9.5.2019

Jere Känsälä

Azure MFA Serverin käyttöönotto yritysasiakkaalle

Opinnäytetyö
Kevät 2019
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikan tutkinto-ohjelma

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Jere Känsälä

Työn nimi: Azure MFA Serverin käyttöönotto yritysasiakkaalle

Ohjaaja: Alpo Anttonen

Vuosi: 2019 Sivumäärä: 49 Liitteiden lukumäärä: 0

Opinnäytetyö tehdään BLC Taito Oy:n kautta yritysasiakkaalle. Työn aiheena on ottaa käyttöön asiakasyrityksen johdolle sekä valitulle ryhmälle sovellusten pääkäyttäjiä kaksiosainen varmistus kirjautumisen yhteyteen. Tämä toteutetaan ottamalla yritykselle käyttöön Azure MFA Server.

Työn teoriaosuudessa käydään yleisesti läpi todentamista sekä muutamaa siihen liittyvää protokollaa. Kerrotaan myös, mitä kaksiosainen todennus on, ja miten se käytännössä toimii. Lisäksi teoriaosuudessa käydään myös hiukan läpi Azuren moniosaisen vahvistuksen -palveluita.

Käytännön osuudessa Azure MFA Server -palvelun asennus tehdään jo entuudestaan olemassa olevalle palvelimelle. Tämä konfiguroidaan vastaamaan asiakkaan tarpeita sekä toiminta testataan alkuun testitunnuksella. Tämän jälkeen kaksiosainen varmennus testataan asiakkaan testiryhmän toimesta, ja kun sen toimintaan ollaan tyytyväisiä, lisätään se valitulle ryhmälle käyttäjiä.

Avainsanat: Multi-Factor Authentication, tunnistautuminen, todentaminen, protokolla, palvelin

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Network Technology

Author: Jere Känsälä

Title of thesis: Deployment of Azure MFA Server for a Business Customer

Supervisor: Alpo Anttonen

Year: 2019 Number of pages: 49

This thesis was done for a business customer of BLC Taito Oy. Its theme was the deployment of multi-factor authentication for the customer's management and a selected group of the root users of different applications. This was realized by deploying Azure's MFA Server for the company.

In the theoretical part of the thesis general information about authentication, and a couple of protocols associated with it was studied. Also multi-factor authentication and how it works in practice was explained. Additionally Azure's multi-factor authentication services were studied.

In the practical part the Azure's MFA Server was installed into an existing server. It was then configured to match the customer's needs and tested with a test user. After this the multi-factor authentication was tested by the customer's test group, and after they were satisfied with how it worked, it was added to the designated group of users.

Keywords: Multi-Factor Authentication, identification, authentication, protocol, server

SISÄLTÖ

Kuvaluettelo

Käytetyt termit ja lyhenteet

AAA -malli	Käytetään puhuttaessa tietoverkon pääsyyn vaikuttavista protokollista. Tulee sanoista authentication eli todentaminen, authorization eli valtuutus sekä accounting eli tilastointi.
AD	Active Directory on Windows-toimialueen käyttäjätietokanta sekä hakemistopalvelu, joka sisältää tietoa esim. käyttäjistä.
Azure	Microsoftin tarjoama laaja valikoima pilvipalveluita yritysten haasteita varten.
Hop-by-Hop	Mahdollistaa tiedon siirron ilman jatkuvaa verkkoyhteyttä. Tämä tapahtuu siirtämällä tietoa laitteelta laitteelle, säilyttäen sitä tarpeen mukaan.
MD5-algoritmi	Algoritmi, jota käyttämällä voidaan tarkastaa datan luotettavuus.
OTP	One-time password eli salasana, joka toimii vain yhden kirjautumisen ajan.
PIN-koodi	Salasanana käytettävä luku, jota on mahdollista käyttää järjestelmiin tunnistautumisessa.
PPP	Protokolla, jonka avulla voidaan muodostaa suora yhteys verkkolaitteiden välille.
SMS	Tulee sanoista short message service, eli kyse on matkapuhelinverkossa lähetettävistä lyhyistä viesteistä.
SMTP relay	SMTP relay on protokolla, joka mahdollistaa sähköpostin lähetyksen verkon yli, poimimalla sen lähettäjältä ja toimittamalla vastaanottajalle.

UPD	Protokolla, joka mahdollistaa tiedostojen siirron laitteiden välillä, vaikka näiden välillä ei olisi yhteyttä.
Vertaisverkko	Verkko, jossa jokainen verkkoon kytketty laite toimii sekä asiakkaana että palvelimena verkon muille jäsenille.
VPN-yhteys	VPN on virtuaalinen erillisverkko, jolla verkkoja voidaan yhdistää julkisen verkon yli keskenään. Tällä tavoin saadaan näennäisesti luotua yksityisverkko.

1 JOHDANTO

1.1 Työn tausta

Moniosainen todennus on yleisesti oiva tapa parantaa tietoturvaa. Sen avulla käyttäjä turvaa tunnuksensa pelkkää salasanaa varmemmin, sillä tunnistautumiseen tulee käyttää salasanan lisäksi toista tunnistautumistapaa.

Asiakasyrityksellä ei entuudestaan ollut moniosaista todennusta ollenkaan käytössä, vaan tunnukselle kirjautuminen suoritetaan pelkkää salasanaa käyttämällä. Nyt se halutaan ottaa johtoryhmälle sekä valikoidulle ryhmälle käyttäjiä käyttöön silloin, kun he yrittävät kirjautua tunnuksille jostain muusta verkkoyhteydestä, kuin yrityksen omasta.

1.2 Työn tavoite

Tavoitteena on parantaa asiakasyrityksen tietoturvaa entisestään lisäämällä valikoidulle ryhmälle moniosainen todennus. Yrityksessä jo olemassa olevalle palvelimelle asennetaan Azuren Multi-Factor Authentication Server, jonka avulla Active Directory -tietokannasta löytyviä käyttäjätietoja käyttäen todennus suoritetaan.

Käyttöönotosta tehdään myös BLC Taito Oy:lle dokumentaatio, josta voidaan jälkikäteen tarkastaa, mitä on tehty. Dokumentaatiota apuna käyttäen voidaan myös myöhemmin tehdä kaksiosaisen todennuksen käyttöönotto muille asiakkaille, mikäli tälle tulee tarve.

1.3 Työn rakenne

Luku 2 kertoo yleisesti, mitä todentaminen on. Tämän jälkeen käydään läpi muutama todentamiseen liittyvä protokolla

Luku 3 käsittelee multi-factor authentication -tunnistautumista, ja mitä se oikein on. Lisäksi käydään myös läpi tunnistustapoja, joita tässä tunnistautumisessa käytetään.

Luku 4 kertoo Azuren Multi-Factor Authentication Serveristä, jota työn käytännön osuudessa käytetään.

Luvussa 5 käydään läpi työn suunnittelua sekä sen toteutusta.

Luvussa 6 käydään läpi, miten käytännön osuus onnistui, ja mietteitä tästä.

1.4 BLC Taito Oy

BLC Taito Oy on osana Blue Lake Communications -konsernia, joka on perustettu vuonna 1889. BLC Taidon lisäksi konserniin kuuluu BLC Telecom, BLC Turva sekä BLC Rahoitus. (BLC [Viitattu 28.3.2019].) Koko konsernilla on työntekijöitä reilu 300, joista noin 70 työskentelevät BLC Taidolle. (BLC 2017).

BLC Taito tarjoaa IT-kokonaispalvelua. Tähän sisältyvät palvelut pilvipalveluista aina käyttäjä- sekä laitepalveluihin. Laitteiden suhteen tarjotaan koko elinkaaren palvelua eli hankkimisesta kierrätykseen. (BLC [Viitattu 29.3.2019].) Firmalla on toimipisteitä Espoossa, Seinäjolla, Turussa, Tampereella, Mikkelissä sekä Savonlinnassa. (BLC 2017).

2 TODENTAMINEN

2.1 Mitä todentaminen on

Käyttäjä on sovellukselle kokoelma attribuutteja, jotka ovat oleellisia sovelluksen toiminnan kannalta. Esimerkkejä attribuuteista on nimi, syntymäaika tai vaikkapa laskutusosoite. Nämä attribuutit, jotka määrittelevät käyttäjän identiteetin, ohjaavat sovelluksen käytöksen: hakeeko se vaikkapa tietyn tiedoston, tai sallii tietyn tehtävän suorittamisen. Eri sovellukset välittävät eri attribuuteista. (Bertocci 2015, luku 2.)

Käyttäjän todentaminen on sitä, että tunnistetaan, onko kyseisillä attribuuteilla oikeus nykyiseen tapahtumaan (Bertocci 2015, luku 2).

Käyttäjille on sovelluksessa profiilit, joissa kyseiset attribuutit sijaitsevat. Käyttäjä tulee todentamisen yhteydessä yhdistää hänen profiiliinsa. Kaikista yksinkertaisin tapa tälle on salasanan käyttö. Alkuvaiheessa sovellus sekä käyttäjä sopivat keskenään salaisesta merkkijonosta, jota kumpikaan osapuoli ei paljasta ulkopuolisille. (Bertocci 2015, luku 2.)

Sovellus yhdistää tämän salasanan attribuutteihin, jotka määrittelevät käyttäjän. Jos jatkossa käyttäjä ilmoittaa kyseisen salasanan, sovellus tietää, mistä käyttäjästä on kyse. Tätä on todentaminen. (Bertocci 2015, luku 2.)

2.2 Todentamiseen liittyviä protokollia

Ensimmäinen osa AAA-mallia on todentaminen, jolloin käyttäjältä yritetään varmistaa, onko hän mitä väittää olevansa. Toisin sanoen tarkistetaan, että vastaavatko salasana ja käyttäjätunnus toisiaan. Tämä on todentamisen yksinkertaisin tapa, ja liuta erilaisia protokollia suorittaa tämän todentamisen. (Price 2019, osa 3 Authentication protocols.) Tässä osiossa käydään läpi muutamaa näistä.

2.2.1 RADIUS

Radius-protokollaa käytetään verkkosivujen suojaamiseen estämällä yleinen julkinen pääsy kyseiselle sivulle. Sillä todennetaan, että verkkosivulle pyrkijällä on tarvittavat oikeudet, jolloin hänet päästetään sisään sivulle. Tätä voidaan käyttää vaikka yritysten toimesta, jos työntekijöille halutaan luoda Intranet-sivusto, jonne vain yrityksen sisäisillä henkilöillä on pääsy. (Hassel 2002, luku 7.)

Radiuksen ominaisuuksia ovat:

- Radius on UDP-protokollaan pohjautuva yhteydetön protokolla, joka ei käyty suoria yhteyksiä.
- Käyttää hop-by-hop-turvamallia.
- Tukee PAP- sekä CHAP-todentamista PPP-protokollan kautta.
- Käyttää MD5-algoritmia salasanojen suojaamiseen.
- Tukee AAA-mallia. (Hassel 2002, luku 2.)

2.2.2 PAP-protokolla

PAP-protokolla (Password Authentication Protocol) mahdollistaa yksinkertaisen menetelmän käyttäjälle todentaa henkilöllisyytensä käyttäen kaksisuuntaista kättelyä. Tämä tapahtuu ainoastaan silloin, kun linkitys perustetaan. Kun linkitys on tehty, käyttäjän toimesta lähetetään tunnusta sekä salasanaa autentikaattorille niin kauan, että todentaminen on suoritettu, tai yhteys suljetaan. (Technologies 2007, osa 5 luku 26.)

PAP ei ole vahva todentamisen menetelmä. Salasana toimitetaan tekstimuodossa, joten sillä todentamista voidaan yrittää tehdä kenen tahansa toimesta. Käyttäjä itse määrittelee, milloin todentaminen yritetään suorittaa. (Technologies 2007, osa 5 luku 26.)

2.2.3 CHAP-protokolla

CHAP-protokollaa (Challenge-Handshake Authentication Protocol) käytetään ajoittain henkilön identiteetin varmistamiseen käyttäen kolmisuuntaista käyttelyä. Tätä varten luodaan alkuun linkitys käyttäjän ja autentikaattorin välille. Kyseistä linkkiä voidaan tämän jälkeen käyttää milloin vain ilman uutta linkitystä. CHAP-protokolla toimii seuraavasti:

- Kun linkitys on tehty, autentikaattori lähettää ”haasteviestin” käyttäjälle.
- Käyttäjä vastaa tähän arvolla, joka on laskettu yksisuuntaisella tarkiste funktiolla.
- Autentikaattori tarkistaa vastauksen verraten sitä omaan, oletettuun tulokseensa. Jos arvot täsmäävät, todentaminen on onnistunut, muussa tapauksessa yhteys lopetetaan.
- Satunnaisin väliajoin autentikaattori lähettää uuden haasteen käyttäjälle, ja yllä mainitut vaiheet toistetaan. (Technologies 2007, luku 22.)

Todentaminen perustuu siis vain autentikaattorin sekä käyttäjän tietoisuudessa olevaan salausavaimeen, jolla ”haasteviestin” arvo ratkaistaan. Itse avainta ei lähetetä linkityksen kautta. Autentikaattori määrää sen, kuinka usein ja milloin todentaminen suoritetaan. Tämä tekee CHAP-protokollasta vahvemman protokollan, kuin mitä PAP-protokolla on. (Technologies 2007, osa 5 luku 22.)

2.2.4 DIAMETER

Diameter on todentamisen protokolla, jota käyttäen tarjotaan valikoima AAA-malliin perustuvia todentamisen keinoja. Se perustuu väljästi Radiukseen. Diameter jaetaan kahteen osaan: Diameter-protokollaan sekä Diameter-sovelluksiin. (Niemi, Khartabil, Mayer & Poikselka 2006, Diameter.)

