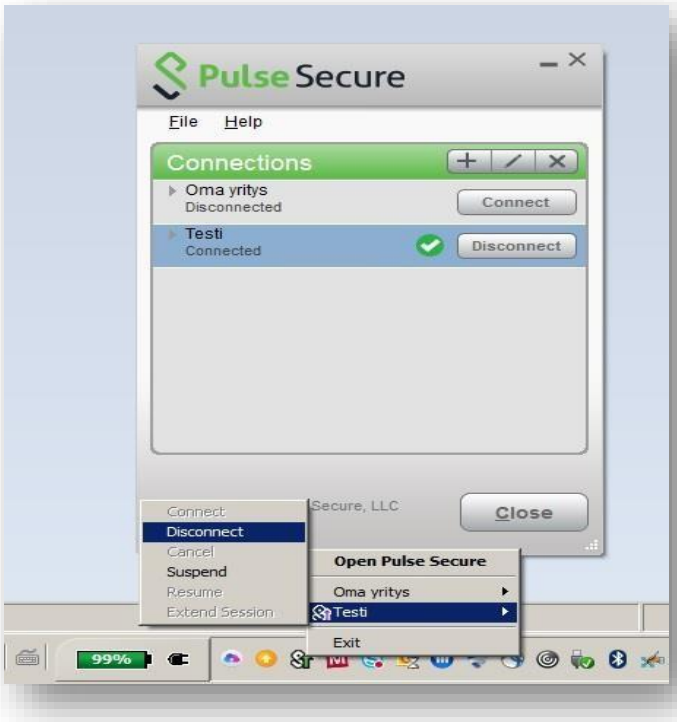
Syötä avautuneeseen Connect to: -ikkunaan User Name -kenttään vpn-yhteyden käyttäjätunnuksesi.

Syötä Please enter your passcode -kenttään käytössäsi olevan tunnistamistavan mukainen salasana/passcode.

Yhteys muodostuu ja näkyy Connections-listassa Connected-tilassa.

Yhteyden purku

Klikkaa vpn-sovelluksen ikkunasta tai Windows-käyttöjärjestelmän tapauksessa tehtäväpalkissa olevasta Pulse valikosta avoinna olevan yhteyden kohdalta Disconnect.



SMS OTP - tunnistuksen käyttöohje SSL VPN palvelussa

Yleistä SMS OTP:stä

SMS OTP on ns. kahden tason tunnistusmenetelmä, jossa käytetään käyttäjän salasanaa (PIN) ja henkilökohtaiseen matkapuhelinliittymään saapuvaa lyhyen ajan voimassaolevaa kertakäyttösalasanaa. Matkapuhelinliittymä sidotaan tunnistamisvälineeksi, joka pitää olla käyttäjän hallussa tunnistamishetkellä.

OTP-koodi toimitetaan puhelimeen ns. flash-tekstiviestillä. Flash-viesti näkyy automaattisesti puhelimen näytössä ja viesti ei tallennu puhelimen muistiin ellei viestiä erikseen talleteta (tallennusta ei suositella).

Käsitteet

PIN-koodi: henkilökohtainen salasana. Käyttäjän tiedossa oleva salaisuus (engl. Something you know) - salasana/PIN-koodi.

OTP-koodi: tekstiviestillä toimitettava ja lyhyen ajan voimassaoleva kertakäyttösalasana (One-Time Password). OTP-koodi toimitetaan käyttäjän hallussa olevaan todentamisvälineeseen (engl. Something you have).

