

Mikko Vellonen

# Käyttäjien hallintaprosessin tehostaminen AD- verkossa

Metropolia Ammattikorkeakoulu  
Insinööri (AMK)  
Koulutusohjelma  
Insinöörityö  
Päivämäärä

Tekijä Otsikko	Mikko Vellonen Käyttäjien hallintaprosessin tehostaminen AD-verkossa
Sivumäärä Aika	31 sivua + 6 liitettä 5.12.2012
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoliikenne
Ohjaajat	projektikumppani Mikko Sorsa lehtori Keijo Länsikunnas
<p>Insinöörityön tavoitteena oli selvittää, kuinka Windows Server 2003 R2 Active Directoryyn luodaan käyttäjiä toimialueeseen sekä kuinka käyttäjätiliin lisätään oikeuksia sekä ryhmiä. Toimialueena toimii laaja yritysverkko, jossa on mukana useita käyttäjiä.</p> <p>Yrityksen Active Directory verkosta sain suoraa tietoa yrityksen sisällä verkkoa hoitavalta henkilöltä, jonka kanssa tein yhteistyötä työn edetessä. Tärkeää oli saada selvä käsitys siitä, kuinka käyttäjien luominen ja sen jälkeiset toimenpiteet suoritetaan käsin Active Directoryn kanssa. Tämän jälkeen esitetään vaihtoehtoinen ratkaisu, kuinka lisäämistä tehostetaan: Active Directory Management tool.</p> <p>Insinöörityössä verrataan näitä kahta tapaa, kuinka käyttäjän lisääminen suoritetaan, niin että käyttäjä on valmis työskentelemään. Insinöörityössä esitetään myös mahdollisia ongelmia ja ratkaisua. Insinöörityön tuloksilla pyritään antamaan selkeä käsitys, että on myös tehokkaampia tapoja suorittaa käyttäjien lisääminen Active Directory verkkoon. Insinöörityössä käy ilmi, miten tehostamista on parannettu ja mietitään, kuinka sitä voisi vielä parantaa enemmän. Näillä kahdella tavalla, joilla lisääminen suoritetaan, voidaan huomata selkeä ero lopussa.</p> <p>Insinöörityön toisena tavoitteena on antaa selkeä käsitys, kuinka käyttäjän lisääminen kahdella toisistaan poikkeavalla tavalla suoritetaan sekä kuinka paljon ne eroavat toisistaan.</p>	
Avainsanat	Active Directory, hallinnan tehostaminen

Author(s) Title	Mikko Vellonen Enhancing user management process in AD network
Number of Pages Date	31 pages + 6 appendices 5 December 2012
Degree	Bachelor of Engineering
Degree Programm	Information Technology
Specialisation option	Telecommunication
Instructor(s)	Mikko Sorsa, Project Partner Keijo Länsikunnas, Senior Lecturer
<p>The purpose of this thesis is to describe how users are created in Windows Server 2003 R2 Active Directory and how to add rights and groups to these users. A wide company domain enabling several users was used.</p> <p>Information about the Active Directory of the company was obtained from a person in charge of maintaining the Active Directory network. The work was coordinated from beginning to end. It was important to get a clear understanding of how a user is created and what the steps after that are to complete the process as Active Directory should only be used manually. After that had been done, an alternative solution was presented on how to enhance the management of adding a user into Active Directory: Active Directory Management tool.</p> <p>The thesis compares two methods regarding how the adding of the users is done, so that the user is ready to work. Possible problems and solutions are also presented. The results of the thesis give a clear indication that there are also more efficient ways of adding users to the Active Directory network. The thesis shows how the enhancing has been made better and how it could be made even more efficient. With these two methods, a clear difference can be noticed when adding users to Active Directory.</p> <p>The second goal of the thesis is to give a clear indication of how the adding of the users has been done in two different ways, and how much they differ from each other.</p>	
Keywords	Active Directory, enhancing management

## Sisällys

### Lyhenteet

1	Johdanto	1
2	Active Directoryssä käytettävä palvelin käyttöjärjestelmä	3
3	Active Directory -toimialue	5
3.1	Active Directory ja DNS	5
3.2	Active Directoryn komponentit	6
4	Käyttäjäprofiilin luomisprosessi	7
5	Käyttäjätilin lisääminen Active Directoryn työkaluilla	11
5.1	Active Directory -prosessi	11
5.2	Ulkoisen sähköpostiosoitteen luominen	12
5.3	Käyttäjätilin tarpeelliset lisäykset, User Properties / options	13
5.4	Manuaaliseen käyttäjän lisäämiseen kuluva aika	14
5.5	Mahdollisia virhetilanteita	14
5.6	Ryhmäkäytännön merkitys	16
5.7	Ryhmäkäytäntöobjektin merkitys	16
6	Käyttäjätilin lisääminen AD management toolin avulla	18
6.1	Käyttäjätilin lisääminen	18
6.2	AD management toolin edut	24
6.3	Virhetilanteiden korjaaminen	25
6.4	Automatisointi AD management -toolilla	26
6.5	AD Management toolin jatkokehitysmahdollisuudet	28
7	Yhteenveto	29
	Lähteet	31

## Liitteet

Liite 1. Toimipaikan valinta

Liite 2. Käyttäjännimen muodostuminen

Liite 3. Active Directoryn työkaluilla tehty prosessi

Liite 4. Ulkoisen sähköpostiosoitteen luominen

## Lyhenteet

AD	Active Directory, aktiivihakemisto.
DC	Domain Controller, toimialueen ohjaukone.
DL	Distribution list, jakelulista.
DNS	Domain Name Service, nimipalvelu.
Domain	toimialue.
GPO	Group Policy Object, ryhmäkäytäntöobjekti.
HTTP	Hypertext Transfer Protocol, protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
OC	Office Communicator, viestintäväline yrityksessä.
OU	Organizational Unit, organisaatioyksikkö.
SCCM	System Center Configuration Manager, Windows-pohjaisten tietokoneiden hallinnointi työkalu.
sg	Security groups, suojausryhmät.
Site	toimipaikka.

## 1 Johdanto

GoExcellent on pohjoismainen Contact Center-alan yritys, jonka palvelut muodostavat puhelinasiakas-, telemarkkinointi-, telemyynti-, back office -palvelut sekä teknisen tuen. GoExcellentillä on konttoreita Suomessa, Ruotsissa, Norjassa sekä Tanskassa. Konttoreita Suomessa on muun muassa Helsingissä, Lahdessa, Jyväskylässä, Pietarsaareissa sekä Taivalkoskella.

GoExcellentin toimeksiantajina ovat muun muassa DNA, Sonera, PlusTV, Viasat, Fortum, Canal Digital ja Bonnier. GoExcellent on Suomessa selkeä markkinajohtaja. GoExcellent toimii Suomessa kahtena sisaryrityksenä, GoExcellent Finland North Oy:nä ja GoExcellent Finland South Oy:nä, joita johdetaan yhtenäisesti, ja niiden hallinto ja tukitoiminnot on keskitetty GoExcellent Southiin. GoExcellent pyrkii kasvamaan vielä enemmän myös vuoden 2013 aikana.

Active Directory -projekti alkoi helmikuussa 2012. Projektissa käydään läpi kaksi eri tapaa lisätä käyttäjä yritysverkkoon, jotta käyttäjä olisi valmis työskentelemään yrityksessä. Pääasiallinen tavoite oli verrata kahta tapaa, joilla tämä voidaan tehdä. Ensimmäiseksi esitellään tapa, jossa käyttäjät lisätään Active Directoryn omilla työkaluilla. Tämän jälkeen esitellään vaihtoehtoinen tapa, jolla pyritään tehostamaan käyttäjien lisäämistä: Active Directory management tool.

Projektin sivutavoitteena oli luoda dokumentaatio käyttäjätilien lisäämisestä GoExcellentin AD-verkon toimialueeseen sekä käyttäjätileille määritettävien oikeuksien sekä ryhmien luomisesta. Kun yritykseen tulee uusia työntekijöitä, heille täytyy luoda kaikki profiilit tietokoneille, sähköpostiin, määrittää, mitä ohjelmia heille tulee käyttöön ja mitä käyttöoikeuksia heillä täytyy olla, sekä luoda tunnukset. Nämä toimenpiteet suoritetaan molemmilla tavoilla.

Tein yhteistyötä GoExcellentin Helsingissä sijaitsevassa toimipisteessä AD-verkkovastaavan kanssa, jonka kanssa myös suunnittelimme työtä yhdessä. Olin tällöin myös itse töissä samassa toimipisteessä, mikä helpotti paljon yhteydenpitoa. Roolini oli siis osallistua projektitiimin jäsenenä työn toteutukseen sekä dokumentointiin. AD-verkkovastaavan rooli työssä oli osallistua toteutukseen sekä tiedon antamiseen

tarvittavaa dokumentointia varten. Lähtötilanteena kartoitimme koko prosessin eri osat alueet, joiden pohjalta lähdimme suunnittelemaan toteutusta.

Työssä käytetty sekä yrityksessä käytössä oleva Active Directory ohjelma oli Microsoft Windows Server 2003 R2. Koko AD-verkon läpi käyminen olisi ollut liian laaja aihe insinööriyölle, joten työssä keskitytään vain käyttäjien lisäämiseen ja heille tehtäviin toimenpiteisiin. Työssä on pyritty käymään molemmat tavat läpi huolellisesti, jotta lukijalle jäisi selkeä mielikuva molempien tapojen hyvistä ja huonoista puolista.

Suunnitelma oli luoda uusi käyttäjä yhteen GoExcellentin toimeksiantoon, jossa tämä käyttäjä tulisi työskentelemään. Prosessi on kuitenkin sama toimeksiannosta riippumatta.



## 2 Active Directoryssä käytettävä palvelin käyttöjärjestelmä

### Windows Server 2003

Windows Server 2003 -käyttöjärjestelmäperheeseen kuuluvat Windows Server 2003, Web Edition; Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition ja Windows Server 2003, Datacenter Edition. Jokaisella näistä on oma käyttötarkoituksensa. Windows Server 2003:ssa järjestelmän luotettavuutta, saavutettavuutta ja hallittavuutta on parannettu huomattavasti. Käyttöjärjestelmä ei ole vain paljon edeltäjiään monipuolisempi, vaan se pohjautuu Windows 2003:ssa käyttöön otettuihin järjestelmänhallinta- ja ylläpitokonsepteihin. [1, s.3–4.]

### Windows Server 2003 Web Edition

Web Edition tarjoaa Web -palveluita ja alustan Web -sivustoille ja Web -pohjaiselle sovelluksille. Siihen sisältyy Microsoft .NET Framework, IIS (Internet Information Services), ASP.NET ja verkon kuormituksen jakaminen, siitä kuitenkin puuttuu monia muita ominaisuuksia, kuten Active Directory. Sen muita tärkeitä ominaisuuksia ovat DFS (Distributed File System), EFS (Encrypting File System) ja etätyöpöytä hallintatarkoituksiin. Se tukee 2 Gt:n RAM-muistia ja kahta prosessoria. [1, s.4.]