Diameter on vertaisverkkoa käyttävä protokolla, sillä sekä päätelaitteet että palvelimet voivat luoda pyyntöjä ja vastauksia. Diameter-protokollassa on vain kahden

tyyppisiä viestejä: pyyntöjä ja vastauksia. Sen sijaan viestin sisältö määritellään komennoilla. Erilliset komennot erotetaan toisistaan komentokoodin avulla, joka määrittelee toiminnon, jonka viestin on tarkoitus suorittaa. Tässä muutama esimerkki suoritettavista komennoista:

- Capabilities-Exchange Request/Response. Komento, joka mahdollistaa vertaislaitteen identiteetin sekä sen valmiudet, esimerkiksi tuetut Diameterin sovellukset ja turvallisuustoimet.

- Disconnect-Peer-Request/Answer. Komento, jolla vertaislaitetta informoidaan aikeesta sulkea kuljetusyhteys.

- Accounting Request/Answer. Komento, jolla Diameteria käyttävä laite pyytää vertaislaitetta jakamaan tilastoituja tietoja. (Nakhjiri & Nakhjiri 2005, Diameter Protocol.)

2.2.5 EAP-protokolla

EAP-protokolla käyttää PPP-protokollaa todentamiseen. Se tukee useita todentamisen mekanismeja. Se valitsee käytettävän todentamisen mekanismin vasta juuri ennen todentamista. Tällä tavoin autentikaattorin on mahdollista tiedustella lisätietoja, ennen kuin se määrittelee käytettävän mekanismin. EAP-protokolla toimii seuraavasti:

- Kun linkitys on suoritettu, autentikaattori lähettää yhden tai useamman pyynnön todentaakseen vertaislaitteen. Pyynnöllä on tyyppikenttä, jolla määritellään pyynnön sisältö. Tyyppi voi olla esimerkiksi identiteetti, OTP-salasana tai vaikka MD5-haaste.

- Vertaislaite lähettää vastauspaketin jokaista pyyntöä kohden. Vastauksessa on tyyppikenttä, joka on vastaavanlainen kuin pyynnön tyyppikentässä.

- Autentikaattori päättä autentikointivaiheen joko hyväksyntä- tai hylkäyspaketilla. (Technologies 2007, osa 5 luku 21.)

3 MFA

3.1 Mitä on MFA

Termi MFA tulee sanoista multi-factor authentication eli moniosainen tunnistautuminen. Se tarjoaa ylimääräisiä kerroksia tunnistautumiselle. Se vaatii salasanojen lisäksi myös erillisen tunnisteen, esimerkiksi virtuaalisella tai fyysisellä autentikaattorilla luodun tunnisteen. MFA-tunnistautumista on hyvä käyttää kaikissa kirjautumistiedoissa turvallisuuden varmentamiseksi. (Kanikathottum 2019, Multi-Factor Authentication (MFA).)

Moniosaisella tunnistautumisella on rikas historia. Hyvä esimerkki tästä on sinettisormuksen käyttö dokumenttien välityksessä. Ensimmäinen tunnistautuminen on se, että paperi sinetöitiin tietyllä sinettisormuksella. Toisena olisi paperissa oleva tarkempi informaatio esimerkiksi jostain tunnistettavan henkilön ruumiinosasta tai arvesta, jota muut henkilöt eivät tiedä. Kolmantena voisi olla sinetöityyn paperiin kirjoitettu koodi, josta vastaanottaja tunnistaa toimittajan. (Stanislav 2015, luku 1.)

Yllä oleva esimerkki sisällyttää kaikki kolme tunnistautumisluokkaa aika ytimekkäästi:

1. Sinettisormus kuvaa sitä, mitä käyttäjällä on. Nykyisin tämä olisi älylaite.
2. Tiedot arvesta kuvaavat käyttäjää. Nykyisin tämä olisi esimerkiksi sormenjälki.
3. Koodi kertoo sen, mitä käyttäjä tietää. Nykyään tämän kattaa salasana.

Moderni teknologia tuo lukuisia eri keinoja, joilla näitä kolmea tunnistautumisluokkaa voidaan käsitellä eri tavoin. (Stanislav 2015, luku 1.)

Suuri osa on käyttänyt moniosaista tunnistautumista, vaikka ei sitä tietäisikään. Raha-automaattia käytettäessä annetaan automaatille aluksi pankkikortti. Tämä kuvaa sitä, mitä käyttäjällä on. Tämän jälkeen syötetään näytölle pankkikortin PIN-

koodi. Tämä kuvaa sitä, mitä käyttäjä tietää. Jo tässä käytettiin kahta kolmesta tunnistautumistavasta, jotain mitä on, sekä jotain mitä tiedetään. (Stanislav 2015, luku 1.)

3.2 MFA-tunnistautumisen välitys

Tunnistautumiseen liittyy kaksi avainkonseptia, in-band- ja out-of-band-menetelmät. Tällä määritellään se, mitä kanavaa pitkin ylimääräinen tunnistautuminen tehdään. (Stanislav 2015, luku 3.)

In-band-menetelmää käyttäessä käyttäjällä on laite tai sovellus, joka tarvittaessa generoi kertakäyttöisen salasanan eli OTP-salasanan. Tämän jälkeen syötetään kyseinen OTP-salasana kirjautumisen yhteydessä. Tällä on kuitenkin omat riskinsä, sillä tämä salasana todennäköisesti välitetään samoja kanavia pitkin, mitä tunnukset. Tämän takia ne voidaan mahdollisesti kaapata jonkun toisen tahon toimesta. (Stanislav 2015, luku 3.)

Out-of-band-menetelmällä tarkoitetaan sitä, että ylimääräinen tunnistautuminen tehdään jonkin toisen kanavan kautta. Tästä hyvänä esimerkkinä on se, että verkkopankkiin kirjautuessa pankilta tulee varmistussoitto puhelimeen. Tällöin varkaalla pitäisi olla tunnusten lisäksi hallussaan myös käyttäjän puhelin, jotta heidän onnistuisi kirjautua sisään. (Stanislav 2015, luku 3.)

3.3 Yleisiä MFA-tunnistustapoja

Yleisenä käsityksenä saattaa olla, että moniosaisella tunnistautumisella viitataan siihen, että jokin sovellus generoi salasanan, joka syötetään kirjautumisen yhteydessä. Nykyisin on kuitenkin useita eri tapoja tehdä moniosainen tunnistautuminen, eikä käsite ole enää niin yksiselitteinen. (Stanislav 2015, luku 4.)

3.3.1 Laitteistopohjainen OTP-generointi

Laitteistopohjainen OPT-generointi on ollut jo vuosikymmeniä erittäin tyypillinen tapa moniosaisen tunnistautumisen suorittamiseksi. Tähän voidaan käyttää monia eri laitteita, esimerkiksi avainkorttia tai puhelinta, mutta tämän lisäksi myös tapa, jolla salasana annetaan, voi vaihdella paljon. Se voi olla esitettynä vaikkapa näytöllä, välittyä USB-laitteen kautta tai jopa suoraan Bluetoothin kautta päätelaitteeseen. Laitteet voivat kestää useita vuosia, mutta näissä on ongelma se, että ne voivat kadota loppujen lopuksi aika helposti. (Stanislav 2015, luku 4.)

3.3.2 SMS-pohjainen OTP-toimitus

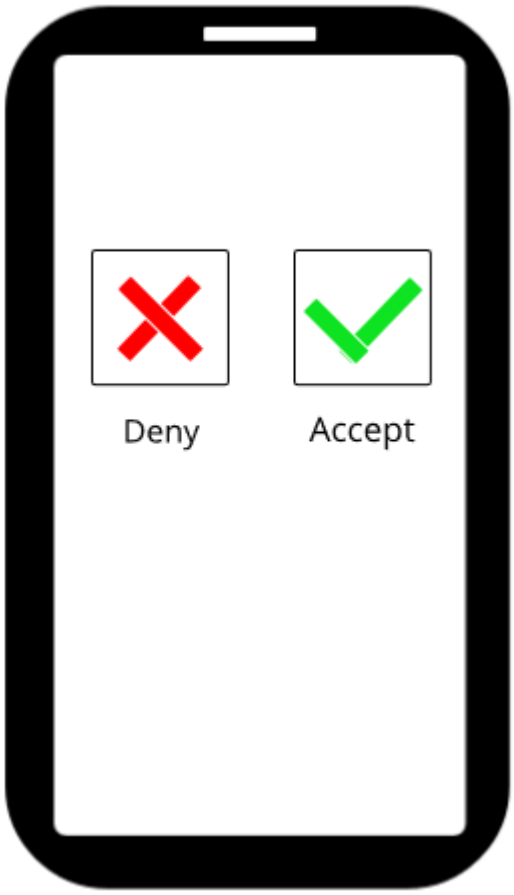
Kirjautumisen yhteydessä käyttäjälle tulee ennalta määriteltyyn puhelinnumeroon tekstiviesti, joka sisältää kirjautumisen yhteydessä käytettävän OTP-salasanan. Tämä on myös suosittu tapa, sillä nykyään lähes kaikilla loppukäyttäjillä on puhelin, joka voi vastaanottaa tekstiviestejä. Tämä on erittäin halpa menetelmä, sillä tekstiviestien hinta on erittäin pieni. Tähän ei siis tarvitsee ostaa mitään erillistä laitetta. (Stanislav 2015, luku 4.)

3.3.3 Puhelinsoitolla varmistaminen

Puhelinsoitolla varmistaminen on hyvin yleinen todentamistapa, jos on kyse taloudellisesta yrityksestä tai toiminnasta. Tunnistautumisen yhteydessä saadaan ennalta määriteltyyn puhelinnumeroon puhelu. Voi olla, että käyttäjä joutuu ilmoittamaan puhelussa esimerkiksi henkilönumeronsa loppuosan, tai vaikka valitsemaan puhelimesta tietty näppäin. Kaiken kaikkiaan tämä antaa kuitenkin jonkinlaisen toisen varmennuksen, sillä puhelimen pitäisi olla käyttäjän hallussa, eikä kenelläkään muulla. (Stanislav 2015, luku 4.)

3.3.4 Push-notification-pohjainen todentaminen

Tunnistautumisen yhteydessä käyttäjän mobiililaitteeseen tulee tästä ilmoitus. Ilmoitus voi olla mahdollisesti painike (kuva 1) tai liu'utettava näppäin, jonka kanssa vuorovaikuttamisella varmistetaan, että oikea henkilö on kirjautumassa sisään. Tällöin myös käyttäjä itse havaitsee, mikäli hänen tunnustaan yrittää käyttää joku muu, sillä hänelle tulee tästä ilmoitus. (Stanislav 2015, luku 4.)



Kuva 1. Esimerkki Push-notification-pohjaisesta todentamisesta.

3.3.5 Biometrinen tunnistautuminen

Tunnistautumisen yhteydessä pyydetään käyttäjältä biologisen osan skannausta, esimerkiksi sormen (kuva 2) tai silmän. Tämän jälkeen sitä verrataan ennalta määriteltyyn tietoon. Mikäli ne täsmäävät, tunnistautuminen onnistuu. Biometrinen tunnistautuminen ei ole ollut pitkää aikaa yleisessä käytössä, sillä laitteet ovat olleet

erittäin kalliita, ja niiden käyttö on saattanut olla ajoittain kankeaa. Tähän on kuitenkin tullut suuri muutos, sillä älypuhelimiin on ruvennut tulemaan erittäin paljon sormenjäljentunnistimia ja esimerkiksi kasvon tunnistimia. (Stanislav 2015, luku 4.)

Kuva 2. Perinteinen biometrinen tunnistin eli sormenjäljentunnistin. (Pixabay 30.10.2015.)

3.3.6 Älykortilla tunnistautuminen

Älykortti on yleensä noin luottokortin kokoinen kortti (kuva 3), jonka sisällä on pieni siru. Tämä siru suorittaa useanlaisia salaustoimintoja. Muita tunnettuja malleja on USB-tikku, avaimenperä ja älypuhelimet. Tunnistautumisen yhteydessä korttia käytetään tunnistuslaitteen sisällä tai se luetaan radioaaltojen avulla. Tätä käytetään yleensä tietokoneella kirjautuessa tai ovien läpikulkuun. (Stanislav 2015, luku 4.)

Kuva 3. Yksi lukuisista älykorttimalleista.

4 AZURE MULTI-FACTOR AUTHENTICATION

4.1 Yleistä

Azure MFA on skaalautuva ja luotettava ratkaisu kaksiosaista varmistusta varten. Se voidaan integroida yrityksen tiloissa olevan Active Directoryn kanssa. Sen käyttöönottaminen on erittäin helppoa. Se voidaan myös integroida jo olemassa olevaan AD-palveluun, sekä erillisiin mukautettuihin sovelluksiin. (Demiliani & Michalski 2018, SSO and MFA.)

4.2 Todentamisen tavat

Kun Azuren MFA on aktivoituna, ja käyttäjät yrittävät kirjautua, heille lähetetään toinen osa todentamisesta. Toisen todentamisen vaihe voi olla yksi seuraavista. Käyttäjä itse saa etukäteen valita, mikä se on.

- Puhelimeen soitto: Käyttäjä vastaanottaa puhelun ennalta määriteltyyn puhelinnumeroon. Hän syöttää puhelimeen PIN-koodin ja painaa #-näppäintä.
- Tekstiviesti: Käyttäjä vastaanottaa kuusinumeroisen koodin tekstiviestillä. Koodi syötetään kirjautumisruudulla olevaan tälle varattuun kenttään.
- Mobiilisovelluksen ilmoitus: Käyttäjälle lähetetään sovelluksen kautta ilmoitus kirjautumisesta. Hän syöttää ennalta määritellyn PIN-koodin sovellukseen, jonka jälkeen kirjautuminen onnistuu.
- Mobiilisovelluksen varmistuskoodi: Sovelluksessa näkyy 30 sekunnin välein vaihtuva varmistuskoodi. Käyttäjä syöttää koodin kirjautumisruudussa sille varattuun kenttään. (Demiliani & Michalski 2018, SSO and MFA.)