Käyttö

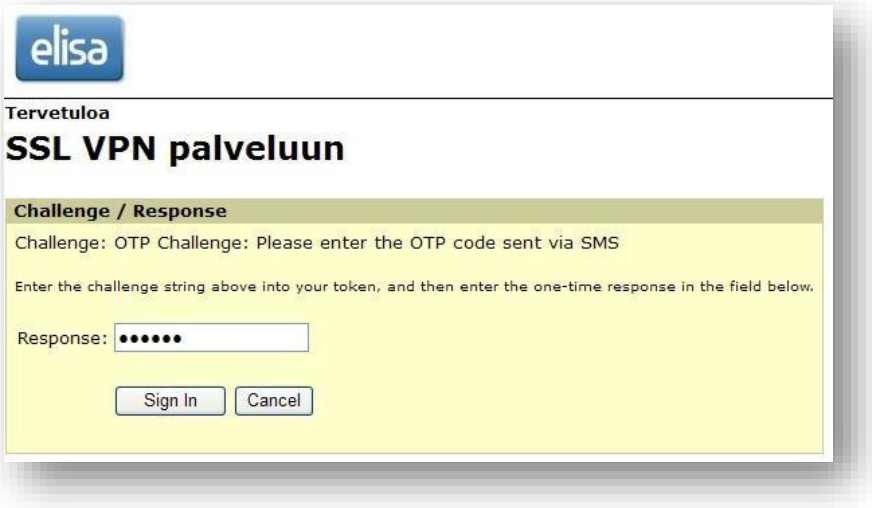
Siirry SSL VPN portaaliin tai avaa yhteys Pulse Secure -sovelluksesta.

Kirjoita *Käyttäjätunnus* kenttään oma käyttäjätunnus.

Syötä *Salasana* kenttään oma henkilökohtainen PIN-koodi.

Saat matkapuhelimeen SMS viestillä kertakäyttöisen OTP-koodin (One-Time Password). Koodi voi sisältää numeroita ja pieniä kirjaimia.

Syötä saamasi OTP-koodi *Response* kenttään.



SSL VPN-palvelu käynnistyy. Mikäli OTP-koodi syötettiin virheellisenä, tunnistus keskeytetään ja aloitetaan alusta

Turvallisuusohjeita

- Paina saamasi PIN-koodi mieleesi. Älä säilytä PIN-koodia puhelimen muistissa.
- PIN-koodi on henkilökohtainen. Älä luovuta tietoa PIN-koodista kenellekkään. Mikäli olet unohtanut PIN-koodin tai epäilet PIN-koodin joutuneen ulkopuolisten tietoon, pyydä organisaatiosi IT-tukea resetoimaan PIN-koodi. Tili menee lukkoon 30 minuutiksi, mikäli PIN-koodi syötetään väärin 5 kertaa peräkkäin tunnin sisällä.
- Mikäli kadotat puhelimen/liittymän (tunnistusväline), ota välittömästi yhteyttä organisaatiosi IT-tukeen.
- Älä talleta OTP-koodeja puhelimen muistiin (flash-viestejä ei suositella tallennettavaksi).
- Palvelun käytön jälkeen kirjaudu ulos SSL VPN-palvelusta asianmukaisesti.
- Huolehdi työasemasi tietoturvasta organisaatiosi ohjeiden mukaisesti.

Mahdolliset ongelmatilanteet ja niiden ratkaisu

OTP-koodi ei saavu puhelimeen tekstiviestillä

1. *Odota hetki ja yritä tunnistautumista uudelleen.*
2. *Tarkista, onko puhelimen näyttö lukossa. Tekstiviesti ei puhelimesta riippuen välttämättä näy heti näytössä, mikäli puhelin on suojalukittu. Avaa suojalukko ja katso näkyykö viesti puhelimessa ja tarvittaessa yritä tunnistautumista uudelleen ilman suojalukkoa.*
3. *Tarkista käyttäjätunnus ja PIN-koodi (salasana). Yritä tunnistaumista uudelleen.*
4. *Tarkista puhelimen verkkoyhteyksien toimivuus, käynnistä puhelin tarvittaessa uudelleen ja yritä tunnistaumista uudelleen.*
5. *Mikäli SMS ei edelleenkään saavu puhelimeen, ota yhteyttä organisaatiosi IT-tukeen.*

