Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Tomi Järvi ja Kalle Lehtonen

MFA Server -roolin asennus ja käyttöönotto RADIUS/NPS-palvelimelle VPN-käyttäjien todennukseen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

19.11.2019

Tekijä Otsikko Sivumäärä	Tomi Järvi ja Kalle Lehtonen MFA Server -roolin asennus ja käyttöönotto RADIUS/NPS-palvelimelle VPN-käyttäjien todennukseen 45 sivua + 1 liitettä
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	tieto- ja viestintätekniikka
Ammatillinen pääaine	Tietoverkot
Ohjaaja	Yliopettaja Janne Salonen

Tämän insinöörityön tarkoituksena on asentaa pilvialustalle Microsoft Server 2016 -palvelin, jolle tulee MFA Server -ominaisuus. Työ toteutettiin asiakkaallemme, joka toimii finanssialan ohjelmistojen parissa. Työ koostuu palvelimen valinnasta, käyttöönotosta, konfiguroinnista, MFA Serverin määrittelystä ja hallinnasta.

Työn alussa tutustutaan MFA Serverin ja kaksivaihetodennuksen komponentteihin ja annetaan lukijalle taustatietoa näistä menetelmistä. Tämän jälkeen alamme tutustumaan itse asennusvaiheeseen alkaen palvelimen valinnasta ja hinnoittelusta, jonka jälkeen aloitamme palvelimen konfiguroinnin ja MFA Server -roolin asennuksen.

Työn jäljiltä asiakkaallamme on toimiva kaksivaihetodennus VPN-yhteyksien kirjautumisissa.

Avainsanat	Azure, MFA, monivaihetodennus, turvallisuus, VPN,

Author	Tomi Järvi and Kalle Lehtonen
Title	Installing and configuring MFA Server role on RADIUS/NPS server for multifactor authentication for VPN Connections
Number of Pages	45 pages + 1 appendix
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	Communication Networks and Applications
Instructors	Principal Lecturer Janne Salonen

The purpose of this Bachelor's thesis was to install Microsoft Server 2016 -server with MFA Server role on cloud based Azure platform. This was created to meet our customer's needs. Our customer works in financial applications. The study is about choosing the right server, installation and configuration of it as well as installing and configuring MFA Server.

At the beginning we take a look at components of MFA server and multi-phase-authentication and provide background knowledge about these methods to a reader. After we start the work itself step-by-step beginning from pricing and choosing a server configuration after choosing right one, we begin configuration of MFA server role.

We completed installing working two-phase-authentication to our client that now uses it for VPN-connections.

Keywords	Azure, MFA, Multi-Factor-Authentication, security, VPN,

Sisällys

1 Johdanto 1

2 Teknologia 1

2.1 MFA-Server ja verkkoturva 2

2.2 Security tokens 2

3 Vertailu erilaisista MFA-teknologioista 3

3.1 Conditional access 3

3.2 Mobiiliautentikaattorit 4

4 Suunnittelu 6

4.1 Lähtöasetelma 6

4.2 Työn aloitus 7

4.3 Lisenssointi ja kustannukset 8

5 Asennus ja konfigurointi 9

5.1 Asiakkuuden luonti Azureen ja pilvipalvelimen asennus 9

5.2 MFA-Server 18

5.3 Verkkoturvallisuus 43

6 Yhteenveto 44

Lähteet 45

Lyhenteet

AAD (Azure Active Directory) Azuressa, eli Microsoftin pilvessä sijaitseva Active Directory. Active Directory on tietokanta toimialueen käyttäjistä ja resurs-seista.

ADDC (Active Directory Domain Controller) Palvelin, joka vastaa käyttäjien kirjautumisesta ja oikeuksista Windows-domainissa.

ADUC (Active Directory Users and Computers) AD-palvelimen käyttäjien ja koneiden hallintanäkymä.

Azure AD Connect
Ohjelmisto, jolla kaksi Active Directoryä saadaan synkronoitua keskenään. Käytetään muun muassa paikallisen Active Directoryn linkittämiseen pilvessä sijaitsevan palvelimen Active Directoryyn tai toisinpäin.

MFA Monimenetelmätunnistautuminen (Multi-Factor Authentication). Lisätunnistautumisen käyttäminen tiettyyn palveluun. Käyttäjä voidaan kirjautumisen jälkeen ohjata tekemään lisätodennus henkilöllisyydestään.

Microsoft Azure
Microsoftin tarjoama pilvipalvelualusta.

NPS (Network Policy Server) Palvelimella sijaitseva Microsoftin käyttäjän todennuspalvelu.

NSG (Network Security Group) Azuren verkkosääntökokoelma. Resurssiryhmälle annetut säännöt.

Office 365 Office-ohjelmistopaketti, joka toimii Mirosoftin Azuren päällä.

OTP (One-time password) Kertakäyttösalasana. Käytetään todella usein monimenetelmätunnistautumisessa. Salasana on voimassa ainoastaan yhdessä kirjautumisessa ja vain tietyn ajan.

RADIUS	(Remote Access Dial In User Service) Etätunnistuksen todennusprotokolla.
RG	(Resource Group) Azuressa käytettävä resurssiryhmä.
RDP	(Remote Desktop Protocol) Etäkäyttöprotokolla Microsoftin etätyöpöytäsovellukselle.
VPN	(Virtual Private Network) Kahden fyysisesti erillään olevan sisäverkon yhdistäminen yhdeksi verkoksi julkisen verkon yli.
VM	(Virtual Machine) Virtuaalinen laite yleensä palvelin tai tietokone.

1 Johdanto

Aloitimme molemmat työskentelyn Jalo IT:llä kahden kuukauden ajalla. Olemme molemmat erikoistuneet tietoverkkoihin ja sovimme hyvin Jalo IT:n yritystoimintaan. Jalo IT:llä työskentelemme erilaisissa työtehtävissä, kuten asiakkaiden IT-tukena, internetyhteyksien palveluntarjoajana, konsultteina, tietoturvaneuvojina ja kouluttajina.

Työskennellessämme Jalo IT:llä saimme toimeksiannon asiakkaaltamme VPN-yhteyksien turvallisuusparannuksista. Samana vuonna oli huomattava määrä Office365-tilejä kaapattu myös Suomessa. Näin ollen ajattelimme, että heidän VPN-yhteyksiin on hyvä saada kaksivaihetodennus toimintaan. Tämä tarkoittaa sitä, että käyttäjä saa kirjautuessaan kertakäyttökoodin tekstiviestillä puhelimeen. Tämän koodin käyttäjä syöttää kirjautuessaan salasanan ohella ja pääsee kirjautumaan [1].

Pääaineemme ollessa tietoverkot oli tämä asia todella mainio esimerkki ja harjoitustyö tulevia työtehtäviämme varten. Työ sisältää Microsoftin Server 2016 -palvelimen käyttöä, jota olimme paljon koulussamme harjoitelleet.

Tässä työssä käydään läpi Microsoft Server 2016 -palvelimen asennusta ja käyttöönottoa toimialueen hallintapalvelimeksi, Microsoft MFA Server -asennusta ja käyttöönottoa sekä käyttäjien konfigurointia.

2 Teknologia

Tietoturvallisuuden ollessa vuosi vuodelta isommassa roolissa ovat yritykset alkaneet etsiä helppokäyttöisiä suojausmenetelmiä IT-palveluihinsa. Monimenetelmätunnistautuminen onkin henkilön todentamiseen erittäin hyödyllinen tapa, sillä tällä tavalla käyttäjän täytyy tarjota toinen, tai jopa useampi erilainen tunnistautumistapa salasanan lisäksi [2].

Tunnistautumismenetelmiä on käytännössä kolmea eri tyyppiä:

- käyttäjän muistiin perustuvaa (esimerkiksi salasana, PIN-koodi tai turvakysymys)

- käyttäjän hallussa olevaan laitteeseen perustuvaa (esimerkiksi puhelimeen tuleva tekstiviesti kirjautumisen yhteydessä)

- käyttäjän omiin ominaisuuksiin (esimerkiksi sormenjälki).

Mikäli näistä tapauksista käytetään kahta tai kaikkia kolmea eri menetelmää, puhutaan monimenetelmätunnistautumisesta.

2.1 MFA-Server ja verkkoturva

Yrityksen VPN-yhteyttä voidaan käyttää muutamaan erilaiseen tarkoitukseen. Tällaisia ovat muun muassa liikenteen reititys yrityksen verkon kautta ja sisäverkossa sijaitsevan resurssin käyttö etäyhteydellä. Mikäli yrityksellä on siis esimerkiksi verkkolevy tai verkkojako palvelimella, voi käyttäjä tunnistautua Internetin yli palvelimelle ja saada palvelimelta oikeudet käyttää kyseistä resurssia. Palvelimelle kirjautuessaan käyttäjä syöttää yleensä käyttäjätunnuksen ja salasanan. Onnistuneen kirjautumisen jälkeen käyttäjä pääsee sisäverkkoon käsiksi. Tämä tietenkin aiheuttaa uhkaavan tilanteen, jossa käyttäjätunnuksen ja salasanan päätyessä vääriin käsiin on yrityksen sisäverkon turvallisuus uhattuna.

Jos käyttäjä kirjautumisen yhteydessä joutuu myös puhelimesta sallimaan kirjautumisen tunnuksillaan, nostaa se tietoturvan tasoa merkittävästi. Murtautujan on siis huomattavasti hankalampi kirjautua sisäverkkoon, jos hän tarvitsee fyysisen laitteen kyseiseltä käyttäjältä. Tähän auttaa monimenetelmätunnistautuminen. Mikäli palvelimelle asennetaan MFA Server -palvelu, hoitaa se juuri tällaisen lisäturvan käyttäjän todennukseen.

2.2 Security tokens

Security token tai MFA token on pieni laite, joka on suunniteltu luomaan yksi MFA:n tunnistautumismenetelmistä kertakäyttöisen, yleensä kuusinumeroisen koodin avulla. Laite generoi sopivan koodin joko kellonaikaan tai kirjautumispyynnön antaman komennon avulla. Suomessa näitä laitteita käytetään muun muassa verkkopankkikirjautumisessa.

3 Vertailu erilaisista MFA-teknologioista

3.1 Conditional access

Conditional Access on Microsoft AAD:n lisäominaisuus, jolla pystyy paremmin kontrolloimaan yrityksen käytössä olevia palveluita. Tämän avulla voidaan rajoittaa eri sovelluksiin pääsyä, mistä (IP-verkko tai sijainti), kuka (käyttäjä tai käyttäjäryhmä) tai mikä (pilvisovellus). Näitä ehtoja hyväksikäyttäen voidaan määrittää eri profiileita, jotka antavat tai hylkäävät pääsyn. Profiileihin voidaan määrätä:

- Latauksen esto: Jos laite ei esimerkiksi ole AAD Registered niin voidaan sen latausoikeudet hylätä.

- Tiedostojen salaus: Latauksen eston sijaan voidaan tiedostot salata, jotta vain käyttäjät, joilla on pääsy tiedostoihin, vaikka tuntematon laite pääsisi käsiksi tiedostoon.

- Riskikäyttäjän valvonta: Voidaan valvoa riskikäyttäjien istuntoja, jotta voidaan määrittää paremmat ehdot tulevaisuudessa.

- Pääsyn esto: Kun laite ei täytä valittuja ehtoja, voidaan siitä pääsy rajoittaa kokonaan pois palveluista tai verkosta.

- Luku-tila: Luomalla estoja joihinkin sovelluksien sisäisiin toimintoihin, voidaan luoda niin sanottu pelkkiä luku-oikeus sääntöjä.

Conditional Access -sovellus hallinta tukee SAML- ja Open ID Connect -sovelluksia, jotka on konfiguroitu ilman kaksivaiheisia tunnistuksia ja yrityksen omissa konesaleissa pidettäviä web-sovelluksia, jotka on konfiguroitu käyttämään Azure AD App Proxyä.

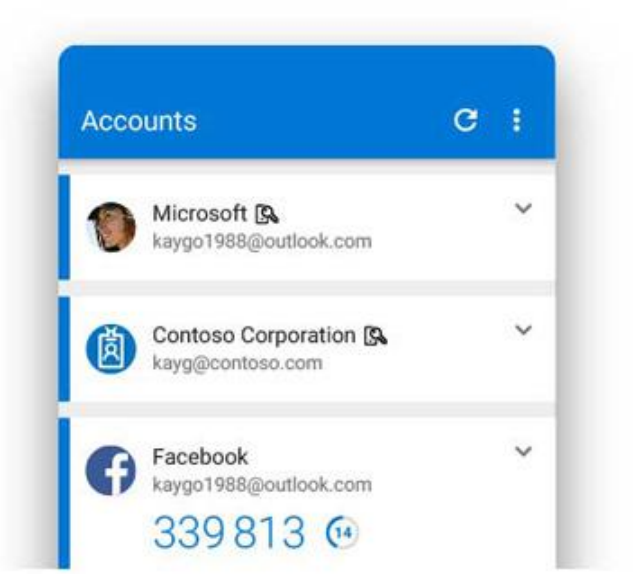
Conditional Accessin Session Control -työtilan avulla voidaan hallita AAD-käyttäjien kirjautumista ja pääsyä mobiili- ja työpöytäympäristöistä yleisimpiin palveluihin. Microsoft saattaa tukea myös muitakin sovelluksia ja alustoja jollakin tasolla, mutta nämä ovat suuremman tuen piirissä. [3.]

3.2 Mobiiliautentikaattorit

Mobiiliautentikaattorit ovat puhelinsovelluksia, jotka auttavat käyttäjää autentikaatiossa. Mobiiliautentikaattorit perustuvat ominaisuuteen, jonka käyttäjä omistaa. Aivan kuten tekstiviestit, jotka tulevat matkapuhelimeen. Autentikaattoreita on monia erilaisia, eri valmistajien sovelluksia, joista alla muutamia on esiteltynä [4].

3.2.1 Microsoft Authenticator

Microsoft Authenticator on Microsoftin luoma, alun perin lähinnä Microsoftin omiin palveluihin kirjautumiseen luotu sovellus. Microsoft tarjoaa tämän sovelluksen ilmaiseksi, ja nykyään sovellukseen saa kaikki muutkin OTP-standardia käyttävien palveluiden kirjautumispyynnöt.

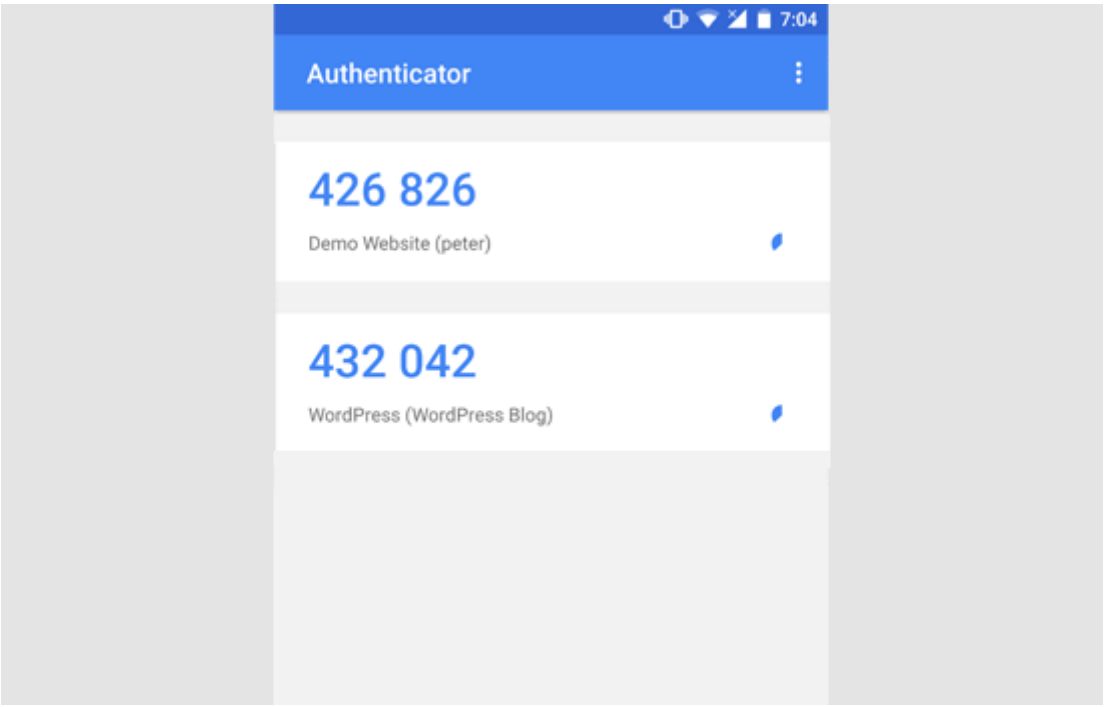


Kuva 1. Microsoft Authenticator

3.2.2 Google Authenticator

Google Authenticator on Googlen kehittämä todella hyvin suosittu ilmainen kirjautumissovellus. Sovellus on yksi ensimmäisistä vastaavista sovelluksista ja jo usean vuoden

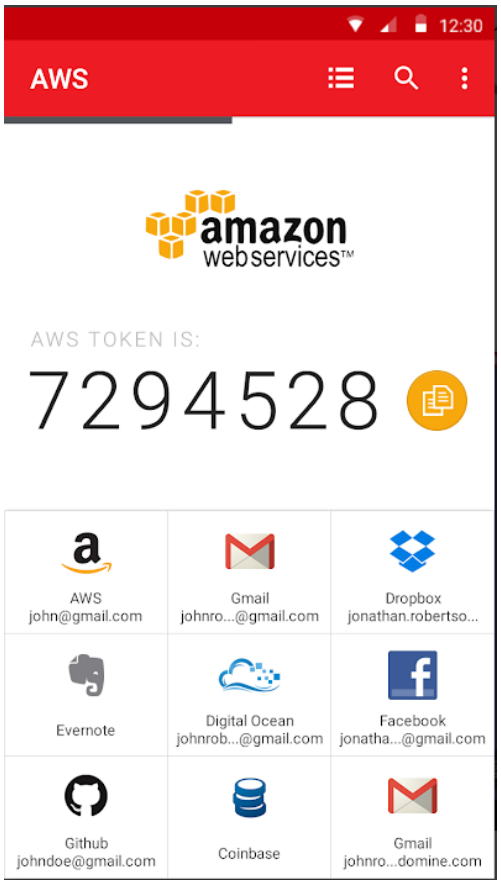
ajan monet palveluntarjoajat ovat ehdottaneet kirjautumisen yhteydessä käyttäjälle Google Authenticatorin asennusta tilin turvaamiseen. Google Authenticator ei toistaiseksi tue useamman puhelimen/laitteen asennuksia.



Kuva 2. Google Authenticator

3.2.3 Authy

Authy on myös suosittu tunnistautumisohjelmisto, joka tarjoaa muutamia pieniä lisäominaisuuksia kahteen aiemmin mainittuun sovellukseen. Authy on myös ilmainen. Authyn suosio perustuu suurelta osin usean laitteen tukeen. Authyn voi laitteelle asennuksen jälkeen asentaa uudelle laitteelle rinnakkaiskäyttöön. Tämä toki vähentää turvallisuutta, mikäli esimerkiksi yksi laite varastetaan. Varastetun tai kadonneen laitteen voi toki Authyn hallinnasta poistaa valtuutettujen laitteiden listalta. Authyn voi myös asentaa PC:lle. Tätä ominaisuutta ei myöskään Googlen tai Microsoftin autentikaattorit tue.



Kuva 3. Authy

4 Suunnittelu

4.1 Lähtöasetelma

Asiakkaallemme oli esitelty MFA-todennuspalvelu alkusyksystä 2017 yrityksemme toimesta. Tällöin asiakkaamme huomasivat heidän käyttäjänsä VPN-todennuksen turvallisuuden suuren parannusmahdollisuuden. He olivat ominaisuudesta erittäin kiinnostuneita. Sovimme, että aloitamme MFA:n käyttöönoton, kun molemmilta osapuolilta liikenee ylimääräistä aikaa. Molemminpuolisista kiireistä johtuen pääsimme aloittamaan käyttöönoton vastan loppuvuodesta 2018.