4.3 Version valinta

Azuren MFA-palvelusta on olemassa kaksi eri versioita, joista yrityksen tulee valita. Nämä ovat pilvipohjainen MFA (Azure MFA Service), sekä yrityksen tiloissa oleville palvelimille asentaminen (Azure MFA Server). (Microsoft 11.10.2018.)

Azure MFA Servicen käyttö ei vaadi yritykseltä minkäänlaista aikaisempaa infrastruktuuria. Sitä voi käyttää myös yrityksen ulkopuoliset tahot. Tämä vaihtoehto on suositeltu, mikäli kyseessä on täysin uusi käyttöönotto. (Microsoft 11.10.2018.)

Azure MFA Serverin käyttöönottoa suositellaan, mikäli yrityksellä on jo entuudestaan infrastruktuuria. Eli mikäli yrityksen tiloissa oleville palvelimille on jo otettu käyttöön AD-ympäristö, ja täältä löytyviä tietoja halutaan käyttää MFA-palvelun yhteydessä. (Microsoft 11.10.2018.)

Seuraavissa kuvissa käydään läpi seikkoja, joiden perusteella yritykselle saadaan valittua oikea palvelumuoto. (Microsoft 11.17.2018.)

4.3.1 Turvaamisen kohde

Oikean kaksivaiheisen vahvistusratkaisun määrittelemiseksi tulee vastata kysymykseen, mitä yritetään suojata ylimääräisellä varmistustekijällä. Onko se kenties sovellus, joka sijaitsee Azuressa, vai esimerkiksi etäyhteys järjestelmä? Selvittämällä tämä, saadaan vastaus sille, missä useampi vaiheinen todennus on otettava käyttöön. Kuvassa 4 näkyy vertailua versioiden turvaamisien välillä. (Microsoft 11.17.2018.)

What are you trying to secure	MFA in the cloud	MFA Server
First-party Microsoft apps	•	•
SaaS apps in the app gallery	•	
Web applications published through Azure AD App Proxy	•	
IIS applications not published through Azure AD App Proxy		•
Remote access such as VPN, RDG using the NPS Extension or an existing NPS Server	•	•

Kuva 4. Mitä MFA-palvelulta halutaan.
(Microsoft 11.17.2018.)

4.3.2 Käyttäjien sijainti

Seuraavaksi selvitetään, missä käyttäjät sijaitsevat. Osa vaihtoehdoista mahdollistaa pelkästään toisen version, mutta välillä voidaan valita molempien väliltä kuten kuvan 5 valinnoista käy ilmi. (Microsoft 11.17.2018, [Viitattu 25.3.2019].)

User Location	MFA in the cloud	MFA Server
Azure Active Directory	•	
Azure AD and on-premises AD using federation with AD FS	•	•
Azure AD and on-premises AD using Azure AD Connect - no password hash sync or pass-through authentication	•	•
Azure AD and on-premises AD using Azure AD Connect - with password hash sync or pass-through authentication	•	
On-premises Active Directory		•

Kuva 5. Käyttäjien sijainti.
(Microsoft 11.17.2018.)

4.3.3 Tarvittavat toiminnot

Kuvan 6 taulukko vertailee versioiden ominaisuuksia keskenään. Näiden perusteella tehdään lopullinen ratkaisu version valinnan suhteen. (Microsoft 11.17.2018.)

Feature	MFA in the cloud	MFA Server
Mobile app notification as a second factor	•	•
Mobile app verification code as a second factor	•	•
Phone call as second factor	•	•
One-way SMS as second factor	•	•
Hardware Tokens as second factor	• (Public preview)	•
App passwords for Office 365 clients that don't support MFA	•	
Admin control over authentication methods	•	•
PIN mode		•
Fraud alert	•	•
MFA Reports	•	•
One-Time Bypass		•
Custom greetings for phone calls	•	•
Customizable caller ID for phone calls	•	•
Trusted IPs	•	•
Remember MFA for trusted devices	•	
Conditional access	•	•
Cache		•

Kuva 6. Tarvittavat toiminnat MFA-palvelulta.
(Microsoft 11.17.2018.)

5 TYÖN TOTEUTUS

5.1 Suunnittelu ja aloitus

Asiakas halusi selvittää kaksivaiheisen varmentamisen käyttöönottoa valikoidulle ryhmälle. Kyseiseen ryhmään kuuluu johtoporras, sekä erinäisten sovellusten ja järjestelmien pääkäyttäjät. Kaksivaiheisella varmentamisella pyritään parantamaan yrityksen tietoturvaa, ja ehkäisemään hyökkäyksiä.

Kaksivaiheisella varmentamisella pyritään turvaamaan ulkoisesta verkosta tehdyt kirjautumisyritykset, joten sitä ei oteta käyttöön yrityksen omissa verkoissa. Tämä mahdollistetaan conditional access -toiminnon avulla, jolla saadaan määriteltyä verkot, joissa kaksiosaista varmennusta ei haluta huomioida. Conditional access -toiminnolla määritellään kaikkien yrityksen toimipisteiden verkot.

Ennen käyttöönoton aloitusta pidettiin vielä pienimuotoinen palaveri asiakkaan IT-vastaavan kanssa. Palaverissa käytiin läpi projektin kulkua, kestoa sekä yksityskohtia siihen liittyen.

Asiakkaalla on jo olemassa olevat fyysiset palvelimet, joissa käyttäjätiedot ovat AD-hakemistopalvelussa. Näitä samaisia käyttäjätietoja tullaan käyttämään myös kaksiosaisen varmennuksen yhteydessä, joten loogiseksi vaihtoehdoksi version valinnan suhteen tulee Azuren MFA Server. Vaihtoehtoina MFA Server-palvelun asennukselle on kaksi sijaintia: joko jo valmiina olevalle palvelimelle, jonne yrityksen SMTP relay on määritelty, tai täysin uudelle virtuaalipalvelimelle. Tässä päädyttiin jo olemassa olevalle palvelimelle, koska täältä löytyi entuudestaan jo SMTP relay määriteltynä. Mikäli varmistukseen käytettävät viestit eivät tule perille, niin tämän avulla voidaan samalla varmistaa, että missä mahdollinen ongelma on. Palvelimesta käytetään nimeä MFAPalvelin.

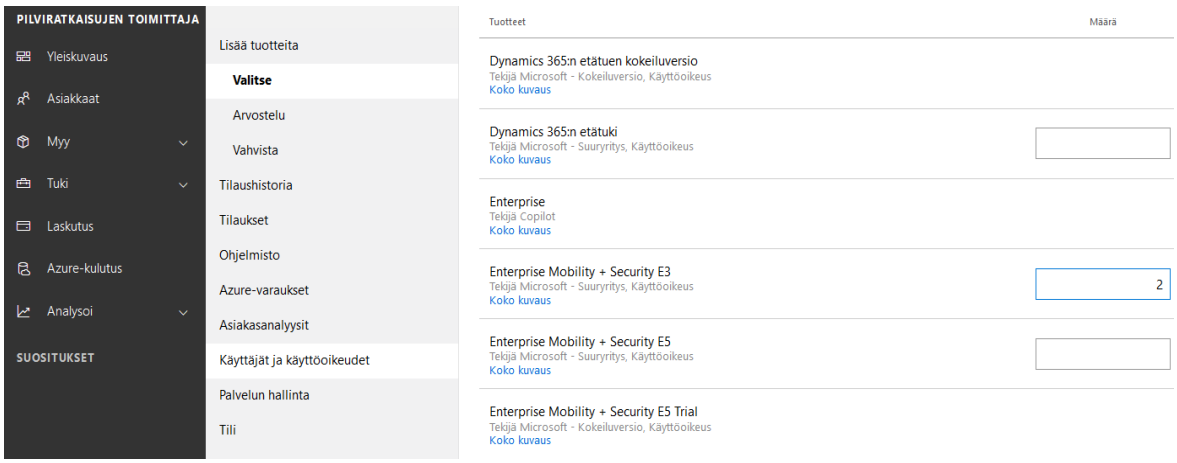
Käyttäjien suhteen tultiin siihen tulokseen, että MFA otetaan käyttöön aluksi erittäin pienelle testiryhmälle, johon kuuluvat muutama asiakkaan IT-henkilöä. Nämä käyttäjät testaavat aluksi varmennuksen toimivuuden, ja raportoivat mahdollisista muokkaustarpeista. Kun toimintaan ollaan tyytyväisi, otetaan MFA käyttöön myös koko johtoryhmälle, sekä esimerkiksi sovellusten pääkäyttäjille.

Asiakkaalle ehdotettiin kahta mahdollista lisenssityyppiä. Vaihtoehtoina oli joko kulutuslisenssi, jolloin tästä maksettaisiin sen mukaan, paljonko MFA-palvelua käytetään, tai kiinteä summa lisenssiä kohden. Tässä päädyttiin kiinteään summaan, sillä tällöin asiakkaan ei tarvitse rajoittaa MFA-palvelun käyttöä.

Lopulta päätettiin vielä, että millä tapaa toinen varmistus kirjautumisen yhteydessä tehdään. Tässä parhaina vaihtoehtoina olivat sähköposti, tekstiviesti tai soitto puhelimeen. Päädyttiin siihen, että tekstiviestillä tulee koodi, joka syötetään kirjautumisen yhteydessä. Tämän koettiin olevan käyttäjille kaikista helpoin tapa suorittaa varmistus.

5.2 Lisenssien hankinta ja allokointi

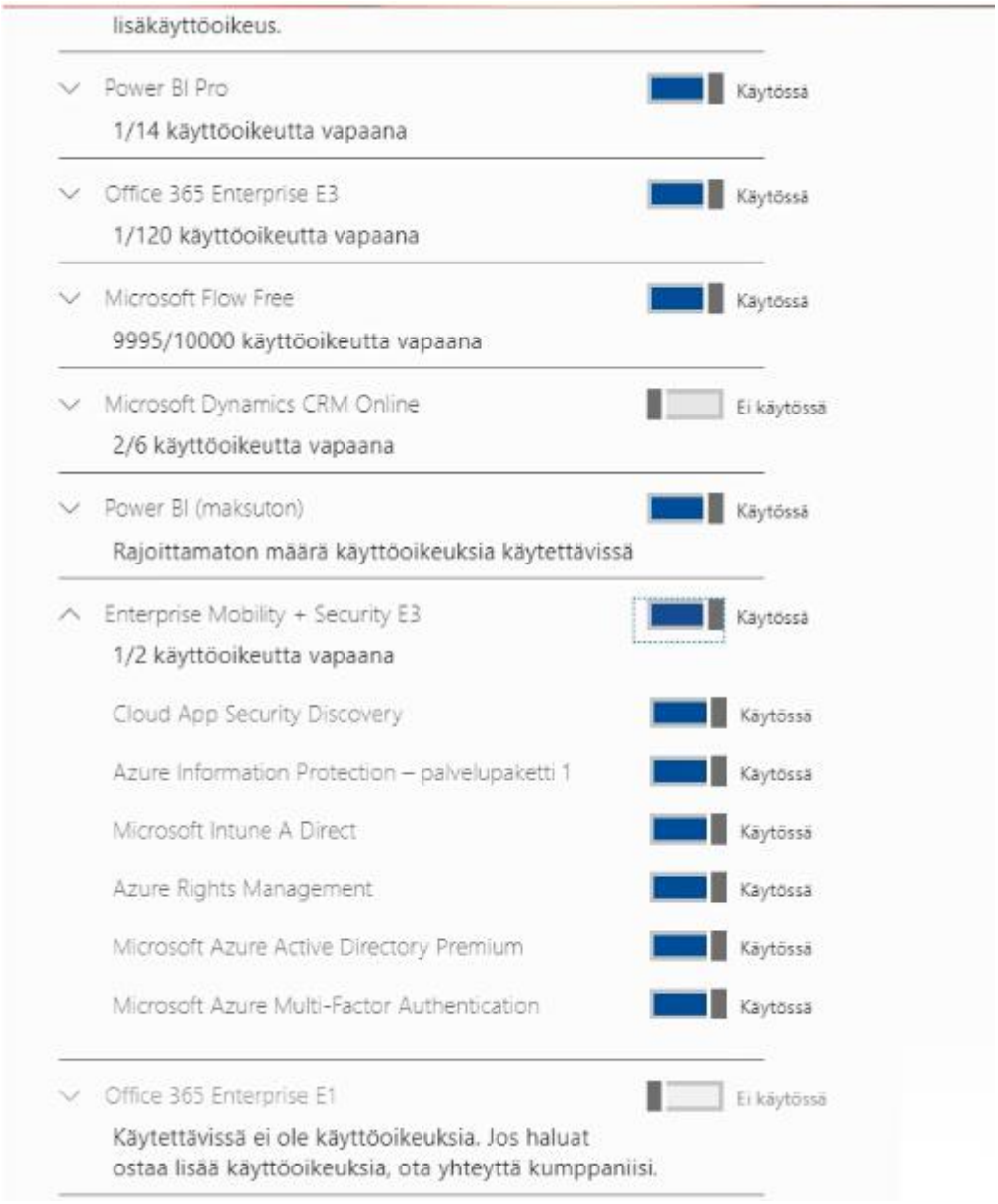
Ensimmäiseksi käydään lisäämässä asiakkaalle tarvittavat lisenssit testikäyttöä varten. Tämä tapahtuu kirjautumalla Microsoftin kumppanikeskukseen. Täältä haetaan ostettavat tuotteet/lisenssit, ja etsitään asiakkaan valitsema lisenssi.



Kuva 7. Lisenssien hankkiminen Microsoftin kumppanikeskuksesta.