### Windows Server 2003 Standard Edition

Windows Server 2003 SE on verkkokäyttöjärjestelmä, jossa yrityskohtaisia ratkaisuja voidaan toteuttaa nopeasti ja helposti. Palvelin on sopiva valinta kaikenkokoisten yritysten päivittäiseen käyttöön. Se sisältää tiedostojen ja tulostinten jakamistoiminnot, suojatut Internet-yhteydet, keskitetyn sovellusten käyttöönoton sekä monipuoliset työntekijöille, yhteistyökumppaneille ja asiakkaille tarkoitetut yhteiskäyttötoiminnot sekä web-pohjaiset työskentelytilat Windows SharePoint -teknologian avulla. Se myös tarjoaa palveluita ja resursseja verkon muille järjestelmille. Siinä on runsaasti ominaisuuksia ja konfigurointivaihtoehtoja. Se tukee 4 gigatavun RAM-muistia ja kahta prosessoria. [1, s.4; 4.] Tämä on työssä käytössä oleva palvelin.

### Windows Server 2003 Enterprise Edition

Windows Server 2003 EE on tarkoitettu keskikokoisten ja suurien yritysten palvelimeksi. Siihen sisältyy yrityksen infrastruktuurin, toimialasovellusten ja sähköisen kaupankäynnin toiminnot. Enterprise Edition sisältää Standard Edition -ominaisuuksien lisäksi Cluster Service -tuen, metahakemistopalvelut ja Services for Macintosh -palvelut. Tukee 64-bittiseen Intel Itanium -prosessoriin pohjautuvia tietokoneita, lennossa vaihdettavaa RAM -muistia ja NUMA -muistiosoitusta (NonUniform Memory Access). Tämän lisäksi Enterprise -palvelimet tukevat kahdeksaa prosessoria sekä 32 Gt:n RAM-muistia x86-tietokoneissa ja 64 Gt:n RAM-muistia Itanium-tietokoneissa. [1, s.4; 4.]

### Windows Server 2003 Datacenter Edition

Windows Server 2003 DE on tarkoitettu yrityksille, jotka asettavat skaalattavuudelle ja käytettävyydelle suuret vaatimukset. Se on perusta erikoistuneille tietokantaratkaisuille, ERP-ohjelmistoille, tehokkaalle reaaliaikaiselle tapahtumienkäsittelylle ja palvelinten yhdistämiselle. Datacenter Edition on tähän asti tehokkain ja monipuolisin Microsoftin toimittama palvelinkäyttöjärjestelmä. [4.]

### 3 Active Directory -toimialue

#### 3.1 Active Directory ja DNS

Active Directoryn avulla voidaan tehokkaasti hallita verkon useita resursseja, kuten käyttäjiä, tietokoneita ja verkon muita resursseja. Yksinkertaistettuna se on tietokanta, joka sisältää tiedot verkon objekteista ja niiden ominaisuuksista.

Active Directory on Windows 2003 -järjestelmän sydän. Sen käyttämä teknologia perustuu standartoituihin internetprotokolliin, mikä mahdollistaa verkon rakenteen selkeän määrittelyn. Active Directory käyttää DNS-järjestelmää. DNS eli Domain Name System on Internetin nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi. DNS:n avulla voidaan organisoida tietokonejoukot toimialueiksi. DNS mahdollistaa IP-osoitteiden selkeän ymmärtämisen, koska sen avulla voidaan muuttaa hankalat numeeriset yhdistelmät selkeämmin ymmärrettäviksi nimiksi. Jos verkossa on esimerkiksi useita tietokoneita, haku on käyttäjäystävällisempää nimen perusteella. Tästä voidaan tehdä johtopäätös, että Active Directory on riippuvainen DNS:stä, joten toimiva DNS on AD:n asentamisen edellytys. Vaikka sekä Active Directory että DNS pitää määrittää Windows Server 2003 -verkossa, Active Directory -toimialueilla ja DNS-toimialueilla on eri tarkoitus. Active Directory -toimialueet auttavat tilien, resurssien ja suojausten hallinnassa. DNS-toimialueet muodostavat toimialuehierarkian, jota käytetään pääasiassa nimien selvittämiseen. [1, s.133–134; 1, s.140.]

Toimialueet muodostavat hierarkkisia rakenteita, jotka voidaan määrittää Internetin laajuisesti julkisia verkkoja varten tai yrityksen laajuisesti yksityisiä verkkoja varten (intranet ja ekstranet). Active Directory ja DNS ovat hyvin tiukasti integroituja. DNS-palvelu pitää asentaa ennen Active Directorya. Kun Active Directory -verkkoon asennetaan ensimmäistä toimialueen ohjauskonetta, DNS voidaan haluttaessa asentaa automaattisesti, jos verkosta ei löydy DNS-palvelinta. Asennuksen yhteydessä voidaan määrittää, integroidaanko DNS ja Active Directory täydellisesti. Täydellisesti integroidussa järjestelmässä DNS-tiedot tallennetaan suoraan Active Directoryyn. Tällä tavalla voidaan hyödyntää kaikkia Active Directoryn ominaisuuksia. [1, s.487–488.]

### 3.2 Active Directoryn komponentit

Active Directory -palvelulle voidaan luoda sekä loogiset että fyysiset rakenteet verkon osia varten. Loogiset rakenteet auttavat organisoimaan hakemisto-objekteja ja hallitsemaan verkon tilejä ja jaettuja resursseja. Loogisia rakenteita ovat organisaatioyksiköt, toimialueet, toimialuepuut ja toimialuemetsät.

Organisaatioyksiköt (Organizational units, OU) ovat toimialueiden alaryhmä, jonka rakenne usein vastaa yrityksen liiketoiminnallista tai toiminnallista rakennetta. Organisaatioyksiköt ovat toimialueella sijaitsevia säilöjä tietokoneilien, käyttäjätilien ja -ryhmien tallennukseen. Siihen voidaan kohdistaa ryhmäkäytäntö (Group Policy), jonka avulla voidaan hallita käyttäjien työasemien käyttöliittymiä, asentaa automaattisesti ohjelmistoja. Hallintaoikeuksia voidaan myös delegoida toisille käyttäjille.

Toimialueet (Domains) ovat ryhmä tietokoneita, jotka jakavat yleisen hakemistotietokannan. Useita toimialueita voi olla samassa metsässä (forests), ja niitä voi hallita samoilla käyttäjätunnuksilla.

Toimialuepuut (Domain trees) ovat yksi tai useita toimialueita, jotka jakavat yhtenäisen nimiavaruuden. Esimerkkinä voidaan käyttää vaikka `dev.microsoft.com` ja `sales.microsoft.com`, joilla on eri toimialueet, mutta sijaitsevat samassa nimiavaruudessa.

Toimialuemetsät (Domain forests) ovat yksi tai useita toimialuepuita, jotka jakavat yleisiä hakemistotietoja.

Palvelinjoukot ja aliverkot ovat taas verkon fyysisiä rakenteita, jotka auttavat kartoittamaan verkon fyysistä rakennetta. Fyysisten rakenteiden avulla ohjataan verkkoliikennettä ja määritetään verkon resurssien fyysiset rajat.

Aliverkot (Subnets) ovat verkkoryhmä, jolla on käytössään tietty IP-osoitealue ja aliverkon peite.

Palvelinjoukot (Sites) ovat yksi tai useita aliverkkoja, joiden avulla määritetään, kuinka hakemistoa käytetään ja monistetaan. [1, s.134–135; 3, s.11.]

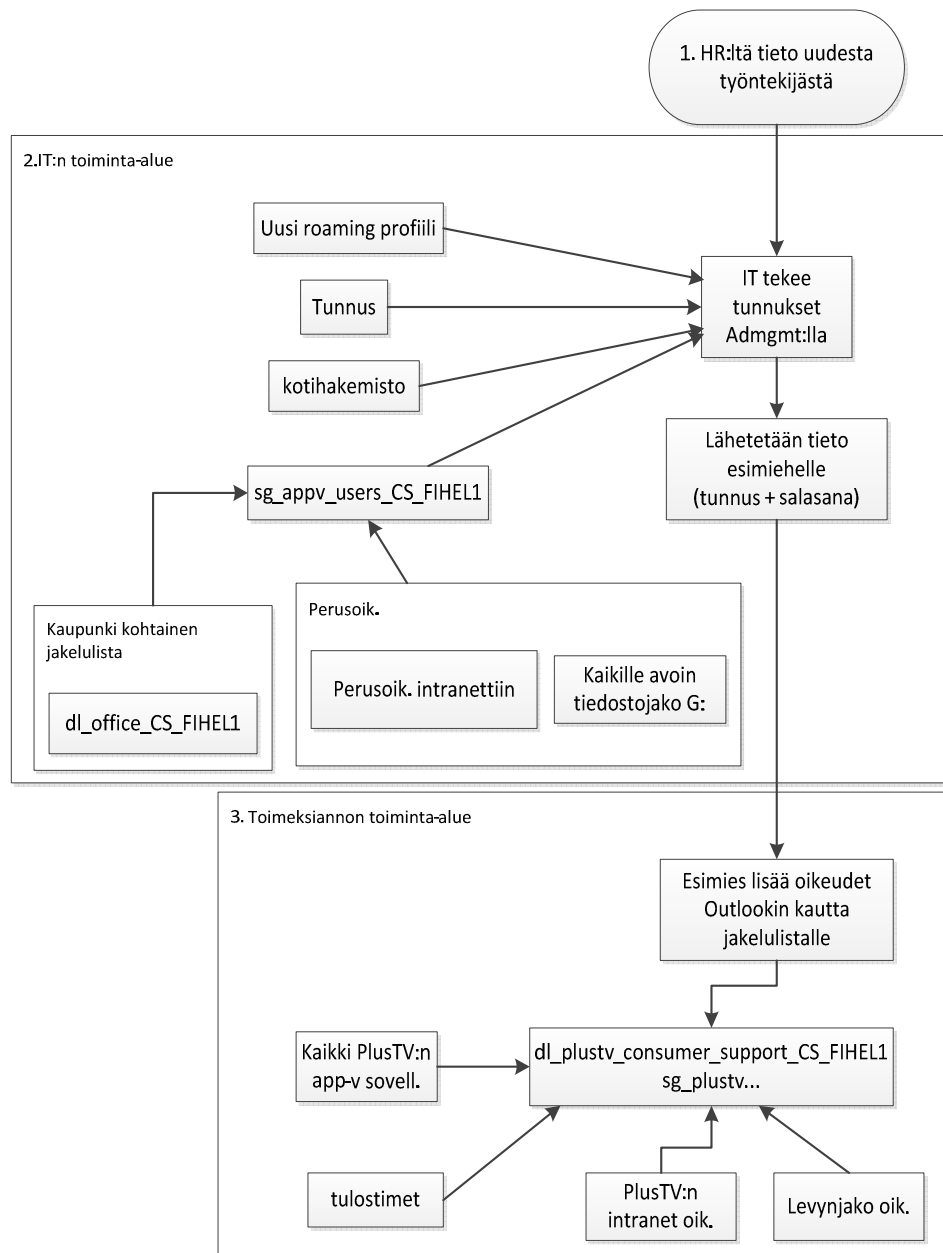
## 4 Käyttäjäprofiilin luomisprosessi

### Käyttäjän lisääminen

Tässä luvussa tutustutaan käyttäjän lisäämisprosessin kulkuun pintapuolisesti. Myöhemmin tutustutaan tarkemmin, kuinka AD management tool luo profiilin Active Directoryyn. Prosessi alkaa, kun HR:n (Human Resources) rekrytoinnin puolelta tulee tieto, että taloon on tulossa uusia työntekijöitä. HR:ltä menee tieto IT-osastolle, jolloin IT alkaa luoda uutta käyttäjäprofiilia. Käyttäjän nimi on riittävä tieto, jonka IT tarvitsee profiilin luomiseksi.