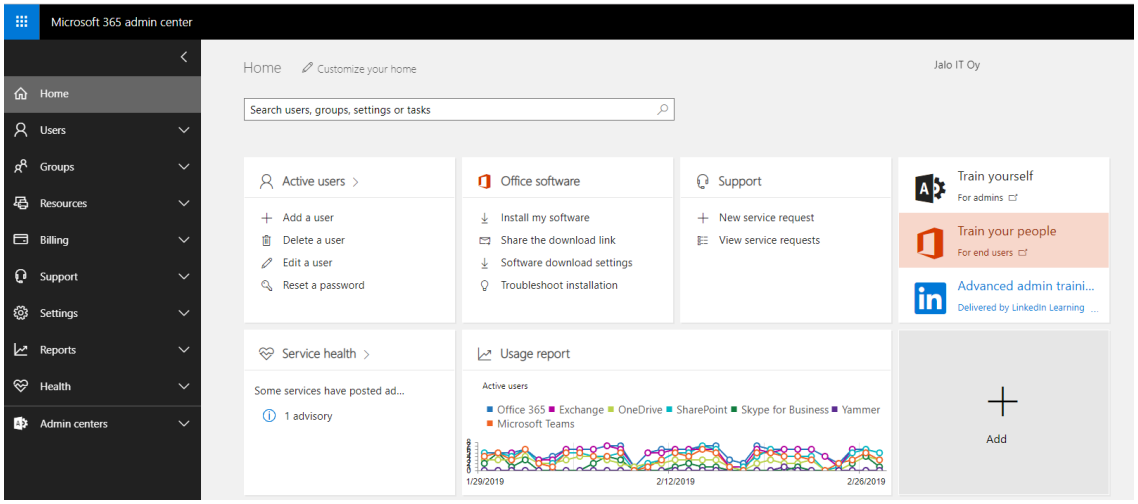
4.1.1 Kiinan palomuurin lävistys

Asiakkaallamme oli jo Active Directory paikallisesti käytössä, mutta pohdittuamme asiaa yrityksemme sisällä päätimme, että aloitamme heille samalla modernien Microsoft Azure -pilvipalveluiden käytön. Päätimme myös jättää muut ominaisuudet vielä toistaiseksi paikalliselle AD:lle ja loimme uuden, Active Directoryn ja Domain Controllerin uuteen, pilveen asentamaamme Windows 2016 -palvelimeen. Paikallinen AD ja uusi Azuressa sijaitsevaan palvelimeen asennettu AD pidetään vielä toistaiseksi erillisinä, ei toisiaan replikoivina tietokantoina.

Opinnäytetyö koostuu siis Azure-portaalin käyttöönotosta, Windows 2016 -palvelimen asennuksesta pilveen ja sille NPS-roolin asennuksesta, MFA -todennuspalvelun käyttöönotosta ja sen konfiguroinnista. Yksi palvelun käyttäjä sijaitsee fyysisesti Kiinassa, joten tätä varten tarvitsemme Mobile App -todennuksen, sillä Kiinan palomuuri ei päästä Microsoftin todennuspuheluita tai tekstiviestejä perille.

4.2 Työn aloitus

Asiakkaallamme oli valmiina käytössä Microsoftin Office 365 -tilaukset jokaiselle käyttäjälle. He siis käyttävät Microsoftin sähköpostia sekä monia muita tilauksen mukana tulevia palveluita kuten Teamsia ja Sharepointtia. Office 365 on täysin pilvipohjainen palvelu, joka mahdollistaa käyttäjien ja asetusten muokkaamisen suoraan Officen portaalin avulla. Portaaliin pääsee kirjautumalla osoitteessa https://portal.office.com. Suoraan admin-portaaliin pääsee osoitteessa https://admin.microsoft.com.



Kuva 4. Näkymä Microsoft 365 -hallintakeskuksesta

4.3 Lisenssointi ja kustannukset

Aloitimme työskentelyn loppuvuodesta 2017 projektin parissa. Työ oli oikein mukava toteuttaa, kun olimme suunnitelleet muutokset etukäteen huolellisesti. Työn järjestys tulisi olemaan seuraava:

1. uuden asiakkuuden luominen Microsoft Azureen asiakkaallemme.
2. palveluiden lisenssin osto tukkurimme Techdatan kautta.
3. sopivan pilvipalvelimen valinta Microsoft Azuresta ja pilviympäristön käyttöönotto.
4. Active Directory -roolin asennus palvelimelle.
5. Azure Multi-Factor Authentication Server -roolin asennus palvelimelle ja sen konfigurointi.
6. käyttäjien manuaalinen migraatio Azure AD: sta.
7. toiminnan testaus.

8. mobiilisovelluksen käyttöönotto ja opastus yhdelle käyttäjälle. [5, 6]

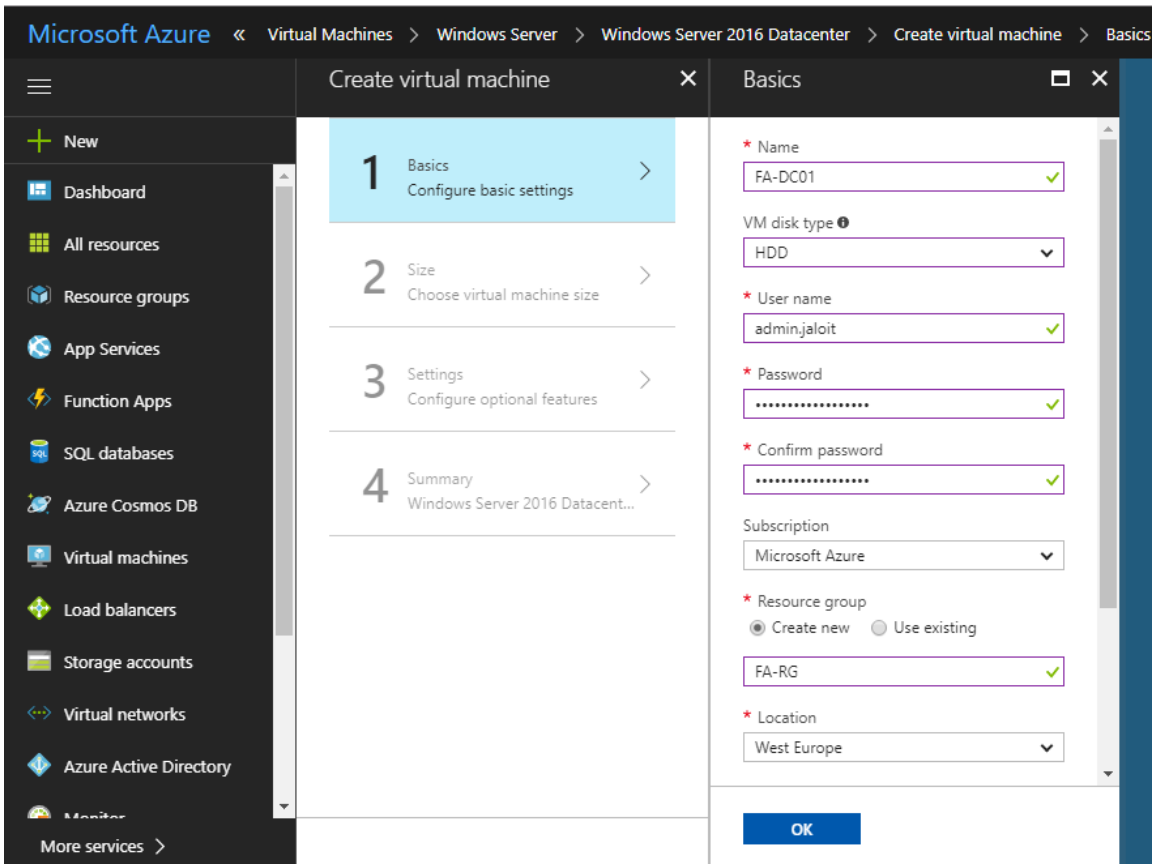
5 Asennus ja konfigurointi

5.1 Asiakkuuden luonti Azureen ja pilvipalvelimen asennus

Ensimmäisenä otimme yhteyttä yhteyshenkilöömme Techdatan puolella. Techdata on suomalainen IT-alan ohjelmisto- ja laitejälleenmyyjä, Microsoftin virallinen jälleenmyyjä ja markkinointipartneri. He neuvoivat meitä palvelimen valinnassa. Asiakkaallamme ei ennestään ollut ylimääräistä Windows Server 2016 -lisenssiä, joten tarvitsimme senkin mukaan, joista tuli pieni lisähinta heille. Azure on myös siinä mielessä erittäin hyvä alusta tarkoitukseemme, koska voimme lisätä resursseja helposti palvelimelle, mikäli asiakas tahtoo siirtää muitakin palveluita tulevaisuudessa pilvipalveluihin.

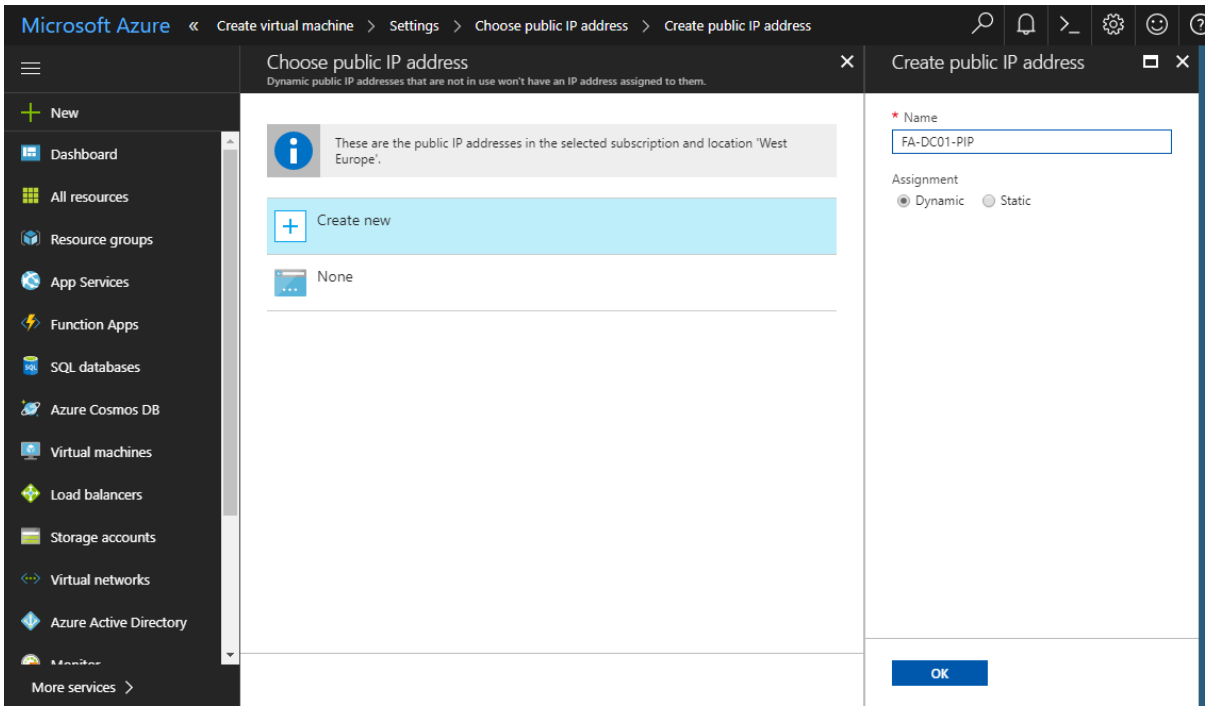
Sopimuksen rekisteröinnin jälkeen asiakkaan Azure -ympäristössä pystyy kyseiseen sopimukseen lisäämään suoraan kuukausiveloituksellisia pilvipalveluita. Kirjaudumme siis Azure portaaliin, josta kaikki tarvitsemamme komponentit sekä itse palvelin valitaan.

Valintamme osui A2 Standard -palvelimeen (kuva 8). Kyseiseen toimintaan ei tarvita paljoa resursseja, koska itse todennus ei tarvitse paljon resursseja. Palvelimen valinnan jälkeen täytyy palvelimen ympäristöön luoda resurssijoukko. Resurssijoukko on kokoelma tiettyjä ominaisuuksia ja palveluita Azuressa, jotka voivat olla yhteydessä toisiinsa. Resurssijoukkoon loimme sekä sisä- että ulkoverkon. Ulkoverkon luomisen yhteydessä saimme palvelimellemme yhden julkisen IP-osoitteen (kuva 6), jonka avulla palvelin voidaan yhdistää yrityksen sisäverkkoon.



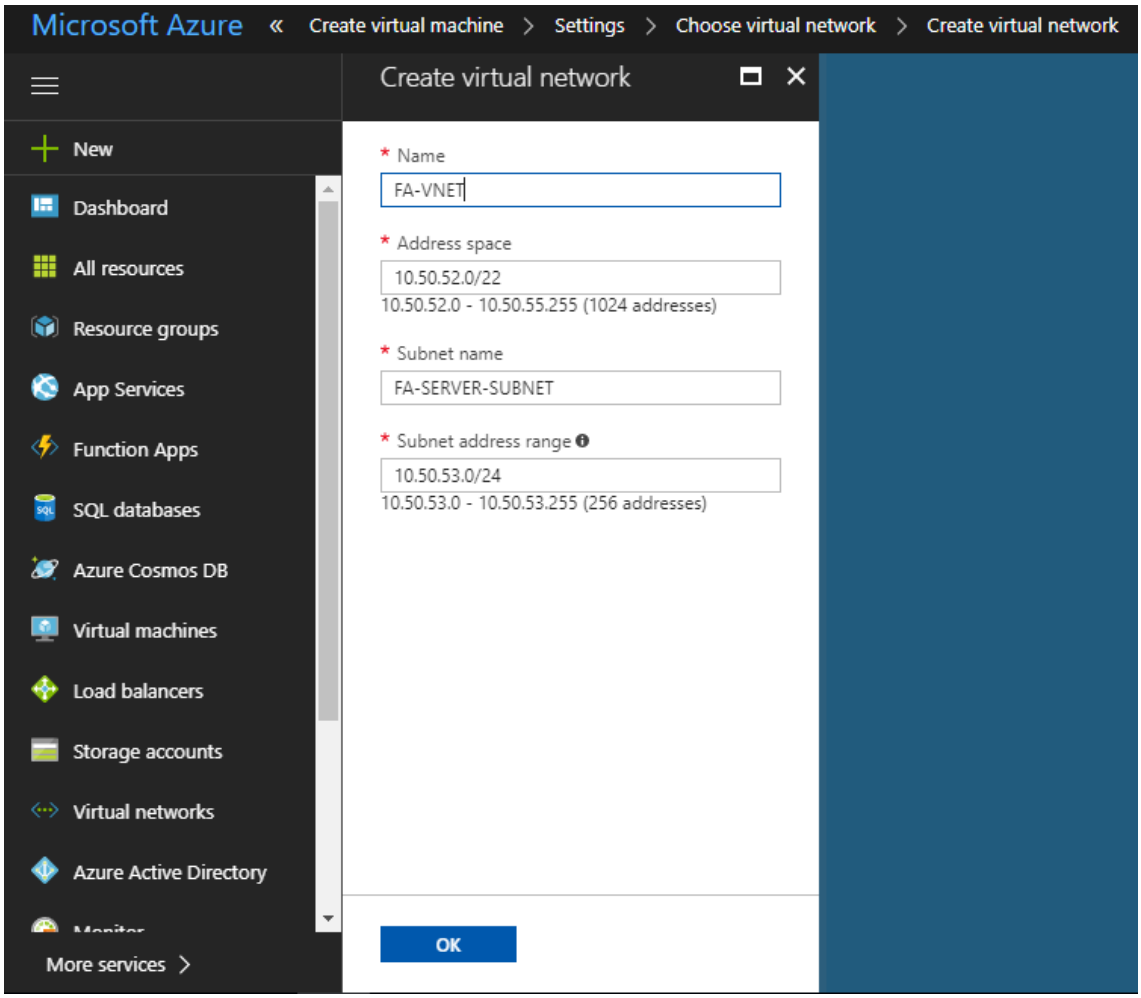
Kuva 5. Virtuaalipalvelimen luonti

Annamme palvelimelle yksinkertaisen ja lyhyen nimen, joka kuvastaa mahdollisimman tarkasti palvelimen toimintaa. FA tulee asiakkaan nimestä, DC tulee sanoista Domain Controller ja 01 kuvastaa, että kyseessä on ensimmäinen palvelin. Emme tarvitse nopeaa levytilaa (SSD) palvelimelle, vaan pelkkä HDD-kovalevy riittää tarpeisiimme. Järjestelmänvalvojan nimesimme admin.jaloit.



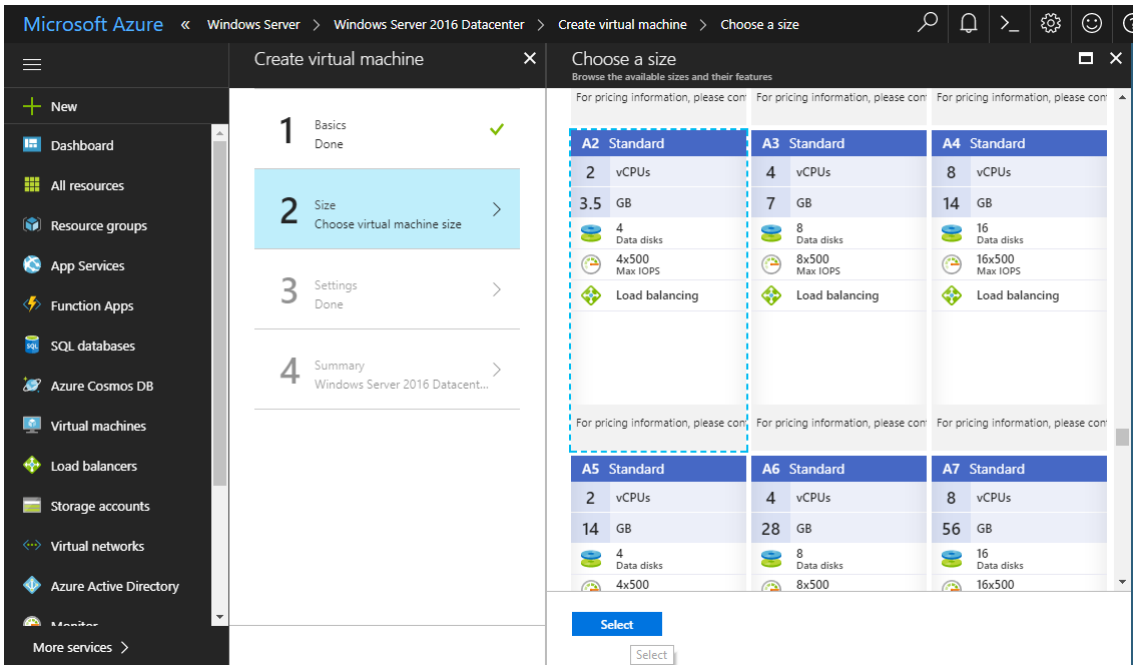
Kuva 6. Virtuaalipalvelimen luonti – Julkinen IP-osoite

Palvelimelle täytyy valita julkinen IP-osoite.



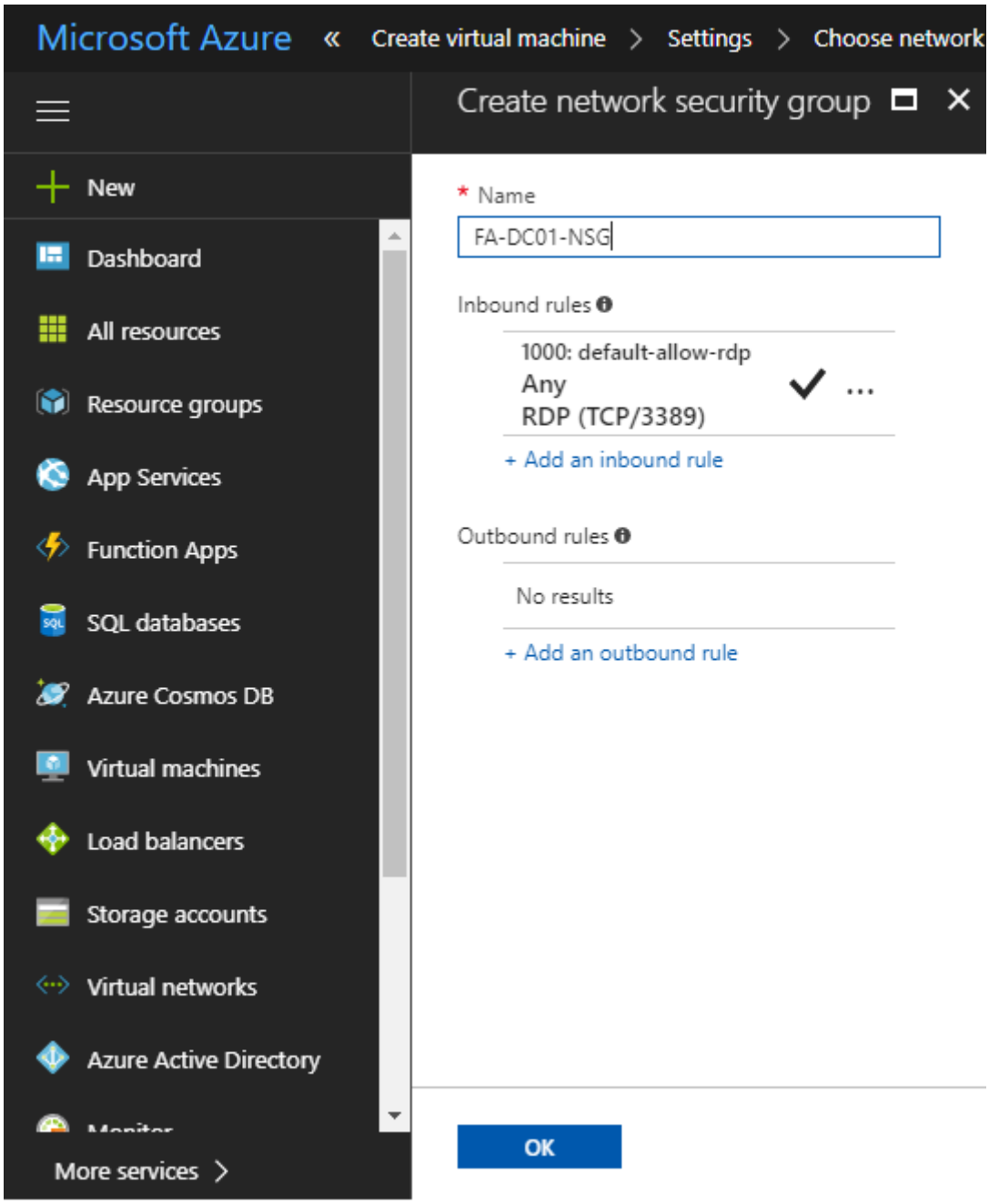
Kuva 7. Virtuaalipalvelimen luonti – Virtuaalisen aliverkon luonti

Luomme virtuaalisen aliverkon nimeltä FA-VNET. Tämä on aliverkko, joka yhdistää Azuressa olevat resurssit keskenään.