Aluksi otetaan pelkästään kaksi lisenssiä (kuva 7), sillä asiakas on ilmoittanut kahdesta testaajasta. Ennen lisenssin lisäämistä heille, käydään yksi lisenssi lisäämässä testikäyttäjälle, jolla voidaan testata MFA-palvelun toiminta, kunhan tarvittavat asennukset on tehty. Myös tämä tapahtuu Microsoftin kumppanikeskuksen kautta. Nyt kuitenkin navigoidaan palvelujen hallintaan. Tätä kautta päästään Microsoftin Admin Centteriin. Täältä haetaan testikäyttäjä, ja lisätään tälle toinen juuri

hankituista Enterprise Mobility + Security E3 -lisensseistä, joka kuvassa 8 on valittu käyttöön.



Kuva 8. Enterprise Mobility + Security E3 -lisenssin lisäys.

Myöhemmin samalla tapaa käydään lisenssit lisäämässä testiryhmälle sekä lopulta kaikille, joille se on tarkoitettu.

5.3 AD-tietokannan henkilötietojen tarkistus

Koska varmistustavaksi tullaan määrittelemään tekstiviestivarmennus, tulee käyttäjien henkilötiedoissa löytyä AD-hakemistopalvelusta puhelinnumero. Tämän asian

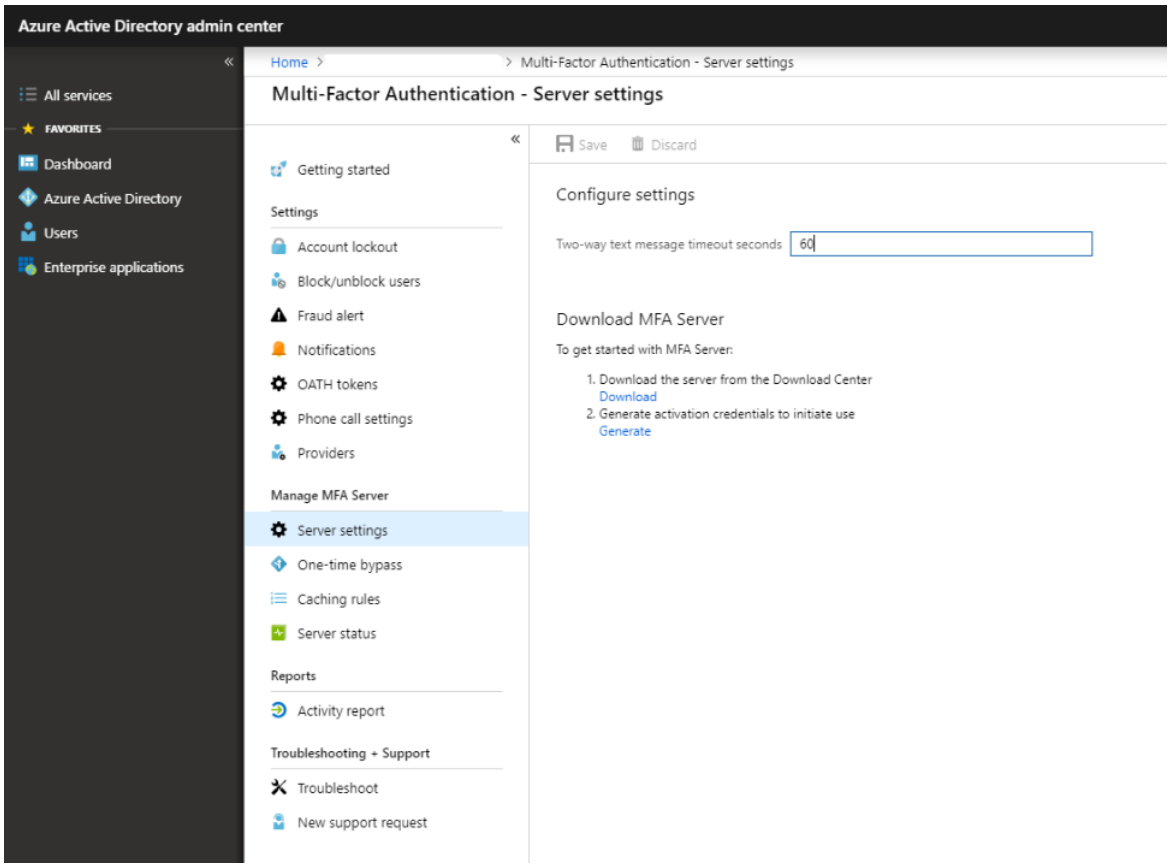
pitäisi olla kuitenkin kunnossa, sillä asiakkaalla on numerotiedot päivitetty viimeksi 2017. Mikäli tiedot eivät kuitenkaan ole ajan tasalla, niin tehdään tarvittavat muokkaukset. Tiedot voidaan tarkistaa henkilöstöhallinnon kautta.

Asiakkaan AD-hakemistopalveluun luodaan O365 Admins -niminen oikeusryhmä. Tänne lisätään asiakkaan testikäyttäjät sekä sellaiset käyttäjät, joilla kaksiosainen varmennus otetaan käyttöön, mutta he eivät kuulu johtoportaaseen, sekä kaksiosaisen varmennuksen testaamiseen käytettävä testikäyttäjä. Johtoportaan henkilöille oli jo olemassa oma oikeusryhmänsä, jonka nimi on Johtoryhma.

Samalla käydään myös lisäämässä ensimmäiseen testaukseen tarkoitetulle tunnukselle puhelinnumero, jota tarvitaan myöhemmin, kun kaksiosaisen varmennuksen toimivuutta testataan.

5.4 Azure MFA Server -palvelun asennus

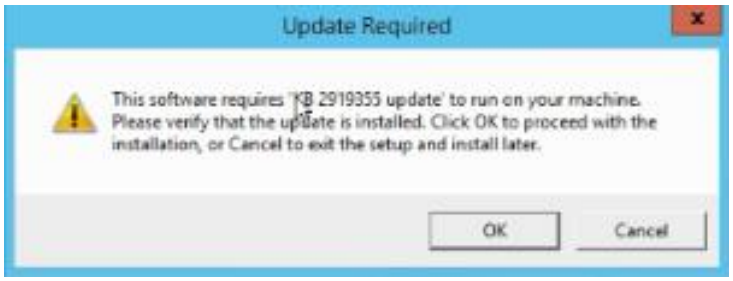
Nyt on itse MFA Serverin asennuksen aika. Tätä varten siirrytään MFAPalvelimelle ja ladataan sinne Azuren hallinnan kautta Azuren MFA Server -palvelun asennuspaketti. Tämä ladataan suoraan palvelimelle, tai siirretään se latauksen jälkeen tietokoneelta.



Kuva 9. Azure MFA Server -palvelun asennus.

Kuvassa 9 näkyvällä Download-painikkeella saadaan asennuspaketti ladattua. Tämän jälkeen samaisessa kuvassa olevalla Generate-painikkeella luodaan aktivointitunnus, jota käytetään MFA Server -palvelun asennuksen yhteydessä. Nämä tunnukset otetaan talteen myöhempää vaihetta varten.

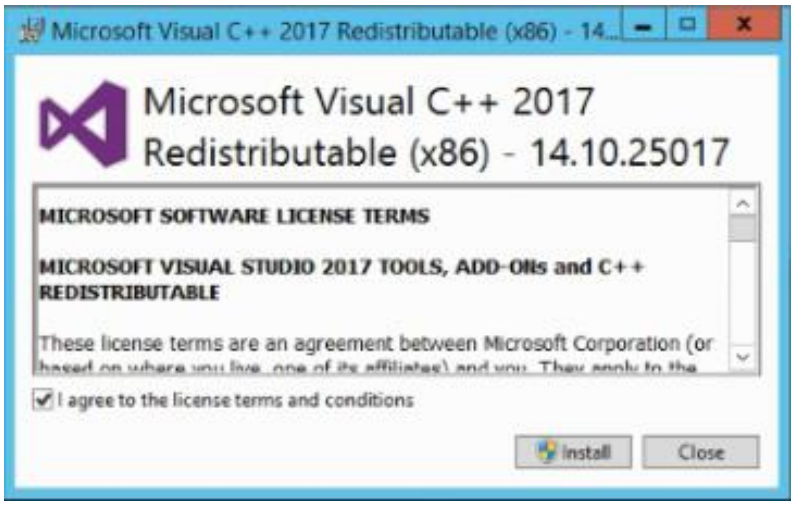
Kun Azuren MFA Server ollaan saatu siirrettyä palvelimelle, voidaan aloittaa sen asennus. Heti asennuksen alkuvaiheessa kuitenkin ilmeni, että palvelimelta puuttui Windowsin Serverin päivitys KB 2119335. Ilman tätä päivitystä ei MFA Server -palvelua saisi palvelimelle asennettua.



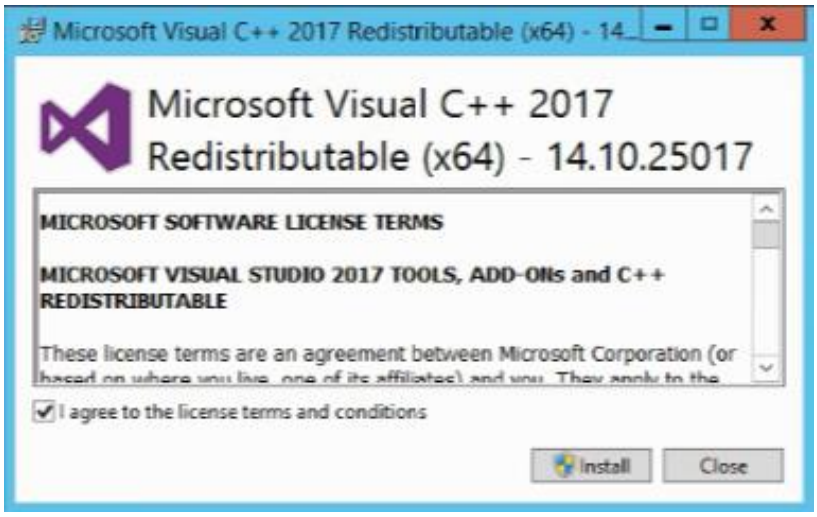
Kuva 10. MFAPalvelimelta puuttuva päivitys.

Päivitys koetettiin asentaa kuvan 10 mukaisen virheilmoituksen kautta painamalla OK-näppäintä. Tämä ei kuitenkaan onnistunut, vaan päivitys ei tällä tapaa suostunut asentumaan. Palvelin käynnistettiin uudelleen, jotta päivitystä päästään asentamaan puhtaalta pöydältä. Käynnistyksen yhteydessä valitaan syyksi (Application: Maintenance[Planned]). Tällä tavoin vältytään, ettei käynnistys aiheuta hälytyksiä toimimattomuudesta. Kun uudelleenkäynnistys on suoritettu, haetaan päivitys suoraan Microsoftin sivuilta ja asennetaan se tämän kautta onnistuneesti.

Nyt kun tarvittavat päivitykset on tehty, niin voidaan jatkaa MFA Server -palvelun asennusta. MFAPalvelimelle tuotu asennuspaketti käynnistetään uudelleen. Asennuksen yhteydessä tulee asentaa kaksi erillistä kuvien 11 ja 12 mukaista Microsoftin Visual C++ Runtime Librarya, joita tarvitaan Azure MFA -palvelun käytössä.



Kuva 11. Visual C++ Runtime Library (x86) -asennus.



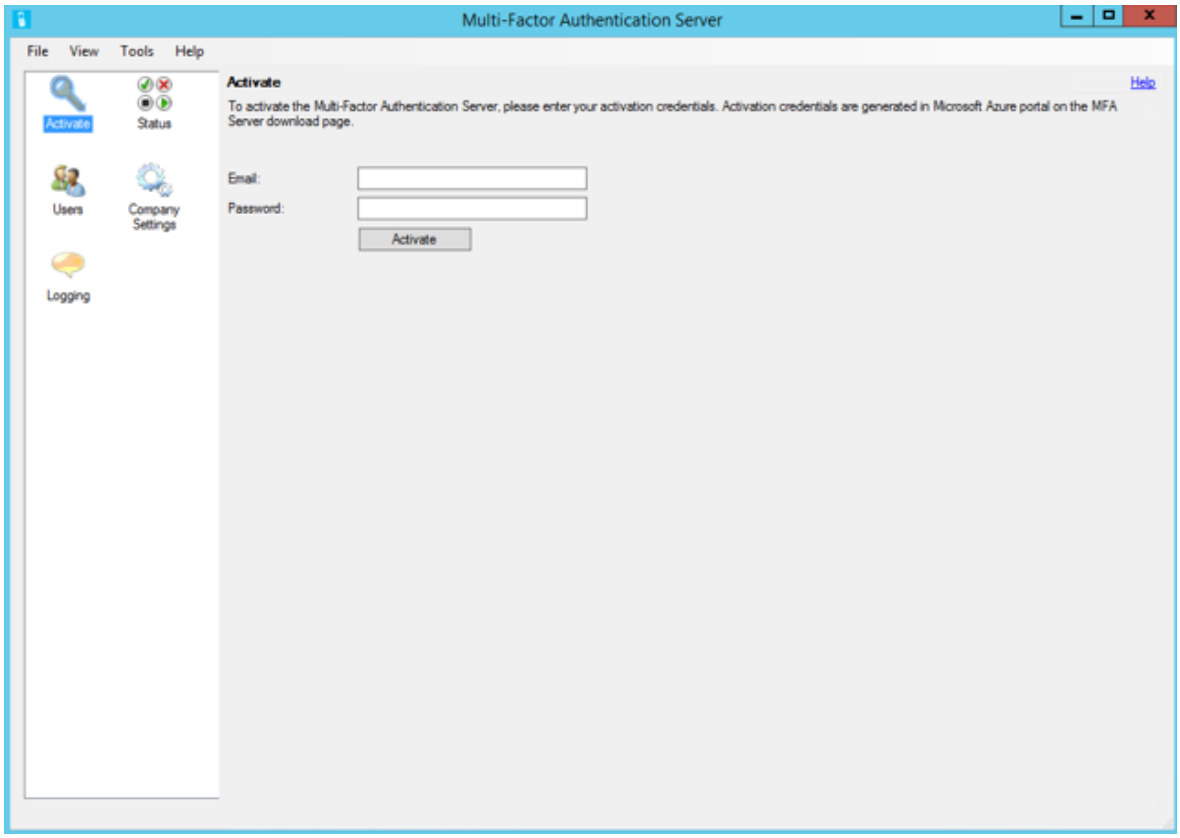
Kuva 12. Visual C++ Runtime Library (x64) -asennus.

