Teemu Heikkinen

**Identiteetinhallinan käyttöönotto Kainuun ammattiopistossa**

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Tradenomi
Tietojenkäsittely
2014

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**OPINNÄYTETYÖ**
**TIIVISTELMÄ**

| Koulutusala<br>Tradenomi | Koulutusohjelma<br>Tietojenkäsittely |
|---|---|
| Tekijä(t)<br>Teemu Heikkinen | |
| Työn nimi<br>Identiteetinhallinan käyttöönotto Kainuun ammattiopistossa | |
| Vaihtoehtoiset ammattiopinnot | Toimeksiantaja<br>Kainuun ammattiopisto |
| Aika<br>2014 | Sivumäärä ja liitteet<br>32, 1 |


Identiteetin ja pääsynhallinta on nykypäivänä tärkeä osa yrityksen tietoturvaa, kustannusten hallintaa ja IT- työntekijöiden työmäärien vähentämistä. Identiteetin ja pääsynhallinnalla tässä tapauksessa tarkoitetaan sitä, kuinka IT-resurssien käyttäjän käyttöoikeuksia luodaan, ylläpidetään, hyödynnetään ja lopetetaan käyttämällä identiteetin ja pääsynhallintaan tarkoitettuja ohjelmistoja.

Tässä työssä kerrotaan yleistä tietoa identiteetin- ja pääsynhallinnasta jonka jälkeen keskitytään Microsoftin Forefront Identity manager- järjestelmään. Käytännön osuudessa testasin Forefront Identity Managerin eri ominaisuuksia Microsoftin virtuaali laboratorion avulla.

Työn toimeksiantajana on Kainuun ammattiopisto. Kainuun ammattiopisto halusi selvittää mitä hyötyä identiteetin hallinnan käyttöönotosta olisi heille ja mitä ominaisuuksia Microsoftin Forefront identity manager tarjoaa. Opinnäytetyö on tarkoitettu myös niille jotka ovat kiinnostuneita identiteetin- ja pääsynhallinnasta.

Työn käytännön osuuden lopputuloksena on dokumentti, jossa käsitellään Forefront Identity managerin ominaisuuksia ja kuvataan niiden toimintoja käytännön esimerkeillä. Käytännön osuuteen tuotettu dokumentti on opinnäytetyön liitteenä. Opinnäytetyö pyrkii hahmottamaan identiteetin hallinnan hyödyllisyyttä ja kuvaamaan identiteetin- ja pääsynhallinnan ominaisuuksia.


| | |
|---|---|
| Kieli | Suomi |
| Asiasanat | Identiteetin- ja pääsynhallinta, Microsoft Forefront Identity Manager |
| Säilytyspaikka | ☐ Verkkokirjasto Theseus<br>☐ Kajaanin ammattikorkeakoulun kirjasto |

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**THESIS**
**ABSTRACT**

| School | Degree Programme |
|---|---|
| Kajaani University of Applied Sciences | Data Processing |
| Author(s)<br>Teemu Heikkinen | |
| Title<br>The Introduction of Identity management in Kainuu Vocational College | |
| Optional Professional Studies | Commissioned by<br>Kainuu Vocational College |
| Date<br>2014 | Total Number of Pages and Appendices<br>32, 1 |


Identity and access management is an important part of a company's security, cost management and reduction of IT staff workloads. Identity and access management in this case refers to how IT resource permissions are created, maintained, utilized and terminated by using identity and access management software.

This work provides general information about the identity and access management, after which it focuses on the Microsoft Forefront Identity Manager system. The practical part includes testing of different properties of Microsoft Forefront Identity manager by using Microsoft's virtual labs as the testing tool.

The client of this thesis is Kainuu Vocational college. They wanted to find out what are the benefits of identity management for them and what features does the Microsoft Forefront Identity Manager provide. This thesis is also intended for those who are interested in identity and access management in general.

The result of the practical part of this thesis is a document which explains Forefront Identity manager properties and describes its functions with practical examples. The document produced for the practical part of this thesis is in the thesis appendices. The work aims to outline the usefulness of identity management and describe the identity and access management features.



| | |
|---|---|
| Language of Thesis | Finnish |
| Keywords | Identity and access management, Microsoft Forefront Identity Manager |
| Deposited at | ☐ Electronic library Theseus<br>☐ Library of Kajaani University of Applied Sciences |

SISÄLLYS

1 JOHDANTO 1

2 IDENTITEETIN JA PÄÄSYNHALLINTA 2
2.1 Identiteetinhallinan eri osa-alueet 2
2.1.1 Tunnistautuminen 3
2.1.2 Valtuuttaminen 3
2.1.3 Käyttäjien hallinta 3
2.1.4 Keskitetty käyttäjä arkisto 4
2.2 Sähköinen Identiteetti 5
2.2.1 Atribuutit 5
2.3 Identiteetin elinkaari 6
2.3.1 Identiteetin luomisprosessi 6
2.3.2 Provisiointi 6
2.3.3 Identiteetin käyttäminen 7
2.3.4 Identiteetin päivittäminen 7
2.3.5 Identiteetin deprovisiointi 8
2.3.6 Identiteettien hallinnointi 8
2.4 Identiteetin hallinnan tärkeys nykypäivänä 9
2.5 Identiteetinhallinnan tarjoamat hyödyt 10
2.6 Identiteetinhallinta järjestelmän toiminnot 10
2.7 Identiteetinhallinnan toteuttamisen haasteet. 11
2.8 Markkinoilla olevia identiteetinhallintajärjestelmiä 12
2.8.1 Oracle Identity Management: 12
2.8.2 IBM Security Identity manager: 13
2.8.3 CA Identity Minder 14
2.8.4 Net IQ Identity Manager 15
2.8.5 Open IAM Identity Manager 16
2.8.6 Shibboleth Identity Provider 17
2.8.7 Gluu Server 18
2.8.8 Open AM ja Open IDM 19

3 MICROSOFT FOREFRONT IDENTITY MANAGER 20
3.1 Forefront identity managerin kompononentit 22
3.1.1 IDM Platform (Identity Management Platform) 22
3.1.2 FIM Service (FIM palvelu) 23
3.1.3 FIM Syncrohronization Service (FIM synkronointi palvelu) 23
3.1.4 FIM-Clients (FIM asiakasohjelmat) 24
3.1.5 FIM Certificate Management ( FIM Sertifikaattien hallinta) 25
3.2 Forefront identity managerin arkkitehtuurin edellytykset 26

4 FOREFRONT IDENTITY MANAGERIN TESTAUS KÄYTÄNNÖSSÄ 27
4.1 Toimeksiantaja Kainuun ammattiopisto 27
4.2 Tavoite 27
4.3 Testaus menetelmät 28
4.4 Testatut ominaisuudet 29
4.5 Testauksen aikana ilmenneet ongelmat 30
4.6 Testauksen lopputulos 30

5 JOHTOPÄÄTÖKSET 31

LÄHTEET 32

LIITTEET

SYMBOLILUETTELO

| | |
|---|---|
| FIM | Forefront Identity Manager |
| LDAP | Lightweight Directory Access Protocol |
| MPR | Management Policy Rule |
| OpenDJ | Avoimen lähdekoodin LDAP |
| SAML | Security Assertion Markup Language |
| SSO | Single Sign On eli kertakirjautuminen |

# 1 JOHDANTO

Yrityksissä on nykyään monia erilaisia tietojärjestelmiä mikä tarkoittaa sitä, että niiden hallinta tulee olemaan vaikeampaa, myös tietoturva ongelmat lisääntyvät tietojärjestelmien lisääntyessä. Näitä ongelmia pyritään hallitsemaan identiteetin- ja pääsynhallinnan ohjelmistoilla. Tässä opinnäytetyössä tarkastellaan identiteetin- ja pääsynhallintaa yleisellä tasolla jonka jälkeen keskitytään Microsoftin Forefront Identity manageriin (FIM) . Opinnäytetyössä tarkastellaan Forefront Identity manager 2010 R2 versiota.

## 1.1 Työn tavoite

Opinnäytetyön tavoitteena on antaa perustietoa identiteetin- ja pääsynhallinnasta ja testata miten Microsoftin Forefront Identity Manager toimii käytännössä identiteetinhallinnassa. Käytännön osuudella pyritään hahmottamaan Forefront Identity managerin hyödyllisyyttä Kainuun ammattiopistolle.

## 1.2 Työn rakenne.

Toisen osion tarkoituksena on antaa perus tietoa identiteetin- ja pääsynhallista, osiossa pohditaan mm. identiteetin- ja pääsynhallinnan tarkoitusta ja miten hyötyä siitä on organisaatiolle. Tässä osiossa esitellään lyhyesti muutama identiteetinhallintaan tarkoitettu ohjelmisto.

Kolmannessa osiossa tarkastellaan Forenfront Identity manageria yleisesti. Osiossa kerrotaan miten ohjelmisto toimii, mitä komponetteja siihen sisältyy ja mitä ominaisuuksia ohjelmistossa on.

Neljännen osion tarkoituksena on kertoa Forefront Identity manegerin käytännön testauksesta. Osiossa käsitellään testaus prosessia, lopputulosta ja testauksen aikana tulleita ongelmia. Testaus prosessissa kirjoitettu dokumentaatio tulee työn liitteeksi (LIITE1).

Viimeisessä osiossa pohditaan työn lopputulosta.

# 2 IDENTITEETIN JA PÄÄSYNHALLINTA

Identiteetin- ja pääsynhallinta on noussut tärkeäksi osaksi yritysten liiketoimintaa, koska siitä saatuja etuja ovat mm. kustannusten laskeminen, hallinointi ja toiminnallinen tehokkuus. Yritysten täytyy hallita pääsyä tietoihin ja sovelluksiin jotka voivat olla yrityksen sisäisiä ja ulkoisia palveluita. Yritysten täytyy myös tarjota pääsy erilaisille yrityksen sisäisille ja ulkoisille identiteeteille vaarantamatta yrityksen tietoturvaa.(Gamatech .1)

Identiteetti- ja pääsynhallinta käsittää prosessit, henkilöt ja tuotteet jotka hallinnoivat identiteettejä ja pääsyä yrityksen resursseihin. Yrityksen tulee myös varmistaa tiedon oikeellisuus, jotta identiteetin- ja pääsynhallinnan viitekehys voi toimia oikein. Identiteetin- ja pääsynhallinnan pääasiallinen tarkoitus on varmistaa, että ihmiset pääsevät käsiksi tiettyyn tietoon sillä hetkellä kun he sitä tarvitsevat.(Gamatech .1)

## 2.1 Identiteetinhallinan eri osa-alueet

Identiteetti- ja pääsynhallian komponentit voidaan luokitella neljään eri kategoriaan: Oikeuksien tarkistaminen eli tunnistautuminen, valtuuttaminen, käyttäjien hallinta ja keskitetty käyttäjä-arkisto. (Gamatech .1)

| **Pääsyn hallinta** | |
|---|---|
| **Tunnistautuminen** | **Varmentaminen** |
| Kerta kirjautuminen | Rooli pohjainen |
| Istunnon hallinta | Sääntö pohjainen |
| Salasana palvelut | Ominaisuus pohjainen |
| Vahva tunnistautuminen | Etä varmentaminen |
| **Käyttäjien hallinta** | **Keskitetty käyttäjä arkisto** |
| Hajautettu hallinta | Hakemisto |
| Käyttäjän ja roolien hallinta | Tiedon syncronointi |
| Varaukset | Meta-hakemistot |
| Salasanojen hallinta | Virtuaali-hakemistot |
| Itsepalvelu | |
| **Identiteetin hallinta** | |

Kuva 1. Identiteetin ja pääsynhallinan osat luokiteltuina. (Gamatech .1)

### 2.1.1 Tunnistautuminen

Tämä kategoria käsittää tunnistaumisen hallinnan ja istunnon hallinnan. Tunnistautumisen avulla käyttäjä toimittaa tarvittavat valtuutukset, jotta hän pääsee käsiksi tiettyihin sovelluksiin ja resursseihin. Kun käyttäjä on tunnistettu, luodaan istunto ja yhteys käyttäjän ja hakujärjestelmän välille siihen asti kunnes käyttäjä kirjautuu ulos tai istunto lopetetaan muulla tavalla. Tunnistus-moduulin mukana tulee yleensä salasana-palvelu moduuli jos käytetään käyttäjätunnus/salasana menetelmää. Keskitetyn istunnon hallinnan avulla tunnistus- moduuli mahdollistaa ns. ”kerta-kirjautumis” palvelun jonka avulla käyttäjä pääsee yhden kirjatumisen jälkeen käsiksi sovelluksiin ja resursseihin jotka ovat saman identiteetin- ja pääsynhallinta viitekehyksen alla. (Gamatech .2)