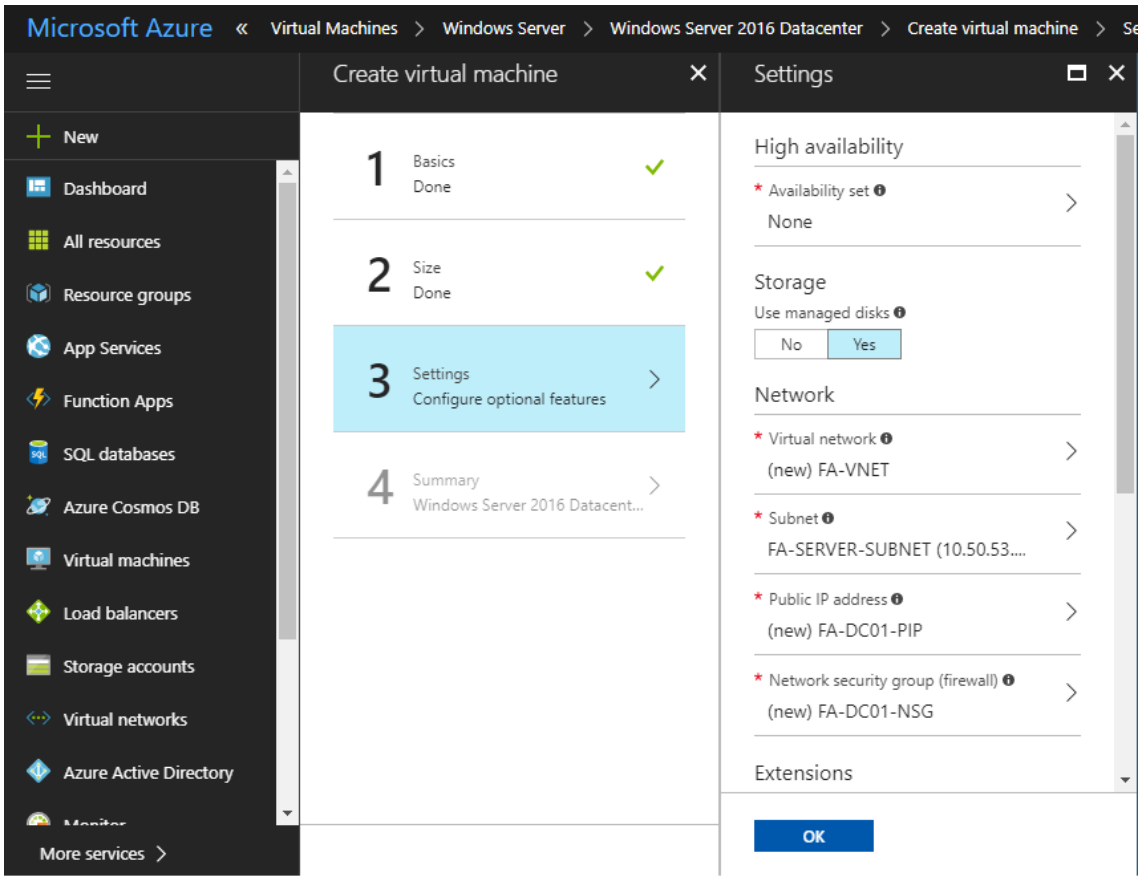
Kuva 8. Virtuaalipalvelimen luonti – Palvelimen valinta

Kuten mainittua, emme tarvitse tarpeisiimme kovinkaan paljoa prosessointitehoa. Käyttöömme riittää kahdella prosessorilla ja 3,5GB:n keskusmuistilla varustettua A2 Standard palvelinta. Hintaa palvelimelle tulee noin 110 €/kk. Liitteessä [7] olevasta linkistä voi tarkastella hintatietoja etsimällä vastaavan palvelimen.



Kuva 9. Virtuaalipalvelimen luonti – NSG:n luonti

Luomme pääsyn RDP-yhteydelle palvelimelle. Näin voimme konfiguroida palvelinta suoraan internetin yli etäyhteydellä. Suora RDP-yhteys kannattaa aina sallia ainoastaan tuntemistamme IP-osoitteista. Tämä tehdään asennuksen loppupuolella.



Kuva 10. Virtuaalipalvelimen luonti – Lisäasetukset

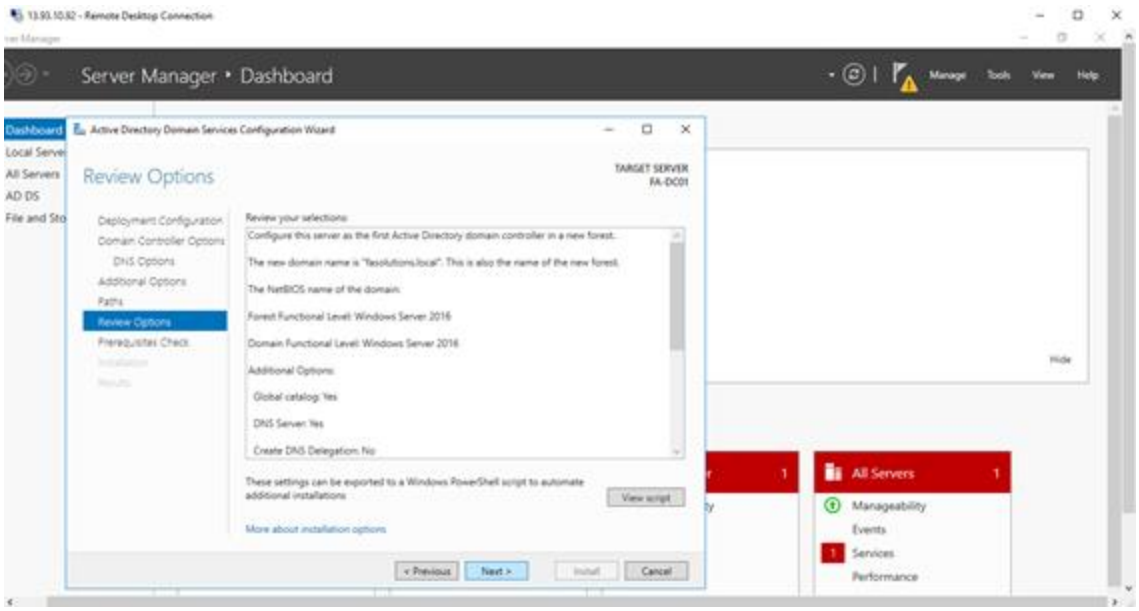
Lisäasetuksissa emme valitse korkeaa saatavuutta palvelimelle. Microsoft tarjoaa 99,9% pääsyvarmuuden ilman palvelimen replikointia. Saatavilla on kaksi muuta vaihtoehtoa; LRS ja GRS.

- Locally Redundant Storage(LRS) replikoi palvelimen samaan konesaliin toiselle fyysiselle palvelimelle. Tämä takaa 99,999999999% (11 yhdeksää) todennäköisyyden pääsyyn.
- Geographically Redundant Storage(GRS) replikoi palvelimen täysin toiselle maantieteelliselle alueelle. Tämä tarjoaa 99,99999999999999% (16 yhdeksää) todennäköisyyden pääsyyn.

Sivulla valitaan aiemmin luodut resurssit tälle palvelimelle käyttöön.

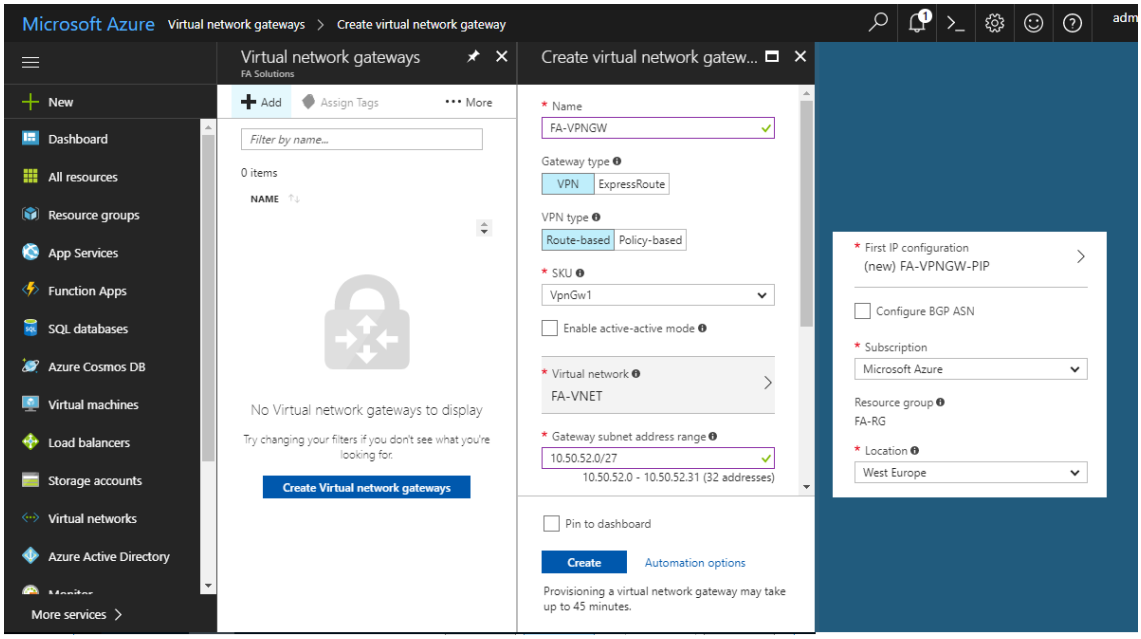
5.1.1 Active Directory Domain Services

Seuraavissa kuvissa on näytetty Active Directoryn asetukset, jotka pitää katsoa ennen kuin Domain Services lähtee käyntiin.



Kuva 11. Virtuaalipalvelimen käyttöönotto – Active Directoryn asennus ja konfigurointi

Samalla kun luotiin Azuressa oleva AD-palvelin laitettiin Azuren päässä oleva VPN-tunneli päälle seuraavin ominaisuuksin.



Kuva 12. Virtuaalipalvelimen käyttöönotto – VPN Gatewayn luonti

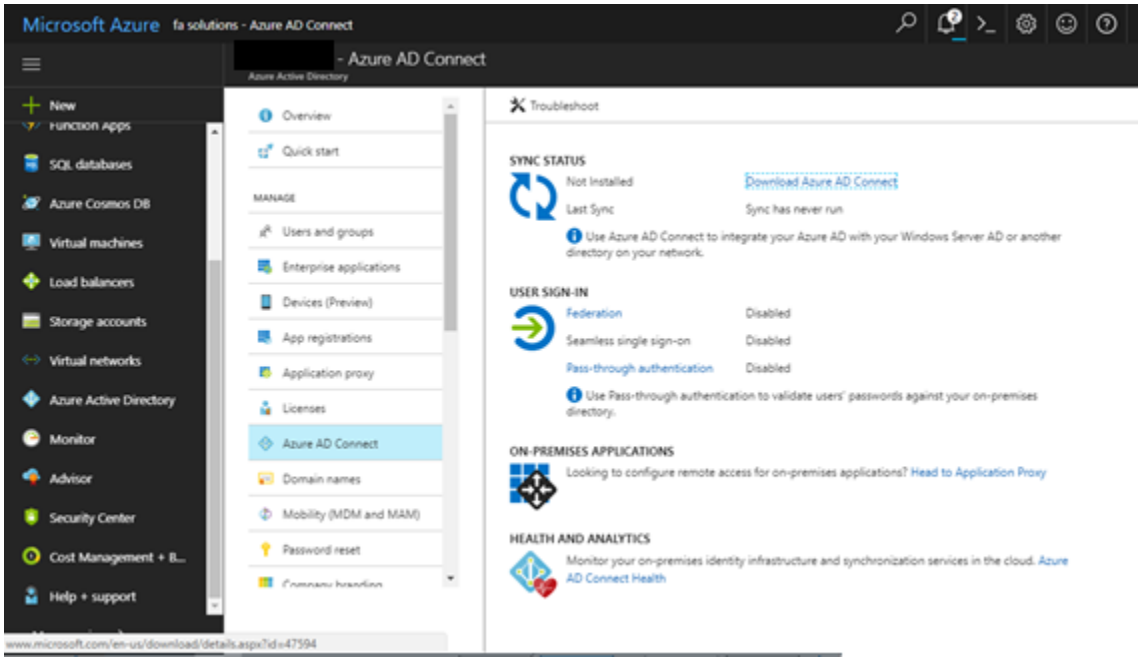
5.1.2 NPS ja RADIUS

Network Policy Service on Windows-palvelimien verkkotunnistautumiseen käytetty ominaisuus, jonka avulla voidaan esimerkiksi VPN- tai Radius-tunnistautuminen tuoda palomuurilaitteetteen omasta muistista AD-palvelimelle. Tämä mahdollistaa keskitetyn kirjautumisjärjestelmän käyttämisen kuten 802.1X standardia hyväksikäyttävät kytkimet,

WLAN-tukiasemat, VPN-palvelimet ja dial-up-yhteyksissä, eivätkä käyttäjät tarvitse monia tunnuksia ja salasanoja. Se taas parantaa huomattavasti yleistä tietoturvaa, kun voidaan pitää yhtä vahvempaa salasanaa sen sijaan, että käyttäjällä olisi monta heikompaa.

AAD-Connect

Azure Active Directory-Connect synkronoi paikallisen AD-palvelimen Azuren pilvi-AD-palvelun kanssa asetettujen määritysten mukaisesti.



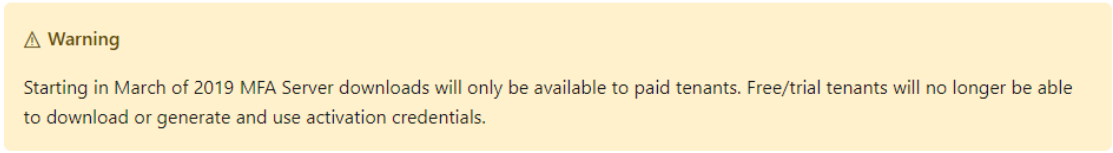
Kuva 13. Virtuaalipalvelimen käyttöönotto – Azure AD Connect -asennus

Asiakkaallamme on siis Microsoft Office 365 käytössä ja kaikille käyttäjille on tätä varten valmiiksi luotuna käyttäjätunnus Azure AD:ssa. Käyttämällä Azure AD Connectia voimme synkronoida valmiiksi luodut Azure käyttäjät uudelle pilvipalvelimellemme. Tässä tapauksessa Azure AD Connectia käytetään tulevien käyttäjien luonnissa, jotta saadaan käyttäjät molempiin järjestelmiin.

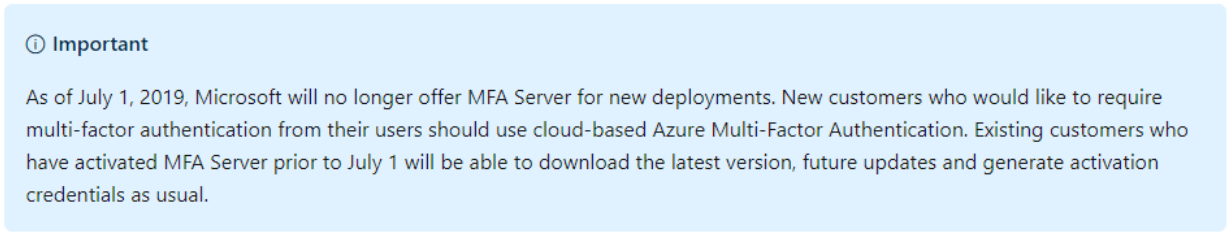
5.2 MFA-Server

5.2.1 MFA Server -palvelun lopetus

Microsoft ilmoitti loppuvuodesta 2018 lopettavansa uusien MFA Server -asennusten tuen tammikuussa 2019 (kuva 14). Työmme ohjetta ei siis enää uusille asennuksille nykyään voi seurata, mutta työstämme löytyy muuten hyödyllistä tietoa aiheesta, mikäli ympäristöön on ennen vuotta 2019 rekisteröity MFA Server -palvelu, on asennus vielä mahdollista.