Uuden roaming profiilin kautta lisätään perusohjelmilla varustettu Windows XP ympäristö, johon sisältyy tietty määrä ohjelmia, jonka kaikki käyttäjät saavat alussa käyttöön, kun tarkempaa luokittelua ei ole vielä tehty. Roaming-profiili on käytössä kaikissa tietokoneissa, joista käyttäjä toimialueelle kirjautuu. Käyttäjälle luodaan myös useampia tunnuksia, joihin sisältyy käyttäjätunnus, salasana tietokoneelle kirjautumista varten sekä sähköpostitunnukset. Käyttäjälle luodaan myös automaattisesti kotihakemisto, johon voi tallentaa tiedostoja omalle käyttäjäprofiilille.

Käyttäjä lisätään myös tarvittavaan suojausryhmään (security group), joka määräytyy toimipaikan perusteella. Tässä tapauksessa suojausryhmä on nimeltään sg\_appv\_users\_CS\_FIHEL1, jonka avulla käyttäjälle aktivoituvat FIHEL1-toimialueelle kuuluvat perusohjelmat. Tämä suojausryhmä on vielä sidoksissa yleiseen kaupunkikohtaiseen jakelulistaan, jonka kautta käyttäjälle määräytyy muita perusoikeuksia, kuten intranetoikeudet ja kaikille avoinna oleva verkkoasema (G:). Käyttäjän luomisen jälkeen lähetetään tieto esimiehelle, jonka alaisuuteen uusi työntekijä laitetaan. Tarvittavat tunnukset ja salasanat ilmoitetaan myös esimiehelle. Tähän loppuu IT:n tehtävät uuden käyttäjän lisäämiseen liittyen. Kuviossa 1 on esitetty käyttäjän luominen AD management toolin avulla. Prosessia kuvataan tarkemmin luvussa 6.



Kuvio 1. Käyttäjän luominen AD management toolin avulla.

Kun käyttäjälle on luotu tunnukset, ne lähetetään tulevalle esimiehelle, jonka vastuulle jää käyttäjän lisääminen oikeisiin suojausryhmiin. Esimies lisää oikeudet Outlookin kautta oikeille jakelulistoille. Esimiehen vastuulle jäävät loput käyttäjää koskevat

toimenpiteet. Outlookin avulla käyttäjä lisätään tarvittaville jakelulistoille, jotka esimies määrittää. Jakelulistan perusteella käyttäjälle tulee tarvittavat ohjelmat, jotka kuuluvat toimeksiantoon, johon käyttäjä sijoitetaan.

Jakelulistan sisällä olevien suojausryhmien perusteella käyttäjälle tulee lisää ominaisuuksia omalle Windows-käyttäjäprofiilille: kaikki tarvittavat Windows-sovellukset, jotka kuuluvat kyseiseen toimeksiantoon ja niihin tarvittavat oikeudet, sekä tulostimet, jotka ovat käytössä samassa kerroksessa, jossa toimeksiantoa suoritetaan. Tämän avulla käyttäjälle tulee näkyviin kaikki tarvittavat tulostimet ja oikeudet niiden käyttöön työtehtävässään. Aivan alussa käyttäjälle määritettiin normaalit intranetoikeudet. Tässä vaiheessa tulee vielä lisäksi toimeksiannon omat intranetoikeudet. Intranet on informaatiokanava, joka toimii yrityksen sisäverkossa, johon voidaan päästä www-sivun kautta verkkoselaimella. Loput tarvittavat verkkoasemat, ja niille oikeanmukaiset oikeudet tulevat näkyviin.

#### Työnjako IT:n ja toimeksiannon välillä

Luvun alussa esitetty kuvio 1 kuvastaa työnjaon toimintaa. IT-osaston työkuormaa on pyritty pienentämään turhista sekä helpoista toimenpiteistä, jotka kuormittaisivat turhaan työtä. IT-osasto hoitaa talon sisäiset tietotekniikkaongelmat, joten sillä ei ole aikaa puuttua toimeksiantojen käyttäjien oikeuksien määrittämiseen, koska ei ole mitään syytä tietää tästä informaatiosta yhtään mitään. IT:n työhön kuuluu paljon muutakin kuin vain käyttäjien lisääminen. Oikeuksien lisääminen Outlookin avulla on nopeasti suoritettava toimenpide, mutta se kuormittaisi IT:n työtä turhaan, koska IT hoitaa työt, joihin vain sen osaaminen riittää. Tällä tavalla pyritään myös säästämään kustannuksissa. Pääasiassa IT on vastuussa tietoturvasta.

#### GoExcellentin verkkorakenne ja sen toiminta

Toimialueeseen kuuluu neljä DC-palvelinta (Domain Controllers). Muutokset tehdään aina Östersundin DC-palvelinta vasten, jonka jälkeen muut DC-palvelimet toisintavat normaalisti tehdyt muutokset keskenään, aivan samaan tapaan, kuin tehdään muutoksia suoraan AD:ssa jotain tiettyä DC:tä kohden. Toisintavälit vaihtelevat muutoksista riippuen, esimerkiksi salasana muutokset toisintuvat heti, mutta käyttäjien

lisääminen toisintuvat noin 15 minuutin kuluttua lisäyksestä. Tietojen toisinnalla on eri prioriteetti luokat.

Tietoturvan merkitys kasvaa sitä suuremmaksi, mitä suurempi yritys on kyseessä. Sen merkitystä korostaa myös se, että kyseessä on kansainvälinen yritys, jolla on toimipisteitä monissa Pohjoismaissa. Tietoturvan tärkeyttä korostaa erittäin laaja Active Directory -verkko, jonka muokkaamisella pystyy vaikuttamaan useamman maan toimipisteiden toimintaan, joten tietoturvaratkaisujen on oltava todella hyvät. Palomuri valvoo verkon sisäänpääsyoikeuksia ja pitää yllä sisäänpääsy-yrityksistä tapahtumakirjaa. Valvonta perustuu liikenteen tunnistamiseen. Tunnistaminen perustuu lähettävän ja vastaanotettavan isäntäkoneen osoitteeseen sekä pyydettyyn palveluun liittyvään informaatioon. Palomuri siten päättää (yrityksen tietoturvapoliitikan pohjalta luotujen access-sääntöjen perusteella), päästetäänkö kyseessä oleva liikenne läpi vai ei. Päätöksistä pidetään myös tapahtumakirjaa. [8, s. 242.]

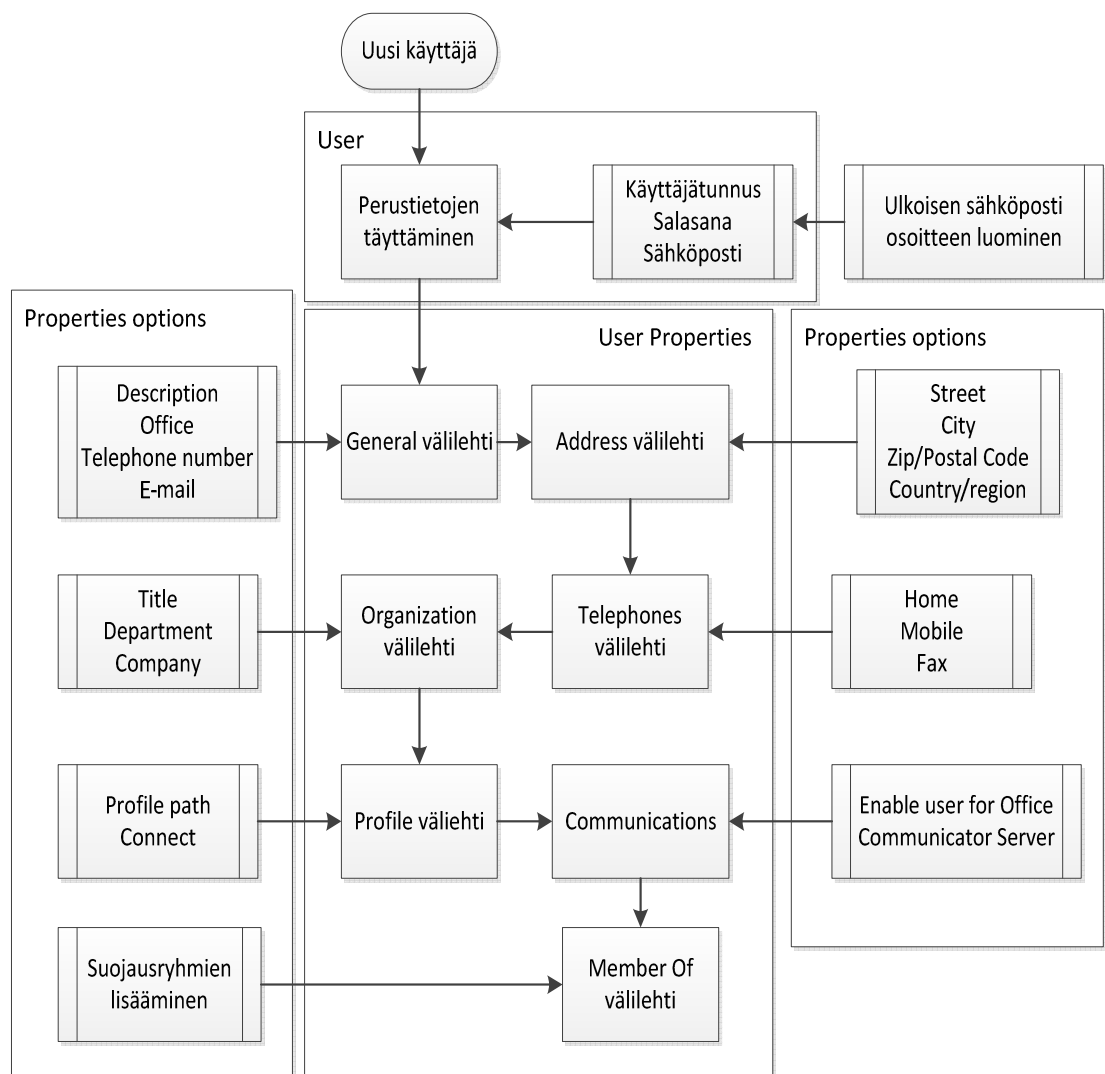
Sovellustason yhdyskäytävä eli proxy toteutetaan ohjelmistollisesti tietokoneessa, joka voi olla tarpeista riippuen yksittäinen PC tai suurempi tietokonejärjestelmä. Sovellustason yhdyskäytävä on palomuurijärjestelmä, jossa verkkoyhteyksien lisäksi valvotaan myös sovellustason protokollia. Paketteja ei päästetä suoraan kulkemaan sellaisenaan verkosta toiseen. Yhteydet muodostetaan sen sijaan erityiseen sovellukseen, proxyyn, joka päättää, otetaanko yhteys lopulliseen pyydettyyn isäntäkoneeseen vai ei. Sovellus-proxylla voidaan estää sovellustason protokollisiin kohdistuvia hyökkäyksiä. Sovellustason palomuurit muuttavat usein vielä liikenteen osoitteita, jolloin liikenne näyttää tulevan palomuurista eikä verkon sisäisestä tietokoneesta. Sovellustason palomuurien rajoituksena on, että kullekin verkkopalvelulle pitää olla omat proxy-sovellukset. Jos palomuurin pitää suojata jotain muuta uutta palvelua, palomuuriin pitää lisätä kyseistä palvelua vastaava uusi proxy-sovellus. [8, s. 256.]