### 2.1.2 Valtuuttaminen

Valtuuttaminen on identiteetin- ja pääsynhallinnan osa joka päättelee onko käyttäjällä oikeus päästä käsiksi tiettyyn resurssiin tai palveluun. Resurssilla tarkoitetaan tässä tapauksessa sähköisiä resursseja kuten esimerkiksi tiedostoja ja sovelluksia joita yrityksen tietojärjestelmät sisältävät. Valtuuttaminen suoritetaan vertaamalla resurssiin pääsy pyyntöä valtuutus käytäntöön, jotka ovat varastoituna identiteetin- ja pääsynhallinan käytäntö varastossa. Valtuutus on ydinmoduuli joka toteuttaa rooliin perustuvaa kulunvalvontaa. Valtuutus tarjoaa myös monimutkaista pääsynvalvontaa joka perustuu informaatioon ja käytäntöihin jotka sisältävät käyttäjän ominaisuudet, käyttäjän roolit / ryhmät, toimet, kulkuväylät, ajan, pyydetyt resurssit, ulkoiset tiedot ja yrityksen säännöt. (Gamatech .2)

### 2.1.3 Käyttäjien hallinta

Käyttäjien hallinta sisältää käyttäjien hallinnan, salasanojen hallinnan, roolien ja ryhmien hallinnan ja käyttäjien ja ryhmien varaukset. Käyttäjien hallinta sisältää hallinnolliset tehtävät kuten identiteetin luomisen ja käyttäjien identiteetin ja etuoikeuksien ylläpitämisen. Yksi käyttäjien hallinnan tehtävistä on käyttäjän elinkaaren hallinta jonka avulla yritys voi määritellä kuinka kauan käyttäjän käyttöoikeudet resursseihin ovat voimassa. (Gamatech .2)

Osaa käyttäjien hallinnan toiminnoista kannattaa hallita keskitetysti, kun taas joitain toimintoja voi jättää loppukäyttäjän hallinnoitavaksi. Hajautettu käyttäjienhallinta auttaa yritystä jakamaa työtaakkoja eri osastojen välille. Hajauttamiinen voi myös parantaa järjestelmän tarkkuutta siirtämällä vastuun sille jota informaatio tai tilanne koskee. (Gamatech .2)

Itsepalvelu on myös tärkeä osa käyttäjien hallintaa. Itsenäisen profiilin hallinnan avulla yrityksen ei tarvitse huolehtia käyttäjätietojen muutoksista vaan käyttäjä voi itse muuttaa käyttäjätiedot paikkaansa pitäviksi. Toinen hyödyllinen itsepalvelu toiminto on käyttäjän salasanan nollaaminen jonka avulla voidaan vähentää helpdeskin työtaakkaa, kun käyttäjältä unohtuu salasana. (Gamatech .2)

### 2.1.4 Keskitetty käyttäjä arkisto

Keskitetty käyttäjä arkisto varastoi ja toimittaa identiteetti tietoja toisiin palveluihin ja tunnistaa käyttäjän antamat käyttäjätiedot. Keskitetty käyttäjä arkisto esittää yrityksen identiteetit joko loogisessa näkymässä tai ryhmitettynä. Hakemistopalvelut jotka käyttävät LDAPv3 standardia ovat hallitsevia teknologioita keskitetylle käyttäjä arkistolle. Sekä meta- ja virtuaali hakemistoilla voidaan hallita tunnistetietoja eri sovelluksista ja järjestelmistä. Meta hakemistot kokoavat yhteen tunnistetietoja yhdistämällä identiteetti tietoja eri tietojärjestelmistä. Virtuaalinen hakemisto tarjoaa yhtenäisen LDAP näkymän identieetti tiedoista, koska virtuaalinen hakemisto yhdistää tietokantojen käyttäjä tiedot yhdeksi kokonaisuudeksi. (Gamatech .3)

## 2.2 Sähköinen Identiteetti

Tietotekniikassa sähköinen identiteetti tarkoittaa kohdetta kuvailemien atribuuttien kokoelmaa. Kohteet ovat yleensä ihmisiä, joita kuvailevia atribuutteja voivat olla esimerkiksi nimi, käyttäjätunnus ja oikeus tietyn palvelun käyttämiseen. Käyttäjän identieetti on tosielämän henkilön abstraktio(ei materiaalinen olio) tietojärjestelmässä, esimerkiksi käyttäjätunnus ”eskmerk” kuuluu tosielämän Esko Esimerkki nimiselle henkilölle. (Linden 2012. 10)

Myös muilla kohteilla kun ihmisillä voi olla oma identiteetti, esimerkiksi verkkoon kytketyllä tietokoneella voi olla oma identiteetti ja sen atribuutteina voi olla IP-numero, domain nimi ja julkinen avain. (Linden 2012. 10)

### 2.2.1 Atribuutit

Identiteetti koostuu atribuuttien kokoelmasta, identiteetin voidaan ajatella olevan jonkin palvelun käyttäjätietokannan tietue, jossa jokainen atribuutti on yksi sarake tietokannassa. Identiteettiin liitettävät atribuutit riippuvat käyttötilanteesta ja muiden kuin tarpeellisten atribuuttien kerääminen ja tallentaminen on kielletty henkilötietolaissa. Käyttäjä tietokantaan kerättyä atribuutti kokoelmaa kutsutaan käyttäjätietokannan skeemaksi. (Linden 2012. 11)

Palvelujen kehittäjät voivat rakentaa skeemansa alusta lähtien itse, mutta identiteetinhallinnantuotteet luottavat usein Internet-standardeina julkaistuihin olioluokkiin (object class). Olioluokat ovat alkujaan kehitetty LDAP-hakemistoja ja sen edeltäjiä varten mutta niitä käytetään identiteetinhallintatuotteissa paljon. (Linden 2012. 11)

## 2.3 Identiteetin elinkaari

Identiteetin elinkaarella tarkoitetaan yleensä niitä vaiheita joita identiteetti käy läpi olemassa olonsa aikana. Nämä vaiheet pystytään jakamaan neljään eri osioon jotka ovat: identiteetin luominen eli provisiointi, identiteetin käyttö, päivitäminen ja käytöstä poistuminen eli deprovisiointi. Lisäksi hallinnointi on osa identiteetin elinkaarta. (Silander 2013. 8)

### 2.3.1 Identiteetin luomisprosessi

Identiteetin luomisen voidaan ajatella koostuvan kolmesta eri vaiheesta: atribuuttien varmistamisesta, valtuutus tietojen myöntämisestä ja varsinaisen identiteetin muodostamisesta. Atribuuttien varmistaminen tarkoittaa jonkin tahon todistusta atribuuttien oikeellisuudesta. Riippuen valtuustiedon tyypistä, valtuutustietoja voi myöntää jokin auktoriteetti tai kohde itse, esimerkkinä organisaation myöntämä digitaalinen varmenne tai käyttäjän määrittämä salasana. Valtuutustietojen lisäksi identiteetin muodostamiseen tarvitaan jokin tunniste, kuten käyttäjänimi tai henkilökohtainen numero. (Silander 2013. 9)

### 2.3.2 Provisiointi

Provisiointi on identiteetin elinkaaren ensimmäinen askel ja se käsittää identiteetin luomisen ja identiteetti tiedon välittämisen eri kohdejärjestelmille.

Provisioinnillla voidaan luoda automaattisesti identiteettejä suoraan jostain lähdejärjestelmästä joka sisältää tarvittavat identiteettiatribuutit kohteelle. Tämä säästää manuaalista työtä ja nopeuttaa uuden identiteetin käyttöönottoa, mikä voi tehostaa esimerkiksi työhönottoa. (Silander 2013. 10)

Kun kohteelle on luotu identiteetti, täytyy sen tiedot täytyy toimittaa kaikille tietoja käyttävälle kohdejärjestelmille, jotta identiteettiä voidaan alkaa käyttämään. Kohdejärjestelmillä tarkoitetaan tässä tapauksessa kaikkia sovelluksia, tietojärjestelmiä tai muita oganisaation resursseja, jotka tarvitsevat identiteetti tietoja. Esimerkki kohdejärjestelmiä voi olla käyttöjärjestelmä,

sähköpostijärjestelmä ja palkanlaskentajärjestelmä. Kohdejärjsrtelmiä voi olla yhden organisaation sisällä paljon, jolloin provisioinnin automatisointi on tärkeää.(Silander 2013. 10)

### 2.3.3 Identiteetin käyttäminen

Kohteet käyttävät identiteettejään esimerkiksi eri järjestelmiin tunnistautumiseen ja oikeuttavat niillä erilaisia toimintoja kuten esimerkiksi kirjautumisen työpaikan sisäverkkoon ja työtuntien kirjaamiseen tuntiseuranta järjestelmään. Identiteettien käyttö mahdollistaa lisäksi luotetun viestinnän, koska vietinnän osapuolet voivat etsiä ja varmentaa muiden identiteettejä. Esimerkiksi sähköpostit on mahdollista allekirjoittaa digitaalisesti jotta lähettäjän identiteetistä voidaan varmistua. Viestinnän lisäksi myös muilla tahoilla on mahdollista käyttää muiden kohteiden identiteettejä, tällaisia tahoja voivat olla esimerkiksi kulunvalvonta tai palkanlaskenta. (Silander 2013. 11)

Myös laitteet voivat tarvita identieettiä, jotta ne voivat tunnistuatua johonkin palveluun tai verkkoon ja suorittaa siellä identiteetin sallimia toimintoja. Laitteet ja sovellukset tarvitsevat identiteettejä löytääkseen toisensa ja kommunikoidakseen luotettavasti keskenään.(Silander 2013. 11)

### 2.3.4 Identiteetin päivittäminen

Kaikkia identiteettejä joudutaan päivittämään ajoittain, koska atribuutit voivat muuttua ajan myötä. Esimerkiksi roolit, työnkuvat, osoitteet ja puhelinumerot voivat muuttua useita kertoja identiteetin olemassaolon aikana. Atribuuttien muutokset saattavat vaikuttaa valtuutustietoihin. Esimerkiksi roolin tai työnkuvan muuttuessa, kohde voi menettää valtuuksia ja saada niiden tilalle uusia. Valtuutustiedot voivat vaatia päivittämistä ilman atribuuttien muutoksia, koska valtuustiedoille on yleensä asetettu jokin voimassaoloaika ja ne täytyy uusia ajan loppuessa. (Silander 2013. 11)

Yleensä kaikki identiteetti päivitykset tulee tehdä viipymättä, ettei synny tilanteita, joissa kohteella ei esimerkiksi ole oikeutta suorittaa tehtäväänsä tai kohteella on oikeuksia jota sillä ei enää pitäisi olla. Automaattinen provisiointi auttaa huomattavasti ajantasaisuuden ja yhteinäisyyden saavuttamisessa etenkin sellaisissa ympäristöissä joissa kohdejärjestelmiä ja päivitettäviä identiteettejä on paljon. (Silander 2013. 12)

### 2.3.5 Identiteetin deprovisiointi

Deprovisioinnin avulla käyttäjäidentiteettejä ja niiden tietoja voidaan poistaa, kun identiteetin elinkaari on tullut päätökseensä. Tiedot voidaan poistaa yhtenäisesti kaikista kohdejärjestelmistä, joita käyttöoikeuksien menetys koskettaa. Esimerkiksi työntekijä joka vaihtaa työtehtävää voidaan deprovisioida jostain kohdejärjestelmästä ja provisioida uuden työnkuvan edellyttämiin kohdejärjestelmiin. Työntekijän työsuhteen päättyessä voidaan hänen identiteettinsä deprovisioida kaikista kohdejärjestelmistä. (Silander 2013. 12)

### 2.3.6 Identiteettien hallinnointi

Identiteeteille tehtäviä toimintoja pitää hallita selkeillä käytännöillä sen koko elinkaaren ajan. Identiteetin hallinnointi on tärkeä osa organisaationlaajuista sisäistä valvontaa ja se on suunniteltava ja toteutettava oikein. (Silander 2013. 13)

Identiteetinhallintaan liittyvät käytännöt koskevat pääasiassa varmennusta ja valtuutusta. Varmennuskäytännöt määrittelevät vaaditun varmuuden identiteetin kaikille eri toimille. Nämä käytännöt määrittelevät olosuhteet, joissa kohteiden annetaan käyttää identiteettin perustuvia palveluita ja resursseja. Jokaisella eri organisaatiolla voi olla omat identiteettikäytännöt. (Silander 2013. 13)

## 2.4 Identiteetin hallinnan tärkeys nykypäivänä

Identiteetin hallinta liittyy erottamattomasti turvallisuuteen ja tuottavuuteen organisaatiossa joka tekee sähköistä kaupankäyntiä. Organisaatiot käyttävät identiteetinhallintajärjestelmiä suojautumaan digitaalisilta hyökkäyksiltä ja liiketoiminnan tuottavuuden parantamiseen. Järjestelmän keskitetyn hallinan ominaisuudet voivat vähentää monimutkaisuutta ja keskeisten prosessien kustannuksia. Keskitetty kulunvalvonta tukee myös johdonmukaista turvallisuuspolitiikkaa. (Waters)

Identiteetinhallintajärjestelmät antavat organisaatioille tavan hallita kytkemättömiä päätepisteitä kuten kannettavia tietokoneita, tablet laitteita ja älypuhelimia. Monet näistä laitteista eivät ole organisaation omistuksessa vaan ne ovat käyttäjän omia laitteita. Kyky valvoa näiden laitteiden käytäntöjä tulee olemaan tarpeellinen ominaisuus identiteetinhallintajärjestelmissä laitteiden turvallisuuden vuoksi. (Waters)

Identiteetinhallinnan avulla organisaatiota voi hyötyä mm seuraavilla tavoilla:

- Paranneltu käyttäjän tuottavuus

  Tuottavuuden kehittäminen tapahtuu yksinkertaistamalla kirjautumisen käyttöliittymää ja kyvyllä muutta nopeasti käyttöoikeuksia

- Parantunut asiakkaan ja yhteistyökumppanin palvelu

  Asiakkaat ja yhteistyökumppanit hyötyvät myös virtaviivaisemmasta ja turvallisesta prosessista , kun he käyttävät organisaation sovelluksia ja tietoja.