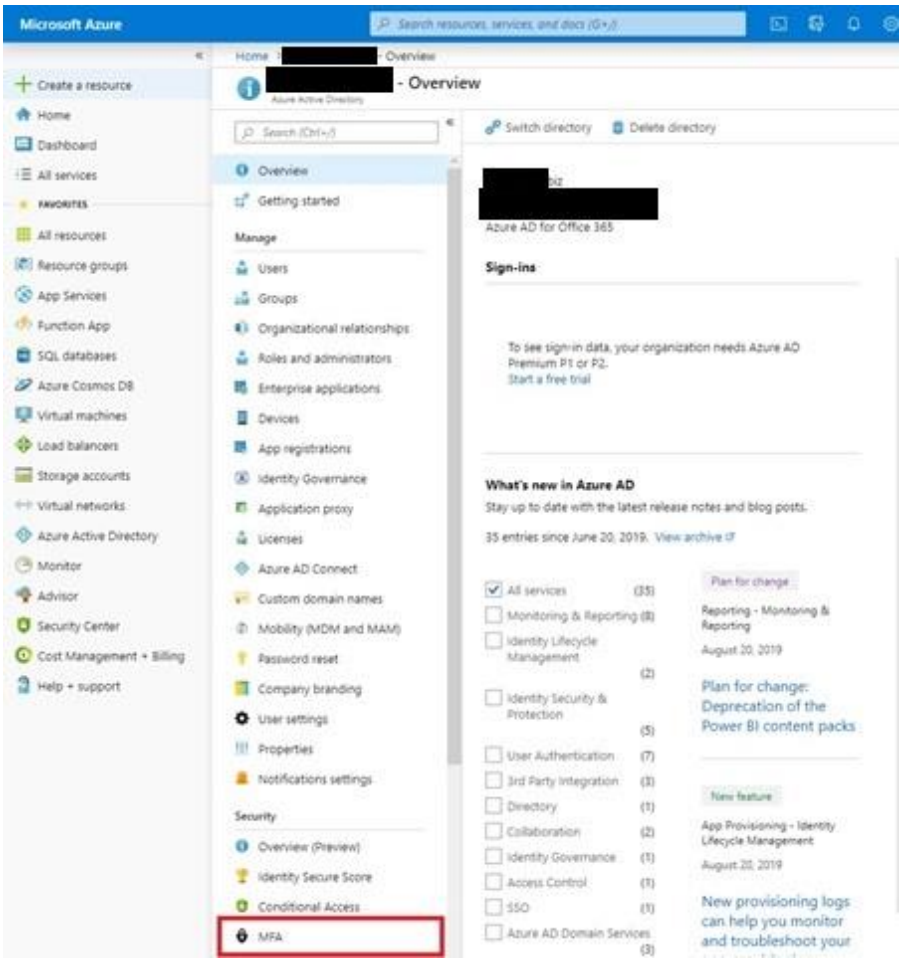
Kuva 14. Ilmoitus Microsoftin sivuilta (1/2)



Kuva 15. Ilmoitus Microsoftin sivuilta (2/2)

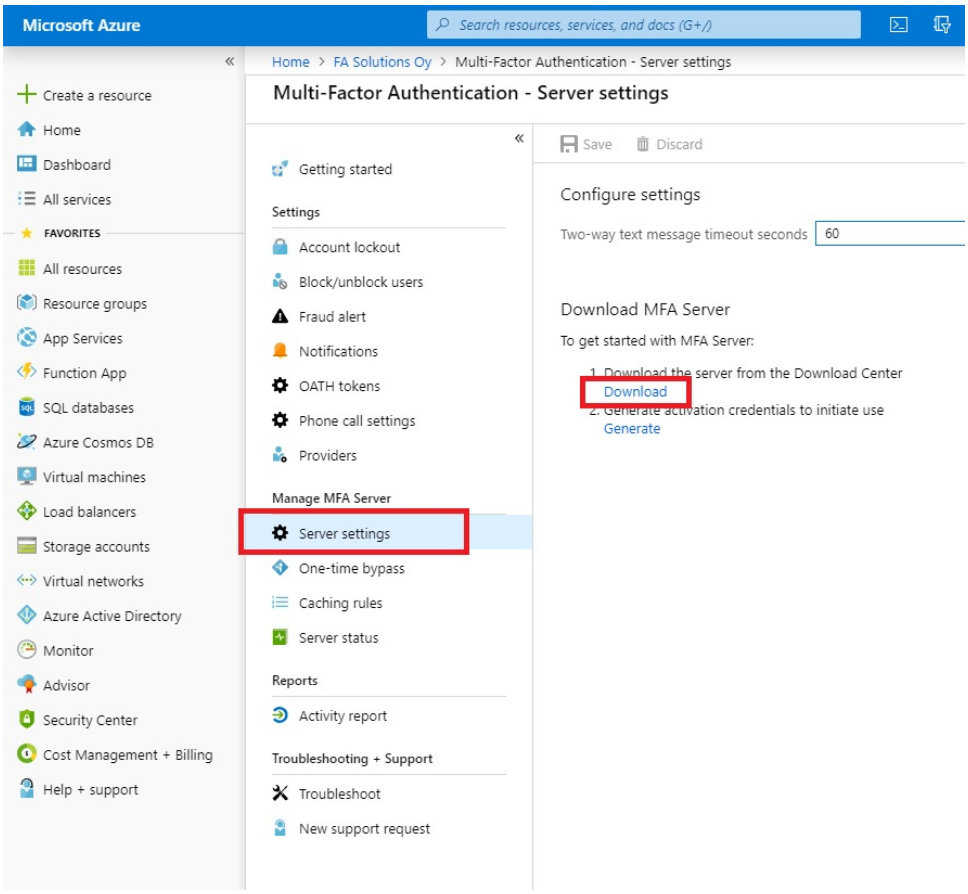
5.2.2 MFA Server -roolin asennus ja konfigurointi palvelimelle

Tässä osassa aloitamme itse MFA Server -ominaisuuden asennuksen palvelimelle. Käytämme toiminnoissamme Azuren portaalia https://www.portal.azure.com/ ja Azureen asennettua Windows Server 2016 -palvelinta. Palvelinyhteyttä käytämme RDP-yhteyden yli ja Azuren päätä konfiguroimme suoraan selaimella. Azuren päähän pitää olla kirjautuessa Azure Administrator -rooli.



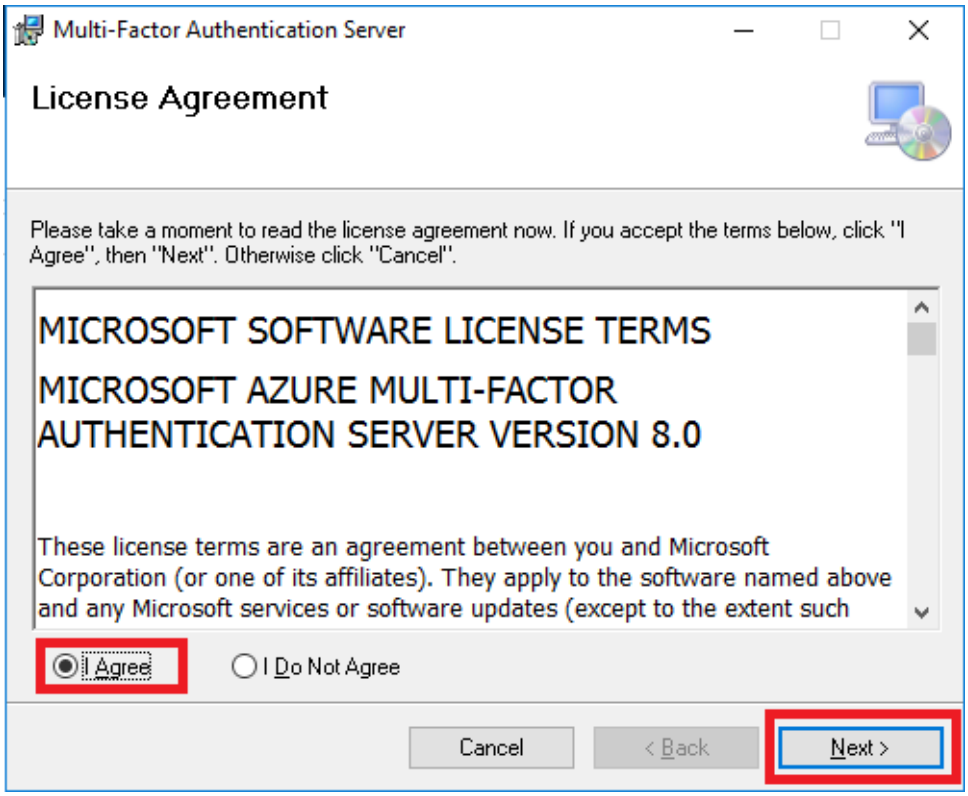
Kuva 16. Microsoft Azure AD:n pääikkuna, jossa MFA-valinta

Kirjauduttuamme Azure-portaaliin järjestelmänvalvojatunnuksilla pääsemme konfiguroimaan sitä. MFA-asetukset löytyvät Azure AD:n valinnan alta. Etsimällä haun kautta MFA:n löydämme samaan paikkaan.

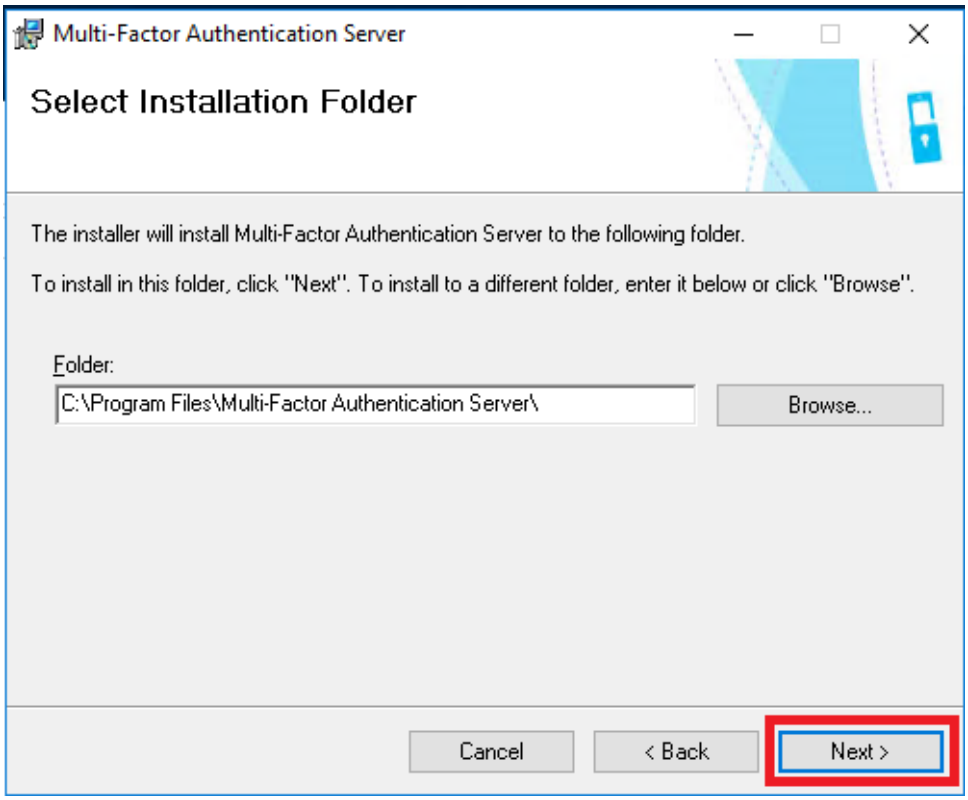


Kuva 17. MFA Server -ohjelmiston latausikkuna

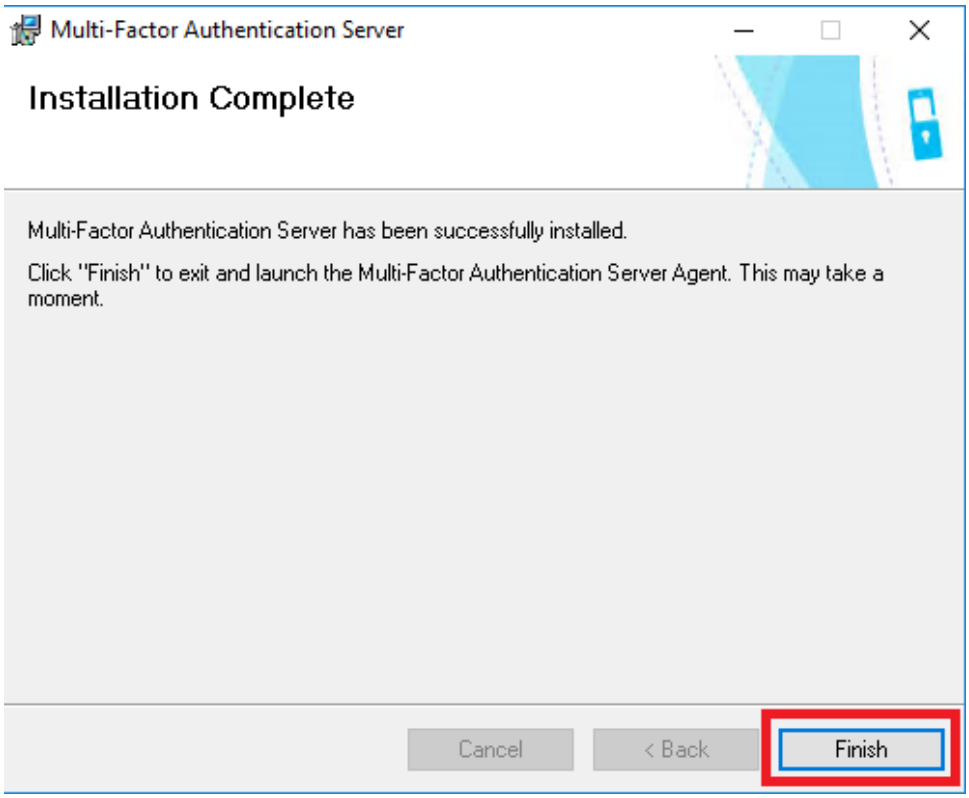
Palvelimen puolelle asennettava ohjelmisto, jolla itse palvelimen puolen konfigurointi onnistuu, ladataan Azure AD:n puolelta *Server settings -> Download MFA server*. Latauksen jälkeen suoritetaan ohjelma palvelimen puolella.



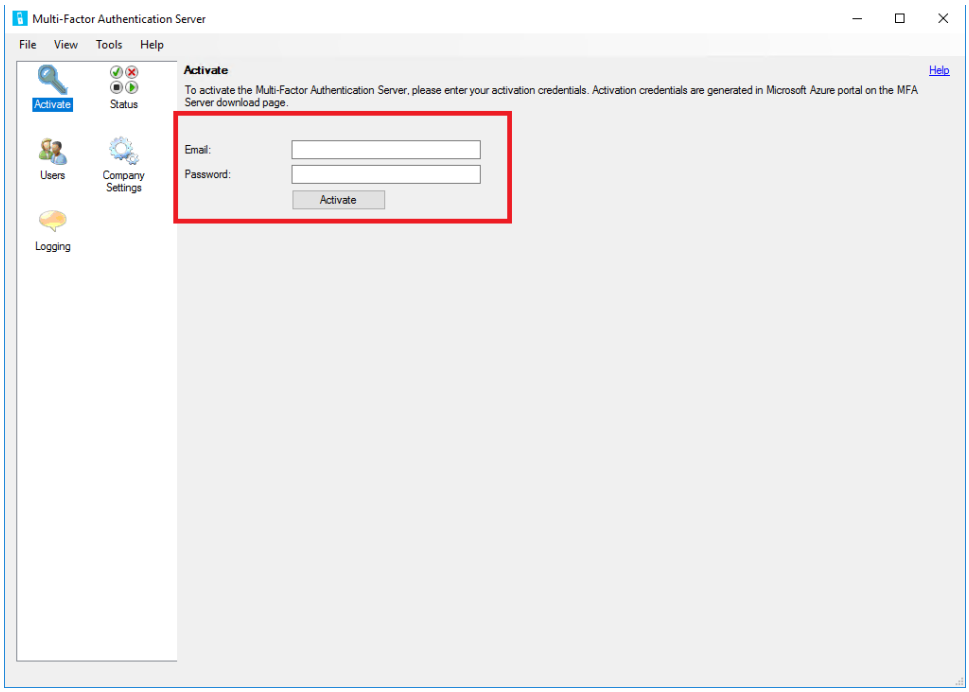
Kuva 18. Sopimusehtojen hyväksyminen



Kuva 19. Asennuskansion valinta



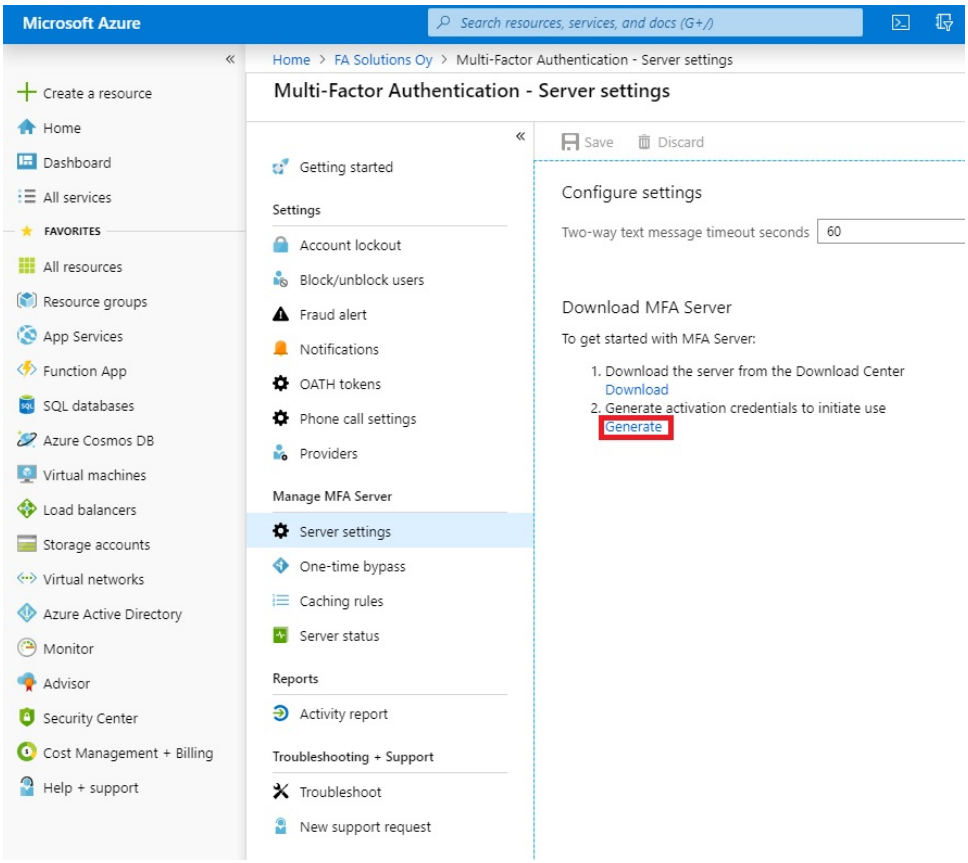
Kuva 20. Asennuksen onnistumisesta ilmoittava ikkuna



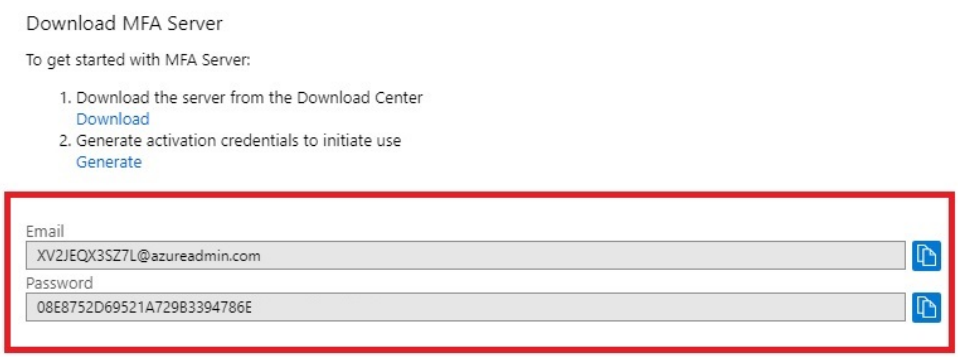
Kuva 21. MFA-ohjelmiston aktivointi

Asennuksen jälkeen täytyy aktivoida ohjelmisto palvelimella. Aktivointi tarvitaan käyttöoikeuden tarkistukseen ja Azure AD:n yhdistämiseen palvelimeen. Tämä käyttäjätunnus

tulee generoida erikseen tätä tarkoitusta varten MFA Server -valinnan takaa löytyvällä ”Generate”-painikkeella (kuva 22).

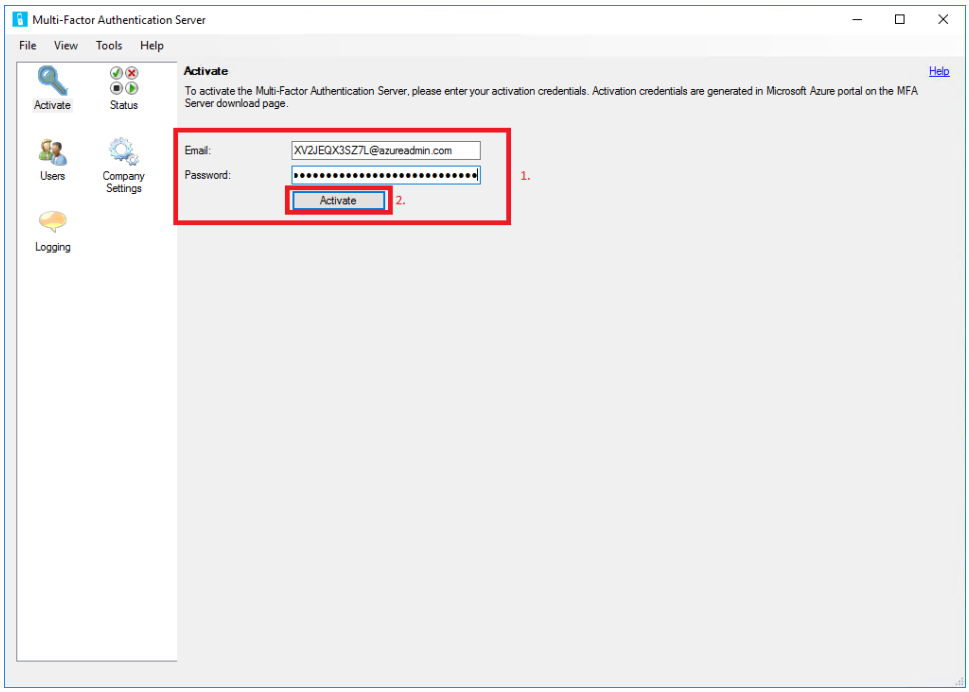


Kuva 22. Aktivointikäyttäjätunnuksen generointi 1

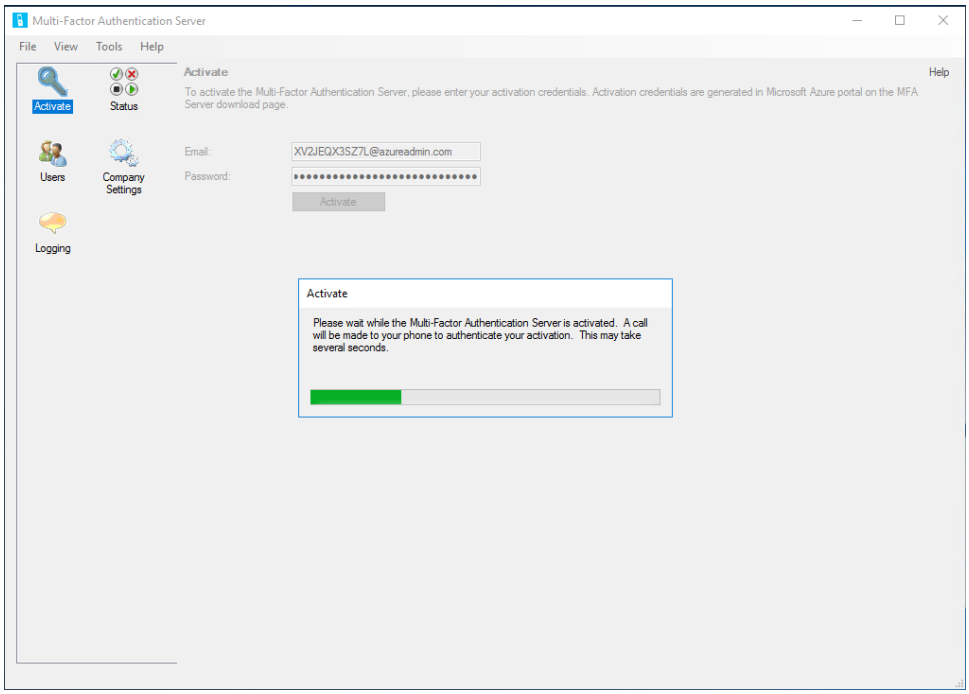


Kuva 23. Aktivointikäyttäjätunnuksen generointi 2

Käyttäjän sähköposti ja salasana voidaan kopioida erikseen oikeassa reunassa olevasta nappulasta, jotta niitä ei tarvitse erikseen kirjoittaa.