Asennus viedään loppuun hyväksymällä Azure MFA Server -palvelun lisenssiehdot, sekä valitsemalla asennuksen sijainti. Lisenssiehdot hyväksyttyä seuraavaan vaiheeseen päästään Next-näppäimellä. MFA Server -palvelun asennussijainniksi valitaan oletuksena oleva polku C:\Program Files\Multi-Factor Authentication Server.

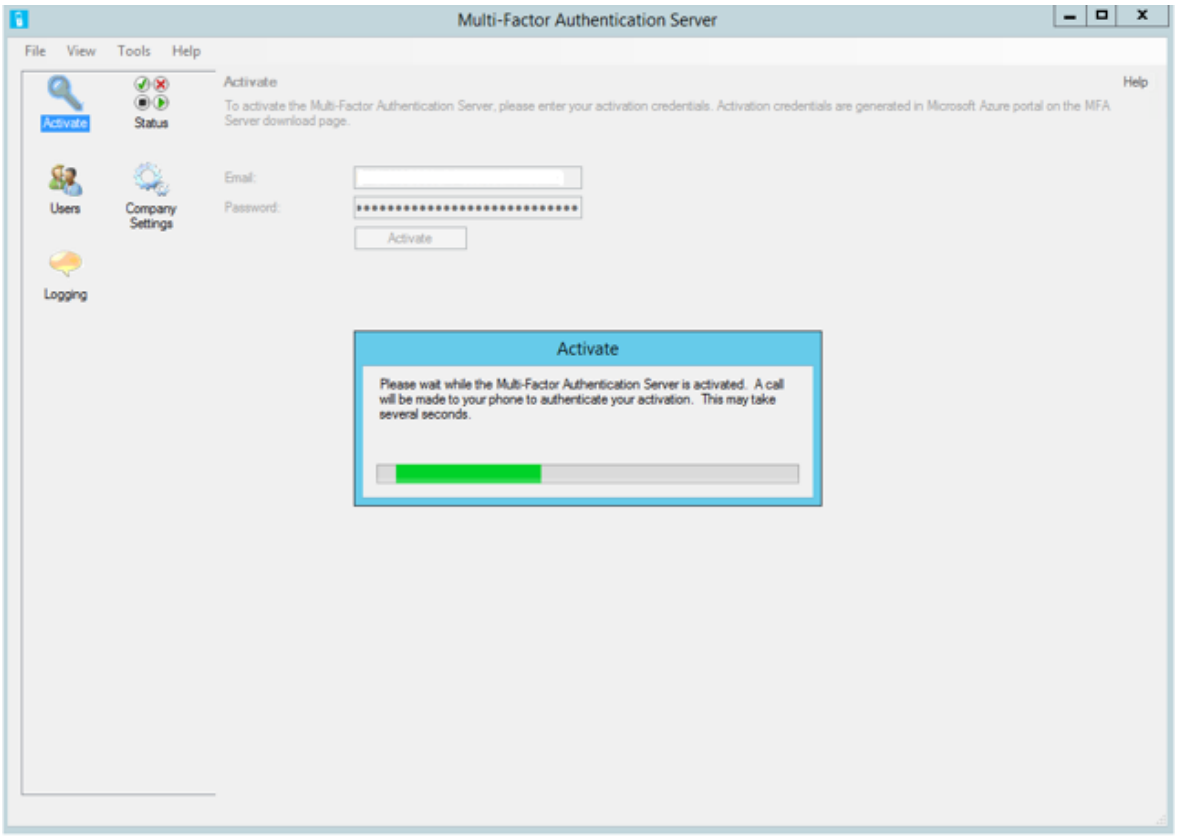
Kuva 13. MFA Server -palvelun kuvake palvelimen työpöydällä.

Asennuksen jälkeen MFAPalvelimen työpöydälle tulee kuvan 13 mukainen kuvake, jolla juuri asennettu MFA Server saadaan aukaistua. Sovellus aukaistaan ja aktivoidaan MFA Server käyttökuntoon.

Kun MFA Server avataan ensimmäisen kerran, aukeaa kuvan 14 mukainen näkymä. Nyt tarvitaan aktivointitunnuksia, jotka generoitiin MFA Server -palvelun asennuksen alkuvaiheessa. Tunnukset haetaan ja syötetään ne Email- ja Password-kenttiin. Tämän jälkeen klikataan Activate ja MFA Server aloittaa aktivoinnin (kuva 15).

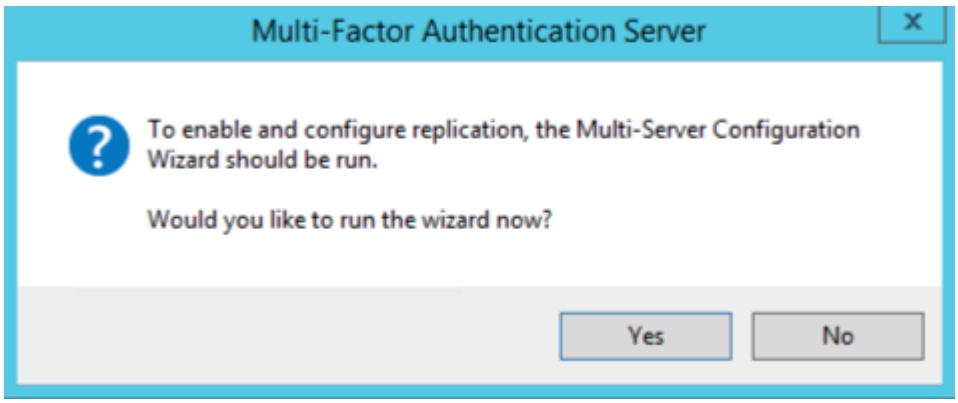


Kuva 14. Azure MFA Server -palvelun ensiavauksen näkymä.



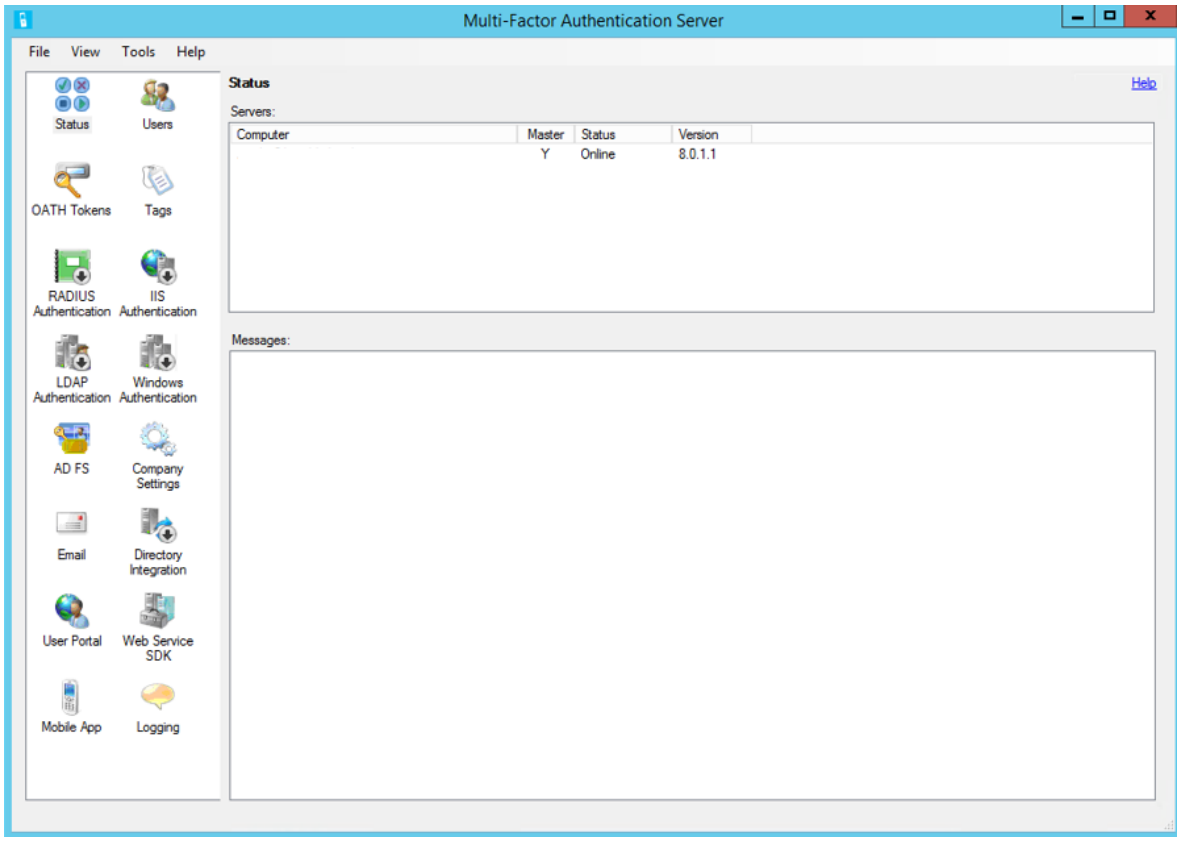
Kuva 15. Azure MFA Serverin aktivointi asennuksen jälkeen.

Kun aktivointi on suoritettu, tulee näytölle kuvan 16 mukainen kysymys. Tässä tapauksessa asennetaan ensimmäistä ja ainoaa MFA-palvelua, joten valitaan vaihtoehdoksi No. Mikäli olisi tarvetta useamman MFA-palvelimen ympäristölle, niin tällöin voitaisiin valita Yes. Tälle ei kuitenkaan tässä tapauksessa ole tarvetta.



Kuva 16. Kysymys useamman MFA Server -palvelun asennukselle.

Kun aktivointi on mennyt läpi, MFA Server -palvelun alkunäkymä muuttuu kuvan 17 mukaiseksi. Näkyviin tulleista valikoista voidaan ruveta konfiguroimaan MFA-palvelua, sekä ottamaan se käyttöön halutuille henkilöille.



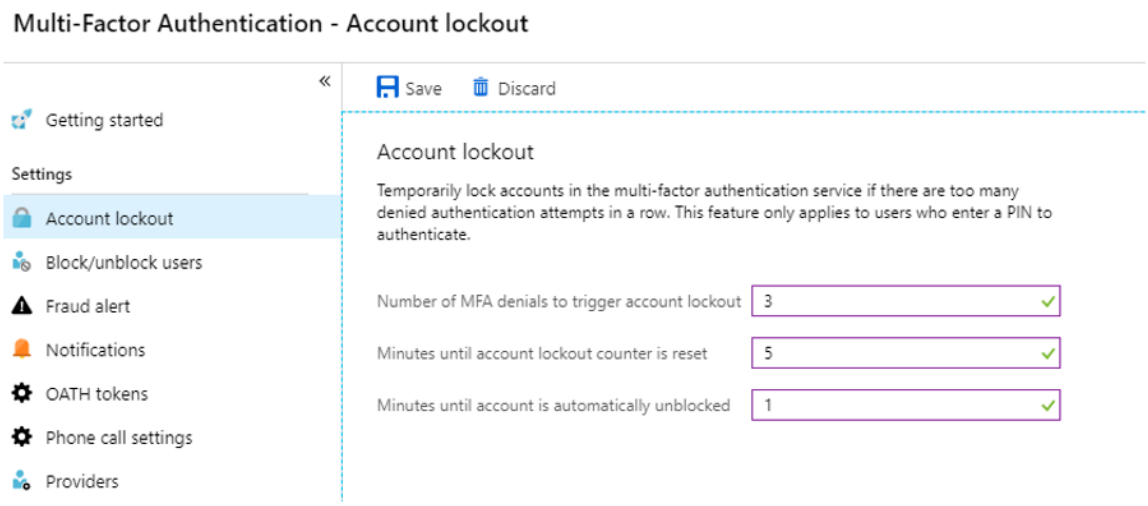
Kuva 17. Alkunäkymä MFA Server -palvelun aktivoinnin jälkeen.

5.5 Azure MFA Server -palvelun konfigurointi

Nyt kun MFA Server -palvelun asennus ja aktivointi on suoritettu, voidaan sitä ruveta konfiguroimaan, ja ottamaan käyttöön halutut asetukset.