- Laskeneet help desk kustannukset

  IT-tukeen tulee vähemmän help-desk soittoja koska esimerkiksi salasanan vaihto työkalu on valmiina identiteetinhallintajärjestelmässä. (Bloor, R., Halper, F., Hurwitz, J., Kaufman, M.)

## 2.5 Identiteetinhallinnan tarjoamat hyödyt

Identiteetinhallinnan toteuttaminen parhaimpien käytäntöjen avulla voi antaa organisaatiolle useita etuja. Nykypäivänä yritykset haluavat tarjota käyttäjilleen välittömän pääsyn organisaation sisäisiin järjestelmiin. Verkon avaaminen asiakkaille, yhteistyökummpaneille, tavaran toimittajille ja tietenkin työntekijöille voi parantaa tuotannon tehokkuutta ja alentaa kustannuksia. Identiteetinhallinnanjärjestelmillä organisaatio laajentaa pääsyä tietojärjestelmiin vaarantamatta tietoturvallisuutta. Hallitulla käyttöoikeiksien hallinnalla on potentiaalia parantaa ulkopuolisten toimitsijoiden tuottavuutta ja tyytyväiysyyttä. (Waters)

Identiteetinhallinnasta voi tulla organisaation turvallisen ympäristön kulmakivi, koska identiteetti on tärkeä osa pääsynhallintaa. Identiteetinhallinta järjestelmä vaatii toimiakseen sen, että organisaatio määrittelee käytännöt jotka määrittelevät kenellä on pääsy mihinkin tietoon. Hyvin hoidettu identiteettien pääsyn valvonta vähentää sisäisten ja ulkoisen hyökkäysten riskiä. (Waters)

Identiteetinhallintajärjestelmä voi parantaa säädösten noudattamista antamalla työkaluja toteuttamaan käyttäjän todentamiseen ja tietojen saatavuuteen perustuvia toimintamalleja. Monet järjestelmät tarjoavat nykyään ominaisuuksia jotka on suunniteltu varmistamaan että organisaatio on ohjeidenmukainen. (Waters)

## 2.6 Identiteetinhallinta järjestelmän toiminnot

Tyypillinen Identiteetinhallintajärjestelmä koostuu neljästä peruselementistä:

- Hakemistosta joka sisältää henkilötiedot.
- Työkalut datan lisäyksiin, muokkauksiin ja poistoon.
- Järjestelmästä joka säätelee käyttäjän käyttöoikeudet.
- Tilintarkastus- ja raportointi järjestelmästä. (Waters)

Käyttäjien käyttöoikeuksien säätelyyn voi liittyä useita todentamis menetelmiä kuten salasanat, digitaaliset sertifikaatit ja älykortit. Laitteistotunnukset ja älykortit ovat toimineet yhtenä komponenttina kahden tekijän autentikoinnissa joka sisältää käyttäjän tietämän salasanan tai tunnuksen  jolla voidaan tarkistaa käyttäjän henkilöllisyys. Älykortti kuljettaa upotettua integroitua piiriä joka voi olla joko turvallinen  mikroohjain tai älykäs sisäinen muisti tai muisti siru. (Waters)

## 2.7 Identiteetinhallinnan toteuttamisen haasteet.

Identiteetinhallinta on luonnostaan haastava. Järjestelmissä olevilla sovelluksilla voi todennäköisesti olla oma data hakemisto ja autentikointi menetelmä. Sovellusten käyttämä identiteetti data ei ole välttämättä järjestelty standardin mukaisesti.

Onnistunut identiteetinhallinnan toteuttaminen vaatii ennakko harkintaa. Organisaatiot jotka luovat yhtenäisen hallinta strategian ja selkeät tavoitteet ennen prosessin alkua, onnistuvat prosessissa todennäköisemmin.

Keskitetetyt toiminnot voivat kiinnittää hakkereiden ja krakkerin huomion. Tuomalla hallintaan kaikki organisaation identiteetinhallinta aktiviteetit, vähentävät monimutkaisuutta muillekin kuin administrattorille. Kun tietoturva on vaarassa niin tunkeutuja voi mahdollisesti luoda  tunnukset ja siihen laajat käyttöoikeudet jolla hän pääsee käsiksi organisaation resursseihin. (Waters)

## 2.8 Markkinoilla olevia identiteetinhallintajärjestelmiä

Markkinoilla on olemassa paljon eri valmistajien identiteetinhallinta ratkaisuja Microsoftin Fore Front Identity managerin lisäksi. Tässä osiossa esitellään lyhyesti neljä kaupallista ja neljä open source identiteetinhallintajärjestelmää.

Kaupalliset:

### 2.8.1 Oracle Identity Management:

Oracle Identity Management on kokonainen ja integroitu, seuraavan sukupolven identiteetinhallinta-alusta joka tarjoaa läpimurrollisen skaalautuvuuden jonka avulla organisaatiot voivat turvata arkaluonteisia sovelluksia ja tietoja riippumatta siitä, ovatko ne isännöity paikallisesti vai pilvessä. (Oracle)

Oracle Identity Management tarjoaa luokkansa parhaan sarjan identiteetinhallinnan ratkaisuja joka mahdollistaa organisaatioissa yksinkertaistetun identiteetin elinkaaren hallinnan ja turvallisen pääsyn resursseihin laitteesta tai palomuurista riippumatta. (Oracle)

Oracle Identity Managementin Ominaisuuksia:

- Pääsynhallinta: Oracle Identity Management: on rakennettu modernille arkkitehtuurille joka antaa asiakkaalle joustavuutta toimittamalla kattavia ratkaisuja mm. tunnistautumiseen, kerta kirjautumiseen, valtuuttamiseen, mobiili kirjautumiseen ja identiteettien lisääntymiseen verkon toiminta alueella. (Oracle)

- Identiteetinhallinta: Oracle Identity Manager tarjoaa kattavan alustan mm. käyttäjän rekisteröitymiseen, roolin elinkaaren hallintaan, varauksiin ja etuoikeutettuun tilin hallintaan. (Oracle)

- Hakemistopalvelut: Oracle toimittaa alan ainoan integroidun hakemisto ratkaisun joka on optimoitu pilvi, mobiili, ja sosiaalisiin ympäristöihin. Laajoilla hakemisto ominaisuuksilla kuten identiteetin virtuaalisoinnilla, varastoinnilla ja synkronointi palveluilla, Oracle tarjoaa tehokasta suorituskykyä monentasoisille yrityksille. (Oracle)

### 2.8.2 IBM Security Identity manager:

IBM Security Identity Manager mahdollistaa organisaatioiden harjoittaa tehokasta identiteetinhallintaa ja hallinnointia koko yrityksessä. Tämä ratkaisu auttaa vahvistamaan sääntelyiden noudattamista ja turvallisuutta vähentämällä identiteetti varkauden riskiä.

IBM Security Identity Manager automatisoi mm. käyttäjän luomisen, muokkaamisen, uudelleen sertifioinnin, käyttöoikeuksien lopettamisen ja se tukee sääntöpohjaista salasanan hallintaa koko käyttäjän elinkaaren ajan. Se sisältää myös liiketoimintaan sopivan käyttöliittymän ja raportointi työkalut jotka auttavat järjestelmänvalvojia tekemään parempia hallintoa koskevia päätöksiä. (IBM)

IBM Security Identity Managerin ominaisuudet:

- Antaa hallinnoijille oikeuden automatisoida ja määritellä käyttäjän pääsyn organisaation resursseihin
- Yksinkertaistaa organisaation identiteettien hallintaa keskitetyillä käytännöillä, integroiduilla rooleilla ja käyttäjän elinkaaren hallinnalla.
- Parantaa käyttäjän tunnistamista vahvalla tunnistautumisella ja aktiviteettien valvomisella.
- Tarjoaa tehokkaan ja käytännöllisen valvonnan keskitetyllä identiteetin- ja pääsynhallinnalla koko yrityksessä.
- Vähentää identiteetinhallinnan monimutkaisuutta (IBM)

### 2.8.3 CA Identity Minder

CA Identity Minder toimittaa yhtenäisen ratkaisun oikeuksien ja käyttäjien hallintaan joka hallinnoi käyttäjän identiteettiä sen koko elinkaaren ajan tarjoamalla asianmukaisen ja riittävän pääsyn sovelluksiin ja tietoihin. (CA Technologies)

CA käyttäjän oikeuksien hallinta ja käyttäjän itsepalvelu ratkaisu tarjoaa organisaatiolle kyvyn virtaviivaistaa käyttäjien oikeuksia hallintaa ja hallinnoida itsepalvelu pääsy pyyntöjä paikallisiin sovelluksiin ja pilvi palveluihin. (CA Technologies)

CA Identity Minder tarjoaa työntekijöille, urakoitsijoille ja kumppaneille pääsyn sovelluksiin ja tietoihin sinä päivänä kun he aloittavat työt, ja annetut oikeudet on helppo poistaa kun he poistuvat organisaatioista tai heidän työnkuvansa vaihtuu. (CA Technologies)

CA Identity Minder Ominaisuuksia:

- Käyttäjän oikeuksien hallinta: Automatisoi tilin oikeudet ja oikeuksien poiston koko käyttäjän elinkaaren ajan.

- Muokattavat hyväksyttävät työnkulut: Joustavat työnkulut voivat tukea ainutlaatuisella tavalla tapaa jolla organisaatiot hyväksyvät, hälyttävät ja ajoittavat identiteettiin liittyviä aktiviteetteja.

- Käyttäjän itsepalvelu: Mahdollistaa käyttäjän hallinnoida omia identiteettejään, vaihtaa salasanaa ja vaatia pääsyä resursseihin.

- Mobiili sovellus: Alkuperäinen mobiili sovellus joka mahdollistaa käyttäjien suorittaa yleisiä identiteettiin liittyviä toimintoja kuten salasanan itsehallinta toiminnot.

- Laaja sovellus tuki: Paikalliset ja pilvi palvelut. (CA Technologies)

### 2.8.4 Net IQ Identity Manager

Identity Manager tarjoaa kattavan ja edullisen ratkaisun hallinnoimaan yrityksen resurssien pääsyä palomuurin sisällä ja pilvi-palveluissa. Se mahdollistaa yritysten tarjota turvallisen ja kätevän pääsyn kriittiseen tietoon yrityskäyttäjille, samalla kun noudatetaan säädettyjä vaatimuksia. (Net IQ)

Net IQ Identity managerin ominaisuuksia:

- Parantaa turvallisuutta ja sääntöjen noudattamista: Identity Manager valvoo kulunvalvontaa fyysisissä, virtuaalisissa ja pilvi-palveluissa.

- Parantaa liiketoiminnan joustavuutta: Identity Manager keskittää pääsynhallinnan ja varmistaa että jokaisella käyttäjällä on vain yksi identiteetti. Identity Managerin kerta kirjautumisen ominaisuus mahdollistaa useiden sovelluksien käyttämisen yhden kirjautumisen jälkeen.