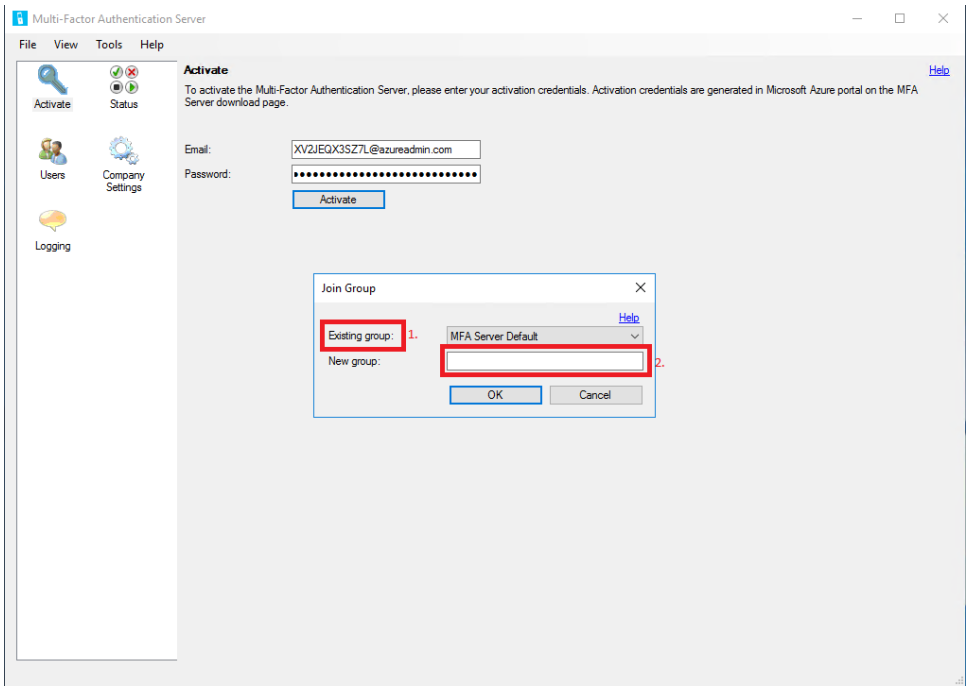


Kuva 24. MFA Server -ohjelmiston aktivointi 1



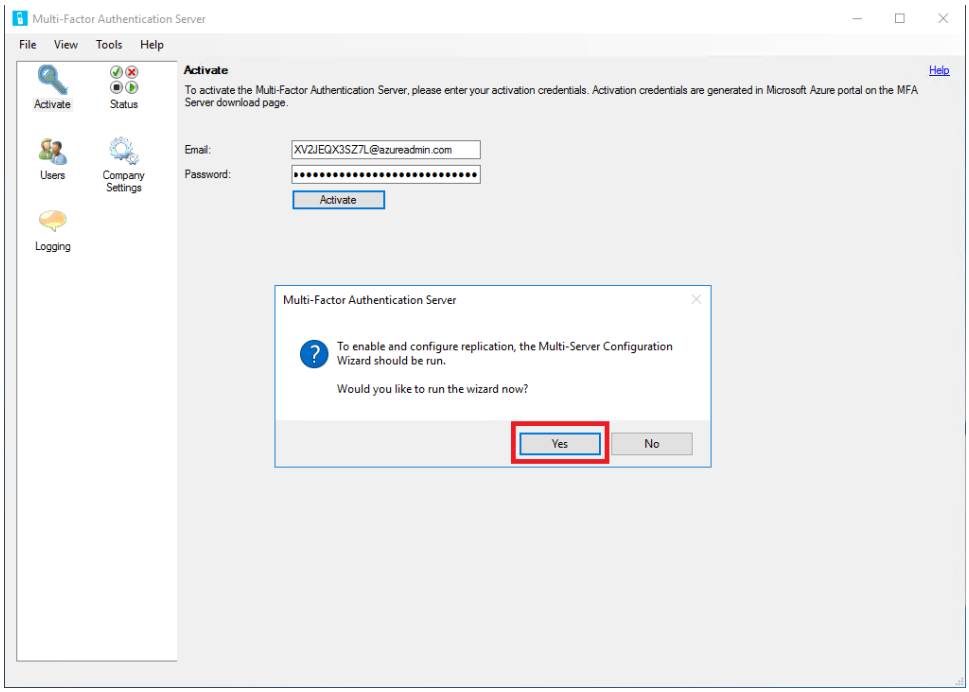
Kuva 25. MFA Server -ohjelmiston aktivointi 2

Azure-portaalista saamillamme tunnuksilla aktivoidaan ohjelmisto. Aktivointi saattaa kestää hetken.



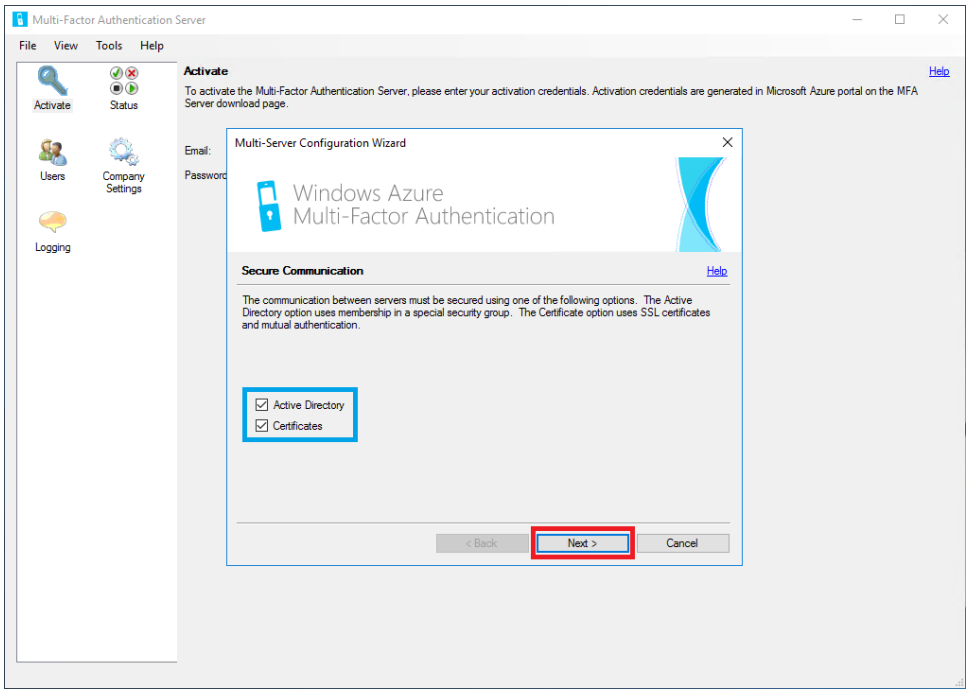
Kuva 26. Paikallisesta AD:stä löytyvän ryhmän valinta

Asennuksessa meidän täytyy valita käyttäjäryhmä oman palvelimen käyttäjäryhmistä. Mikäli meillä ei ole valmiina käyttäjäryhmää, voimme luoda sen tästä. Kaikki käyttäjät lisätään aina ”Active Directory Users And Computers” -kohdasta.



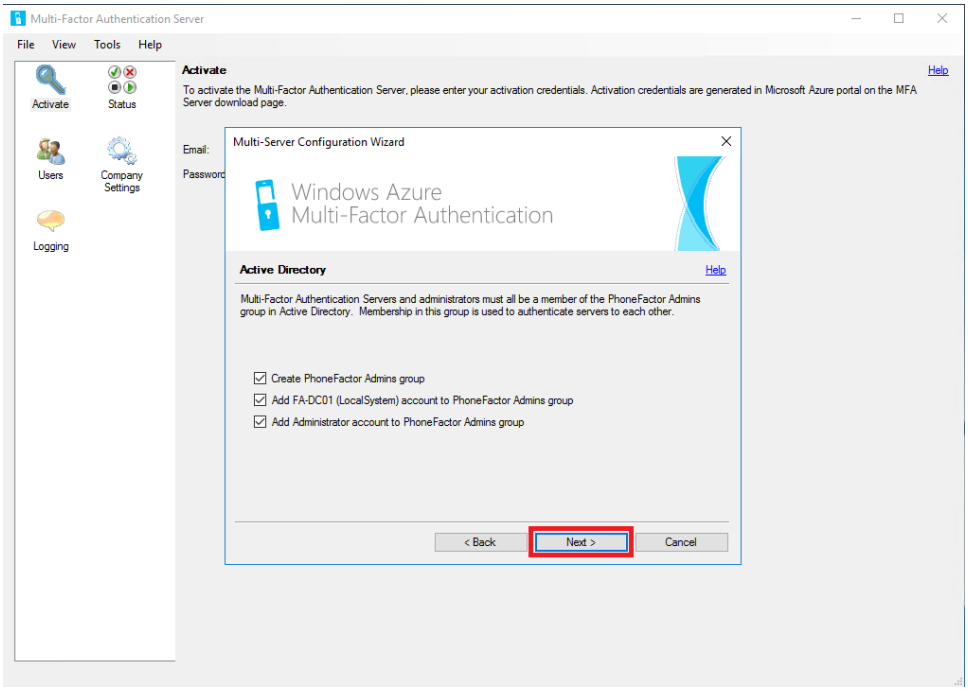
Kuva 27. Asennuksen jälkeen kysymys asennusvelhosta

Asennuksen jälkeen tahdomme tehdä asennusvelhon käyttöönotosta. Tällä velholla saamme ohjelmiston käyttöön tarvittavat ensiasetukset.



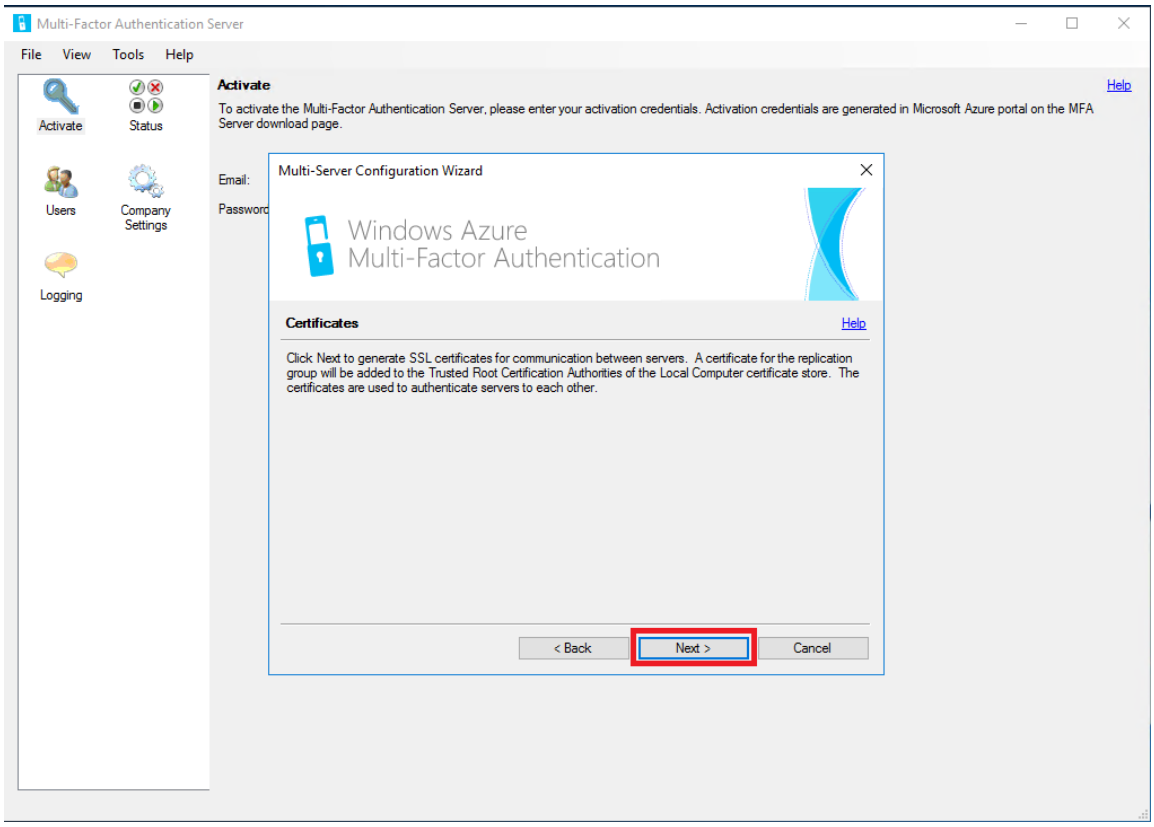
Kuva 29. Käyttäjän todennuksen valinta

MFA-tunnistautumisen voi tehdä, joko sertifikaatti- tai AD-käyttäjäpohjaisesti.



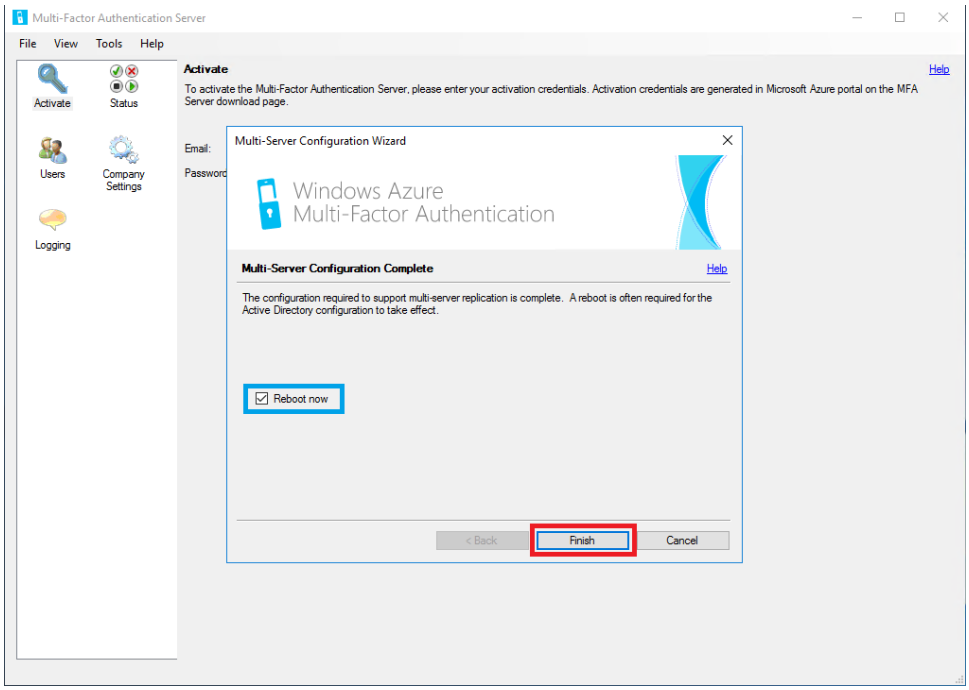
Kuva 30. ”PhoneFactor Admins” -käyttäjäryhmän luonti

Mikäli käyttäjä tahtoo konfiguroida MFA Serverin ominaisuuksia, täytyy hänelle antaa ”PhoneFactor Admins” -käyttöoikeus. Tällainen ryhmä luodaan aina MFA Server-ohjelmiston asennuksen yhteydessä, mikäli ryhmää ei jo ympäristössämme ole. Voimme myös valita nykyisen paikallisen järjestelmänvalvojan sekä toimialueen järjestelmänvalvojan saamaan kyseiset oikeudet.

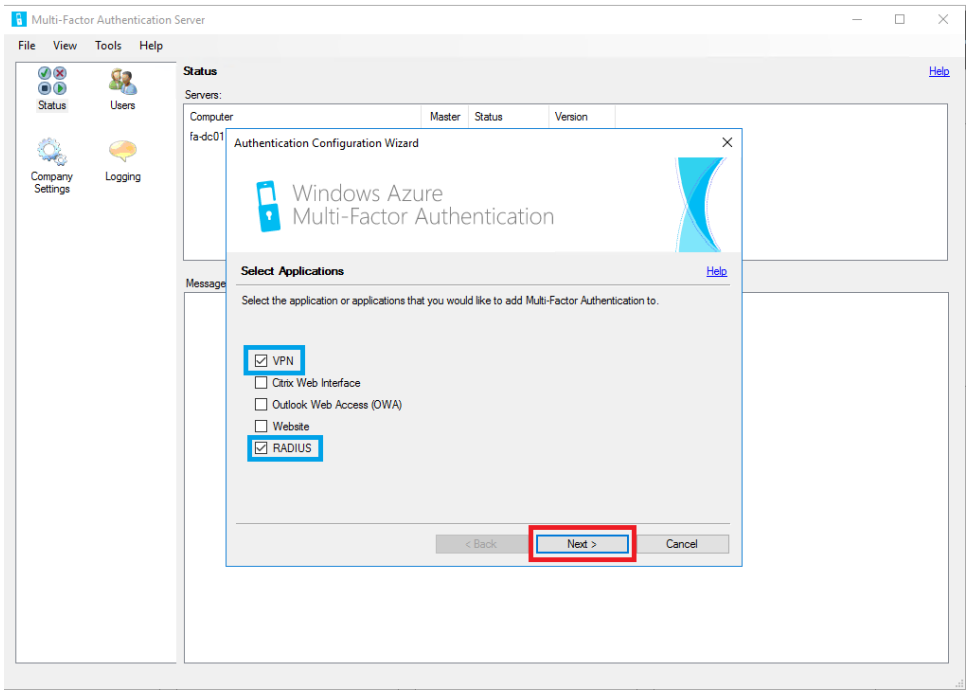


Kuva 31. MFA-Server -sertifikaatin luonti

Asennusvelho luo palvelimelle palvelin ja käyttäjäsertifikaatit automaattisesti.