## 5 Käyttäjätilin lisääminen Active Directoryn työkaluilla

### 5.1 Active Directory -prosessi

Tässä luvussa tutustutaan käyttäjän lisäämiseen käyttäen vain Active Directoryn omia työkaluja. Prosessissa on useita vaiheita, joita olen pyrkinyt kuvaamaan pintapuolisesti kuviolla 2. Käyn läpi tarkemmin kuhunkin kohtaa kuuluvat toimenpiteet. Työn lopussa on yksityiskohtaisempi kuvaus lisäämisen vaiheista liitteenä.



Kuvio 2. Käyttäjän luominen Active Directoryn työkaluilla.

## Käyttäjän lisääminen

Käyttäjätili täytyy luoda jokaiselle käyttäjälle, joka haluaa käyttää verkon resursseja. Täysin uuden käyttäjätilin luominen aloitetaan painamalla hiiren oikealla painikkeella kohdetta, johon halutaan lisätä uusi käyttäjätili, valitsemalla sitten New (Uusi) ja valitsemalla User (käyttäjä). Kun luodaan uusi tili, siinä käytetään oletusjärjestelmäasetuksia. Asetukset, jotka käyttäjälle määräytyvät, riippuvat organisaatioyksikölle määräytyistä asetuksista, joita on mm. Member Of, eli mihin ryhmään käyttäjä kuuluu. Ryhmällä voidaan määritellä oikeuksia sekä ominaisuuksia, joita käyttäjällä alussa on, kun kirjautuu yritysverkossa omilla tunnuksilla tietokoneelle. Organisaatioyksikön asetuksia voi muokata, mikäli on järjestelmänvalvoja. [2, s. 457.]

### Prosessin kuvauksen selvitys, User

Aluksi on päätettävä, mihin organisaatioyksikköön käyttäjä lisätään, oikeaksi yksiköksi tulee `internalprod.com/ROOT/CS/FIHEL1/Users`. Käyttäjän lisääminen aloitetaan käyttäjän perustietojen täyttämällä, jonka yhteydessä käyttäjälle määritetään etu- ja sukunimi, käyttäjätunnus Windows-käyttöjärjestelmälle kirjautumista varten, salasana sekä sähköpostiosoite. Käyttäjätunnuksen luomisessa on oltava tarkkana, jotta käyttää oikeata nimeämiskäytäntöä, joka on `<etunimi>.<kolme ensimmäistä kirjainta sukunimestä>`. On myös valittava asetus, että käyttäjä joutuu muuttamaan salasanansa ensimmäisen Windows XP -kirjautumisen yhteydessä.

Kun käyttäjän lisäys on suoritettu, täytyy olennaisia tietoja ottaa muistiin, ja lähettää ne eteenpäin, jotta luotu käyttäjä saa omat tunnukset. Tähän toimenpiteeseen menee oma aikansa, kun tiedot täytyy kirjoittaa muistiin käyttäjää luodessa.

## 5.2 Ulkoisen sähköpostiosoitteen luominen

Lisäämisprosessin jälkeen on vielä käytävä luomassa ulkoinen sähköpostiosoite, joka on muotoaan `etunimi.sukunimi@goexcellant.com`. Tätä sähköpostiosoitetta ei pystytä luomaan suoraan käyttäen Active Directoryn -työkaluja, vaan on yhdistettävä toiseen palvelimeen, jonka kautta luodaan sähköpostiosoite. Yhdistetään toiselle palvelimelle, jossa on Exchange Management Console (EMC), jonka avulla osoitteen luominen tapahtuu. Osoitteen luomisen yhteydessä on oltava tarkkana, jotta valitaan New

Mailbox -> User Mailbox -> Existing users, minkä jälkeen listalta etsitään uusi käyttäjä, jolle osoite halutaan luoda. Käyttäjä on nyt lisätty osaksi organisaatioyksikköä.

### 5.3 Käyttäjätilin tarpeelliset lisäykset, User Properties / options

Tässä luvussa pyritään selvittämään, mitä kaikkia lisäyksiä Active Directory -työkaluun täytyy tehdä, jotta lisätty käyttäjä olisi valmis työskentelemään yritysympäristössä. Luvussa 6 esitetään vaihtoehtoinen tapa käyttäjän lisäämiseen, jotta voidaan huomata, kuinka paljon nopeammin ja tehokkaammin lisäys voidaan suorittaa.

Kun käyttäjätili on luotu, täytyy tehdä tarpeelliset lisäykset käyttäjän asetuksiin (properties). Active Directory -työkalun kautta täytyy lisätä useita eri tietoja asetuksiin. Asetusten lisääminen aloitetaan General-välilehdeltä, johon täytyy täyttää neljä kohtaa, jotka ovat Description (Employee), Office (Helsinki), Telephone number (+358941585000) sekä e-mail. Tiedot, joita näihin kenttiin täytetään, vaihtuvat toimipaikoittain. Ainoa poikkeuksellinen kenttä on e-mail, koska siihen tulee EMC:llä luotu ulkoinen sähköpostiosoite, jolla voidaan ottaa vastaan sekä lähettää sähköpostia.

Ensimmäinen välilehti on täytetty, joten voidaan siirtyä tarkastelemaan seuraavaa, joka on Address-välilehti. Tällä välilehdellä sijaitsee tiedot toimipaikan tarkemmasta sijainnista, jossa käyttäjä tulee työskentelemään. Työssä käytettiin esimerkkinä Helsingin toimipaikkaa, jolloin osoitteeksi tulee Munkkiniemen puistotie 25, postinumeroksi 00330 sekä maaksi Finland.

Seuraavaksi siirrytään täyttämään puhelinnumerot eli Telephones välilehti, joihin kirjoitetaan toimipaikan vaihteen numero, joka esimerkkitapauksessa on +358941585000. Matkapuhelinnumero on vaihtoehtoinen valinta, sen täyttäminen riippuu käyttäjän työtehtävästä. Mikäli henkilö täytyy saada vapaa-ajalla kiinni, tämä kenttä on täytettävä. Viimeiseen kenttää laitetaan yleinen faksin numero.

Seuraavalla välilehdellä vaaditaan organisaatioon liittyviä tietoja, jotka voivat vaihdella työnkuvan perusteella. Title-kenttään on lisättävä käyttäjän toimikuva työpaikassa. Department-kenttä on vaihtoehtoisesti täytettävä, mikäli käyttäjän toimeksianto on tiedossa. Company-kohtaan tulee kirjata yritys johon, käyttäjä tulee töihin, tässä tapauksessa yritys on GoExcellent.

Seuraavan välilehden täyttäminen on kaikista työläin, koska se edellyttää yhdistämistä kahdelle eri palvelimelle, joihin luodaan tarvittavat hakemistot käyttäjälle. Ensimmäinen palvelin, johon on yhdistettävä on SCCM (System Center Configuration Manager), jonka kautta asetetaan oikeudet, jotka käyttäjälle sallitaan Windows XP:n käytössä. Kotihakemiston luomiseksi on yhdistettävä tiedostopalvelimelle, johon käydään lisäämässä kotihakemisto kansio käsin. Käytettäväksi asemaksi on myös valittava H-asema.

Viimeiseksi täytyy aktivoida Office Communicator, jonka aktivoimiseksi täytyy yhdistää vielä toiselle palvelimelle. Aktivointi on kuitenkin melko nopeata, täytyy vain laittaa ruksi kohtaan Enable user for Office Communications Server. Tätä asetusta ei ole ollenkaan Windows Server 2003:ssa, vaan se on lisättävä 2008:n kautta. Lopuksi täytyy vielä määrittää käyttäjälle oikeudet suojausryhmiin, joiden kautta käyttäjä saa käyttöönsä perusohjelmat ja oikeuksia. Nämä kaksi ryhmää ovat toimeksiannoista poikkeavia: sg\_appv\_users\_CS\_FIHEL1 sekä sg\_costarea\_XXXXX\_user\_CS\_FIHEL1

#### 5.4 Manuaaliseen käyttäjän lisäämiseen kuluva aika

Käyttäjän lisääminen manuaalisesti on melko suuri työ, ja siihen menee paljon aikaa, jos käytetään vain Active Directoryä. Koko toimenpide kestää noin 30–40 minuuttia riippuen siitä, kuinka huolella kaiken tekee. Suurissa organisaatioissa saattaa rekrytoinnin yhteydessä tulla useampia henkilöitä samaan aikaan töihin, joten usean käyttäjän lisääminen kestäisi hyvin kauan.

#### 5.5 Mahdollisia virhetilanteita

Käyttäjien lisääminen käsin on hyvin altis virheille, koska prosessi kestää melko kauan. Mikäli lisättäviä käyttäjiä on monta, on tietoa myös paljon. Pitää olla tarkkana, että tiedot eivät mene sekaisin, mikä taas lisää prosessin kestoja. Pahimpia virheitä olisi käyttäjän lisääminen väärään OU:hun, joka voisi esimerkiksi olla kilpaileva toimeksianto, mikä johtaisi siihen, että käyttäjälle ei kohdistu oikeat GPO:t (Group Policy Object). Mikäli näin käy ja sen huomaa heti, on se helppo korjata ja siirtää käyttäjä oikeaan OU:hun. Jos virhe jää huomaamatta, saattaa sillä on ikäviä

vaikutuksia käyttäjälle tai yritykselle, koska käyttäjälle tulee vääränlaisia oikeuksia, jotka eivät kuulu hänen työhönsä.

Kirjoitusvirheet ovat toinen virhemahdollisuus. Jos lisää käyttäjiä nopeasti, saattavat ne jäädä huomaamatta. Salasanoja määriteltäessä täytyy olla tarkka, että ne kirjoitetaan oikein, jotta ei tule vaikeuksia jatkossa. Kirjoitusvirheet näkyvät esimerkiksi automaattisesti luodussa allekirjoituksessa, joka lisätään sähköpostiin. Kirjoitusvirheitä voidaan käydä muokkaamassa jälkeenpäin, mikä kuitenkin aiheuttaa ei toivottua lisätyötä.

Tyypillisesti edellä mainittujen virheiden korjaamiseen ei kulu kovin paljon aikaa, jos ne huomataan käyttäjää lisättäessä. Toinen asia on, jos jälkeenpäin ihmetellään, miksi käyttäjä ei toimi, jolloin täytyy lähteä etsimään ongelmaa. Suoraan Active Directoryn kanssa työskentely vaatii paljon tarkkaavaisuutta.

Käyttäjätunnusten luomisen jälkeen käyttäjänimet, salasanat sekä sähköpostiosoite jaetaan käyttäjille, jotka aloittavat työskentelyn. Yleisimpiä virheitä, joita käyttäjälle voi alussa tulla ovat, muun muassa tietyt ohjelmat eivät avaudu profiilin mukana, tulostin asetukset ovat väärin, kaikkia tunnuksia ei ollut luotu tai ohjelmien yleiset asetukset ovat väärin. Suurin osa näistä virheistä johtuu siitä, että käyttäjää ei ole lisätty tietylle suojausryhmälle, josta määräytyvät muun muassa käytetyt ohjelmat sekä tulostimet. Tästä annetaan tieto omalle esimiehelle, joka lisää käyttäjän Outlookin avulla suojausryhmään, jonka jälkeen tietokone käynnistetään uudelleen ja uudet asetukset ovat tallentuneet profiilille.