- Alentaa kokonaiskustannuksia mm keskitetyllä identiteetti varastolla, laajalla sovellustuella ja itsepalvelu työkaluilla.

- Täydellinen pilvi-valmius: Laajentaa identiteetinhallinnan toimialutta SaaS-palveluihin ja muihin palomuurin ulkopuolella oleviin resursseihin.. (Net IQ)

Open Source:

### 2.8.5 Open IAM Identity Manager

Open IAM Identity Manager automatisoi identiteettienhallinnan laitteissa ja sovelluksissa joita organisaatio käyttää. Tämä sisältää sovellukset kuten Active Directory ja Exchange, ja pilvi-pohjaiset sovellukset kuten Google Apps. (Open IAM)

Uusien työntekijöiden ei enää tarvitse odottaa pääsyä tarvittaviin resursseihin yrityksiin liittyessä. Työntekijän poistuessa yrityksestä annetut oikeudet poistetaan yrityksen käytännön mukaisesti jolla varmistetaan se että ulkopuolille käyttäjille ei anneta pääsyä yrityksen resursseihin. (Open IAM)

Open IAM Identity Manager ominaisuuksia

- Oikeuksien antaminen ja poistaminen, työnkulut
- Salasanojen hallinta, salasana käytännöt, synkronointi
- Itsepalvelu, mahdollistaa lukittujen käyttäjien tilien palauttamisen ja profiilien hallinnan
- Tunnistautuminen, vahvistaminen ja raportointi
- Delegoitu hallinta
- Integroituu saumattomasti Open IAM Access Managerin kanssa käyttäen jaettuja palveluja ja yhteistä tietolähdettä. (Open IAM)

### 2.8.6 Shibboleth Identity Provider

Identity Provider tarjoaa kertakirjautumis palveluita ja se ulottuu toisiin organisaatioihin ja uusiin palveluihin käyttäjän tunnistuksen avulla ja tarjoamalla asianmukaista tietoa vastaamaan palvelujen pyyntöihin. Yksinkertaisen kyllä/ei autentikoinnin lisäksi Identity Provider tarjoaa laajan valikoiman käyttäjä-kohtaista tietoa palvelun tarjoajalle. Tämä tieto voi auttaa palveluita tarjoamaan henkilökohtaisemman käyttäjäkokemuksen, säästää käyttäjän manuaaliselta tiedon lisäämiseltä palveluun ja päivittää tietoja joka kerta kun käyttäjä kirjautuu palveluun. (Shibboleth)

Shibboleth Identity Provider ominaisuuksia

- Tukee mm. LDAP, Kerberos ja verkko serveri pohjaisia autentikointi järjestelmiä.
- Tukee käyttäjän tiedon lukemista LDAP hakemistoista ja relaatiotietokannoista ja tekemällä yksinkertaisia tai monimutkaisia muunnoksia hankittuun tietoon.
- Vapauttaa vain valittua tietoa ja varmistaa sen perille pääsyn turvallisesti.
- Erinomainen skaalautuvuus, yksi istunto pystyy käsittelemään miljoonia autentikointipyyntöjä päivässä ja voi kommunikoida tuhansien palveluntarjoajien kanssa.
- Toimii kaikkien tunnettujen SAML toteutuksien kanssa.
- Dokumentoitu ohjelmointirajapinta mahdollistaa ohjelmiston tukemaan mukautettuja palveluita. (Shibboleth)

### 2.8.7 Gluu Server

Gluu Server on ilmainen ja avoimen lähdekoodin pääsynhallinta työkalu joka on kirjoitettu pääasiassa java ja python ohjelmointi kielillä. Gluu Server yhdistää avoimen lähdekoodin identiteetin- ja pääsynhallinnan ohjelmia helpolla hallinnalla ja se on suunniteltu tukemaan yrityksien vaatimuksia käytettävyydestä ja saatavuudesta. (Gluu)

Gluu Server koostuu komponenteista joista jokainen täyttää eri vaatimuksen:

- **Shibboleth** tarjoaa kertakirjautumis palvelun
- **Asimba SAML Proxy** mahdollistaa organisaation yhdistää saapuvan SAML autentikoinnin identiteetin tarjoajan kumppaneilta verkkosivustoon tai sovellukseen.
- **oxAuth**, on alan johtava UMA (user managed access) valtuuttaja serveri
- **Gluu OpenDJ LDAP** on Gluun kokoama ja tuettu versio OpenDJ:stä joka tarjoaa pysyvyyttä Gluu-serverille.
- **oxTrust** on serverin hallinnointi sovellus. (Gluu)

Gluu Serveri voidaan ottaa käyttöön klustereissa ja sitä voidaan skaalata horisontaalisesti tarjoamaan, maantieteellisesti hajautettua todentamis- ja valtuutus palvelua. Servereitä voi poistaa tai lisätä klusterin sisällä ilman että palvelu keskeytyy. (Gluu)

### 2.8.8 Open AM ja Open IDM

Open AM ja Open IDM kuuluvat Forgerock:in identiteetinhallinta ratkaisuun joka koostuu neljästä komponentista. Open AM ja Open IDM lisäksi kokoelmaan kuuluu OpenDJ hakemistopalvelu ja Open IG on ohjelmointi rajapinta jolla vanhat ja uudet sovellukset saadaan identiteetinhallinnan piiriin ilman että sovelluksiin tarvitsee tehdä muutoksia. (Forgerock )

Open AM

Open AM on suunniteltu jo valmistusvaiheessa tarjoamaan palveluja mm. verkko, pilvi ja mobiili sovelluksiin. Open AM:lla on erittäin skaalautuva, modulaarinen ja helposti käyttöön otettava arkkitehtuuri joka sisältää ominaisuudet kuten todentamisen, kertakirjautuminen (SSO), valtuuttamisen, mukautuvan todentamisen, vahvan todentamisen ja verkkopalvelujen suojauksen. (Forgerock )

Open IDM

Open IDM mahdollistaa organisaatioiden automatisoida käyttäjän elinkaaren hallinnan reaaliajassa, sisältäen käyttäjän tilien ja käyttöoikeuksien hallinnan sovelluksissa. Open IDM on suunniteltu auttamaan organisaatioita varmistamaan käytäntöjen ja sääntöjen noudattamisen yritys, pilvi, sosiaalisissa ja mobiili ympäristöissä, ja se sopeutuu nykypäivän identiteettien suhteiden hallinnointi haasteisiin helposti. (Forgerock )

# 3 MICROSOFT FOREFRONT IDENTITY MANAGER

Forefront identity manager (FIM) pyrkii muuttamaan identiteetinhallinnan nykytilaa tarjoamalla itsepalvelu työkaluja loppukäyttäjälle. IT- ammattilaisille on myös tarjolla monenlaisia työkaluja kuten delegoitu hallinta ja työnkulkujen luominen yleisille identiteetinhallinta tehtäville. FIM 2010 on rakennettu .NET ja WS-* sovellus alustalle jotta ohjelmistokehittäjät voivat rakentaa entistä räätälöidympiä ja laajennettavia ratkaisuja. (Microsoft)

FIM 2010 tarjoaa ratkaisuja käyttäjienhallintaan ja pääsyynhallintaan tukemalla salasanoja, sertifikaattipohjaisia identiteettejä kuten älykortteja ja identiteetti pohjaisia käytäntöjä jotka ovat hajautettuna Windows- ja heterogeenisissä ympäristöissä.(Microsoft)

Käytäntöjen hallinta

FIM 2010 luo viitekehyksen automatisoimalla ja integroimalla identiteetinhallinnan jotta kaikki yrityksen järjestelmät voivat käyttää samoja käytäntöjä. Tämä tapahtuu seuraavilla ominaisuuksilla: (Microsoft)

- **Keskitetty käytäntöjen valtuuttaminen, valvonta ja tarkistus.**
  Järjestelmänvalvojat voivat hallita käyttäjiä ja ryhmiä koskevia käytäntöjä valikko pohjaisen työkalun avulla, joka vähentää vaatimustenvastaisuuden riskiä.

- **Laajennettavat Windows Workflow pohjaiset työnkulut.**
  Järjestelmän valvojat voivat käyttää näitä työnkulkuja käyttäjätilien luomisessa, tehtävien delegoinnissa ja muissa samankaltaisissa tehtävissä. Työnkulkuja voi myös helposti laajentaa toimittamaan monimutkaisia mukautettuja työnkulkuja

Kirjautumistietojen hallinta

FIM 2010 integroi järjestelmien valvojien ja loppukäyttäjien hallinnan käyttämällä seuraavia ominaisuuksia. (Microsoft)

- **Käyttäjätietojen elinkaaren hallinta integroituna varauksiin**.
  IT-ammattilaiset voivat hallita varaus prosesseja ja käyttäjätietoja yhdellä työkalulla.

- **Keskitetty useiden käyttäjätietojen hallinta.**
  Microsoftin ja kolmannen osapuolien todistukset viranomaisille.

- **Salasanojen sykronointi**
  Salasanojen synkronointi kaikissa käytetyissä järjestelmissä mahdollistaen yksinkertaisen kertakirjautumisen.

- **Intuitiiviset windows työpöydälle rakennetut ominaisuudet**
  Käyttävät voivat kirjautuessa palauttaa salasanat ja hallinnoida käyttämiään älykortteja.

Käyttäjien hallinta

FIM 2010 tarjoaa työkalut tehokkaampaan käyttäjien hallintaan. Näitä työkaluja ovat mm: (Microsoft)

- **Paranneltu käyttäjien hallinta työkalu**
  Automatisoitu käyttäjätilien hallinta käyttöliittymällä monimutkaisen koodin kirjoittamisen sijasta.

- **Integroitu käyttätietojen, identiteettien ja resurssien hallinta.**
  Järjestelmänvalvojat voivat käyttää FIM 2010:ä luomaan käytäntöjä jotka hallinnoivat sujuvasti asianmukaiset tilit, resurssit ja kirjautumistiedot.

- **Profiilien itsenäinen hallinta käyttäjille.**
  Järjestelmänvalvojat voivat pyytää käyttäjää päivittämään jotain profiilitietoa tai vaatia käyttäjän hyväksyntää käyttäjätietoja muutettaessa. Käyttäjät voivat myös etsiä muiden käyttäjien profiileja tällä työkalulla.

Ryhmien hallinta

FIM:in ryhmien hallinta auttaa lisäämään loppukäyttäjien työn tuottavuutta, vapauttaa järjestelmänvalvojat toistuvista identiteetinhallinta tehtävistä ja tarjoaa paremman tietoturvan seuraavalla ominaisuudella: (Microsoft)

- **Itsepalvelu ryhmien hallintatyökalut ovat integroituina MS Officeen ja Sharepointtiin.**
  Näiden avulla käyttäjät voivat hallinnoida ryhmien jäsenyyksiä tuttujen ohjelmistojen avulla**.**

- **Automatisoidut dynaamiset päivitykset ryhmiin ja jakelu ryhmiin.**
  Järjestelmän valvojat voivat käyttää FIM 2010 hallinta työkaluja luomaan käytäntöjä, jotka pitävät ryhmät ja jakelu ryhmät ajantasalla automaattisesti.

## 3.1 Forefront identity managerin komponentit

Forefront identity manager koostuu useista eri komponenteista. Tässä osiossa tarkastellaan Forefront Identity managerin komponentteja ja niiden toimintoja.

### 3.1.1 IDM Platform (Identity Management Platform)

IDM alusta koostuu FIM palvelusta (FIM Service) ja FIM synkronointi palvelusta. FIM palvelu tarjoaa putken käsiteltäville pyynnöille jotka kulkevat eri työnkulkujen kautta ja se ohjaa mitä synkronointi palvelussa tapahtuu. FIM synkronointi palvelu kommunikoi eri tietolähteiden kanssa käyttämällä hallinta agentteja (management agents). Tietolähteet ovat joko identiteetti varastoja tai jokin yhdistetty tietokanta/tietolähde. (Calderon, Lundell, Turner, Zamora. 2010.)

Esimerkiksi henkilöstö-osasto joutuu päivittämään tietoihinsa jonkun työntekijän saaman ylennyksen. Henkilöstö-osasto päivittää tiedon oman hallinta paneelinsa kautta henkilöstö-osaston tietokantaan joka on yhteydessä FIM:iin. Sen jälkeen FIM synkronointi palvelu kuljettaa päivitetyn tiedon henkilöstö-osaston hallinta agetin läpi ja tieto menee henkilöstö-

osaston tietokantaan. Tämä tuo päivitetyn tiedon FIM synkronointipalvelun ulottuville jonka jälkeen se päivittää muuttuneen tiedon FIM:n keskushakemistoon ja tuo tiedon ns. taukopaikalle josta tieto siirtyy Active Directoryyn ja FIM palveluun. (Calderon, Lundell, Turner, Zamora. 2010.)