OTP-koodi ei toimi

1. *Yritä tunnistaumista uudelleen. Saat uuden OTP-koodin.*
2. *OTP-koodi on voimassa oletuksena 120 sekuntia (2 min). Tätä vanhemmat OTPkoodit eivät toimi. Syötä OTP-koodi 2 minuutin kuluessa.*
3. *OTP-koodi on kertakäyttöinen. Vanhaa jo kertaalleen käytettyä koodia ei voi käyttää uudelleen. Tunnistaudu palveluun uudelleen ja saat uuden OTP-koodin.*
4. *Tarkista, että yrität syöttää viimesimmän OTP-koodin. Ainostaan viimeisin tilattu OTP-koodi toimii.*
5. *Tarkista, että yrität syöttää OTP-koodin ruutuun, jossa lukee "Response".*
6. *Luo huolellisesti OTP-koodin merkistö. OTP-koodi voi sisältää sekä numeroita ja pieniä kirjaimia.*
7. *Mikäli OTP-koodi ei edelleenkään toimi, ota yhteyttä organisaatiosi IT-tukeen.*

PIN-koodi ei toimi

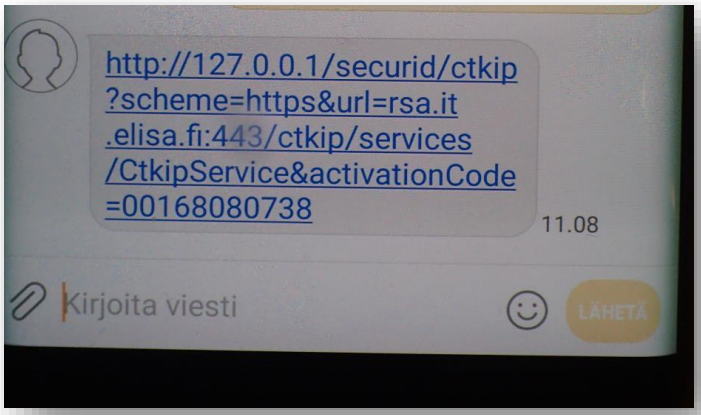
1. *Tarkista käyttäjätunnus ja PIN-koodi.*
2. *Tili menee automaattisesti lukkoon, mikäli PIN-koodi tai OTP salanana on syötetty väärin 5 kertaa peräkkäin tunnin sisällä. Odota 30 minuuttia ja älä yritä autentikointia tänä aikana. Tili avautuu ja voit syöttää PIN-koodin uudelleen.*
3. *Mikäli olet unohtanut PIN-koodin, ota yhteyttä organisaatiosi IT-tukeen.*

RSA SecurID -tunnistautumisen käyttö

SecurID -ohjelmistotokenin aktivointi

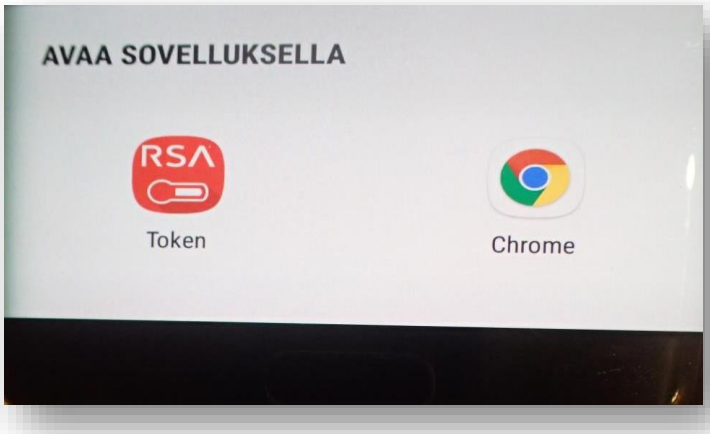
Asenna puhelimeesi RSA SecurID Token -sovellus puhelinkohtaisesta verkkokaupasta, Android-puhelimille Google Playsta ja iPhonelle iTunes Storesta,

Avaa Elisalta saamasi tekstiviesti, joka sisältää ohjelmistotokenin aktivointilinkin ja paina aktivointilinkkiä. Puhelimen on aktivoinnin aikana oltava verkossa.