Mikäli ongelma on sellainen, että esimies ei pysty sitä ratkaisemaan, on pyydettävä IT-osastoa katsomaan ongelmaa. Tunnuksiin liittyvät ongelmat menevät myös suoraan esimiehelle, joka pystyy luomaan tarvittavat tunnuksat. Ohjelmien asetuksiin liittyvien ongelmien kanssa käännetään SU:n (SuperUser, henkilö, jolla on paljon kokemusta työstä) puoleen, jolla on enemmän kokemusta ohjelmien asetuksista ja niiden käytöstä. Mikäli käyttäjälle tulee jokin ongelma, joka estää työskentelyn niin ilmoitetaan tästä FM:lle (Floor Manager, työnohjaaja), joka ohjeistaa jatkotoimenpiteisiin.

## 5.6 Ryhmäkäytännön merkitys

Ryhmäkäytännöt yksinkertaistavat hallintatehtäviä, sillä niiden avulla järjestelmänvalvojat voivat hallita sekä käyttäjien että tietokoneiden oikeuksia ja lupia keskitetysti. Ryhmäkäytännön avulla voidaan luoda hallittuja hakemistoja erikoiskansioille, kuten My Documents -kansiolle, sekä hallita Windowsin komponenttien, järjestelmäresurssien, verkkoresurssien, Control Panel -apuohjelmien, työpöydän sekä Start-valikon käyttöä. Sen avulla voidaan myös määrittää käyttäjän ja tietokoneen skriptejä, jotka käynnistetään tiettyinä aikoina, sekä määrittää käytännöt tilien lukitsemiselle ja salasanoille, valvonnalle, käyttäjien oikeuksien asettamiselle ja suojuuksille. [1, s. 85–86.]

Ryhmäkäytäntö on joukko sääntöjä, jotka auttavat järjestelmänvalvojaa hallitsemaan käyttäjiä ja tietokoneita. Ryhmäkäytäntöjä voi määrittää useisiin toimialueisiin, yksittäiseen toimialueeseen, toimialueen alaryhmään tai yksittäisiin järjestelmiin. Yksittäisten järjestelmien käytäntöjä kutsutaan paikallisiksi ryhmäkäytännöiksi, ja ne tallennetaan vain paikalliseen järjestelmään. Muut ryhmäkäytännöt linkitetään Active Directoryn -hakemistopalvelun kautta. [1, s. 86.]

Jokaisella palvelinjoukolla, toimialueella ja organisatorisella yksiköllä voi olla useita ryhmäkäytäntöjä. Group Policy -luettelossa ylempänä olevilla ryhmäkäytännöillä on suurempi prioriteetti. Tällä tasolla määritetyt ryhmäkäytännöt liittyvät Active Directoryyn, millä varmistetaan, että käytäntöjä sovelletaan asianmukaisesti vastaavissa toimialueissa ja organisatorisissa yksiköissä. [1, s. 90.]

## 5.7 Ryhmäkäytäntöobjektin merkitys

Ryhmäkäytäntöasetukset tallennetaan ryhmäkäytäntöobjekteiksi (GPO). GPO-objektia voidaan pitää käytössä olevien käytäntöjen ja niiden asetusten säilönä. Voidaan käyttää useita GPO-objekteja yksittäisessä palvelinjoukossa, toimialueessa tai organisatorisessa yksikössä. Koska käytäntö määritetään objektien avulla, monet oliokonseptit ovat voimassa. GPO-objektit toimivat myös isä–lapsisuhteen periytymisen lailla. Periytymisen kautta isäsäilön käytäntö periytyy lapsisäilöön. Pohjimmiltaan tämä tarkoittaa, että isäobjektin käytäntöasetukset tulevat myös lapsiobjektin asetuksiksi.

Voidaan esimerkiksi määrittää tietyt käytäntöasetukset toimialueeseen, josta asetukset periyvät toimialueen organisatorisiin yksiköihin.

Periytyminen voi myös ohittaa määrittämällä lapsisäilöön käytäntöasetuksen, joka eroaa isäsäilön asetuksesta. GPO:n kautta määräytyy, mihin sovelluspalveluun, ja mihin maakohtaiseen sovelluspalveluun käyttäjät ottavat yhteyttä. Myös kaikki toimeksiantopohjaiset sovellukset tulevat GPO:n kautta. Myös selaimen kohdistuvat asetukset tulevat tätä kautta. Kuviossa 3 on esitelty muutamia ryhmäkäytäntöobjekteja. [1, s. 86–87.]



Kuvio 3. Customer Service ryhmäkäytäntöobjekteja.

## 6 Käyttäjätilin lisääminen AD management toolin avulla

### 6.1 Käyttäjätilin lisääminen

Uuden käyttäjätilin lisäämisprosessi on melko suoraviivainen, mutta työläs. Kun lisätään suuria määriä uusia käyttäjiä, prosessi saattaa kestää kauan, minkä takia käyttäjätilin lisäämisen apuna voidaan käyttää ulkoistettuja ohjelmia, joiden avulla käyttäjätilin lisäämisprosessia voidaan parantaa tehokkaammaksi. Tämä prosessi esitellään tässä luvussa.

Kaikki alkaa uuden työntekijän rekrytoinnista, jonka hoitaa HR-osasto. IT saa tiedon HR:ltä, että tulee lisätä uusia käyttäjiä, niin IT tekee tunnukset käyttämällä AD Management Tool web -sovellusta. AD management toolin avulla käyttäjälle tulee automaattisesti seuraavat tiedot Active Directoryyn.

#### AD management tool

Active Directory management tool on web-sovellus, jonka avulla käyttäjien lisäys onnistuu helposti ja nopeasti. Tällä hetkellä sovellus on käytössä vain yhdessä yrityksessä, joka on GoExcellent. AD management tool on suunniteltu nimenomaan GoExcellentin käyttöön, sen skriptiin on lisätty tietoja, joita tulee automaattisesti AD-verkkoon käyttäjän asetuksiin, kun käyttäjä luodaan. Tiedot, jotka siirtyvät määräytyvät tietenkin toimipaikan ja maan mukaan.

Sovelluksella olisi potentiaalisuutta pienillä muokkauksilla toimia missä tahansa yrityksessä. Useat yritykset käyttävät samantyylistä ratkaisua tehostamaan käyttäjien hallintaa. Ohjelman avulla voidaan myös tehdä muita lisäyksiä AD-verkkoon. Sen avulla on pyritty automatisoimaan käyttäjän lisääminen helpoksi ja nopeaksi toimenpiteeksi. Ohjelman sisään on rakennettu skripti, jonka avulla se luo annettujen tietojen pohjalta uuden käyttäjän tiedot ja muut Active Directoryyn lisättävät tiedot.

Automatisoinnilla on pyritty välttämään mahdolliset kirjoitusvirheet, joita saattaa tapahtua, mikäli kaiken lähtee tekemään pelkästään AD:n työkaluja käyttäen. Virheiden korjaaminen voisi olla todella vaikeata, jos sen huomaa vasta myöhemmin, mutta AD management toolin avulla virheiden määrää voidaan minimoida. Skriptin ansiosta tiedot



ovat tarkasti määritetty ja virheitä ei voi tapahtua. Skriptin toimintaa käydään läpi tarkemmin myöhemmissä luvuissa sekä esitetään muutama esimerkki sen sisältävistä funktioista.

Käyttäjää lisättäessä yhdistetään verkkosivulle, jolla AD management tool -ohjelma sijaitsee. Heti alussa voidaan huomata, että erilaisia valintamahdollisuuksia on enemmän. Näistä tärkeimpiä ovat Create New Process sekä Creater New User. Ensiksi on kuitenkin hyvä osoittaa, että verkkosivuosoite, jonka kautta AD management tool toimii, on vain yrityksen sisäverkossa, joten siihen ei pääse ulkopuolelta mitenkään. Myös suojaukset ovat hyvin tiukat kaikissa tiedoissa, joilla voi muokata Active Directoryä. Kuviossa 4 nähdään kaikki valintamahdollisuudet, joita aloitussivulla on.



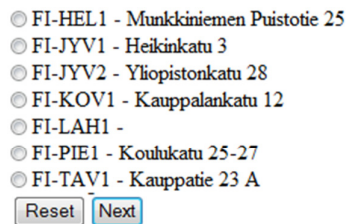
Kuvio 4. AD Management tool aloitussivu.

Create New Process -toiminta on tarkoitettu uuden toimeksiannon lisäämiseksi. Aluksi täytyy kuitenkin lisätä Active Directoryyn uusi organisaatioyksikkö, jonka jälkeen voi luoda uuden prosessin, sekä määrittää prosessille käyttäjä, jolle siirtyy oikeudet sen muokkaamiseen. Samalla toimeksiannolle luodaan automaattisesti jakelulistat (distributing lists, dl) sekä suojausryhmät (security groups, sg).

Create New User -toiminnon avulla luodaan käyttäjät sekä kaikki tarpeellinen tieto, jonka käyttäjä tulee tarvitsemaan. Uuden käyttäjän lisäämisen jälkeen IT:n työ on tehty, ja se lähettää tiedon luoduista tiedoista oikealle esimiehelle. Kehitteillä on myös toiminta, jonka avulla voidaan lisätä useita käyttäjiä samanaikaisesti.

View Sites and Services, DNS-settings, IP-networks -valikolla voidaan tarkastella olemassa olevia toiminta-alueita joita on luotu Active Directoryyn, sekä minkäläiset DNS-asetukset täytyy olla käytössä. Server List -toimintaa käytetään laskujen lähetykseen, se myös luo automaattisesti listan palvelinten resursseista.

Kun Create New User -valikko on valittu, ilmestyy seuraava ikkuna, jossa voidaan valita toimialue, johon käyttäjä lisätään. Normaalisti listassa olisi myös muiden maiden toimialuenimiä, kuten Ruotsin, Norjan sekä Tanskan. Koska keskitytään Suomeen, on vain Suomen toimialueet listattu. Tiedoissa nähdään myös toimialueiden osoitteet, joissa ne toimivat.



[Reset/Restart](#)

Kuvio 5. Suomen toimialueet.

Kuviossa 5 esiintyy kaikki sen hetkiset Suomen toimipisteet, jotka on listattu paikkakunnittain.

- FI-HEL1: Helsingin toimipiste.
- FI-JYV1: Jyväskylän toimipiste.
- FI-JYV2: Jyväskylän toinen toimipiste.
- FI-KOV1: Kouvolan toimipiste.
- FI-LAH1: Lahden toimipiste.

- FI-PIE1: Pietarsaaren toimipiste.
- FI-TAV1: Taivalkosken toimipiste.

Oikean toimipisteen valinnan jälkeen päästään käyttäjän tietojen lisäämiseen. Niiden kautta luodaan tarvittavat tiedot AD-verkkoon. Punaisella merkatut kentät ovat pakollisia täyttää. Kuviossa 6 esiintyy käyttäjän lisäämiseen tarvittavat tietokentät.

Create user in FI-HEL1

Firstname:

MiddleName:

Lastname:

Manager (Username):

Orderer:

Department:

Costarea

Create mailbox:

Create Communicator :

Softgrid User:

Create Profile:

Create Home folder:

Fields marked in read must be filled in.

[Reset/Restart](#)

Kuvio 6. Käyttäjän perustietojen lisääminen.

Heti alussa voidaan huomata, että ylhäällä lukee Create user in FI-HEL1. Teksti ilmoittaa, mihin toimialueeseen ollaan lisäämässä käyttäjää, jotta voidaan olla varmoja, että on valittu oikea toimialue. Käyttäjän lisääminen muistuttaa kovasti Active Directory työkalulla käyttäjän luomista, kun lisätään vain uusi käyttäjä, mutta ei mitään tarkempia tietoja käyttäjälle.