### 3.1.2 FIM Service (FIM palvelu)

FIM palvelu tarjoaa verkkopalvelu putken joka vastaa mm. seuraavista asioista.

- **Pyyntöjen käsittely**
  Kaikki pyynnöt jotka ovat toimitettu verkkopalvelun päätepisteeseen käsitellään FIM serverissä ja siihen sisäänrakennetussa toimintatapa moottori(policy engine).

- **Isännöi työnkulkuja(workflow)**
  FIM-server isännöi kaikkia Windows työnkulkuja joita toimintatapa moottori toteuttaa sillä hetkellä. FIM mahdollistaa myös sen, että pitkään käynnissä olevat työnkulut voidaan täysin poistaa muistista.

Pyynnöt syötetään FIM-palveluun verkkopalvelun avulla. Kaikki tulevat pyynnöt arvioidaan, jotta voidaan päätellä onko pyytäjällä oikeus toteuttaa pyydetty toiminta. Pyynnöt myönnetään hallinnan käytännön sääntöjen avulla. (Management Policy Rules). Näitä sääntöjä voidaan myös käyttää eri työnkulkujen toimeenpanossa. (Calderon, Lundell, Turner, Zamora. 2010.)

### 3.1.3 FIM Syncrohronization Service (FIM synkronointi palvelu)

FIM synkronointi palvelu on keskeinen kompononentti joka hoitaa tiedon synkronoinnin eri tietolähteiden välillä. Synkronointi palvelu kokoaa yhteen tietoa identiteeteistä ja tarjoaa tavan yhdistää eri tietolähteitä ilman välivaihetta. FIM- synkronointi palvelu toteuttaa identiteettien luonnin ja ylläpidon niissä ympäristöissä joissa FIM-serveri vaikuttaa. (Calderon, Lundell, Turner, Zamora. 2010.)

### 3.1.4 FIM-Clients (FIM asiakasohjelmat)

FIM arkkitehtuurissa voi olla monentyyppisiä asiakasohjelmia( Clienttejä) jotka voivat olla mm. Outlookin lisäosa, salasanan resetointiin tarkoitettu lisäosa, hallinta portaali tai jokin kustomoitu asiakasohjelma kuten HR manager. Alla olevassa luettelossa kerrotaan eri eri asiakasohjelma tyypeistä. (Calderon, Lundell, Turner, Zamora. 2010.)

- **FIM-Synkronointipalvelu**
  Suurin osa pynnöistä tulee itse synkronointipalvusta ku tiedot päivittyvät eri tietolähteistä.

- **FIM portaali**
  Käyttäjät voivat käyttää portaalia internet-selaimella. Riippuen käyttöoikeuksista, käyttäjät voivat tehdä pyyntöjä, vastata hyväksyttyihin pyyntöihin tai peruuttaa olemassa olevia pyyntöjä.

- **Exchange 2007/2010 ja Outlook 2007 (joissa on FIM- lisäosa Outlookille)**
  Organisaatioissa joissa on käytössä vähintään yksi Exchange 2007 tai 2010 serveri jossa on käytössä FIM:n outlookille tarkoitettu apuohjelma, voidaan käyttää Outlookkia pyyntöjen hyväksymiseen, hylkäämiseen, ryhmiin liittymiseen ja ryhmistä eroamiseen. Tämä voidaan hoitaa ilman että käyttäjän tarvitsee poistua Outlook kokemuksesta.

- **Salasanan nollaukseen tarkoittettu asiakasohjelma (FIM asiakasohjelma asennettuna)**
  Kun FIM asiakasohjelma on otettu käyttöön Windows XP SP2, Windows Vista tai Windows7:ssa, kirjautumis ikkunaa on muokattu siten että käyttäjä voi halutessaan nollata salanansa kirjautumis ikkunasta suoraan. Salasanan nollauksen voi hoitaa myös FIM portaalin kautta.

- **Powershell**
  Powershell asiakasohjelmia voidaan käyttää tuomaan hallinta käytäntöjä ja muita objecteja FIM-palvelun tietokannasta johonkin muuhun käyttöön.

- **Kustomoitavat asiakasohjelmistot**
  Ohjelmistokehittäjät voivat luoda omia powershell asiakasohjelmia joiden avulla he voivat olla vuorovaikutuksessa verkkopalvelun kanssa ja aloittaa pyyntöjä.

### 3.1.5 FIM Certificate Management ( FIM Sertifikaattien hallinta)

FIM Sertifikaattien hallinta koostuu sertifikaattien hallinta tietokannasta (Certificate Management Database) ja sertifikaattien hallinta portaalista. Sertifikaattien hallinta tietokanta pitää yllä työnkulut(workflows), sertifikaattien tiedot ja sertifikaattien hallinta portaali sisältää FIM moduulit jotka asentuvat sertifikaatti palvelimille ja ovat vuorovaikutuksessa FIM sertifikaattien web hallinta portaalin kanssa. FIM sertifikaattien hallinta palveluita kutsuttiin ennen sertifikaatin elinkaaren hallinta palveluksi (Certificate Lifecycle Manager). (Calderon, Lundell, Turner, Zamora. 2010.)

## 3.2 Forefront identity managerin arkkitehtuurin edellytykset

Tässä osiossa käydään läpi mitä edellytyksiä FIM:n eri komponentit tarvitsevat toimiaikseen. Kaikki komponentit tarvitsevat 64-bittisen version Windows server 2008:sta tai Windows server 2008 R2:sta.

| **Serverin komponentti** | **Edellytykset** |
|---|---|
| FIM Synchronization Service | Windows installer 4.5,<br>Windows Powershell 1.0 or 2.0,<br>Microsoft.NET Framework 3.5 Service Pack 1 |
| FIM Synchronization SQL Server | SQL Server 2008 SP1 x64 Standard or Enterprise |
| FIM Service | Windows Installer 4.5<br>Windows PowerShell 1.0 or 2.0<br>.NET Framework 3.0 Features<br>.NET Framework 3.5 SP1 |
| FIM Service SQL Server | SQL Server 2008 SP1 x64 Standard or Enterprise joka sisältää koko tekstin haku toiminnon |
| FIM Portal | Windows SharePoint® Services 3.0 SP1 or SP2<br>.NET Framework 3.0 ominaisuudet<br>.NET Framework 3.5 SP1<br>Windows SharePoint Services 3.0 kieli paketti |
| FIM Password Reset Portal | Samat edellytykset kuin FIM-portaalilla |

Taulukko 1 (Calderon, Lundell, Turner, Zamora. 2010.)

# 4 FOREFRONT IDENTITY MANAGERIN TESTAUS KÄYTÄNNÖSSÄ

Tässä osiossa käsitellään opinnäytteen käytännön osuutta, sen tavoitteesta, työ tavoista, kohdatuista ongelmista ja lopputuloksesta. Osiossa esitellään myös lyhyesti työn toimeksiantaja.

## 4.1 Toimeksiantaja Kainuun ammattiopisto

Kainuun ammattiopisto järjestää toisen asteen koulutusta nuorille ja aikuisille. Kainuun ammattiopisto toimii valtakunnallisesti ja sillä vakituisia toimipaikkoja Kajaanissa, Kuhmossa, Kuusamossa ja Vuokatissa. Kainuun ammattiopistossa opiskelee vuosittain noin 2600 nuorta ja aikuista. Muussa aikuiskoulutuksessa opiskelee noin 5000 aikuista. Työntekijöitä Kainuun ammattiopistossa on lähes 450 ja ammattiopiston liikevaihto oli noin 43.6 miljoonaa euroa vuonna 2013. Kainuun ammattiopisto on osa Kajaanin kaupungin koulutusliikelaitosta joka koostuu Kainuun ammtiopistosta ja Kajaanin lukiosta. (Kainuun ammattiopisto)

Ammattiopistolla ja lukiolla on tällä hetkellä asiakkaita noin 4400 ja työasemia noin 3500. Kainuun ammattiopiston tietohallinto on yhdistymässä Kajaanin ammattikorkeakoulun ja perusopetuksen tietohallintojen kanssa yhdeksi suureksi kokonaisuudeksi. Uuden tietohallinnon asiakasmäärä tulee olemaan noin 10700 asiakasta ja ylläpidettäviä työasemia on noin 4800. Yhdistymisen tavoitteena on tarjota koko Kajaanin koulutoimialalle yhteinen tietojärjestelmä, jossa Microsoftin Forefront Identity Managerilla on keskeinen tehtävä organisaatioiden ja eri järjestelmien käyttäjätunnusten hallinnassa.

## 4.2 Tavoite

Käytännön osuuden tavoitteena on tutkia Forefront Identity managerin ominaisuuksia jotta Kainuun ammattiopisto saisi kuvan siitä mihin identiteetinhallintajärjestelmää voi käyttää ja miten se hyödyttäisi uutta yhdistettyä tietohallintoa.

## 4.3 Testaus menetelmät

Työn alkuperäinen testaus menetelmä oli rakentaa demo ympäristö koulumme tietojärjestelmä laboratorioon yhdessä toisen saman vuosikurssin opiskelijan kanssa joka teki myös opinnäytetyötä Kainuun ammattiopistolle Sharepoinstista. Toimivan FIM demo ympäristön asentaminen osoittautui ongelmaksi koska en saanut toimivaa FIM ympäristöä aikaseksi joten jouduin siirtymään toiseen testaus menetelmään.

Lopullinen testaus menetelmä löytyi Microsoftin virtuaali laboratoriosta josta löytyi erilaisia demo scenaarioita joita pystyi suorittamaan Microsoftin virtuaali koneilla. Suoritin Forefront Identity manageria koskevat virtuaali laboratoriot ja raportoin testauksen dokumentaatioon joka löytyy liitteistä (LIITE1).

## 4.4 Testatut ominaisuudet

Microsoftin virtuuali laboratoriossa oli rajallinen määrä demo scenaarioita jonka vuoksi päädyin testaamaan seuraavia FIM:n ominaisuuksia.

Käyttöliittymän esittely

- Käyttöliittymästä kävin läpi FIM portaalina ja Fim synchronization service managerin käyttöliittymät

- Käyttäjien hallinta FIM-portaalissa. Keskitetty hallinta yksinkertaistaa käyttäjien hallintaa tuomalla kaikki identiteetit yhden hallintapaneelin alle.
    - Käyttäjien hallinnasta kävin läpi uuden käyttäjän luomisen, FIM setit, Management Policy Rules(MPR), käyttäjän scheman muokkaamisen ja ryhmien jäsenyyden hallinnan.
- Active Directory käyttäjien synkronointi. Käyttäjien synkronointi tuo kaikki hallinnoitavat identiteetit Active Directorysta yhden hallinnan alle helpottaen niiden hallintaa.
    - AD käyttäjien synkronoinnista kävin läpi Management agentit, run profiilit, synkronointi säännöt, työnkulut, uuden säännön tuonnin ja käyttäjätietojen synkronoinnin.
- Salasanan vaihtaminen itsepalvelu työkalulla. Salasana pyynnöt kuormittavat yleensä help-deskiä paljon ja salasanan uusiminen itsepalvelulla vähentää help-deskin työtaakkaa.
    - Salasana työkalusta kävin läpi salasanan resetoinnin ja rekisteröinnin asetusten muokkaamisen, salasanan resetoinnin testaamisen, salasanan resetoinnin lukituksen testauksen ja PCNS:n määrittämien
- Tietojen tuonti ja synkronointi tuo kaikki hallittavat identiteetti tiedot yhden hallinnan piiriin ja identiteetteihin tehdyt muutokset päivittyvät kaikkiin identiteetin hallinnan piirissä oleviin järjestelmiin.

- Tietojen tuonti ja synkroinointi osiossa testasin HR(Human Resources) järjestelmään yhdistämistä ja tietojen tuontia, tarskastelin metaversumia ja testasin muutoksien tuontia.

## 4.5 Testauksen aikana ilmenneet ongelmat

Testaus prosessissa ilmenneet ongelmat koskevat pääasissa demoympäristöä jonka pystytys epäonnistui. Ongelmina olivat mm. FIM synkronointi palvelun sammuminen muutaman minuutin välein ilman automaattista uudelleen käynnistämistä ja yhteyden saaminen FIM:n hallintapaneeliin. Yritin ratkaista kyseisiä ongelmia monilla eri tavoilla ja asensin FIM ympäristön uudelleen useaan otteeseen mutta törmäsin aina samoihin ongelmiin. Tästä syystä päädyin vaihtamaan testaus menetelmää. Myös kesällä 2013 tapahtunut koulumme tietojärjestelmä laboratorion konesali remontti viivästytti demo ympäristön rakennusta.