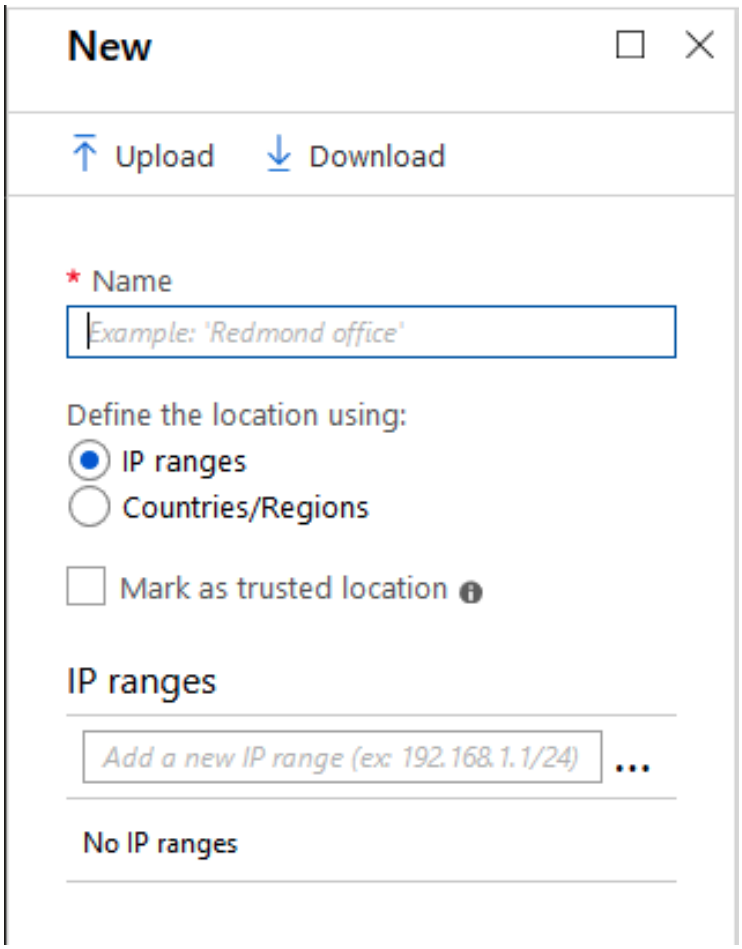
Aluksi siirrytään takaisin Office 365:n kumppanikeskuksen kautta Azuren hallintaan. Täältä valitaan MFA ja kuvan 18 mukaisesti asetusten alta muokataan asetuksia tunnusten lukittautumisen suhteen, mikäli kaksiosaista todentamista kokeillaan liian useasti väärin. Tässä määritellään, että kolmen väärän koodin yrittämisen jälkeen tunnus menee lukkoon. Mikäli lukkiutuminen tapahtuu, se aukeaa itsestään minuutin kuluttua, jonka jälkeen kirjautumista voidaan yrittää uudelleen. Mikäli vääriä yrityksiä tulee vähemmän kuin kolme, ne nollaantuvat viiden minuutin kuluttua, jonka

jälkeen kirjautumista voidaan taas yrittää kolmeen otteeseen, ennen kuin tunnukset lukkiutuvat.



Kuva 18. Asetukset väärien kirjautumisyritysten suhteen.

Tämän jälkeen pysytään Azuren hallinnan puolella, mutta navigoidaan sivulla turvallisuusasetusten kautta määrittelemään Condition Access -toiminnot, eli IP-osoitteet, joissa kaksiosainen varmitus ei ole käytössä. Näiden määritteleminen tapahtuu Azuren hallinnan turva-asetusten kautta kohdasta Conditional Access. Täältä valitaan uuden osoitteen määritys, jolloin aukeaa kuvan 19 mukainen näkymä. Kentät täytetään tarvittavilla tiedoilla, ja valitaan Mark as trusted location -vaihtoehto. Toistetaan tämä samainen verkon lisäys jokaisella asiakkaan toimitilojen verkoille. Tällä tapaa määriteltiin asiakkaan sisäinen verkko, jossa kaksiosainen todentaminen ei ole käytössä. Mikäli kirjautumista yritetään verkosta, jota ei tässä vaiheessa merkitty, tulee kirjautumisen yhteydessä todentaa kirjautuminen MFA Server -palvelulle määritetyn valinnan avulla.



Kuva 19. Conditional Access -verkkojen määritys.

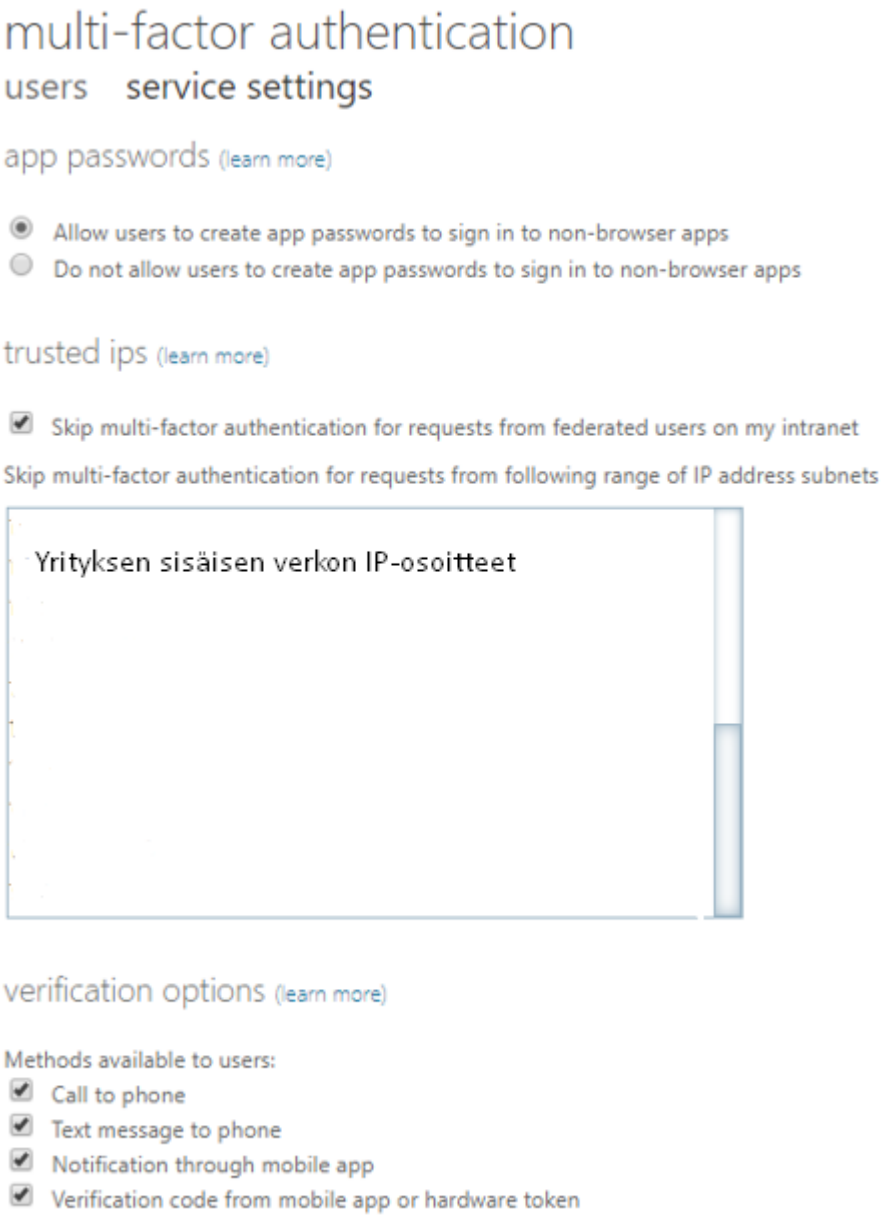
Tämän jälkeen siirrytään Azuren hallinnassa ylimääräisten pilvi-pohjaisten MFA-asetusten pariin. Tämän kautta saadaan määriteltyä seuraavat kuvan 20 mukaiset asetukset:

- Sovellussalasanat. Nämä ovat salasanoja, joita käytetään sellaisiin sovelluksiin kirjautuessa, jotka eivät tue kaksiosaista todentamista. Tällaisia sovelluksia ovat esimerkiksi Office 2010 ja aikaisemmat versiot tai Apple Mail -käyttöjärjestelmän versiota 11 aikaisemmat versiot.

- Conditional Access -vaiheessa määritellyt sisäiset verkot saadaan otettua tämän kautta käyttöön.

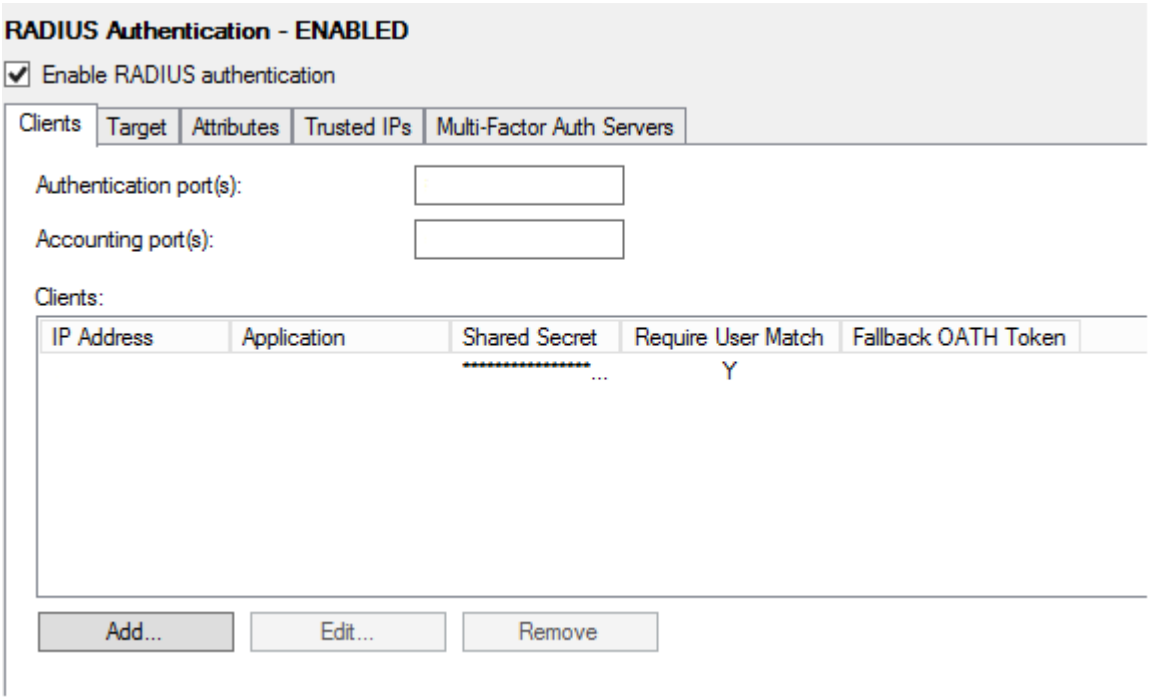
- Tapa, jolla asiakkaan käyttäjät tekevät toisen todennuksensa. Aikaisemmasta poiketen jokainen vaihtoehto jätetään mahdolliseksi, mutta ohjeistuksessa suositellaan käyttämään tekstiviestillä varmennusta.

- Viimeisenä vaihtoehtona olisi, että voivatko käyttäjät tehdä laitteesta luotetun korkeintaan 60 päivän ajaksi. Tämä tarkoittaisi sitä, että kun käyttäjä on kertaalleen suorittanut todennuksen, ei sitä tarvitsisi kyseisellä laitteella valittuna aikana enää tehdä. Tämä jätetään asiakkaalta pois käytöstä, sillä todennus halutaan suoritettavaksi joka kerta.



Kuva 20. Pilvi-pohjaiset asetukset Azuren hallinasta.

Viimeiseksi konfiguroinnin kohdalta siirrytään takaisin MFAPalvelimelle ja siirrytään MFA Server -palvelussa kuvassa 17 näkyvään RADIUS Authentication -valikkoon. Tänne lisätään kuvan 21 mukaisesti Clients-välilehdelle palomuurin tiedot, sekä palomuurille käydään lisäämässä MFA Server -palvelun tiedot. Tämän jälkeen laitteiden yhteyden salaamiseksi määritellään Shared Secret eli salasana, joka syötetään molempiin sille varattuun kenttään. Tämän avulla saadaan otettua kaksiosainen varmennus käyttöön myös VPN-yhteyttä ottaessa.

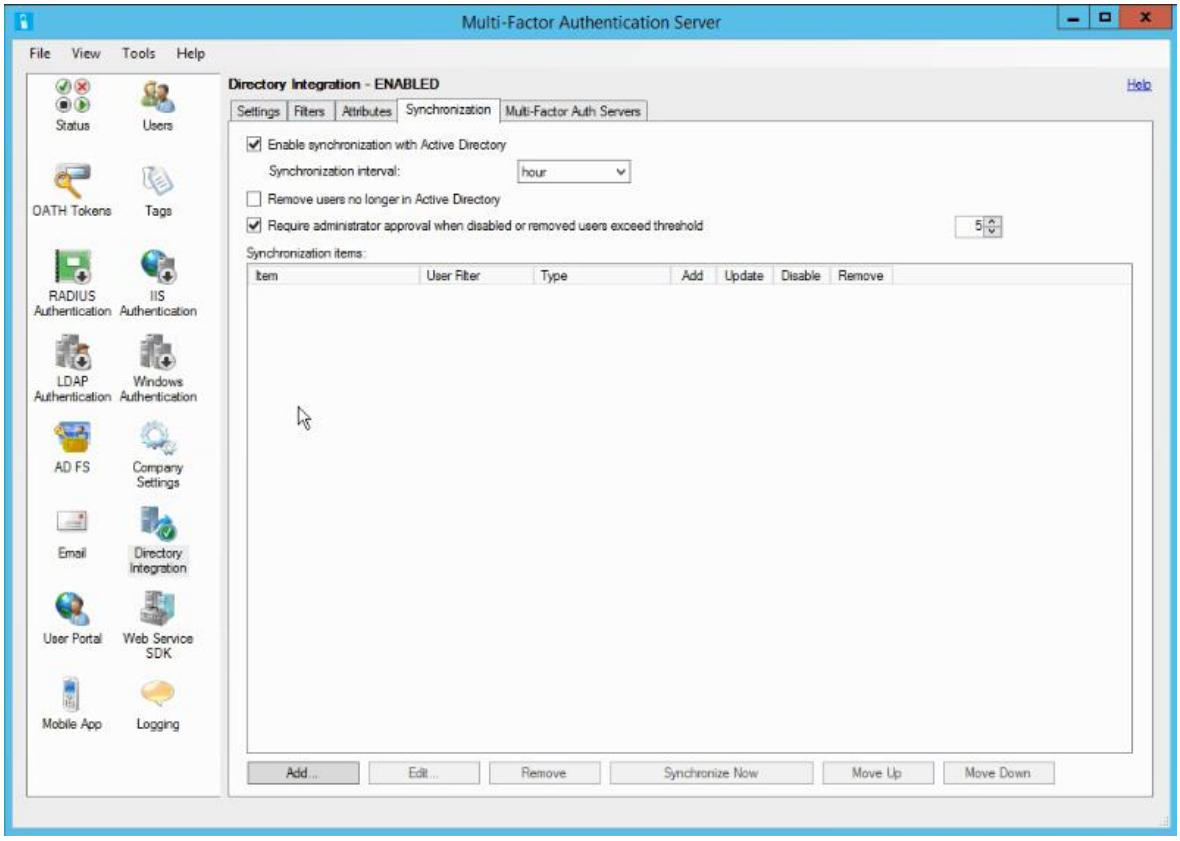


Kuva 21. RADIUS-valikon asetukset.