Pakollisia tietoja ovat käyttäjän etu- ja sukunimi, käyttäjän esimiehen käyttäjätunnus, käyttäjän lisäämisen tilannut henkilö sekä toimeksianto, johon yleensä kirjoitetaan jotain havainnollistavaa, koska ei voida tietää alussa, mihin käyttäjä menee töihin. Cost-arean perusteella käyttäjälle muodostuu tietty jakelulista, jonka avulla voidaan seurata kustannustarpeita. Lopuksi täytyy päättää viisi kohtaa, joihin joko laitetaan rasti tai ei laiteta.

Ensimmäisessä kohdassa päätetään, luodaanko käyttäjälle sähköpostiosoite, joka tulee henkilökohtaiseen käyttöön. Tätä osoitetta voidaan käyttää ulkoisena osoitteena.

Seuraavassa kohdassa päätetään, luodaanko käyttäjälle Office Communicator, joka on yrityksen sisäinen viestintäväline. Kolmas kohta on hyvin tärkeä, se valitsemalla käyttäjä lisätään tiettyyn suojausryhmään, jonka kautta määräytyy perusohjelmat Windows XP -profiilille. Kaksi viimeistä valintaa päättävät, luodaanko käyttäjälle profiili Windows XP -ympäristöön sekä saako käyttäjä oman kotihakemiston, johon voi tallentaa tiedostoja omalle profiilille.

Tämän jälkeen käyttäjien lisäämisessä tulee vastaan varmistusivu, jonka avulla voidaan käydä läpi tiedot, joita ollaan luomassa, sekä varmistaa, että kaikki on tullut merkittyä oikein. Sivulta voidaan nähdä käyttäjälle muodostuneet tiedot, jotka täytettiin edellisessä valikossa. Tarkistuksen jälkeen voidaan joko palata muokkaamaan tai varmistaa lisätyt tiedot. Kuviossa 7 nähdään varmistussivu, josta tarkastetaan käyttäjätiedot.



Kuvio 7. Tietojen varmistussivu.

Käyttäjän antaman etu- ja sukunimen perusteella luodaan käyttäjätunnus, jonka avulla käyttäjä voi kirjautua omaan Windows XP -profiiliin. Käyttäjän nimi määräytyy aina muotoon etunimi.kolme ensimmäistä kirjainta sukunimestä, joka on sovelluksen sisäinen toiminto. Käyttäjän tuleva asema organisaatiossa on Employee, joka määräytyy automaattisesti.

Käyttäjän lisäämisen viimeistelyn jälkeen tulee vielä viimeinen ikkuna, jossa on kaikki tieto, joka käyttäjälle tulee omalle tunnukselleen. Voidaan huomata, että salasana on määräytynyt automaattisesti. Salasanan määräytyminen on määritetty sovelluksen

sisällä. Lopuksi käydään vielä läpi kaikki tiedot, jotka luotiin lisäämisen yhteydessä. Käyttäjän lisääminen on nyt suoritettu loppuun. Käyttäjä voisi nyt mennä mille tahansa koneelle, joka on yhdistetty toimipisteen verkkoon. Kuvassa 8 esiintyy viimeinen sivu, kun käyttäjän tiedot on varmistettu.

```
The password: "Goodluck8093528"
Note, the password is without the quotations, 15 char length
Created the user: teppo.tes
```

---

```
DN: 'CN=Teppo Testaaja,OU=Users,OU=FIHEL1,OU=CS,OU=ROOT,DC=internalprod,DC=com'
CN: 'Teppo Testaaja'
Office: 'Helsinki'
telephoneNumber: '+358 9 4158 5000'
department: 'IT'
company: 'GoExcellent'
homeMDB: 'CN=DB20,CN=SG20,CN=InformationStore,CN=SEOSD3CMBX1,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=internalprod,DC=com'
Home: 'H:'
Logon script: ""
Groups: Drawing Array Value
0:sg_costarea_95002_user_CS_FIHEL1
1:sg_appv_users_CS_FIHEL1
Mail: Drawing Array Value
0:smtp.teppo.tes@internalprod.com
1:smtp.teppo.testaaja@internalprod.com
2:SMTP:teppo.testaaja@goexcellent.com
```

Kuvio 8. Käyttäjän tietojen lopullinen tarkastelu.

Käyttäjälle luotiin automaattisesti salasana, jolla voi kirjautua Windows XP - ympäristöön omalla tunnuksellaan. Ensimmäisen kirjautumisen yhteydessä salasana on myös muutettava. Kerrotaan vielä käyttäjän nimi, jotta se ei mennyt ohitse.

Yksikäsitteinen nimi, Distinguished Name (DN), käyttäjä lisätään kyseisiin listoihin.

- CN: Common Name, käyttäjän nimi joka näkyy Active Directoryssä.
- OU: Organizational Unit, käyttäjä on lisätty vain Users organisaatioyksikköön, jonka yläpuolella on ROOT, CS ja FIHEL1. Tämä kuvaa hyvin AD:n rakennetta. Ensimmäinen OU on ROOT -> CS -> FIHEL1 -> Users.

Jakelulistat, joihin käyttäjä lisättiin automaattisesti ja joiden kautta tulevat muun muassa perusohjelmat Windows XP -käyttöön, ovat määräytyneet Groups-kohdassa. Näiden jakelulistojen mukana tulee myös useita muita osia, jotka kuuluvat listan alempaan päähän.

Käyttäjälle luotiin automaattisesti etu- ja sukunimen perusteella sähköpostiosoite sisäiseen viestintään sekä ulkoiseen viestintään tarvittava osoite, joka on muotoa etunimi.sukunimi@goexcellent.com.

Kun kaikkien käyttäjien lisääminen on suoritettu, IT lähettää tiedon oikealle esimiehelle käyttäjien käyttäjänimistä sekä salasanoista, jotta esimies voi lisätä käyttäjän oikean toimeksiannon jakelulistalle ja työskentely voi alkaa.

## 6.2 AD management toolin edut

Kun käyttäjää luodaan AD management toolin avulla voidaan olla varmoja, että kaikki tarvittavat kentät tulevat aina täytetyiksi. Toiminta on automatisoitu juuri sopivaksi GoExcellent yrityksen AD-verkolle, että uuden käyttäjän lisäämiseen kuluu aikaa maksimissaan viisi minuuttia. AD management tool on myös paljon tehokkaampi tietoturvallisuuden kannalta. Kun henkilö lisää uutta käyttäjää käyttäen AD management toolia, henkilön ei edes tarvitse mennä Active Directoryyn luomisen jälkeen, koska kaikki tarpeellinen tieto on jo lisätty. Tämä mahdollistaa myös käyttäjien lisäämisen delegoimisen muille henkilöille, joilla ei muuten olisi pääsyä Active Directoryyn.

Delegoimista on mietitty paljon yrityksen IT-osastolla, koska tällä hetkellä käyttäjän lisääminen kuormittaa työtä aivan turhaan. Käyttäjien lisääminen on tehty niin helpoksi AD management toolin avulla, joten sen käyttäminen voidaan helposti delegoida esimerkiksi HR-osaston puolelle. HR ei tarvitse muita erityisiä oikeuksia kuin pääsyn käyttöliittymän web-osioon. Oikeudet tähän määritellään AD:n security groupin avulla.

Muutokset, joita työkalulla voi tehdä, on määritetty itse työkalussa. Työkaluun voitaisiin määritellä myös erilaisia oikeustasoja sen mukaan, mitä työtä halutaan delegoida, kuten pelkkä uusien käyttäjien lisääminen. Tässä olisi järkeä siltä kannalta, että ensimmäinen tieto uusista työntekijöistä tulee juuri HR:lle.

AD management toolin käyttöä on rajoitettu juuri tarvittaviin toimintoihin, joten sen käyttäminen on helppoa eikä se vaadi juurikaan osaamista itse Active Directory -verkosta. Käyttäjän lisäämisellä on pääsy vain käyttöliittymän web-osioon, jota kautta ei pysty tekemään mitään muita muutoksia tai lisäyksiä AD-verkkoon kuin käyttäjän

lisäämisen. Sovelluksen käyttöä monitoroidaan myös kokoajan, jokainen kirjautuminen sekä tehdyt muutokset menevät automaattisesti tapahtumakirjaan, josta voidaan nähdä, kuka on kirjautunut ja mitä muutoksia henkilö on tehnyt. Kirjautumiseen vaaditaan myös omat tunnukset.

### 6.3 Virhetilanteiden korjaaminen

Mikäli käyttäjän luomisessa on tapahtunut jokin virhe, voidaan käyttäjä poistaa kokonaan, jolloin kaikki käyttäjän luomisen yhteydessä syntyneet tiedot sekä profiilit häviävät. Toisin sanoen on helpompaa poistaa käyttäjä ja lähteä luomaan käyttäjän profiilia uudestaan kuin lähteä korjaamaan jotain virheitä, joka saattaa vaikuttaa moneen osa-alueeseen käyttäjän toiminnassa. Käyttäjän lisääminen on kuitenkin tehty niin helpoksi ja nopeaksi, että lisäämiseen menee vain muutaman minuutti. AD management tool-sovelluksen avulla voidaan eliminoida useita käyttäjästä johtuvia virheitä, kuten salasanan väärinkirjoitus, väärälle jakelulistalle lisääminen ja käyttäjänimen väärin määrittely. Suurin osa näistä toimenpiteistä suoritetaan skriptien avulla, joiden avulla on pyritty automatisoimaan lisäysprosessia. Lisääminen onnistuu todella nopeasti.

#### Toimipaikkojen poistaminen ja lisääminen

Mikäli halutaan muokata tai lisätä uusia toimipaikkoja AD management tooliin, skriptiä ei tarvitse muokata mitenkään. Toimipaikan toiminnan päätyttyä se voidaan poistaa Sites.ini-tiedostosta, jolloin sitä ei ole enää olemassa AD management toolissa. Kaikki toimipaikkaan liittyvät tiedot tulevat tästä tiedostosta. Mikäli halutaan lisätä uusia toimipaikkoja sovellukseen, täytyy vain lisätä haluttu toimipaikka Sites.ini-tiedostoon. Tällä tavalla vältetään turhalta skriptin muokkaamiselta sekä pidetään skripti puhtaana turhasta informaatiosta. Toimipisteen organisaatioyksikkö täytyy käydä lisäämässä Active Directoryyn, jolle täytyy antaa vastaava nimi Sites.ini-tiedostoon.

Uuden toimeksiannon lisääminen on suoritettu Create New Process -toiminnalla, joka on yksi osa AD management tool -sovellusta. Ensiksi toimeksiannolle täytyy kuitenkin luoda organisaatioyksikkö Active Directoryyn, jonka jälkeen voidaan lisätä tarvittavat jakelulistat sekä suojausryhmät Create New Process avulla. Skriptiä ei kuitenkaan

tarvitse muokata mitenkään, kun lisätään uusia toimeksiantoja. Toimipisteen tietojen muokkaaminen ja poistaminen tapahtuu kokonaan Sites.ini-tiedoston kautta. Tällä mahdollistetaan skriptin selkeys.

#### 6.4 Automatisointi AD management -toolilla

AD management tool on toteutettu käyttäen .ASP-koodia. Käytössä on yksi suuri skripti, jonka sisällä on useita funktioita, joiden avulla ohjelman toiminnot on automatisoitu. Funktiot-tiedostoon sisältyy noin 50 eri funktiota. Funktiot kutsuvat muita funktioita, joiden avulla luodaan tietoa sovellukseen.