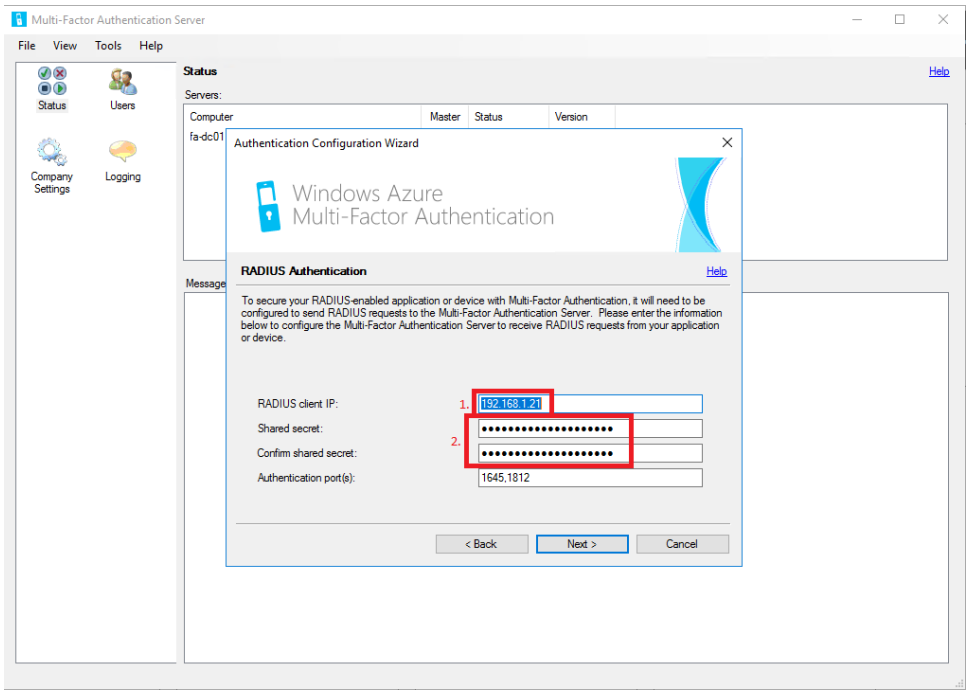
Kuva 32. Palvelin käynnistetään uudelleen asennuksen jälkeen



Kuva 33. MFA-ominaisuutta käyttävien ominaisuuksien valinta

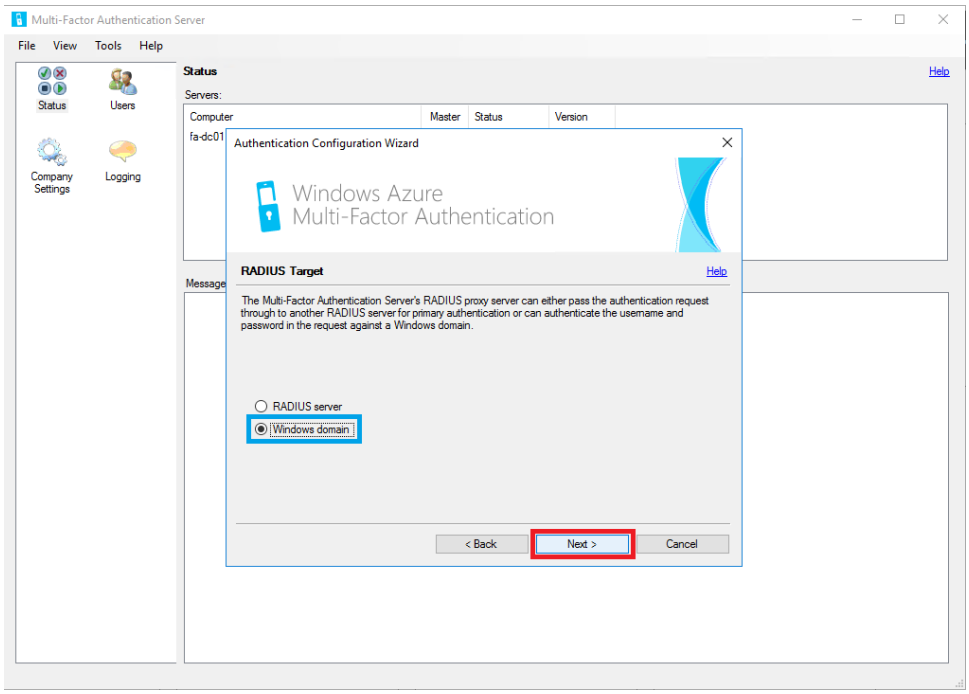
MFA-ominaisuutta voi siis käyttää muutama ominaisuus. Me valitsemme tässä RADIUS- ja VPN-ominaisuudet. VPN-ominaisuus ei tosin työssämme ole pakollista, mutta mikäli

tahdomme tulevaisuudessa käyttää Windowsin VPN-ominaisuutta ja VPN-roolia, niin valitaan se samalla. Työssämme vahvistus toimii täysin RADIUS:n piirissä.



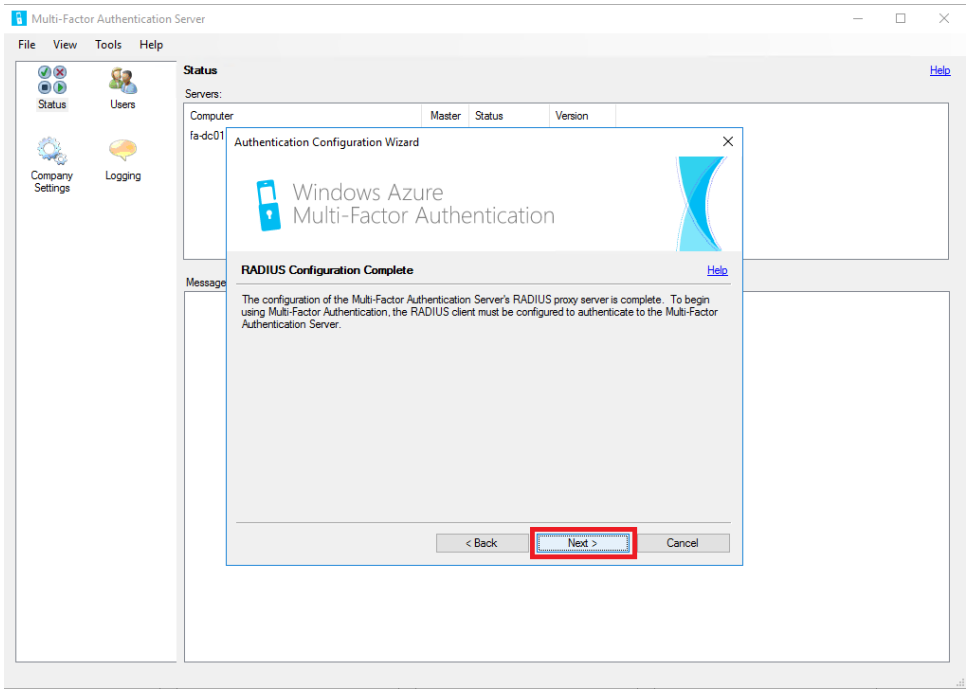
Kuva 34. RADIUS-palvelimen IP-osoitteen asetus ja jaettu salausavain

Tässä kohtaa määritellään RADIUS-palvelimen IP-osoite. Mikäli RADIUS sijaitsee samalla palvelimella kuin tämä MFA Server, niin voimme käyttää myös localhost-osoitetta.

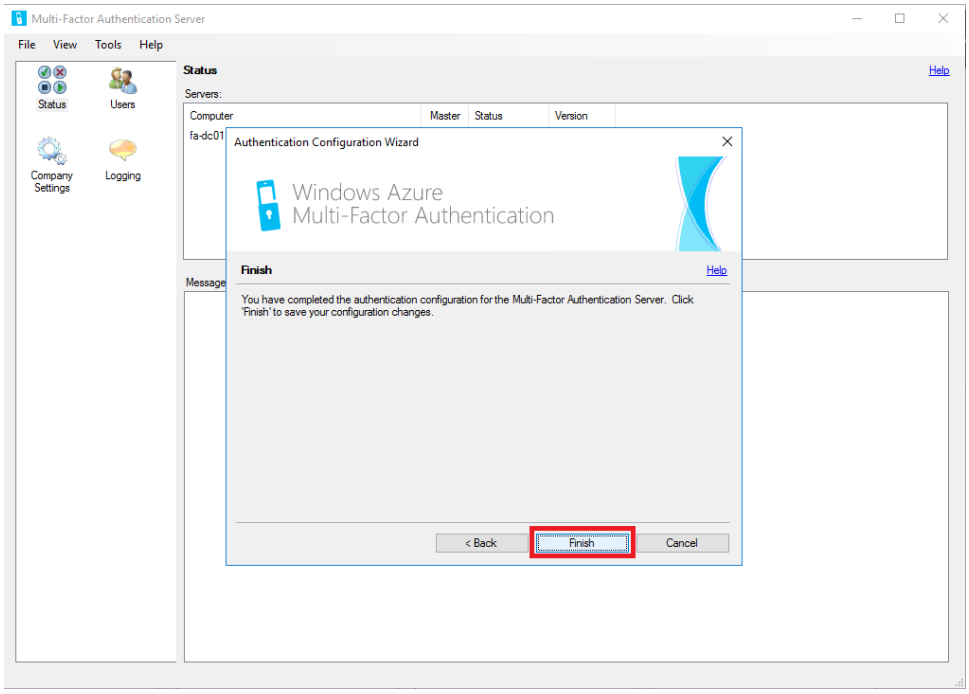


Kuva 35. RADIUS-tunnistautumiskohde

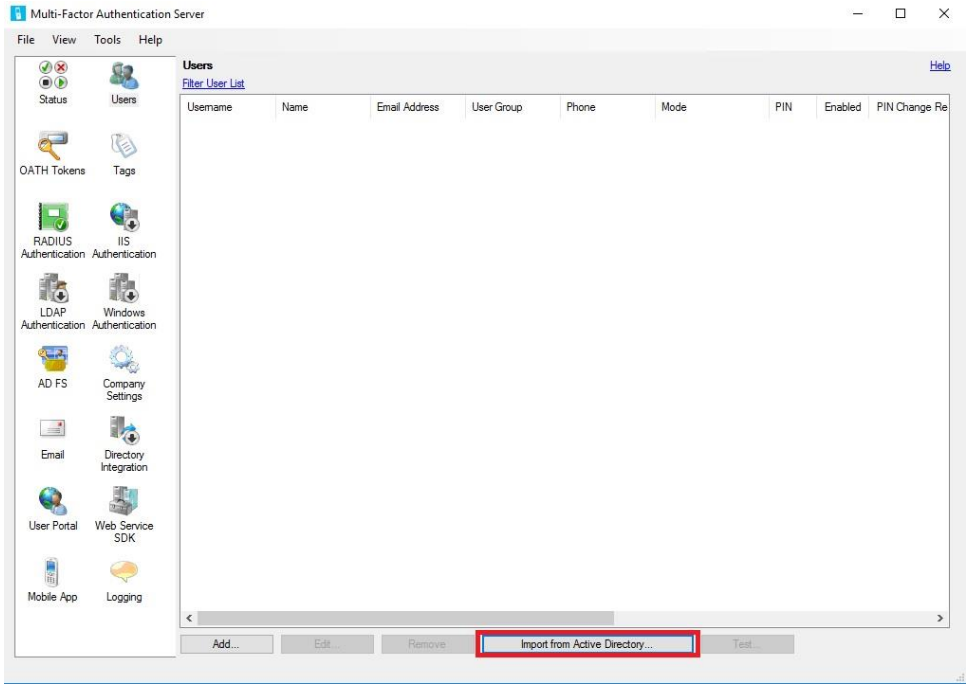
Tässä (kuva 35) valitsemme oikean kohteen, mihin käyttäjätunnistus ohjataan. RADIUS-palvelimemme kuitenkin aina ohjaa kyselyt suoraan Windows-toimialueelle, joten erilisiä RADIUS-käyttäjiä ei ole.



Kuva 36. Konfiguroinnin valmistumisilmoitus

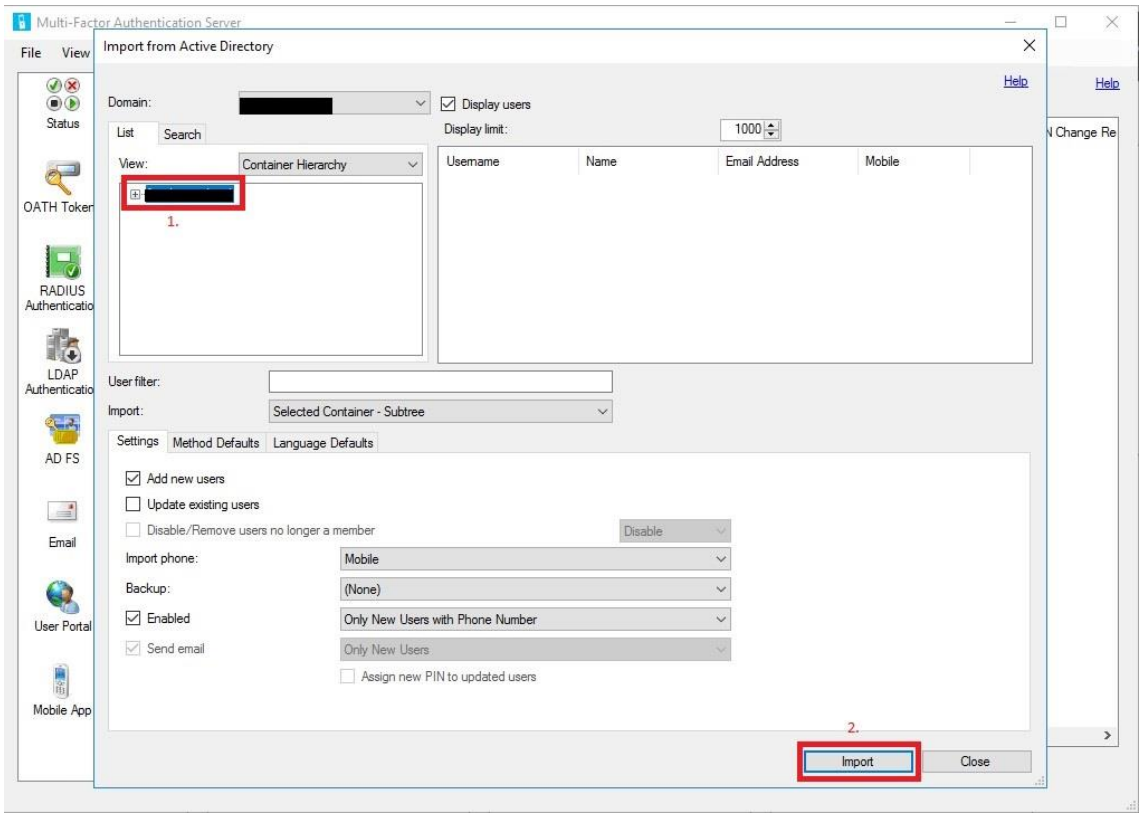


Kuva 37. Konfigurointi valmis



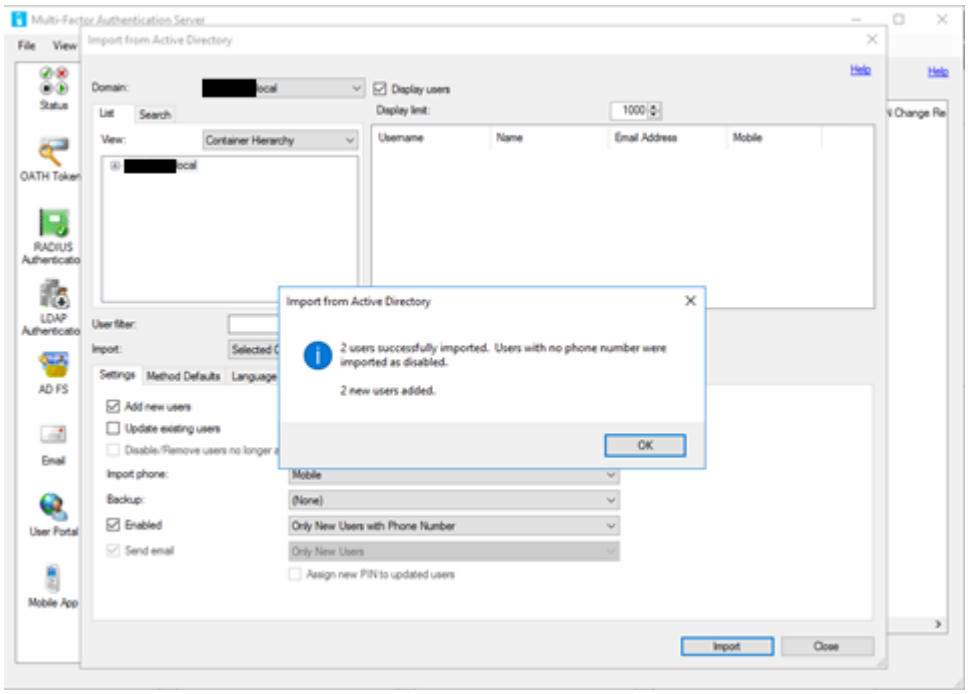
Kuva 38. Käyttäjien tuonti AD:stä

MFA:ta käyttävät käyttäjät tuodaan MFA Server -ohjelmistoon AD:stä. Tästä käyttäjälistauksesta voimme konfiguroida käyttäjäkohtaisia asetuksia, kuten käyttäjän todennustapaa ja puhelinnumeroa.



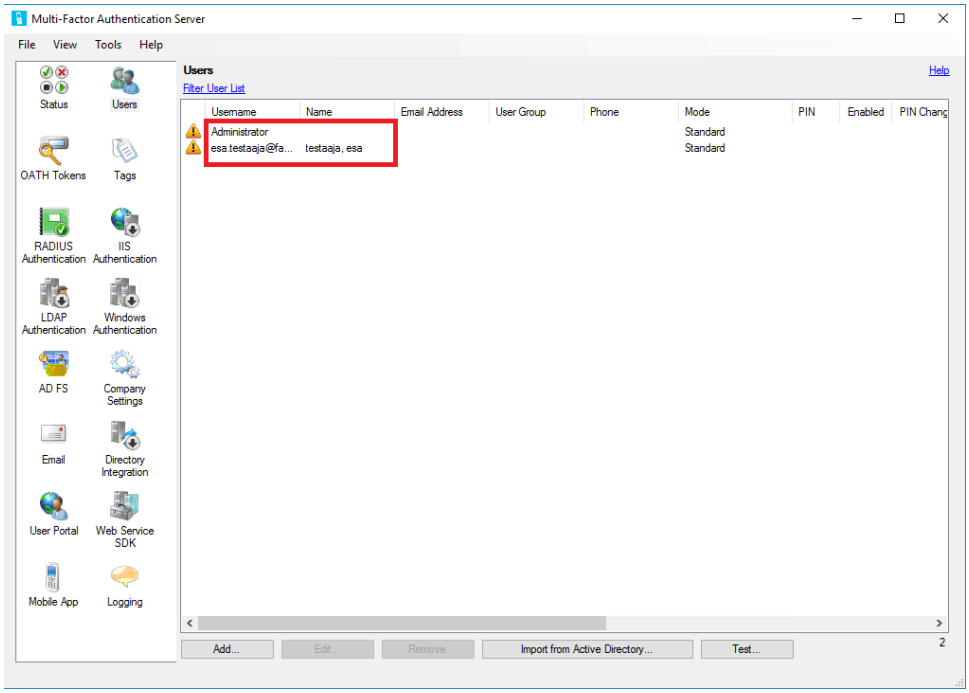
Kuva 39. Active Directoryn tuontiasetukset

MFA-palveluun tuodaan suoraan ADUC-tietokannasta käyttäjät haluttujen OU:iden alta. Tähän voidaan valita myös koko AD forest, joka tuo kaikki organisaation sisällä olevat käyttäjät MFA:n alaisuuteen.



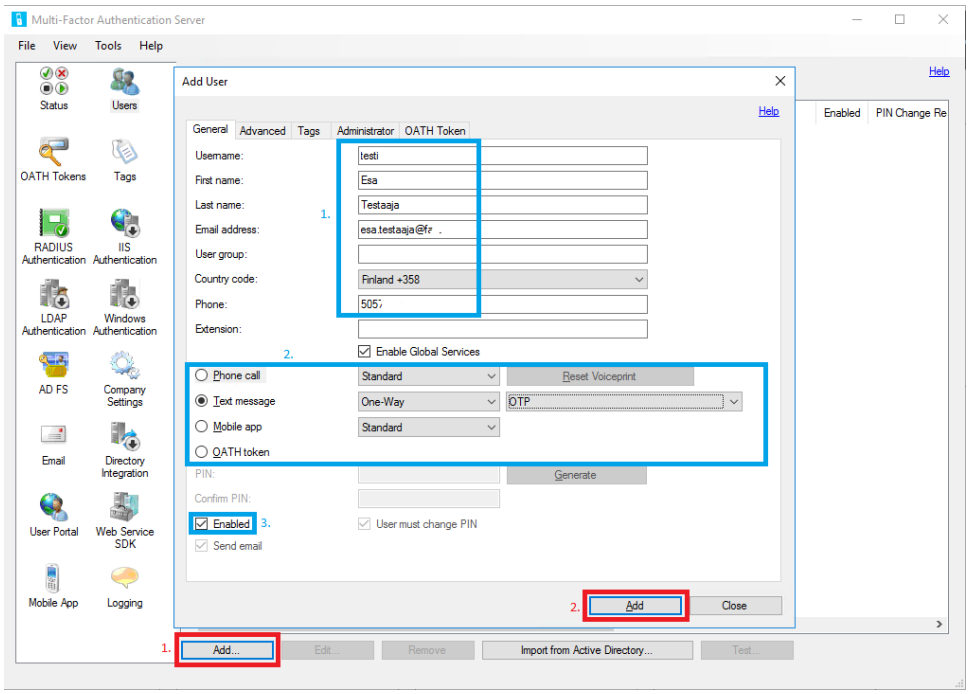
Kuva 40. Käyttäjien tuonnin raportti

Käyttäjien tuonnin jälkeen asennusvelho kertoo tuotujen käyttäjien ja myös virheellisten tuontien määrän.