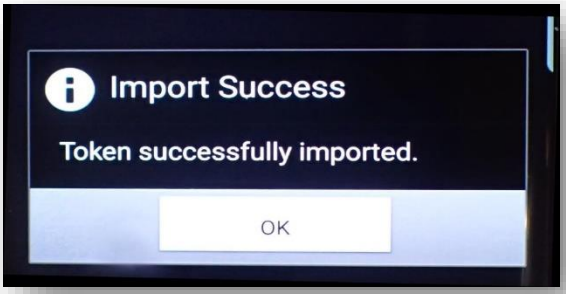
Aktivointilinkin painamisen jälkeen puhelin, hieman mallista riippuen, joko käynnistää RSA SecurID Token -sovellluksen, tai pyytää käyttäjää valitsemaan avataanko linkki Token-sovelluksella vai selaimella.

Valitse avaaminen Token-sovelluksella.

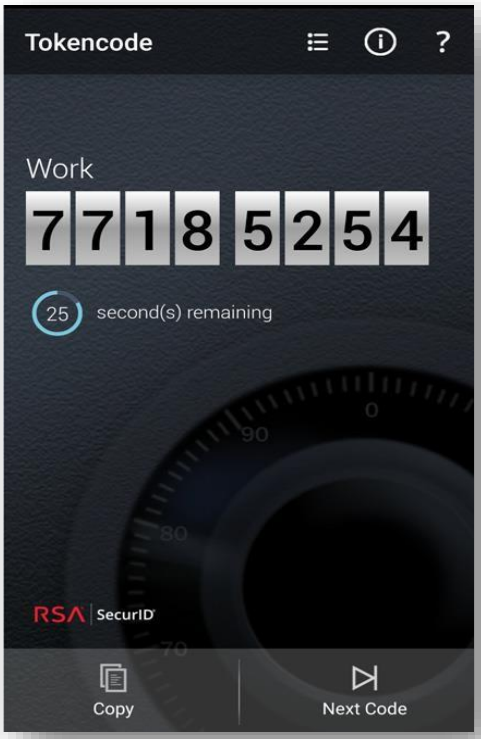


Puhelin siirtyy Token-sovellukseen ja aktivointi käynnistyy.

Aktivointi voi puhelinmallista riippuen kestää joitakin kymmeniä sekunteja. Älä siirry välillä muihin sovelluksiin. Sovellus ilmoittaa tokenin aktivoituneen. Kuittaa ilmoitus painamalla OK.



Puhelin siirtyy Token-sovelluksen päänäkymään.



SecurID-tokenin käyttö (laitteistotoken ja ohjelmistotoken)

PIN-koodi: henkilökohtainen PIN-koodi (määritetään ensimmäisen kirjautumisen yhteydessä). PASSCODE: PIN-koodin ja vaihtuvan numerosarjan yhdistelmä (PIN+Tokenkoodi). Esim. jos PIN olisi 1234 ja vaihtuva tokenkoodi 159759, olisi Passcode tällöin 1234159759.

PIN-koodin määrittäminen ensimmäisellä käyttökerralla tai resetoinnin jälkeen.

1. Avaa VPN- clientohjelmisto
2. Syötä Username kenttään toimitettu käyttäjätunnus ja Password kenttään ainoastaan oman tokenlaitteesi ilmoittama tokenkoodi (tokenin numerosarja).
3. Järjestelmä pyytää tämän jälkeen määrittämään PIN-koodin (Are you ready to enter a newpin) -> vastaa y
4. Määritä uusi PIN-koodi (enter a new pin). Suosituksena vähintään 6 merkkiä. Tietoturvasyistä järjestelmä ei anna määrittää helposti arvattavia koodeja, esim. 123456, 11111 jne.
5. Toista uusi PIN-koodi (re-enter new pin to confirm)
6. PIN-koodi on nyt vahvistettu (PIN accepted, wait for the tokencode to change, then enter a new PASSCODE). Syötä kenttään uusi PASSCODE (PIN + Tokenkoodi). Varmista, että laitteen tokenkoodi on vaihtunut vaiheesta 2.
7. Mikäli et pysty kirjautumaan VPN:ään vaiheessa 6, odota hetki ja yritä kirjautumista uudelleen.
8. PIN-koodin määrityksen jälkeen kirjaudut VPN:ään aina käyttäjätunnuksella ja PASSCODELLA (PIN+vaihtuva tokenkoodi).Kirjautuminen PIN-koodilla ja tokenin