Microsoftin virtuaali laboratorion kanssa työskennellessä ongelmia ilmeni vain muutama. Isoin ongelma oli yhtäkkinen yhteyden menetys FIM:n hallintapaneeliin jonka lopputuloksena jouduin alottamaan kyseisen menossa olevan demo scenaarion alusta.

## 4.6 Testauksen lopputulos

Testauksen lopputuloksena on raportti jossa on dokumentoitu useiden FIM:n ominaisuuksien testauksia ja käytännön ohjeita kyseisten ominaisuuksien toimivuuteen. Testattavaa olisi ollut enemmänkin mutta oman demoympäristön asennuksen epäonnistuttua ja Microsoftin FIM:ä koskevien virtuaali laboratorioiden vähäisyyden vuoksi päädyin tyytymään tähän määrään mitä olen saanut testattua. Testauksen perusteella FIM helpottaa identiteettienhallintaa organisaatioissa ja yksinkertaistaa identiteetinhallinta tehtäviä ja vähentää tietohallinnon työntekijöiden työtaakkoja. Omasta näkökulmasta FIM on toimiva identiteetinhallinta ratkaisu mutta sen käyttöönotto voi olla raskasta ja vaatii suunnittelua.

Toimitin FIM:n testaus dokumentaation Kainuun ammattiopistolle joulukuussa 2013. Mutta Forefront Identity managerin käyttöönottaminen siellä on vielä niin alkuvaiheessa, että testaus dokumentin hyödyllisyyttä ei pystytty vielä hahmottamaan.

# 5 JOHTOPÄÄTÖKSET

Opinnäytetyön tavoitteena oli tutkia identiteetinhallinnan tarkoitusta ja hyötyjä sekä tutkia perusteellisemmin Microsoftin identiteetinhallinan ratkaisua Forefront Identity manageria. Keskitetty identiteetinhallinta on nykyään tärkeä osa yritysen tietoturvaa ja se helpottaa useita ylläpitotehtäviä ja vähentää IT-henkilöstön työtaakkoja automatisoimalla toimintoja ja itsepalvelu työkaluilla. Nyky päivänä identiteetinhallinnan ratkaisuja on monenlaisia. Useimmat identiteetin hallinan ratkaisut ovat periaatteeltaan samanlaisia ja sisältävät samoja ominaisuuksia, joten järjestelmän valinta voi olla vaikeaa. Oikeaa ratkaisua valittaessa tärkeäksi tekijöiksi muodustuu hinta sekä järjestelmän helppokäyttöisyys.

Microsoftin Forefront Identity manager on identiteetinhallinta ohjelmisto, joka mahdollistaa monipuolisen keskitetyn identiteetinhallinnan. Johtuen FIM:n suuresta koosta ja monista komponententeista sen käyttöönotto voi olla aluksi hankalaa. Tämän opinnäyetyön perusteella voidaan todeta että, suurin haaste tulee olemaan FIM asentaminen toimintakuntoon.

Opinnäytetyön käytännön osuuden tavoitteet saatiin toteutettua lähes suunnitelmien mukaan. Tavoitteena oli testata Forefront Identity manageria rakentamalla pieni demoympäristö koulumme konesaliin jossa tavoitteena oli testata FIM:n eri ominaisuuksia ja tutkia mitä hyötyä FIM:n käyttöönotosta olisi Kainuun ammattiopistolle. Demoympäristön epäonnistuttua testaus menetelmä vaihtui Microsoftin virtuaali laboratorioon jolla testaus saatiin suoritettua loppuun.

LÄHTEET

Bloor, R., Halper, F Hurwitz, J., Kaufman, M. (2012). How to benefit from identity management in cloud computing. Retrieved 2/4, 2014, from http://www.dummies.com/how-to/content/how-to-benefit-from-identity-management-in-cloud-c.html

Calderon,C. Lundell,D., Turner,B., Zamora,J., (2010). Microsoft forefront identity manager 2010 technical overview. Retrieved 11.9, 2013, from http://technet.microsoft.com/en-us/library/ff621362(v=ws.10).aspx

CA Technologies. CA Identity Minder.Retrieved 3/9,2014, from http://www.ca.com/us/products/detail/ca-identity-manager.aspx

Forgerock. Open Identity Stack. Retrieved 4/9,2014, from http://forgerock.com/products/open-identity-stack/

Gamatech.What is identity and access management. Retrieved 11.9, 2013, from http://www.karingroup.com/eng/about/what_is_identity.pdf

Gluu. The Gluu Server Overview. Retrieved 4/9,2014, from http://www.gluu.org/gluu-server/overview/

IBM. IBM Security Identity Manager.Retrieved 2/9,2014, from http://www-03.ibm.com/software/products/en/identity-manager/

Kainuun ammattiopisto. Kainuun ammattiopisto. Retrieved 21.10.2014, from http://www.kao.fi/fi/info/kainuun-ammattiopisto.html

Linden M. Identiteetin- ja pääsynhallinta luentomoniste. Retrieved 28.10.2014 from

http://www.cs.tut.fi/~linden/iam-pruju.pdf

Microsoft.What is forefront identity manager. Retrieved 11.9, 2013, from

http://www.microsoft.com/en-in/server-cloud/forefront/identity-manager-overview.aspx

Net IQ. Identity Manager. Retrieved 4/9,2014, from

https://www.netiq.com/products/identity-manager/advanced/

https://www.netiq.com/products/identity-manager/advanced/features/

Open IAM. Open IAM Identity and Access Management. Retrieved 4/9,2014, from

http://www.openiam.com/products/identity-manager/idm-overview/

Oracle. Oracle Identity management. Retrieved 2/9,2014, from

http://www.oracle.com/us/products/middleware/identity-management/overview/index.html

Shibboleth. Shibboleth Identity Provider. Retrieved 4/9,2014, from

https://shibboleth.net/products/identity-provider.html

Silander J. Katsaus identiteetin hallinnan teknologioihin ja niiden tulevaisuuden näkymiin. Retrieved 22.10.2014, from

https://aaltodoc.aalto.fi/bitstream/handle/123456789/10426/master_Silander_Jon_2013.pdf?sequence=1

Waters, J.The ABCs of identity management. Retrieved 2/4, 2014, from

http://www.csoonline.com/article/205053/the-abcs-of-identity-management?page=1

# LIITTEET

LIITE1 Forefront Identity managerin testaus dokumentaatio

# Forefront Identity Managerin:n testaus dokumentaatio

## Sisältö


Forefront Identity Managerin esittely ..... 1

Käytäntöjen hallinta ..... 1

Kirjautumistietojen hallinta ..... 1

Käyttäjien hallinta ..... 2

Ryhmien hallinta ..... 2

Käyttöliittymän esittely ..... 3

FIM portaali ..... 3

FIM synchronization service manager ..... 5

Käyttäjien hallinta FIM-portaalissa ..... 8

Uusien käyttäjien luominen: ..... 8

FIM Set's ..... 9

Management Policy Rules (MPR) ..... 10

Käyttäjän Scheman muokkaaminen ..... 11

Ryhmien jäsenyyden hallinta: ..... 13

AD käyttäjien synkronointi ..... 14

Active directory management agentin (MA) luominen ..... 14

Run profiles ..... 16

Synkronointi säännöt ( Synchronization Rule) ..... 17

Kohde setin luominen uudelle säännölle ..... 19

Työnkulun (Workflown )luominen joka lisää tai poistaa synkronointi säännön ..... 21

Management Policy Rule (MPR) luominen käyttämään työnkulkuja (workflow) ..... 22

Uuden säännön tuonti ja itse synkronointi ..... 23

Käyttäjätietojen automaattinen  synkronointi ..... 24

FIM:n salasanan uusiminen itsepalvelu työkalulla ..... 25

Ympäristön tarkistus ja muokkaus ..... 25

Salasanan rekisteröinnin ja resetoinnin asetusten muokkaaminen ..... 26

Salasanan resetoinnin testaus käyttäjällä ..... 29

Salasanan resetoinnin lukituksen muokkaaminen ja testaus ..... 31

PCNS:n Määrittäminen (Password Change Notification Service) ..... 33

Tietojen tuominen ja synkronointi ..... 37

HR tietojärjestelmään yhdistäminen ja identiteetti tietojen tuominen ..... 37

Metaversumin tarkastelu ..... 40

Muutoksien tuonti ..... 41

# Forefront Identity Managerin esittely

Forefront identity manager (FIM) pyrkii muuttamaan identiteetin hallinnan nykytilaa tarjoamalla itsepalvelu työkaluja loppukäyttäjälle. IT- ammattilaisille on myös tarjolla monenlaisia työkaluja kuten delegoitu hallinta ja työnkulkujen luominen yleisille identiteetin hallinta tehtäville. FIM 2010 on rakennettu .NET ja WS-* sovellus alustalle jotta ohjelmistokehittäjät voivat rakentaa entistä räätälöidympiä ja laajennettavia ratkaisuja. (Microsoft Corporation)

FIM 2010 tarjoaa ratkaisuja käyttäjien hallintaan ja pääsyynhallintaan tukemalla salasanoja, sertifikaattipohjaisia identiteettejä kuten älykortteja ja identiteetti pohjaisia käytäntöjä jotka ovat hajautettuna Windows- ja heterogeenisissä ympäristöissä. (Microsoft Corporation)

## Käytäntöjen hallinta

FIM 2010 luo viihekehyksen automatisoimalla ja integroimalla identiteetin hallinnan jotta kaikki yrityksen järjestelmät voivat käyttää samoja käytäntöjä. Tämä tapahtuu seuraavilla ominaisuuksilla: (Microsoft Corporation)

- **Keskitetty käytäntöjen valtuuttaminen, valvonta ja tarkistus.**
  Järjestelmänvalvojat voivat hallita käyttäjiä ja ryhmiä koskevia käytäntöjä valikko pohjaisen työkalun avulla, joka vähentää vaatimusten vastaisuuden riskiä.

- **Laajennettavat Windows Workflow pohjaiset työnkulut.**
  Järjestelmänvalvojat voivat käyttää näitä työnkulkuja käyttäjätilien luomisessa, tehtävien delegoinnissa ja muissa samankaltaisissa tehtävissä. Työnkulkuja voi myös helposti laajentaa toimittamaan monimutkaisia mukautettuja työnkulkuja.

## Kirjautumistietojen hallinta

FIM 2010 integroi järjestelmien valvojien ja loppukäyttäjien hallinnan käyttämällä seuraavia ominaisuuksia. (Microsoft Corporation)

- **Käyttäjätietojen elinkaaren hallinta integroituna varauksiin**.
  IT-ammattilaiset voivat hallita varaus prosesseja ja käyttäjätietoja yhdellä työkalulla.

- **Keskitetty useiden käyttäjätietojen hallinta.**
  Microsoftin ja kolmannen osapuolien todistukset viranomaisille.

- **Salasanojen sykronointi**
  Salasanojen synkronointi kaikissa käytetyissä järjestelmissä mahdollistaen yksinkertaisen kertakirjautumisen.

- **Intuitiiviset windows työpöydälle rakennetut ominaisuudet**
  Käyttävät voivat kirjautuessa palauttaa salasanat ja hallinnoida käyttämiään älykortteja.

## Käyttäjien hallinta

FIM 2010 tarjoaa työkalut tehokkaampaan käyttäjien hallintaan. Näitä työkaluja ovat mm: (Microsoft Corporation)

- **Paranneltu käyttäjien hallinta työkalu**
  Automatisoitu käyttäjätilien hallinta käyttöliittymällä monimutkaisen koodin kirjoittamisen sijasta.

- **Integroitu käyttätietojen, identiteettien ja resurssien hallinta.**
  Järjestelmänvalvojat voivat käyttää FIM 2010:ä luomaan käytäntöjä jotka hallinnoivat sujuvasti asianmukaiset tilit, resurssit ja kirjautumistieodot.

- **Profiilien itsenäinen hallinta käyttäjille.**
  Järjestelmänvalvojat voivat pyytää käyttäjää päivittämään jotain profiilitietoa tai vaatia käyttäjän hyväksyntää käyttäjätietoja muutettaessa. Käyttäjät voivat myös etsiä muiden käyttäjien profiileja tällä työkalulla.