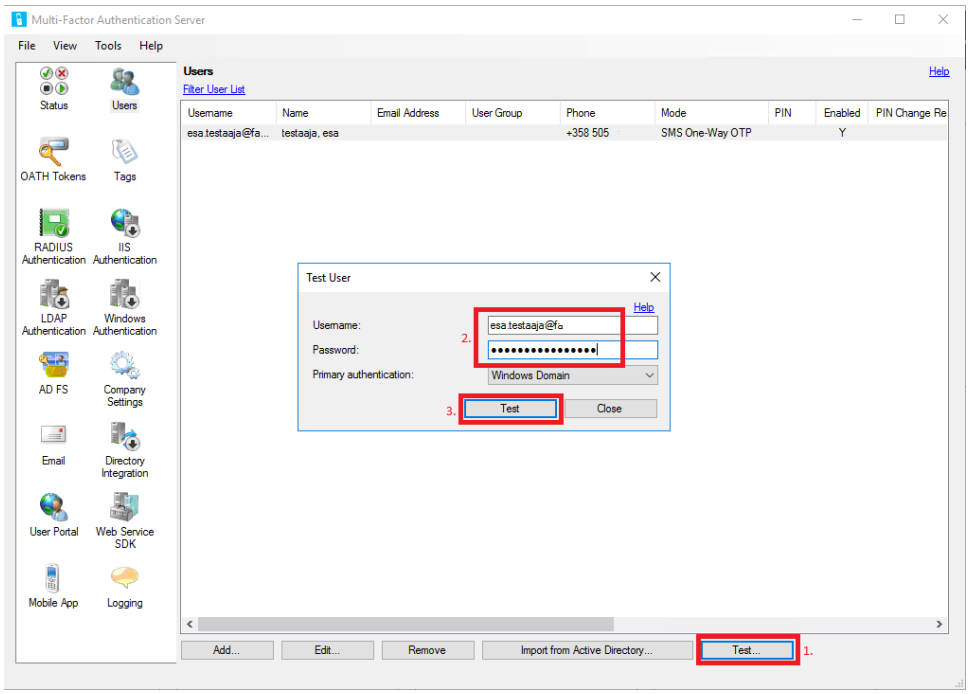
Kuva 41. MFA-käyttäjälistaus

Käyttäjät on listattu aakkosjärjestyksessä ja merkattu huomiokolmiolla, koska käyttäjille ei ole merkattu tarvittavia tietoja, jotta MFA voi toimia.



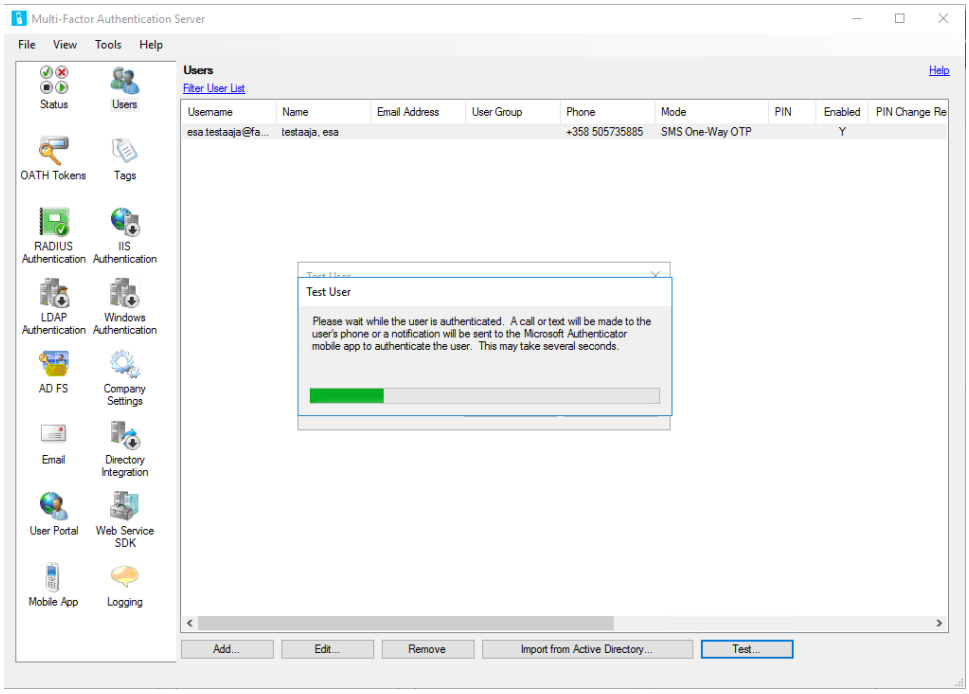
Kuva 42. Käyttäjän asetukset

Käyttäjällä pitää olla tiedossa puhelinnumero, sähköposti ja tunnistautumistapa. Käyttäjälle pitää myös erikseen laittaa ominaisuus päälle.



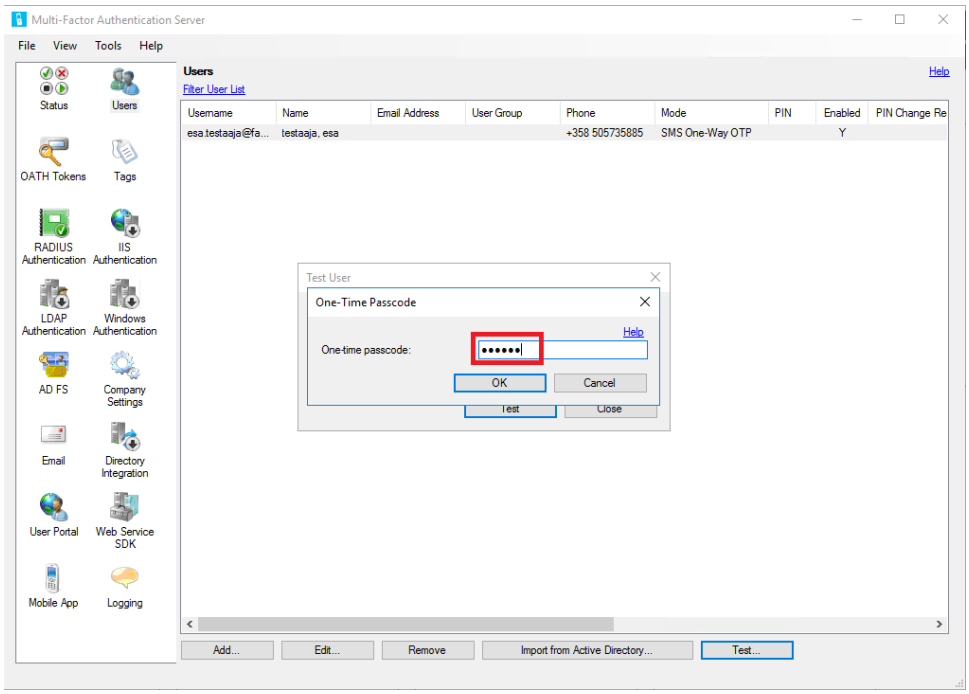
Kuva 43. Käyttäjän MFA-tunnistustestaus

Palvelussa voi testata suoraan sen asetusten toimintaa “Test”-nappulan avulla.



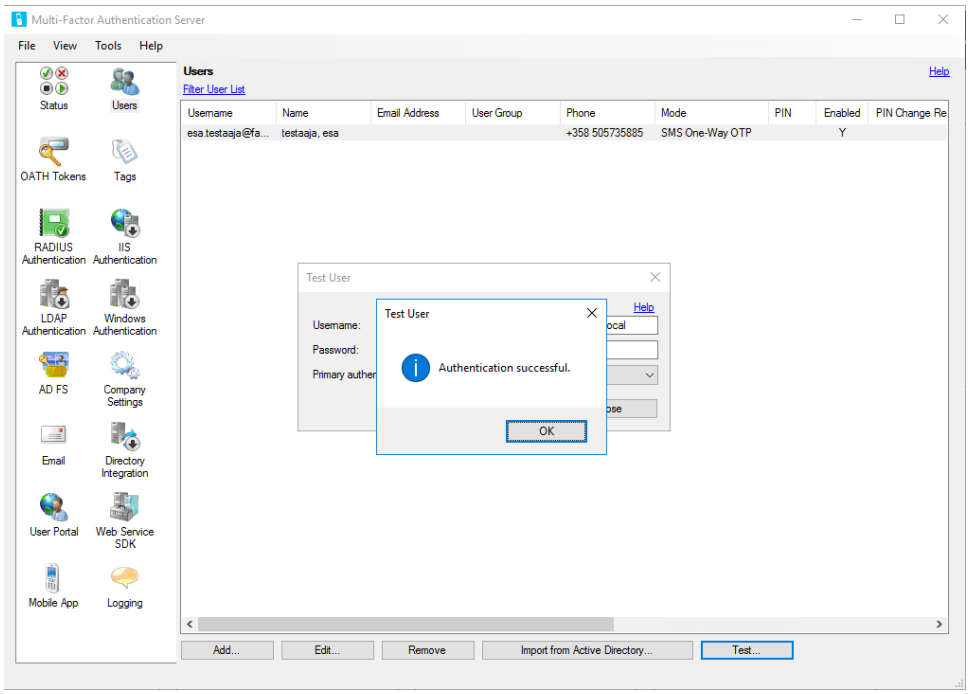
Kuva 44. Käyttäjän testitunnistuksen eteneminen

Tunnistautumisen eteneminen ei ole relevantti tunnistuksen oikeaan etenemiseen. Se näyttää vain, että jotain tapahtuu.



Kuva 45. MFA:n 6-numeroinen tunnistuskoodi

Microsoft lähettää annettuun puhelinnumeroon viestillä 6-numeroisen koodin, jonka syöttämällä kirjautuminen menee läpi.



Kuva 46. Onnistunut tunnistus

Jos tunnistautuu onnistuneesti, siitä saa hyväksytyn viestin.

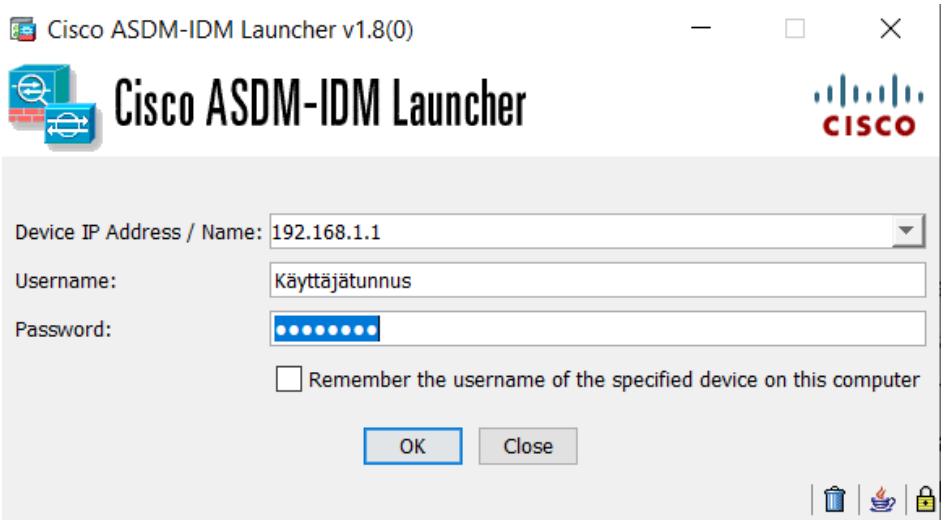
Tunnistuksen onnistumisen jälkeen MFA-server toimii halutusti, jonka jälkeen se voi tuoda käyttöön esimerkiksi VPN-tunnistukseen, joko RADIUS-toiminnon kautta tai Windows Server VPN -palvelun avulla.

5.2.3 Cisco ASA 5506-X

Palomuurilaitteen valinnassa ei meidän osallamme ollut suurta valinnan vaikeutta. Ciscon ASA-mallisto on ollut laajalti käytössä asiakkaillamme. Olemmekin käyttänyt tätä kyseistä muuria hyvin usein ja todenneet sen hyvin toimivaksi ja varmaksi yritysten palomuurilaitteeksi. Cisco ASA:n konfigurointi ei toki ole lainkaan yksinkertaista, mutta kun sen hallitsee, niin laitteesta saa varsin monia ominaisuuksia tukevan kivijalan yrityksen turvallisuuteen. Valitsemamme 2018 ASA 5506-X -malli on yleisin asiakkaillamme. Sen hinta on noin 470 €, joten laite tarjoaa erittäin hyvän hinta-laatu suhteen.

Konfiguroinnissa tarvitsee erillisen Ciscon internetsivustolta ladattavan asiakasohjelmiston, jolla laitteeseen voi ottaa yhteyden konsoliportin kautta. Tämän asiakasohjelmiston

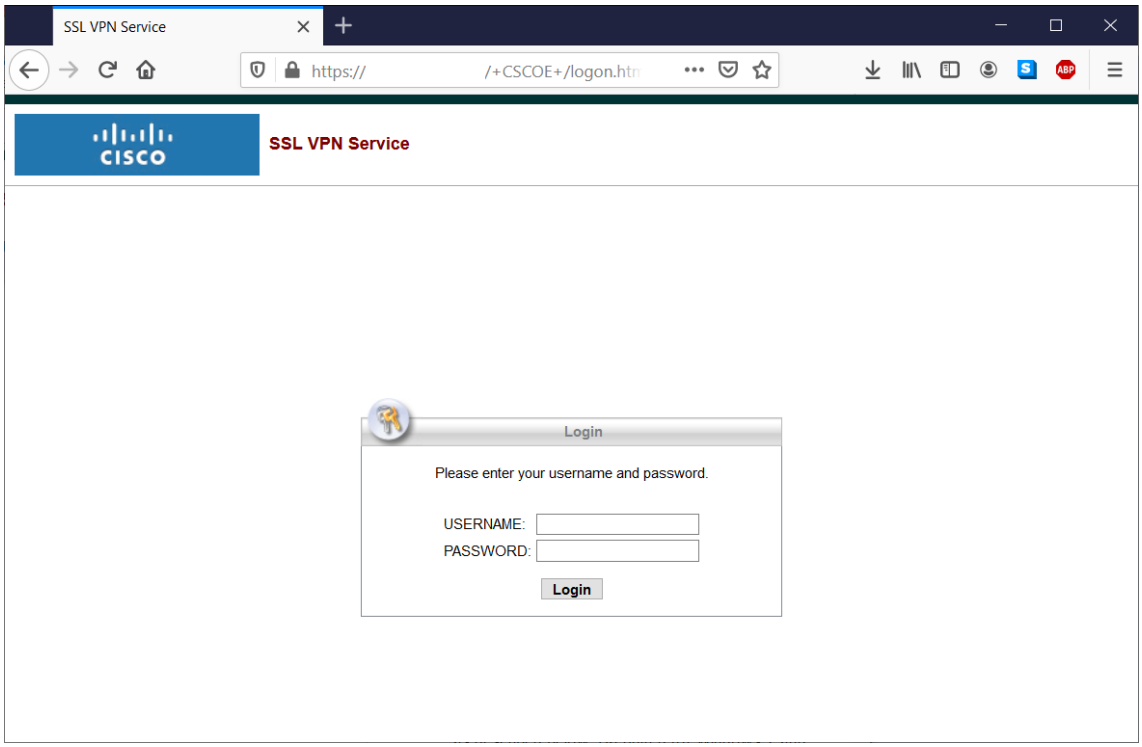
nimi on ASDM, eli ”Adaptive Security Device”. Ohjelmisto mahdollistaa sekä graafisen että komentorivipohjaisen konfiguroinnin.



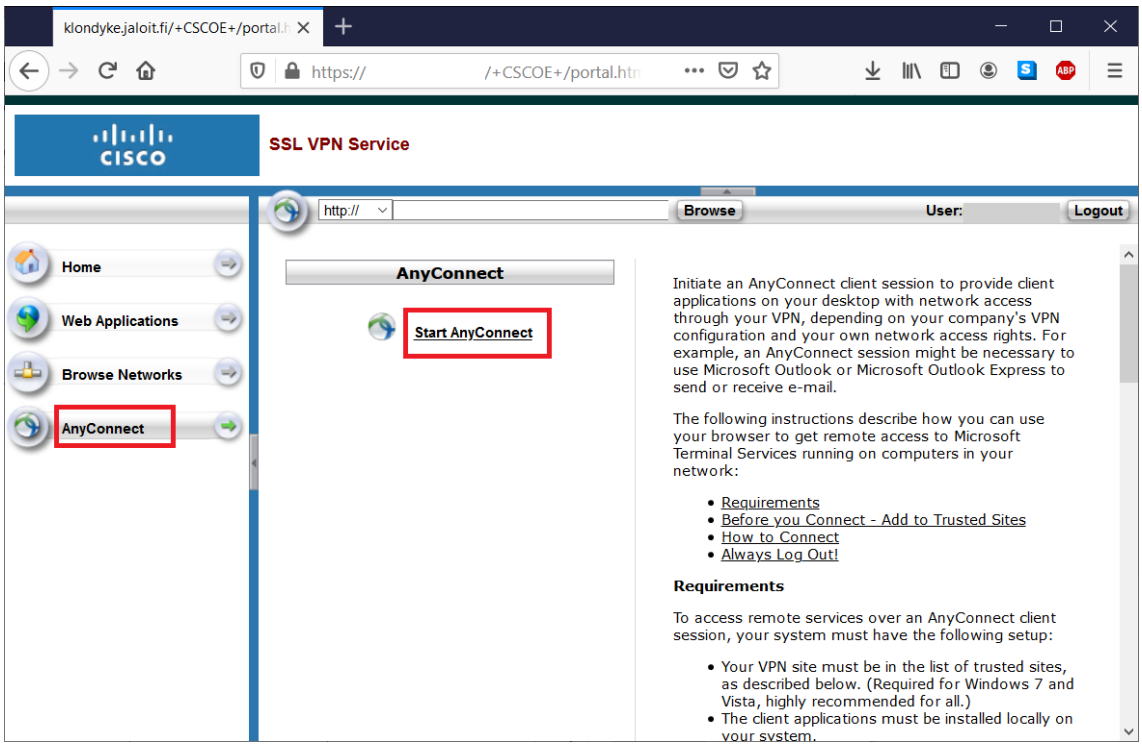
Kuva 48. Kuvakaappaus ASDM-kirjautumisikkunasta

5.2.4 Käyttäjien VPN

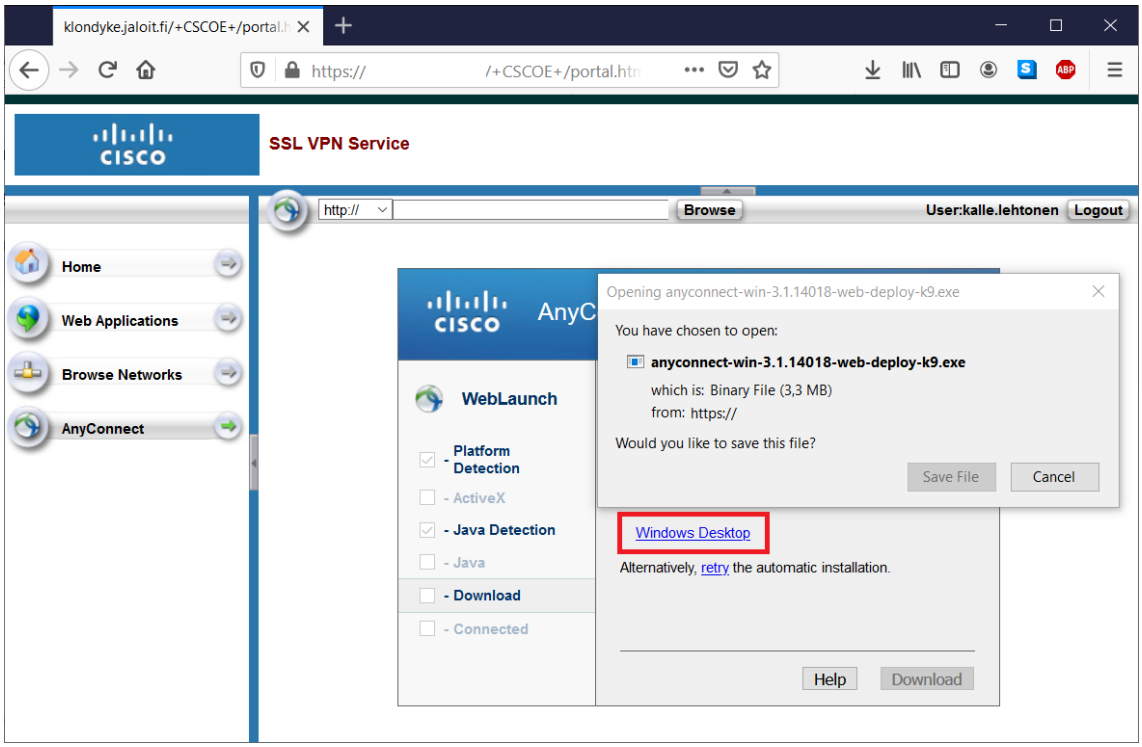
Cisco ASA tarjoaa käyttäjille SSL-VPN-sovellusta Cisco AnyConnect Secure Mobility Client sen voi ladata selaimella Cisco ASA:n verkkopohjaisesta käyttöliittymästä.