ASP (Active Server Pages) on Microsoftin kehittämä dynaamisten www-sivujen luomiseen tarkoitettu palvelinpuolen ohjelmointimenetelmä, jolla voidaan tehdä interaktiivisia HTML-sivuja ja internet-sovelluksia palvelimeen. ASP toteutetaan sekakoodina, joka sisältää normaaleja HTML-tageja sekä lisäksi palvelimen ohjaamiseen tarkoitettuja skripti käskyjä. ASP-skriptit suoritetaan, kun loppukäyttäjän selain pyytää .ASP-tiedostoa palvelimelta. Palvelin avaa tiedoston ja suorittaa kaikki siinä olevat käskyt ja HTML-koodin ja palauttaa tuloksen eli Websivun pyytävälle selaimelle.

Koodi suoritetaan palvelimessa, joten loppukäyttäjän selaimen tyyppi tai versio eivät vaikuta toimintaan. Sivua lähetetään standardi-HTML-muodossa selaimelle. Loppukäyttäjä ei näe palvelimessa suoritettavaa koodia, vaan ainoastaan palautettavan HTML-koodin. ASP-tiedostot ovat tekstitiedostoja joiden tarkenne on .ASP. Ne voivat sisältää eri yhdistelminä tekstiä, HTML-tageja ja ASP-skriptikomentoja.

ASP-oliomalli koostuu viidestä oliosta (Request, Response, Server, Application ja Session). Request-olio välittää tietoa selaimelta palvelimelle. Response-olio välittää tietoa palvelimelta selaimelle. Server-olio käsittelee erilaisia funktioita ja palvelinkomponentteja. Application-olio, käsittelee kaikille istunnoille yhteiset asiat. Session-olio, käsittelee yhdelle istunnolle kuuluvat asiat. [6; 7.]

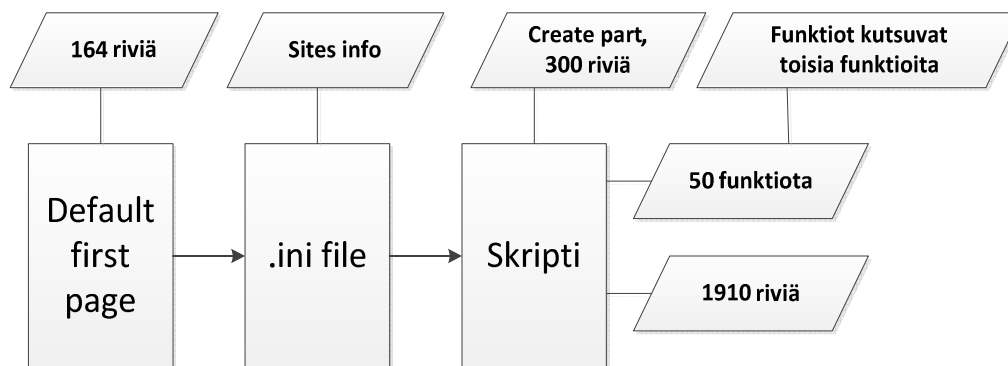
ASP-koodilla toteutetut web-sovellukset eivät myöskään vaadi mitään erityistä selainta toimiakseen, sitä voi käyttää millä selaimella vain. Koska .ASP-koodi suoritetaan palvelimella, ei selaimen tarvitse tehdä mitään työtä.



Skriptin rakenteessa on pyritty keskittymään siihen, että se .ASP-koodi on helppo lukuista. Käytössä on lukuisia objekteja, jotka kutsuvat funktioita, joskus pelkästään merkkijonoja. Skriptissä on muun muassa funktio virheellisten aakkosten poistamiseksi sähköpostiosoitteista sekä muista nimistä, joissa ei voi käyttää virheellisiä aakkosia. Skripti sisältää lukuisia tauluja (array) samankaltaisille funktioille, joten ei tarvitse tehdä suuria funktioita useasti, vaan voidaan vain kutsua tauluja.

Skriptin muokkaamisesta on tehty myös helppoa. Jos päivitetään jotakin tiettyä skriptin osaa, voidaan vanha funktio nimetä uudelleen ja ottaa uudelle versiolle vanhan version nimi. Tällä tavalla voidaan säilyttää vanha funktio. Jonkin mennessä pieleen voidaan helposti palata vanhempaan funktioon.

Skriptiin on suunnitteilla ominaisuus, jonka avulla voidaan lisätä useampia käyttäjiä samanaikaisesti, jolloin vanha funktio nimettäisiin uudelleen ja se korvattaisiin uudella funktiolla, jossa on päivitetty koodi. Skripti täyttää noin 20 eri tietoa automaattisesti Active Directoryyn. Skripti sisältää noin 50 eri funktiota, joissa suurin funktio on käyttäjien lisääminen. Koko skriptin pituus on noin 2400 riviä. Skriptin päivitys on tällä hetkellä sen suunnittelijan Ola Franssonin käsissä. Kuvassa 9 näemme skriptin perustoimintaperiaatteen.



Kuvio 9. .ASP-koodin rakenne.

Liitteessä 1 ja 2 on esitetty kaksi eri funktiota, joilla molemmilla on tärkeä toiminnallinen tarkoitus käyttäjän luomisessa. Aluksi oli tarkoitus saada funktio, jolla luodaan käyttäjälle profiili ja kotihakemisto, mutta tämä olisi tarvinnut koko koodin liittäminen työhön. Valitsin esimerkiksi kaksi melko alkupuolella käytettävää toimintoa. Ensimmäisen liitteen funktiolla valitaan toimipaikka. mukaiselta listalta. Toimipaikan

valinnan yhteydessä funktio kutsuu Sites.ini-tiedostoa, jossa on kaikki toimipaikat ja niiden osoitteet listattu, osoite siirtyy automaattisesti Active Directoryyn käyttäjän profiiliin. Toisessa liitteessä oleva funktio määrittää käyttäjälle kirjautumistunnuksen annetun etunimen ja sukunimen perusteella. Tämä funktio täten luo nimen oikean mukaiseksi.

## 6.5 AD Management toolin jatkokehitysmahdollisuudet

Aikaisemmin mainitsin mahdollisista lisäyksistä AD management tooliin, joiden avulla pyritään viemään automatisointia vielä pidemmälle. Sovellukseen on mahdollisesti suunnitteilla ominaisuus, jotta voidaan lisätä useita käyttäjiä samanaikaisesti yksittäisen käyttäjän lisäämisen ohella. Vaikka toimenpide on tälläkin hetkellä nopea, tällä tavalla sitä saataisiin vieläkin nopeammaksi ja tehokkaammaksi. Mietinnässä on myös muita kehitysmahdollisuuksia, kuten toimeksiannon lisäämistä käyttäjän lisäämisen yhteydessä. Tämä kuitenkin edellyttäisi heti alussa tietoa siitä, mihin toimeksiantoon käyttäjä ollaan lisäämässä, mutta tätä tietoa ei aina alussa ole, joten se on hieman hankalaa toteuttaa.

## 7 Yhteenveto

Insinöörityössä tarkasteltiin kahta vaihtoehtoista tapaa suorittaa käyttäjän lisääminen ja käyttöönottoon tarvittavat toimenpiteet. Aluksi esitelty normaali tapa Active Directoryn avulla on toimiva tapa, mutta melko työläs, kun lisättävä on paljon käyttäjiä. Yhden käyttäjän lisäämiseen kului suunnilleen aikaa noin 30–40 minuuttia. Kun käyttäjää lisätään AD:n avulla ollaan suoraan yhteydessä verkkoon, joten on oltava tarkkana, minkälaisia muutoksia tekee AD:n sisällä. Paljon tietoa on lisättävä käsin, mikä lisää virheiden määrää. Lisäämisen yhteydessä on käytettävä useata palvelinta, mikä saattaa aiheuttaa sekaannusta, kun lisäämisiä on tullut tehtyä useampi.

Vaihtoehtoisena ratkaisuna on yrityksessä kehitetty web-sovellusta, joka toimii yrityksen sisäverkossa. Sen avulla käyttäjän lisääminen on automatisoitu tekemään samat toimenpiteet kuin käsin lisättäessä. Kyseisen web-sovelluksen eli AD management toolin avulla säästyy aikaa käyttäjien lisäämisessä. Sovelluksella lisääminen kestää viisi minuuttia. Ohjelma on helppokäyttöinen. Vaikka sillä tulisi tehtyä pieniä virheitä, ne ovat helposti korjattavissa. Syötettävät tiedot eivät ole kovin hankalia.

Vaikka virheitä tapahtuisi, ei sillä voida tehdä minkäänlaista vahinkoa Active Directoryyn, koska suoraa muokkausmahdollisuutta AD:hen ei ole. Käsin syötettäessä käyttäjällä on koko AD käytössään, ja väärin tehdyt toimenpiteet voivat vaikuttaa moneen asiaan. Täyttämällä 11 eri kohtaa yhdeltä sivulta saadaan tehtyä kokonaan valmis käyttäjä. Itse olin todella vaikuttunut tästä kyseisestä sovelluksesta ja sen mahdollisuuksista.

Kehitysmahdollisuuksista merkittävin olisi se, että mikäli yhteen toimeksiantoon tulee useampi henkilö töihin, voisi kaikki henkilöt lisätä yhdellä kerralla. Tämä nopeuttaisi prosessia vielä enemmän. Käyttäjien lisäämisen voisi myös ottaa kokonaan pois IT:ltä, jolloin IT voisi keskittyä vaativampiin tehtäviin. Olisi hyvin mahdollista delegoida lisääminen kokonaan HR:n tehtäväksi. AD management tool on suunniteltu niin, että sen käytössä ei pitäisi tulla ongelmia. Mikäli jokin menee pieleen, voidaan lisätty käyttäjä käydä poistamassa. Poistaminen täytyy kuitenkin käydä tekemässä Active Directory puolella, johon HR:llä ei ole pääsyä, joten tämä on tehtävä IT:n puolelta.

Tietojen lisääminen on kuitenkin melko yksinkertainen prosessi, joten virhemahdollisuus ei ole suuri.

## Lähteet

- 1 Stanek, William R. 2003. Microsoft Windows Server 2003 – Asiantuntijan Käsikirja. Helsinki: IT Press.
- 2 Kivimäki, Jyrki. 2005. Windows Server 2003 Active Directory – Tehokas Hallinta. Readme.fi.
- 3 Kivimäki, Jyrki. 2004. Inside Active Directory – verkkohallinta. IT Press.
- 4 Windows Server 2003. Yleistä tietoa. 2012. Verkkodokumentti. <<http://www.microsoft.com/finland/products/windowsserver2003/techinfo/overview/default.msp>>. Luettu 24.3.2012.
- 5 Windows Server 2003 R2 FAQ. 2012. Verkkodokumentti. <<http://www.winsupersite.com/article/faqtip/windows-server-2003-r2-faq>>. Luettu 6.4.2012.
- 6 ASP. 2012. Verkkodokumentti. Wikipedia. <<http://fi.wikipedia.org/wiki/ASP>>. Luettu 28.5.2012 .
- 7 ASP –tietokantaohjelmointi. 2012. Verkkodokumentti. <[http://edu.phkk.fi/opiskelu/asp\\_mate/ASP.zip](http://edu.phkk.fi/opiskelu/asp_mate/ASP.zip)>. Luettu 28.5.2012.
- 8 Kerttula, Esa. 1998. Tietoverkkojen tietoturva. EDITA Liikenneministeriö.