5.6 Käyttäjien tuominen Active Directory -hakemistopalvelusta MFAPalvelimelle

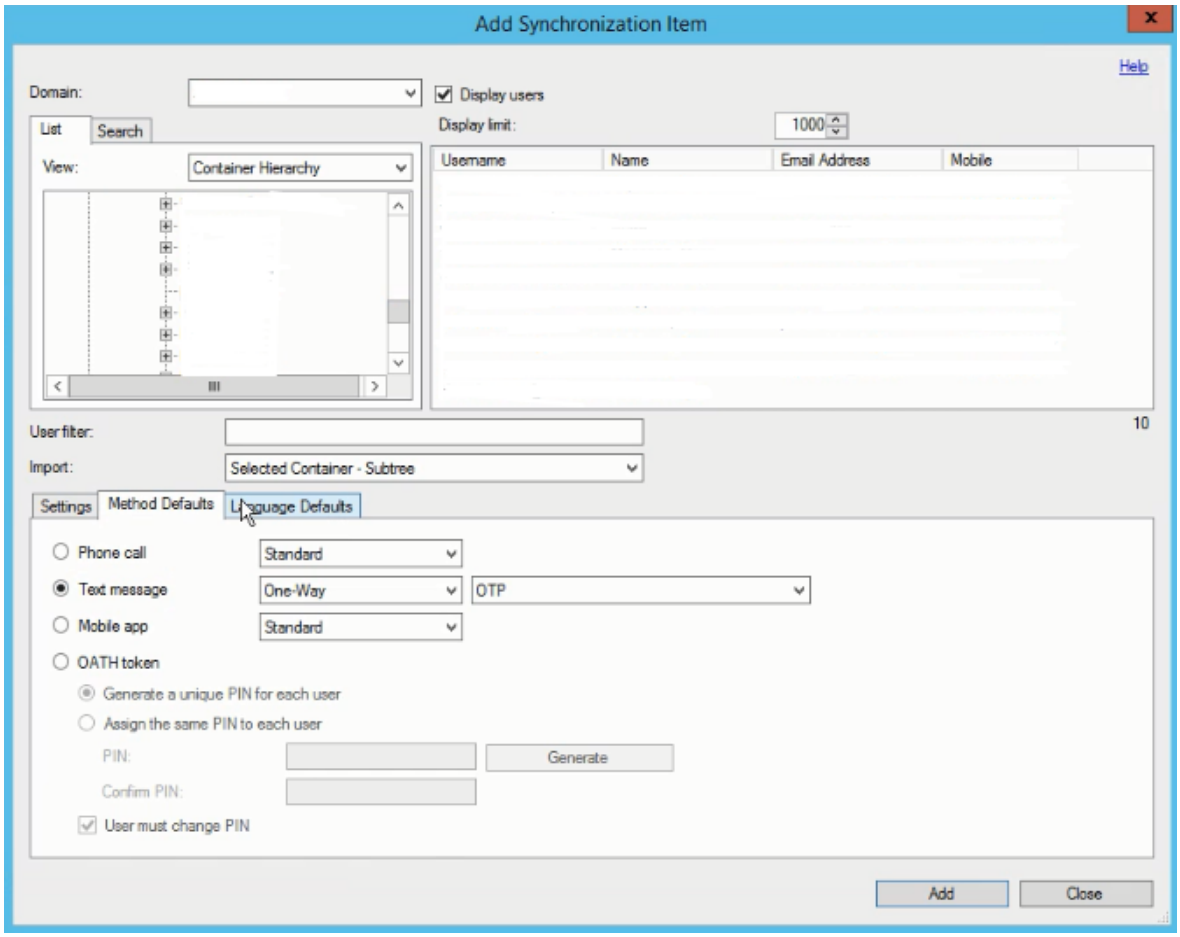
Nyt on aika tuoda tarvittavat käyttäjät Active Directory -hakemistopalvelusta Azuren MFA Server -palveluun. Tämä tehdään MFAPalvelimelta, jossa edellinen istunto on edelleen auki. Siirrytään kuvassa 17 näkyvään valikkoon Directory Integration. Tänne siirtyessä avautuu kuvan 22 mukainen näkymä. Tätä kautta saadaan tuotua asiakkaan Active Directory -hakemistopalvelusta tarvittavat käyttäjätiedot kaksiosaista varmennusta varten. On syytä varmistaa, että Enable synchronization with

Active Directory -valinta on valittuna, jonka jälkeen painetaan näkymän alareunassa olevaa Add… -painiketta. Tällöin aukeaa kuvan 23 mukainen näkymä.



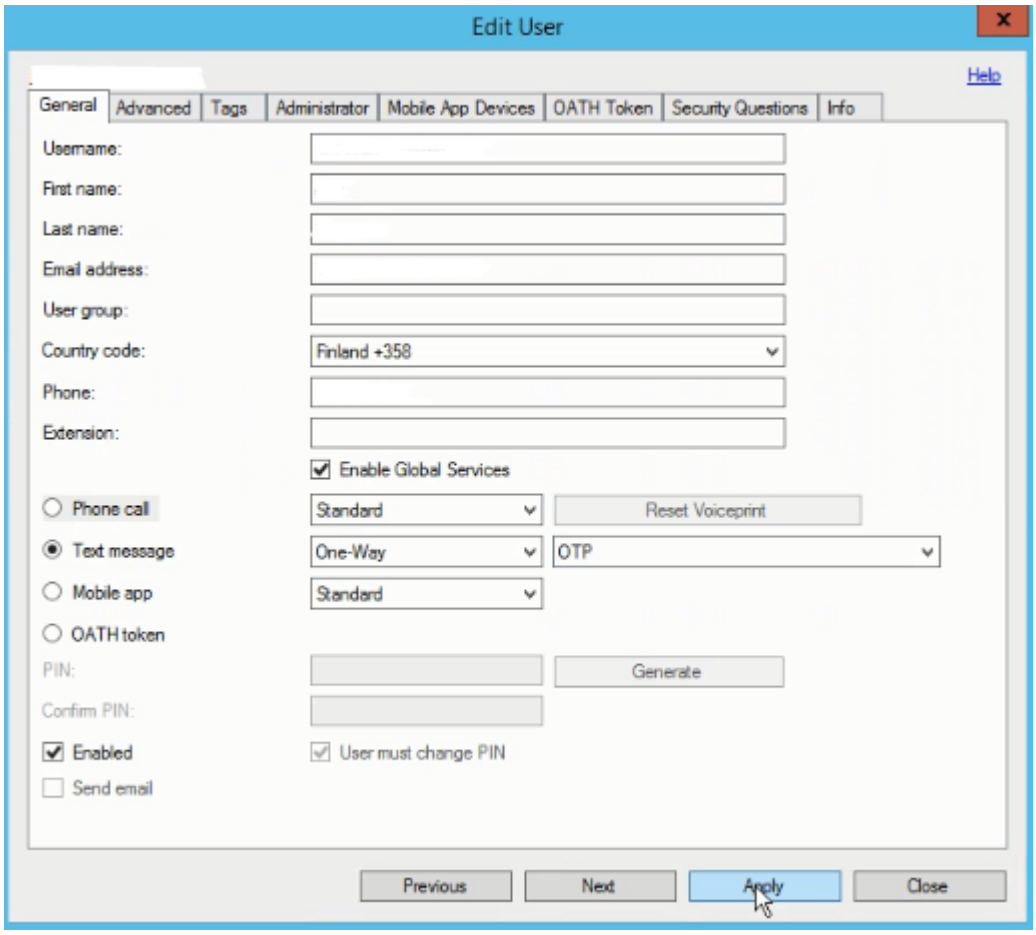
Kuva 22. Directory Integrationin avausnäkymä.

Kuvassa 23 vasemmassa yläreunassa olevan valikon avulla haetaan asiakkaan Active Directory -hakemistopalvelusta sijainti, jonne jonkun henkilön tunnus, kenelle kaksiosainen varmennus otetaan käyttöön, on luotu, ja tuodaan kyseisessä sijainnissa olevat käyttäjät Azuren MFA Server -palveluun valitsemalla Add-painike. Varmistetaan myös, että valinnat ovat samat kuin mitä Method Defaults -välilehdellä ollaan valittu. Tämän jälkeen toistetaan tämä jokaiselle sijainnille, jossa tarvittavia henkilöitä on.



Kuva 23. Käyttäjien synkronointi MFAPalvelimelle.

Kun kaikki tarvittavat henkilöt on saatu synkronoitua MFAPalvelimelle, siirrytään kuvassa 22 näkyvään Users-valikkoon. Täältä etsitään alkuun testikäyttäjä, sekä jo valmiiksi asiakkaan testiryhmän jäsenet. Jokaisen kohdalta Valitaan vuorottain Edit-painike, ja käydään varmistamassa, että käyttäjillä on tarvittavat tiedot kunnossa. Nyt valitaan myös vaihtoehto Enabled (kuva 24), jolloin kaksiosainen varmennus tulee valitulle käyttäjälle MFAPalvelimen kautta. Lopuksi Azuren hallinnan kautta käydään hakemassa haluttu käyttäjä ja painetaan kuvassa 25 näkyvää Multi-Factor Authentication -painiketta, jolla saadaan kaksiosainen varmennus käyttöön. Tämä tehdään aluksi vain testikäyttäjälle, jolla nyt ruvetaan tätä testaamaan.

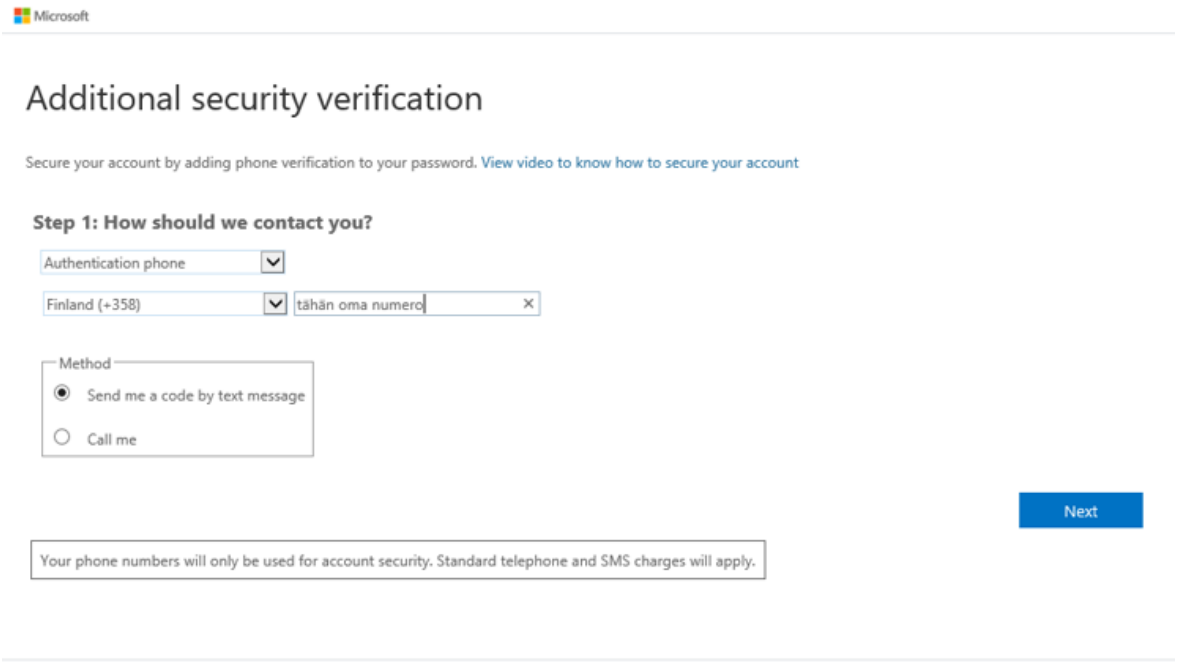


Kuva 24. Käyttäjätietojen varmistus.

Kuva 25. Kaksiosaisen varmistuksen päälle laittaminen Azuren hallinnan kautta.