## Ryhmien hallinta

FIM:in ryhmien hallinta auttaa lisäämään loppukäyttäjien työn tuottavuutta, vapauttaa järjestelmänvalvojat toistuvista identiteetin hallinta tehtävistä ja tarjoaa paremman tietoturvan seuraavalla ominaisuudella: (Microsoft Corporation)

- **Itsepalvelu ryhmien hallintatyökalut ovat integroituina MS Officeen ja Sharepointtiin.**
  Näiden avulla käyttäjät voivat hallinnoida ryhmien jäsenyyksiä tuttujen ohjelmistojen avulla**.**

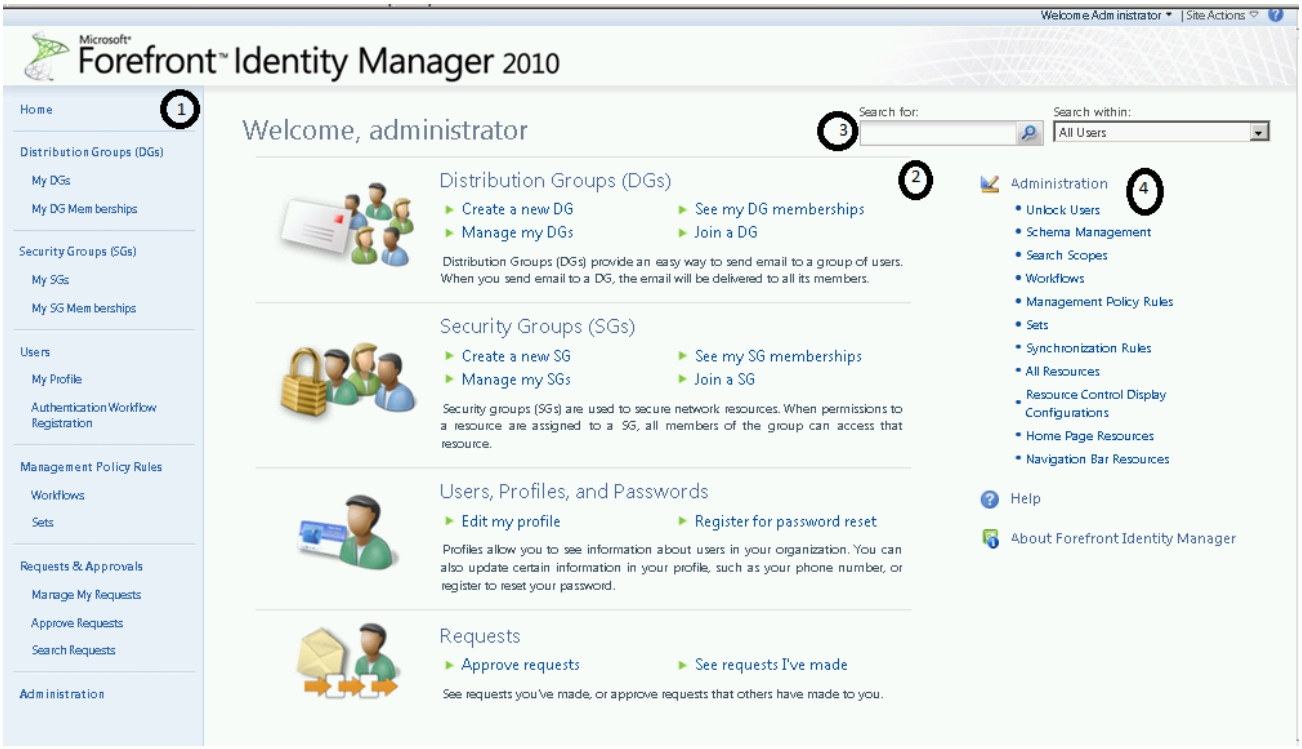
- **Automatisoidut dynaamiset päivitykset ryhmiin ja jakelu ryhmiin.**
  Järjestelmän valvojat voivat käyttää FIM 2010 hallinta työkaluja luomaan käytäntöjä, jotka pitävät ryhmät ja jakelu ryhmät ajantasalla automaattisesti.

# Käyttöliittymän esittely

Tässä osiossa on tarkoitus esitellä Forefront Identity Managerin käyttöliittymää kuvien ja kuvien selvityksien avulla. Osiossa käydään läpi FIM portaalin ja FIM synchronization service managerin käyttöliittymät.

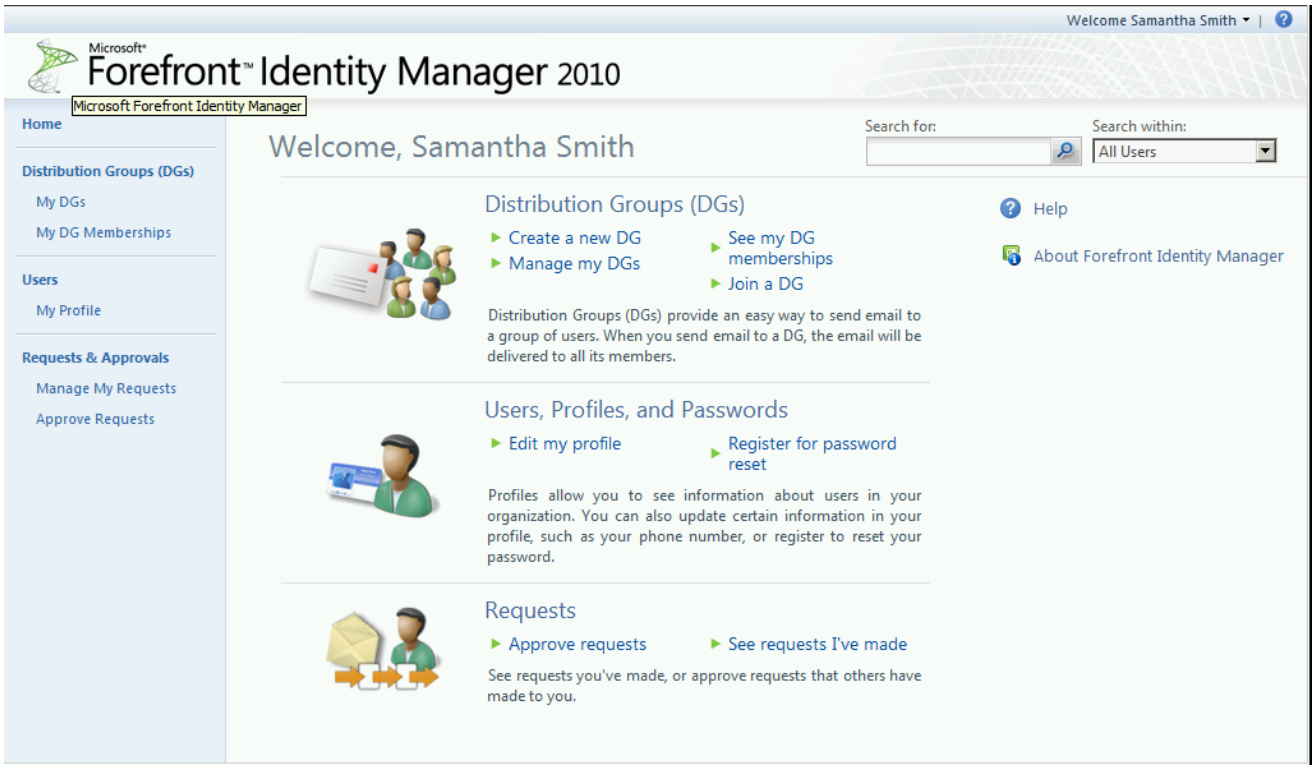
## FIM portaali

FIM portaalista käyn läpi aloitus näkymän administraattorin ja käyttäjän näkökulmasta




Kuva1: FiM portaalin Home näkymä administraattorin näkökulmasta

1. Navigointipaneeli
    a. Navigointipaneelista pääsee käsiksi kaikkiin FIM portaalin toimintoihin
2. Home sivu
    a. Sisältö muokattavissa administrator työkaluilla
    b. Oletuksena home sivustossa on jakeluryhmien toiminnot, käyttäjän profiilin ja salasanan resetoinnin toimminnot, turvallisuus ryhmät, jne.
3. Haku palkki
    a. Haku palkista voi hakea FIM sisältöä. Haku tehdään siten että ensimmäiseen palkkiin kirjoitetaan haettava asia jonka jälkeen valitaan pudotusvalikosta haun kohde.
4. Administration paneeli
    a. Sisältää administrator työkaluja kuten käyttäjien lukituksen poistaminen, scheman hallinta, resurssien hallinta, navigointipaneelin resurrsien hallinta jne. ( administrator työkalut löytyvät myös navigointipaneelin administration painikkeen alta.)

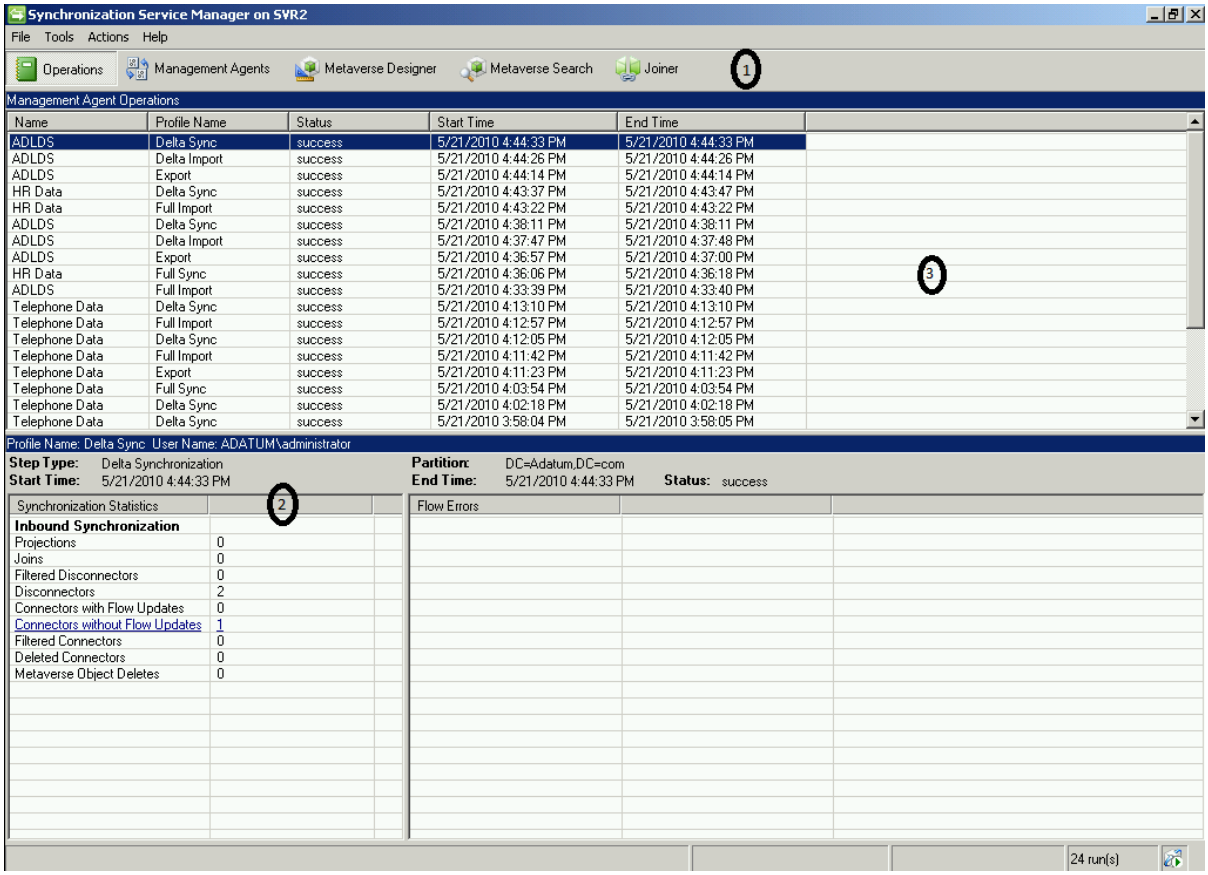



Kuva2: Normaalin käyttäjän portaali näkymä

Normaalin käyttäjän portaali:n ulkoasu on lähes sama kuin administraattorilla mutta se sisältää vain peruskäyttäjälle tarkoitetut toiminnot kuten jakeluryhmät, käyttäjätiedot, salasanan resetointi jne.