## Toimipaikan valinta

```

*****
' returns a list with configures sites in Sites.ini that this user have access to (is member of the group configured in
Sites.ini)
*****
Function getPossibleSites
    Dim arrFileLines()
    Dim arrTemp
    Dim i,objFSO,objFile,l, strLine, strTemp, y, objGroups, strSiteName, colGroups
    Set objGroups = CreateObject("Scripting.Dictionary")
    y = 0
    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objFile = objFSO.OpenTextFile(Server.MapPath("Sites.ini"), forReading)
    colGroups = getGroups
    Do Until objFile.AtEndOfStream
        strLine = objFile.ReadLine
        If LCase(Trim(Left(strLine,5))) = "site:" Then 'om raden börjar med "site:"
            arrTemp =
                Split(strLine,",")
                'skapa en array av raden
                For i=1 To UBound(arrTemp)
                    'vi startar på 1 eftersom 0 är site namnet, sen loopar vi igenom alla grupper
                    ShowMe "If Memberof :" & arrTemp(i)
                    If isMemberOf(arrTemp(i),colGroups)
                        'om användaren är medlem av denna grupp
                        ShowMe "User is member of :" & arrTemp(i) & " adding
it to array on place " & y & " and I is " & i
                        strSiteName = Trim(Mid(arrTemp(0),6)) & " - " &
getValueFromFile(Trim(Mid(arrTemp(0),6)) & ".ini","Street")
                        If Not objGroups.Exists(strSiteName)
                            Then
                                objGroups.Add
                                strSiteName, strSiteName
                                End If
                                'arrFileLines(y) = Trim(Mid(arrTemp(0),6)) & " - " &
getValueFromFile(Trim(Mid(arrTemp(0),6)) & ".ini","Street") lägg till site namnet i arrayen och gå till nästa rad i filen
                                y = y + 1
                                Else
                                    ShowMe "**** User is NOT member of :" & arrTemp(i)
                                End If
                            Next
                        End If
                    Loop
                    objFile.Close
                    Erase arrTemp
                    getPossibleSites = objGroups.Items
                ' DrawArray(arrFileLines)
                If debugon Then If not IsArray(getPossibleSites) Then DebugEntry "Error in: getCongifuredSites
returned a non Array value"
            End Function
*****
*****

```

## Käyttäjänimen muodostuminen

```

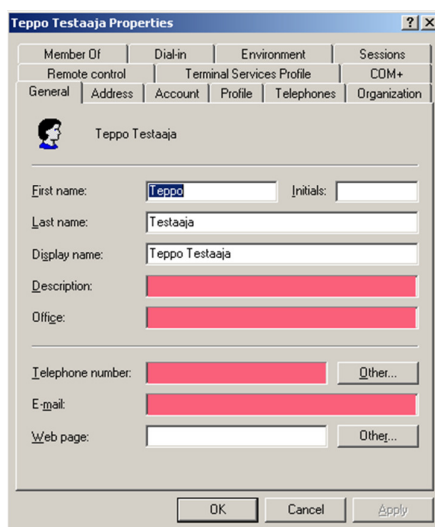
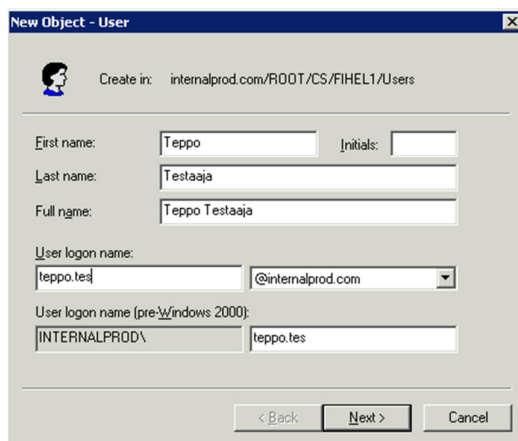
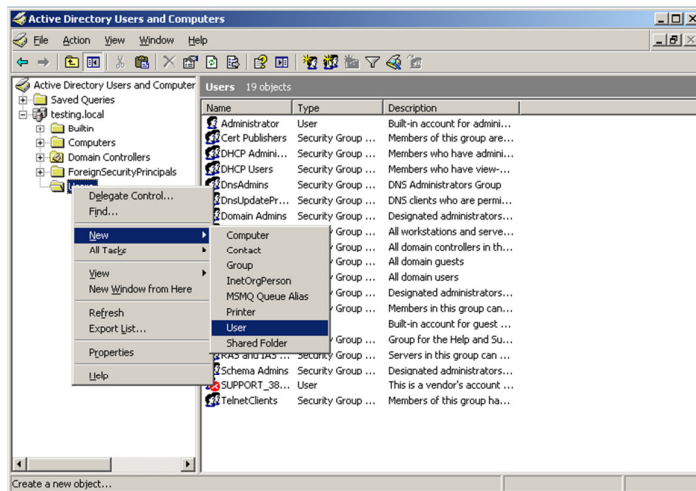
Function getUser_name(strFirstName, strMiddleName, strLastName)
Dim iCount

strFirstName = CleanUpUserName(strFirstName)
if Session("accounttype") = "EXT" then strFirstName = "ext." & strFirstName
if Session("accounttype") = "SLCOMMON" then
    strFirstName = "ca." & replace(Session("strComputerName"), "-", "")
    getUser_name = lcase(trim(left(strFirstName, 16)))
    if not existsInAD(getUser_name) then Exit Function
    for iCount=1 to 20
        getUser_name = lcase(trim(left(strFirstName, 16))) & "_" & iCount
        if not existsInAD(getUser_name) then Exit Function
    next
else
    strMiddleName = CleanUpUserName(strMiddleName)
    strLastName = CleanUpUserName(strLastName)
    strFirstName = LCase(CleanStr(strFirstName))
    strLastName = LCase(CleanStr(strLastName))

    ' we need to make sure samaccount name is only 20 characters in length
    ' börja med att ta förnamn + tre första i efternamnet
    getUser_name = lcase(trim(left(strFirstName, 16)) & "." & trim(left(strLastName, 3)))
    if not existsInAD(getUser_name) then Exit Function
    ' om användaren inte finns hoppa ur denna funktion eftersom att vi redan tilldelat rätt username till
    ' getuser_name redan
    ' om användaren finns, lägg till första bokstav i mellannamn
    ' kolla först att vi fått ett mellannamn
        if strMiddleName <> "" then
            getUser_name = lcase(trim(left(strFirstName, 14)) & "." &
trim(left(strMiddleName, 1)) & "." & trim(left(strLastName, 3)))
            if not existsInAD(getUser_name) then Exit Function
        End if
    ' om även denna användare finns använd förstabokstaven i förnamnet
        getUser_name = lcase(trim(left(strFirstName, 14)) & "." & trim(left(strFirst, 1)) & "." &
trim(left(strLastName, 3)))
        if not existsInAD(getUser_name) then Exit Function
    ' om även denna användare finns använd förstabokstaven i efternamnet
        getUser_name = lcase(trim(left(strFirstName, 14)) & "." & trim(left(strLast, 1)) & "." &
trim(left(strLastName, 3)))
        if not existsInAD(getUser_name) then Exit Function
    ' om även denna användare finns använd enslumpad bokstav, acsii 97-122 är små bokstäver försök 20
    ' gånger sen ger vi upp, observera att vi inte utesluter redan testade bokstäver, men om vi har otur att få 20 stycken
    ' som vi haft tidigare så har vi redan här ett problem :)
    Randomize
    for iCount=1 to 20
        getUser_name = lcase(trim(left(strFirstName, 14)) & "." & chr(Int((122 - 97 +
1) * Rnd + 97)) & "." & trim(left(strLastName, 3)))
        if not existsInAD(getUser_name) then Exit Function
    Next
    for iCount=1 to 20
        getUser_name = lcase(trim(left(strFirstName, 13)) & "." & chr(Int((122 - 97 +
1) * Rnd + 97)) & chr(Int((122 - 97 + 1) * Rnd + 97)) & "." & trim(left(strLastName, 3)))
        if not existsInAD(getUser_name) then Exit Function
    Next
    for iCount=1 to 20
        getUser_name = lcase(trim(left(strFirstName, 12)) & "." & chr(Int((122 - 97 +
1) * Rnd + 97)) & chr(Int((122 - 97 + 1) * Rnd + 97)) & chr(Int((122 - 97 + 1) * Rnd + 97)) & "." &
trim(left(strLastName, 3)))
        if not existsInAD(getUser_name) then Exit Function
    Next
end if
getUser_name = ""
DebugEntry "Could not create a unique username"
End Function

```

## Active Directory työkaluilla tehty prosessi





**Teppo Testaaja Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile	COM+	
General	Address	Account	Profile
Telephones	Organization		

Street:

P.O. Box:

City:

State/province:

Zip/Postal Code:

County/region:

OK Cancel Apply

**Teppo Testaaja Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile	COM+	
General	Address	Account	Profile
Telephones	Organization		

Telephone numbers

Home:  Other...

Pager:  Other...

Mobile:  Other...

Fax:  Other...

IP phone:  Other...

Notes:

OK Cancel Apply

**Teppo Testaaja Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile	COM+	
General	Address	Account	Profile
Telephones	Organization		

Title:

Department:

Company:

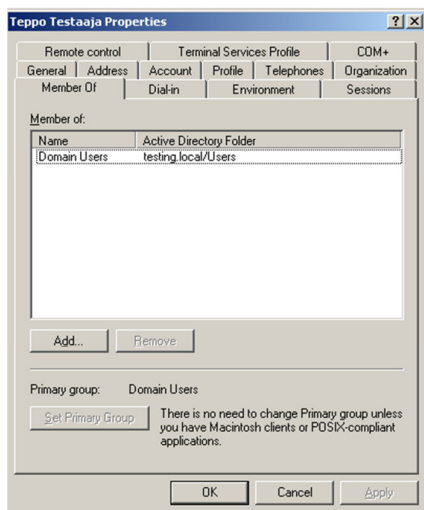
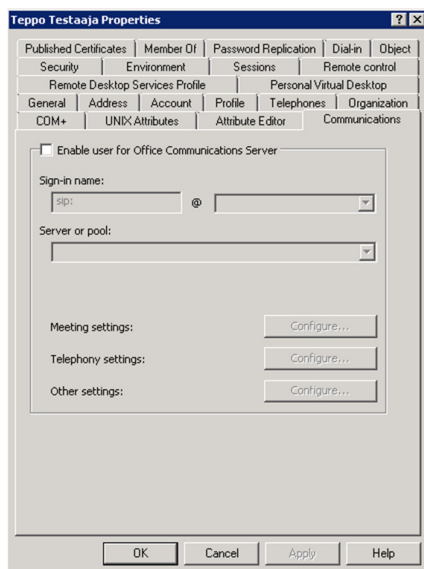
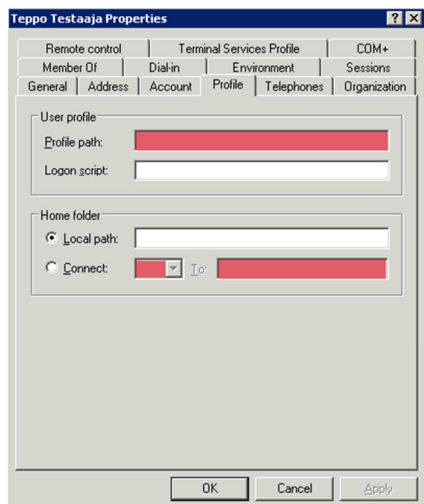
Manager

Name:

Change... Properties Clear

Direct reports:

OK Cancel Apply



## Ulkoisen sähköpostiosoitteen luominen