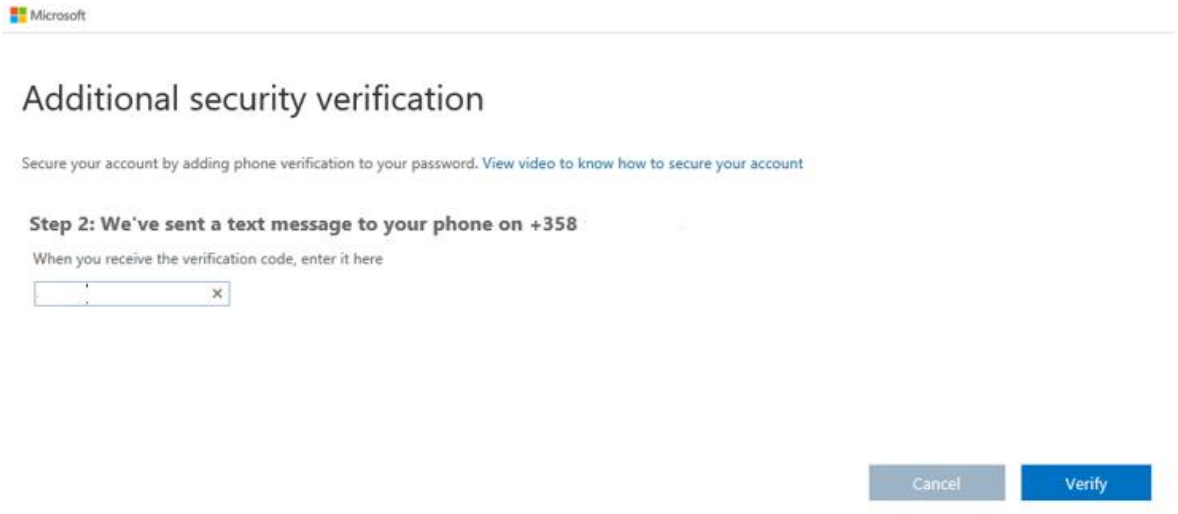
5.7 Kaksiosaisen varmennuksen testaus ja projektin tilannekatsaus

Ennen testausta tulee kaksiosainen varmennus ottaa käyttäjän toimesta käyttöön ensimmäisen kirjautumisen yhteydessä. Selaimella mennään verkkosivulle https://login.microsoftonline.com, ja syötetään kirjautumistiedoiksi testitunnuksen tiedot. Salasanan syötön jälkeen Microsoft ohjaa käyttäjän kuvan 26 mukaiselle sivulle, jossa syötetään vielä käyttäjän oma puhelinnumero ja tapa, jolla kaksiosaisen varmistuksen ensimmäinen koodi tulee. Valinnaksi tehdään koodin vastaanottaminen tekstiviestillä, sillä tämän on yksinkertaisin vaihtoehto. Tämän jälkeen siirrytään eteenpäin valitsemalla Next-painike.



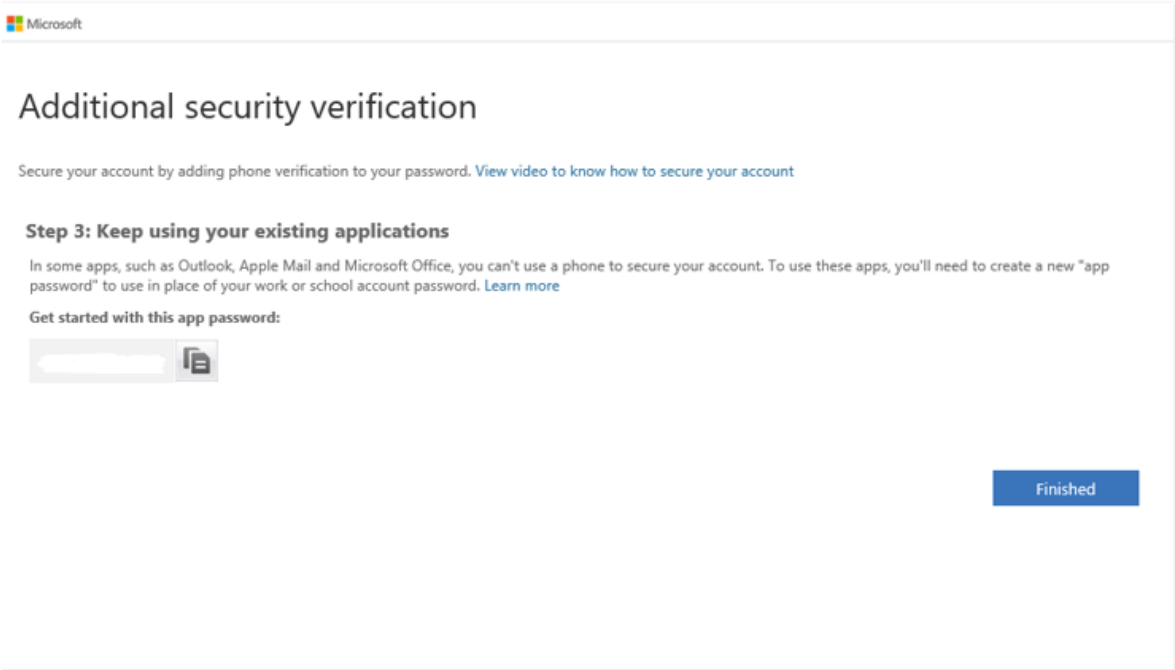
Kuva 26. Kaksiosaisen varmistuksen määrittely ensimmäisen kirjautumisen yhteydessä.

Nyt äskeisessä vaiheessa syötettyyn puhelinnumeroon tulee tekstiviesti, jossa ilmoitettu koodi syötetään kuvan 27 sille varattuun kenttään. Tämän jälkeen valitaan Verify-painike ja siirrytään käyttöönotossa eteenpäin.



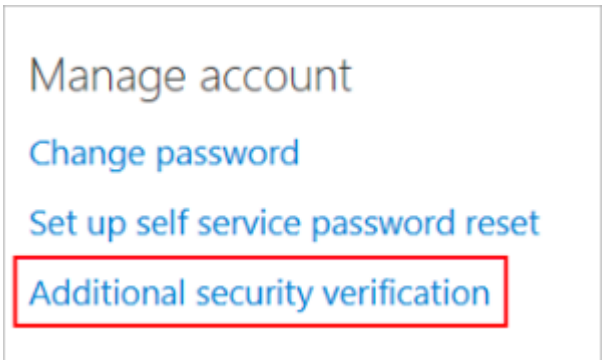
Kuva 27. Kenttä viestillä saatua koodia varten.

Nyt aukeaa kuvan 28 mukainen näkymä. Tästä saadaan otettua talteen sovellussalasana. Tämä kannattaa ottaa talteen, mikäli jokin sovellus ei tue kaksiosaista varmennusta, tulee kirjautuminen tehdä tämän salasanan avulla. Salasanan voi kuitenkin luoda myöhemmin uudemman kerran, mikäli sen unohtaa. Tämä tapahtuu kirjautumalla Microsoftin sivuille ja navigoimalla Office 365:n asetuksiin.



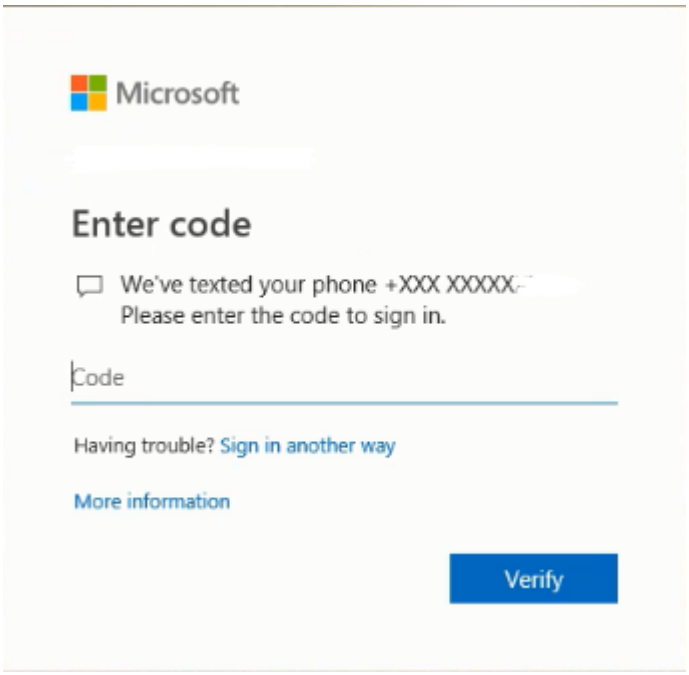
Kuva 28. Sovellussalasana

Lopuksi voidaan asettaa ylimääräinen kirjautumistunniste, mikäli oletusvarmennus ei ole mahdollista, esimerkiksi puhelimen hukkaamisen takia. Tämä tapahtuu sivulta https://myapps.microsoft.com/, josta valitaan kuvan 29 valikko. Tätä ei testitunnukselle kuitenkaan tehdä, sillä tämä tunnus ei testauksen jälkeen enää ole kaksiosaisessa varmennuksessa mukana.



Kuva 29. Vaihtoehtoisen varmennuksen määrittely.

Nyt kun tarvittavat määritykset on tehty, kokeillaan kirjautua asiakkaan Office 365 -palveluihin Microsoftin sivuilta. Syötetään tunnus sekä salasana ja yritetään suorittaa kirjautuminen. Tämän jälkeen kirjautumisruutu ohjataan kuvan 30 mukaiseen näkymään. Hetken kuluttua puhelimeen saapuu varmistuskoodi. Tämä koodi syötetään sille varattuun kenttään, ja sisäänkirjautuminen onnistuu.



Kuva 30. Koodin syöttäminen kirjautumisen yhteydessä.

Testaus saatiin siis tehtyä, ja kaksiosainen varmistus toimi tarkoitetulla tavalla. Nyt käydään poistamassa kuvan 8 mukaisesti määritetty lisenssi testikäyttäjältä ja lisätään molemmat hankitut lisenssit samalla tapaa asiakkaan kahdella testaajalle. Tämän jälkeen heille käydään aktivoimassa kaksiosainen varmistus kuvan 25 mukaisesti.

Seuraavaksi luodaan asiakasta varten ohjeet, joiden avulla he saavat otettua kaksiosaisen varmistuksen tunnukselleen käyttöön. Lisäksi luodaan myös Excel-tiedosto, johonka he saavat kirjata, kuinka heidän mielestään kaksiosaisen varmennuksen käyttö onnistuu, ja tarvitaanko tähän parannuksia.

Tällä hetkellä projekti on siinä tilanteessa, että odotetaan tilannekatsausta, sekä asiakkaan testikäyttäjien mielipidettä kaksiosaisen vahvihstuksen toimivuuteen liittyen. Projektia ei siis saatu loppuun oletetulla aikavälillä, mutta sitä jatketaan opinnäytetyön valmistumisenkin jälkeen.

6 YHTEENVETO JA POHDINTA

Työn tavoitteena oli kaksiosaisen varmennuksen käyttöönotto asiakasyrityksen valikoidulle väelle Azuren MFA Server -palvelua käyttäen. Kaksiosaista varmennusta ei kuitenkaan vielä kaikille tarvittaville henkilöille saatu otettua käyttöön. Tällä hetkellä se on käytössä asiakkaan kahdella testikäyttäjällä, jotka testaavat sen toimivuutta, ja tulevat ehdottamaan mahdollisia parannuksia.

Vaikka työ ei käytännössä vaikuttanut kauhean laajalta, oppi siitä paljon, vaikka projektia ei saatu vielä loppuun saakka vietyä. Aiheesta ei myöskään ollut itselläni paljon tietoa yksittäisten omille tunnuksille asetettujen kaksiosaisten varmennusten lisäksi. Tästä johtuen aiheeseen liittyen tuli paljon uutta, ja tulevaisuudessa hyvin todennäköisesti tarpeellista tietoa.

Dokumentointi aiheesta jatkuu yritykselle projektin edetessä.

LÄHTEET

Bertocci, V. 2015. Modern Authentication with Azure Active Directory for Web Applications. [Verkkokirja]. Microsoft Press. [Viitattu 16.2.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

BLC. 2017. Vuosikatsaus. [Verkkojulkaisu]. BLC. [Viitattu 28.3.2019]. Saatavilla: https://content.blc.fi/vuosikatsaus

BLC. Ei päiväystä. Konserni. [Verkkosivu]. BLC. [Viitattu 28.3.2019]. Saatavilla: https://www.blc.fi/blc/konserni

BLC. Ei päiväystä. Taito. [Verkkosivu]. BLC. [Viitattu 29.3.2019]. Saatavilla: https://www.blc.fi/yrityksille/it/taito

Demiliani, S. & Michalski, O. 2018. Implementing Azure Cloud Design Patterns. [Verkkokirja]. Packt Publishing. [Viitattu 9.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Hassel, J. 2002. RADIUS. [Verkkokirja]. O'Reilly Media. [Viitattu 23.2.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Kanikathottum H. 2019. Serverless Programming Cookbook. [Verkkokirja]. Packt Publishing. [Viitattu 26.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Microsoft. 11.10.2018. How it works: Azure Multi-Factor Authentication. [Verkkosivu]. Microsoft corp. [Viitattu 25.3.2019]. Saatavana: https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/concept-mfa-howitworks

Microsoft. 11.7.2018. Which version of Azure MFA is right for my organization?. [Verkkosivu]. Microsoft corp. [Viitattu 25.3.2019]. Saatavana: https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/concept-mfa-whichversion

Nakhjiri, M. & Nakhjiri, M. 2005. AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility. [Verkkokirja]. John Wiley & Sons. [Viitattu 30.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Niemi, A., Khartabil, H., Mayer, G. & Poikselka, M. 2006. The IMS: IP Multimedia Concepts And Services, Second Edition [Verkkokirja]. John Wiley & Sons. [Viitattu 30.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Pixabay. 30.10.2015. Biometrinen Skanneri. [Verkkojulkaisu]. [Viitattu 1.4.2019]. Saatavana: https://pixabay.com/fi/photos/biometrinen-skanneri-biometristen-1006668/

Price, R. 2019. CompTIA Server+ Certification Guide. [Verkkokirja]. Packt Publishing. [Viitattu 1.4.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Stanislav, M. 2015. Two-Factor Authentication. [Verkkokirja]. IT Governance Publishing. [Viitattu 9.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Technologies, J. 2007. Network Protocols Handbook. [Verkkokirja]. Javvin Press. [Viitattu 24.2.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.