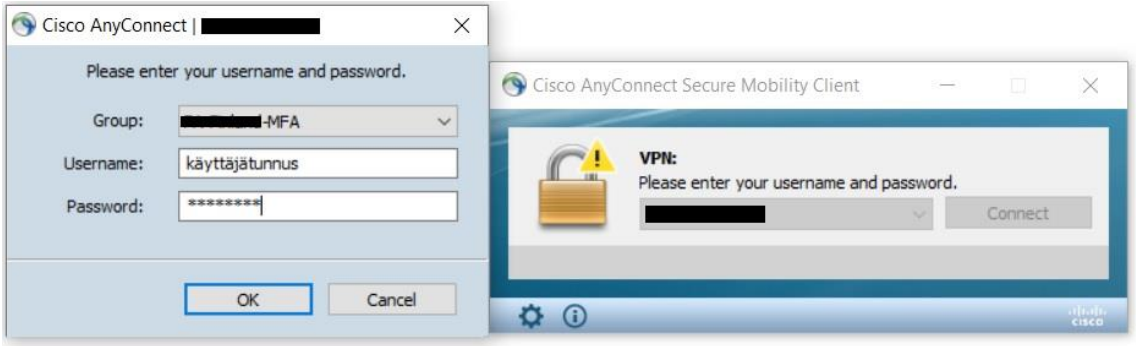
Kuva 49. Selainpohjainen kirjautumisikkuna



Kuva 50. AnyConnect-ohjelmiston lataus selaimella



Kuva 51. AnyConnect-ohjelmiston asennus



Kuva 52. Käyttäjän AnyConnect VPN -kirjautumisikkuna

Asennuksen jälkeen voidaan syöttää AnyConnectiin ASA:n osoite ja painaa “Connect”, jolloin käyttäjälle tulee ilmoitus vahvistuskoodista. Vahvistuskoodi tulee siis tässä vaiheessa tekstiviestinä puhelimeen. Käyttäjän on myös mahdollista käyttää matkapuhelimen todennussovellusta.

5.2.5 Azure-tunneli

Asiakkaalla on käytössä Microsoft Azuressa DC-palvelin, jolloin tarvitaan IPSec -tunneli heidän toimistoltaan Azureen. Tämä on toteutettu Cisco ASA -palomuurin ja Microsoft

Azure Virtual Network Gatewayn välillä, jossa käytettiin reittipohjaista VPN-tunnelia. (Liite 1. Azure -tunnelin konfiguraatio.)

5.3 Verkkoturvallisuus

Verkkoturvallisuuden ollessa nykyään entistä isommassa roolissa tulee konfiguraatioiden olla mahdollisimman turvallisia ja olennaisia. Turvallisuus pilven ja laitteen välillä onkin konfiguroitava moderneilla salausmenetelmillä, että voidaan olla mahdollisimman varmoja, ettei verkkomme ole tunkeuduttavissa. Tunneli konfiguroidaan molempiin päihin laitetta IPSsec-teknologialla. Seuraavana ovat konfiguroinnin vaiheet molempiin päihin tunnelia.

```
aaa-server FA-RADIUS protocol radius
 realm-id 1
aaa-server FA-RADIUS (inside2) host XXX.XXX.XXX.XXX
 key *****
 radius-common-pw *****
```

ASA:n RADIUS-konfiguraatio:

```
crypto ipsec ikev2 ipsec-proposal AES-256
 protocol esp encryption aes-256
 protocol esp integrity sha-1
!
crypto map outside_map1 1 match address outside_cryptomap_1
crypto map outside_map1 1 set pfs group24
crypto map outside_map1 1 set peer XXX.XXX.XXX.XXX
crypto map outside_map1 1 set ikev2 ipsec-proposal AES-256
crypto map outside_map1 1 set security-association lifetime seconds 7200
crypto map outside_map1 1 set security-association lifetime kilobytes 102400000
crypto map outside_map1 interface outside
crypto isakmp identity address
!
crypto ikev2 policy 1
 encryption aes-256
 integrity sha384
 group 24
 prf sha384
 lifetime seconds 86400
```

Ohessa Cisco ASA:lta haettu konfiguraatio Azure-tunneliin. Tärkeinä kohtina on IKEv2 Policy, jossa kerrotaan, millä salausalgoritmillä tunneli luodaan ja, IPSec-protokolla, jolla itse tunnelissa kulkeva tieto salataan. Crypto Map kertoo, mitä tietoa ja kuinka paljon tunneli hyväksyy ennen kuin se tarvitsee luoda uudelleen.

6 Yhteenveto

Tässä insinöörityössä suunniteltiin ja toteutettiin kaksivaihetunnistus asiakasyrityksemme VPN-yhteyksiin.

Projekti alkoi tutustumalla yrityksen tietoturvallisuuden parannusmahdollisuuksiin. Huomasimme yrityksen suuressa käytössä olevan VPN-yhteyden olevan keskisuuri tietoturvariski. Tämän kaksivaihetunnistuksen käyttöönotolla paransimme yrityksen tietoturvallisuutta huomattavasti.

Työn aikana asensimme Azure-pilvipalvelimen ja tälle palvelimelle Active Directory -roolin. Kopiomme jokaisen käyttäjän erikseen manuaalisesti Azure AD:stä pilvipalvelimelle. Asensimme tämän jälkeen Microsoft MFA Server -ominaisuuden sille. Tehtyämme tämän konfiguroimme MFA Serverin toimintaan.

Asennettuamme toimivan ympäristön testikäyttäjineen ja testattuamme toiminnan aloimme kouluttamaan käyttäjiä toiminnan käytöstä. Otimme ensin pienen testierän avainkäyttäjiä. Kun tämä testierä oli todennut palvelun toimivaksi, aloitimme palvelun käyttöönoton lopuille henkilöille. Käyttöönotto sujui erittäin hyvin ja koulutuksessakaan ei mennyt kovinkaan kauaa. Henkilökunta myös omaksui uuden vaiheen kirjautumiseen hienosti.

Työhön meni noin kolme kuukautta aloituksesta. Asennus ja konfigurointi on ollut erittäin antoisaa tietoturvallisuuden, salausmenetelmien ja pilvipalveluiden ollessa nykypäivänä erittäin ajankohtaista.

Lähteet

1. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota!. 2018. Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. Verkkoaineisto. <https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota>. 3.2018. Luettu 20.06.2019.

2. Getting started with the Azure Multi-Factor Authentication Server. 2019. Microsoft Oy. Verkkodokumentti. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-deploy>. 20.05.2019. Luettu 05.09.2019.

3. Azure Active Directory Conditional Access settings reference. 2019. Microsoft Oy. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference>. 10.07.2019. Luettu 05.09.2019.

4. Simon Thorpe. 2017. Authy vs Google Authenticator. Verkkoaineisto. <https://authy.com/blog/authy-vs-google-authenticator/>. 08.03.2017. Luettu 03.08.2019.

5. What is hybrid identity with Azure Active Directory?. 2019. Microsoft Oy. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>.17.05.2019. Luettu 05.09.2019.

6. Plan virtual networks. 2018. Microsoft Oy. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm>. 16.05.2018. Luettu 03.08.2019.

7. Pricing calculator. 2019. Microsoft Oy. Verkkoaineisto. <https://azure.microsoft.com/en-us/pricing/calculator/>. Luettu 2019.

8. Remote access to on-premises applications through Azure Active Directory's Application Proxy. 2019. Microsoft Oy. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>. 09.05.2019. Luettu 03.08.2019.

```
! Microsoft Corporation
! ------------------------------------------------------------------------
------------------------------------------------------------
! Generic configuration templates
!
! DISCLAIMER : THIS IS A SAMPLE CONFIGURATION SCRIPT OFFERED BY MICROSOFT FOR
YOUR 3RD PARTY DEVICE. IF YOU NEED
!                  HANDS-ON SUPPORT OR FURTHER ASSISTANCE, PLEASE CONTACT YOUR
VENDOR DIRECTLY.
!
!
! IMPORTANT :
!
!    > YOU ARE RUNNING A CISCO ASA FIRMWARE VERSION BETWEEN 9.6(4) AND 9.7(x),
USE THIS CONFIGURATION SCRIPT (you are in the right place!)
!         >> IKEv2 RouteBased IPSec tunnel, operating 0/0 Traffic Selectors,
and crypto configurations (no IKEv2 VTI Support available for these versions)
!
!    > IF YOUR ASA VERSION IS 9.8(1) OR HIGHER, PLEASE USE THE OTHER AVAILABLE
SCRIPTS THAT ARE MORE SUITABLE FOR THIS VERSION:
!
!
!    > IF YOUR ASA VERSION IS BELOW 9.6(4), PLEASE USE THE OTHER AVAILABLE
SCRIPT THAT IS MORE SUITABLE FOR THIS VERSION:
!         >> "Cisco_ASA_[9.6(4)-or-BELOW_ONLY]_(IKEv2-NoBGP)_REQUIRED:Custom-
Azure-IPSec-Policies_w/Narrow_TrafficSelectors"
!         >> YOU MUST ALSO HAVE YOUR AZURE CUSTOM IPSEC POLICIES WITH NARROW
TRAFFIC SELECTORS ALREADY ENABLED ON THE CONNECTION:
!              > https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gate-
way-connect-multiple-policybased-rm-ps
!
!
!    This configuration template shows all the VPN configuration parameters
associated with your S2S VPN connection.
!    The script you need to copy onto your ASA 9.6(4)-9.7(x) to setup a Route-
Based IKEv2 VPN Tunnel to Azure is found below [#10]
! ------------------------------------------------------------------------
------------------------------------------------------------
! [1] Resource names
!     CONNECTION NAME               : This field is the name of your connec-
tion resource
!     VIRTUAL NETWORK GATEWAY   : The name of your Azure VPN gateway resource
for the connection
!     LOCAL NETWORK GATEWAY         : The name of your local network gateway
resource for the connection
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/CONNECTION_NAME = Helsinki
/Data/VNG_NAME        = XXXXXXXXXXXX-XXXXXXXXXXXXX-XXXXXXXXXX-XXXXXX
/Data/LNG_NAME        = Helsinki
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [2] Public IP address of the Azure VPN gateway
!     Active-Standby VPN gateway (single public IP address)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/VNG_GATEWAYIP   = XXX.XXX.XXX.XXX
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!     Active-Active VPN gateway (A/A mode if more than one public IP is listed
below)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

/Data/VNG_GATEWAYIPS/IpAddress/IP = XXX.XXX.XXX.XXX
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [3] Public IP address of the on-premises VPN device
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/LNG_GATEWAYIP   = XXX.XXX.XXX.XXX
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [4] VNet address prefixes: a list of all VNet address prefixes in different
formats
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

/Data/VnetSubnets/Subnet/SP_NetworkIpRange = XXX.XXX.XXX.XXX
  SP_NetworkSubnetMask   = 255.255.252.0
  SP_NetworkWildcardBits = 0.0.3.255
  SP_NetworkCIDR         = XXX.XXX.XXX.XXX/XX
  SP_TunnelName          = SP_TunnelName
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [5] On-premises address prefixes: a list of all on-premises address prefixes
defined in LNG
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

/Data/OnPremiseSubnets/Subnet/SP_NetworkIpRange = 10.0.0.0
  SP_NetworkSubnetMask   = 255.255.255.0
  SP_NetworkWildcardBits = 0.0.0.255
  SP_NetworkCIDR         = 10.0.0.0/24
  SP_TunnelName          = SP_TunnelName
/Data/OnPremiseSubnets/Subnet/SP_NetworkIpRange = 10.0.1.0
  SP_NetworkSubnetMask   = 255.255.255.0
  SP_NetworkWildcardBits = 0.0.0.255
  SP_NetworkCIDR         = 10.0.1.0/24
  SP_TunnelName          = SP_TunnelName
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [6] Phase 1/Main Mode:
!     IKE encryption algorithm
!     IKE hashing algorithm
!     IKE Diffie-Hellman group
!     IKE SA lifetime (seconds)
!     IKE SA data size (Kilobytes)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/IKE_ENCRYPTION_1 = aes-256
/Data/IKE_INTEGRITY_1  = sha384
/Data/IKE_DHGROUP_1    = 24
/Data/IKE_SALIFETIME_1 = 28800
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [7] Phase 2/Quick Mode:
!     IPsec encryption algorithm
!     IPsec hashing algorithm
!     PFS Group (Perfect Forward Secrecy)
!     IPsec SA (QMSA) lifetime (seconds)
!     IPsec SA (QMSA) lifetime (kilobytes)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/IPsec_ENCRYPTION_1   = aes-256
/Data/IPsec_INTEGRITY_1    = sha-1
/Data/IPsec_PFSGROUP_1     = group24
/Data/IPsec_SALIFETIME     = 7200
/Data/IPsec_KB_SALIFETIME   = 102400000
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [8] Connection pre-shared key
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/CONNECTION_PSK = ******************
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! [9] BGP parameters - Azure VPN gateway
!     Enable BGP
!     BGP ASN for Azure VPN gateway
!     BGP speaker IP address for the Azure VPN gateway
!     BGP peer IP address(es)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/CONNECTION_BGP_ENABLED  = False
/Data/VNG_ASN                 = VNG_ASN
/Data/VNG_BGPIP               = VNG_BGPIP
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
! [10] BGP parameters - on-premises network / LNG
!      BGP ASN for the on-premises network
!      BGP speaker IP address for the on-premises network
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
/Data/LNG_ASN                = LNG_ASN
/Data/LNG_BGPIP              = LNG_BGPIP
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!



!
##############################################################################
##########################
! !!! Search for "REPLACE" to find the values that require special considera-
tions
!
##############################################################################
##########################

!
==============================================================================
! Example - Cisco ASA (9.6(4) to 9.7(x) ) in Active/Passive Azure GW Mode
!
==============================================================================



! Creating Object Groups for my LOCAL and REMOTE (Azure) Networks.
! Note: The networks are represented as [obj_any], in other words as 0/0. That
is to allow for dynamic routing.
!     REPLACE as needed.
!
!
object-group network AzureNetworksANY
  description Azure-Virtual-Network_ANY[0/0]_Representation
  network-object 0.0.0.0 0.0.0.0
exit
!
object-group network OnpremisesNetworksANY
  description Onpremises-Network_ANY[0/0]_Representation
  network-object 0.0.0.0 0.0.0.0
exit
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
!
! Some VPN devices require explicit ACL rules to allow cross-premises traffic
towards Azure:
! 1. Allow traffic between on premises address ranges and VNet address ranges
! 2. Allow IKE traffic (UDP:500) between on premises VPN devices and Azure VPN
gateway
! 3. Allow IPsec traffic (Proto:ESP) between on premises VPN devices and Azure
VPN gateway
!
! Note: The Access List Identifier here is "Azure-ACL"
!
access-list Azure-ACL extended permit ip object obj_any object obj_any log no-
tifications
!
! NAT'ing for this Azure tunnel for all on-premises and azure networks.
! Note: The ANY network object (0/0) is used to create the NAT. This is to al-
low flexible dynamic routing.
!          REPLACE as needed.
```

```
!
nat (inside,outside) source static obj_any obj_any destination static obj_any
obj_any no-proxy-arp route-lookup
!
!
! PHASE 1 : IKEv2 POLICY
!    Note: The Azure policy Priority # used for the Azure tunnel is "1" here.
REPLACE AS NEEDED}
!
!
crypto ikev2 policy 1
encryption aes-256
integrity sha384
group 24
prf sha384
lifetime seconds 28800
!
!=================
! PHASE 2:
!
!
crypto ipsec ikev2 ipsec-proposal Azure-Ipsec-Tunnel-Helsinki-XXX.XXX.XXX.XXX
 protocol esp encryption aes-256
 protocol esp integrity sha-1
!
crypto ipsec security-association lifetime seconds 7200
! Note: The KB_LIFETIME for Phase 2 is not required for RouteBased Tunnels. It
is commented out below due to a known Cisco bug causing the ASA to stop en-
crypting traffic during
!       SA rekeys when both Time and Data-based rekeys are used (CSCup37416)
!
!crypto ipsec ipsec security-association kilobytes 102400000
!
crypto ipsec security-association pmtu-aging infinite
crypto ipsec inner-routing-lookup
!
! This is your internal group policy for Azure, inheriting all built-in set-
tings except for the Tunneling Protocol (specified as "IPSec IKEv2" only)
! Note: The GroupPolicy used for Azure is labeled "AzureGroupPolicy".
!          REPLACE as needed
!
group-policy AzureGroupPolicy internal
group-policy AzureGroupPolicy attributes
 vpn-tunnel-protocol ikev2
dynamic-access-policy-record DfltAccessPolicy
tunnel-group XXX.XXX.XXX.XXX type ipsec-l2l
tunnel-group XXX.XXX.XXX.XXX general-attributes
 default-group-policy AzureGroupPolicy
tunnel-group XXX.XXX.XXX.XXX ipsec-attributes
 ikev2 remote-authentication pre-shared-key ********************
 ikev2 local-authentication pre-shared-key ********************
 no tunnel-group-map enable peer-ip
 tunnel-group-map default-group XXX.XXX.XXX.XXX
!
!-------------------------------------------------------------------------------
-------------------------------------------------------------
!  This is the crypto map you will use for your OUTSIDE interface (connected
to the Azure Gateway) in order to process any traffic passing through this in-
terface and destined to Azure.
!  The crypto map is what you will use to create the Quick Mode association
for this tunnel, and thereby to control all "interesting" traffic that crosses
it.
!  NOTE: The map Identifier used here is "1". This crypto map is mapped to my
ACL list, which is labeled "Azure-ACL" above.
!              REPLACE both values as needed.
```

```
!
crypto map outside_map 1 match address Azure-ACL
crypto map outside_map 1 set peer XXX.XXX.XXX.XXX
crypto map outside_map 1 set ikev2 ipsec-proposal Azure-Ipsec-Tunnel-Helsinki-
XXX.XXX.XXX.XXX
crypto map outside_map 1 set ikev2 pre-shared-key ******************
crypto map outside_map 1 set security-association lifetime seconds 7200
!
! Note: Once again, the KB_LIFETIME for Phase 2 is not required for RouteBased
Tunnels. It is commented out below due to a known Cisco bug causing the ASA to
stop encrypting traffic during
!        SA rekeys when both Time and Data-based rekeys are used (CSCup37416)
!
!crypto map outside_map 1 set security-association lifetime kilobytes
102400000
!
crypto map outside_map 1 set nat-t-disable
tunnel-group-map default-group XXX.XXX.XXX.XXX
!
! NOTE: As before, your outside/WAN interface that's connected to Azure is la-
beled as "outside".
! REPLACE if named differently on your device  (NAMEIF of the ASA's WAN inter-
face connected to Azure)
!
crypto map outside_map interface outside
!
! Enabling the IKEv2 policy on the OUTSIDE interface of your ASA
!   NOTE: your outside/WAN interface connected to Azure is labeled "outside".
REPLACE if named differently on your device.
!
crypto ikev2 enable outside
!
!-------------------------------------------------------------------------------
-----------
!    Set up your static route to push the Azure-bound traffic through your WAN
Interface.
!    The following is an example, consisting of a wildcard network prefix
0.0.0.0/0, with your local VPN Public IP as the next hop:
!
route outside 0.0.0.0 0.0.0.0 XXX.XXX.XXX.XXX 1
!
!
!-------------------------------------------------------------------------------
-------------------------------------------------------
! Built-in trustpool policy for Cisco ASA
!
crypto ca trustpool policy
!
! Setting traffic control for Azure tunnels (MSS=1350 bytes, and preserving
vpn flows during tunnel rekeys)
!
sysopt connection tcpmss 1350
sysopt connection preserve-vpn-flows
!
!-----------------------------------------------END-------------------------
-------------------------------!
```