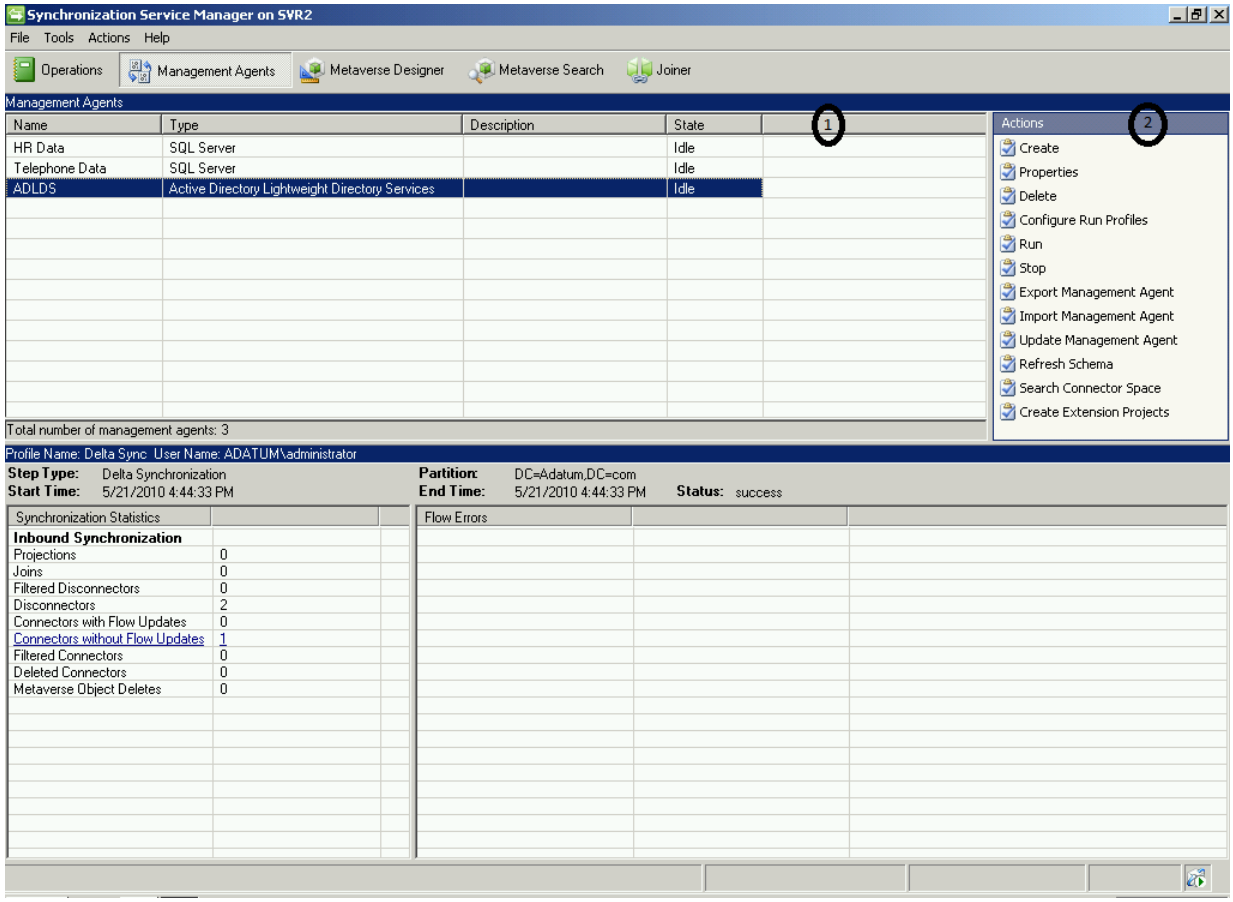
## FIM synchronization service manager

FIM Synchronization service managerista käyn läpi Operations, Management Agent ja Metaverse designer toimintojen käyttöliittymät. Metaverse search osiosta löytyy esimerkki Tietojen tuominen ja synkronointi osiosta.



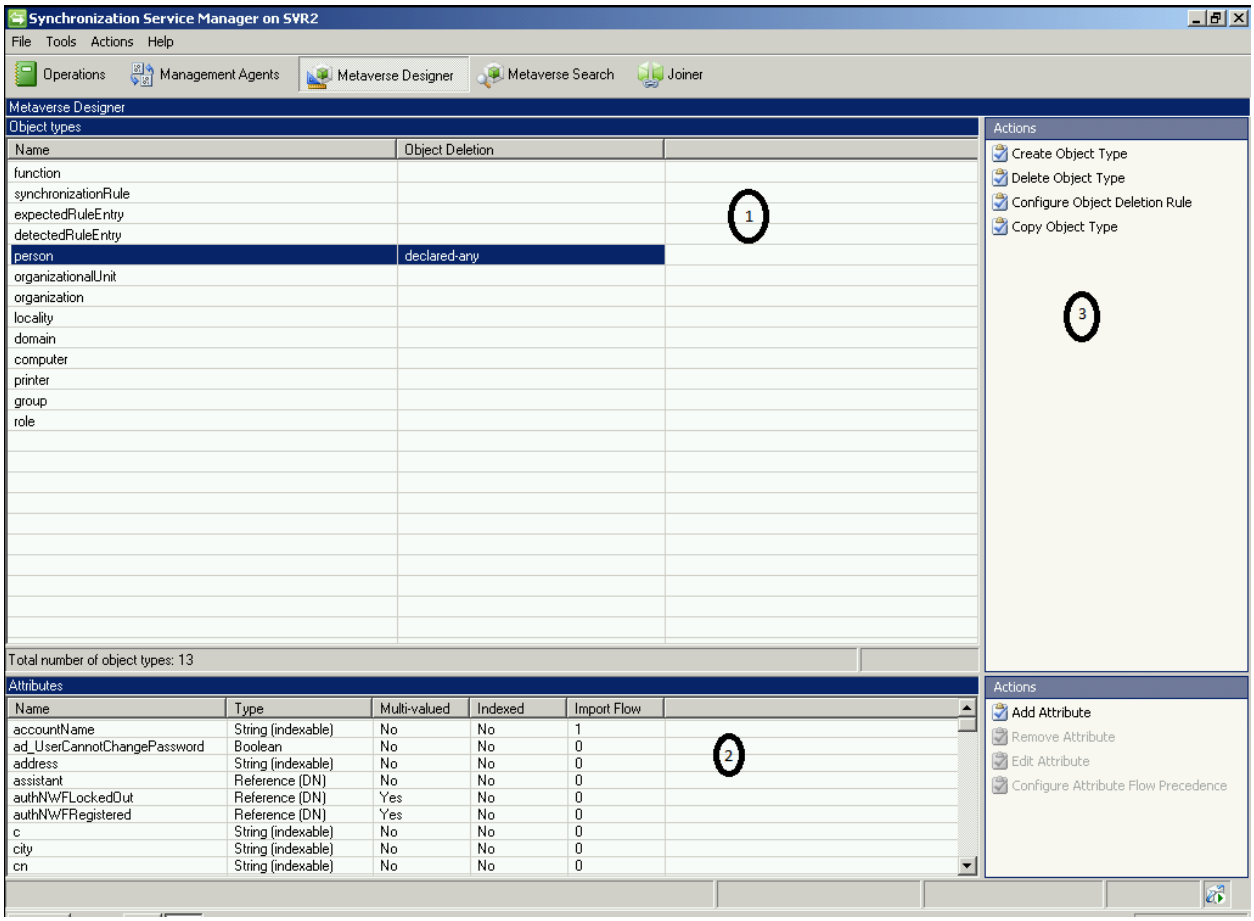

Kuva3: FIM synchronization service managerin operations välilehti

1. Navigointipaneeli
    a. Navigointipaneelista pääsee käsiksi FIM sync managerin eri toimintoihin kuten Management agenttien hallintaan, metaverse designer:iin, jne.
2. Operaation tilastot
    a. Valitun operaation tilasto tiedot josta näkee mitä operaatiossa on tapahtunut.
3. Suoritetut Management agent operaatiot
    a. Sisältää suoritettujen operaatioiden tiedot, sisältää suoritetun MA:n nimen, run profiilin, aloitus ajankohdan, jne.




Kuva4: FIM Synchronization service managerin Management Agents välilehti

1. Management Agentit
    a. Sisältää kaikki käytettävissä olevat Management Agentit
2. Actions (toiminnot)
    a. Sisältää toiminnot kuten MA:n luominen, ominaisuudet, MA:n poistaminen, MA:n suorittaminen, jne.




Kuva5: FIM synchronization service managerin Metaverse designer välilehti

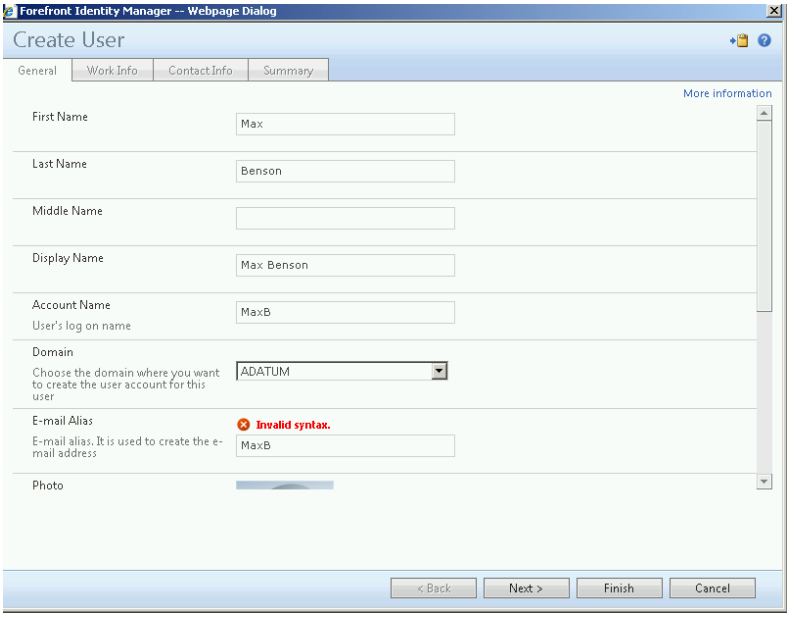
1. Objekti tyypit
    a. Sisältää metaversumin objekti tyypit kuten esimerkiksi person, domain, group ,jne
2. Valitun objektin atribuutit
    a. Sisältää valitun objecktin atribuutit ja niiden tiedot
3. Actions (toiminnot)
    a. Sisältää toiminot kuten objecti tyypin luominen, poistaminen ja kopioiminen
    b. Objekti tyypin toimintojen alapuolella on atribuuttien toiminnot joska ovat atribuuttien lisäys, poisto, muokkaus

# Käyttäjien hallinta FIM-portaalissa

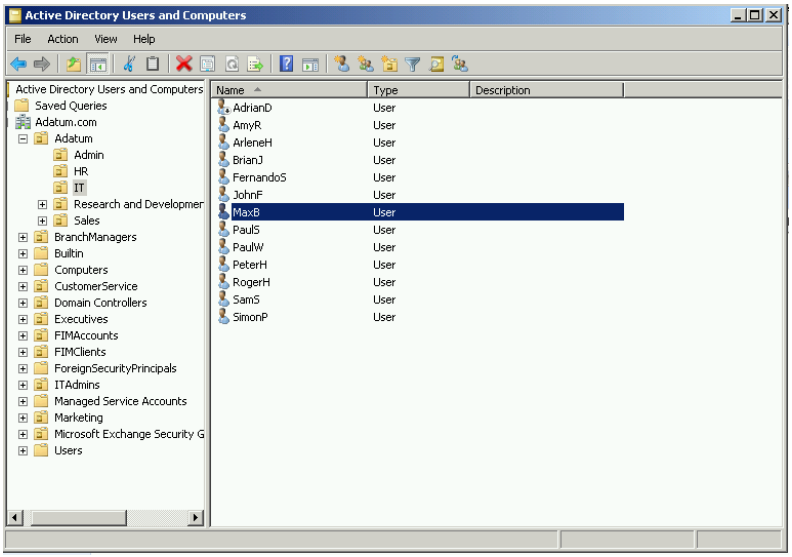
Tässä osiossa kuvataan käyttäjien hallintaan tarkoitettuja keinoja

## Uusien käyttäjien luominen:

Uusia käyttäjiä voi luoda AD:sta, FIM:n portaalista tai jollain muulla työkalulla joka kuuluu FIM:n hallintaan. Jos käyttäjä luodaan esimerkiksi portaalista niin uusi käyttäjä ilmestyy AD:seen seuraavan synkronoinnin yhteydessä. Demossa testasin käyttäjän lisäystä HR-managerin (Human recources – manager) ja FIM-portaalin kautta.



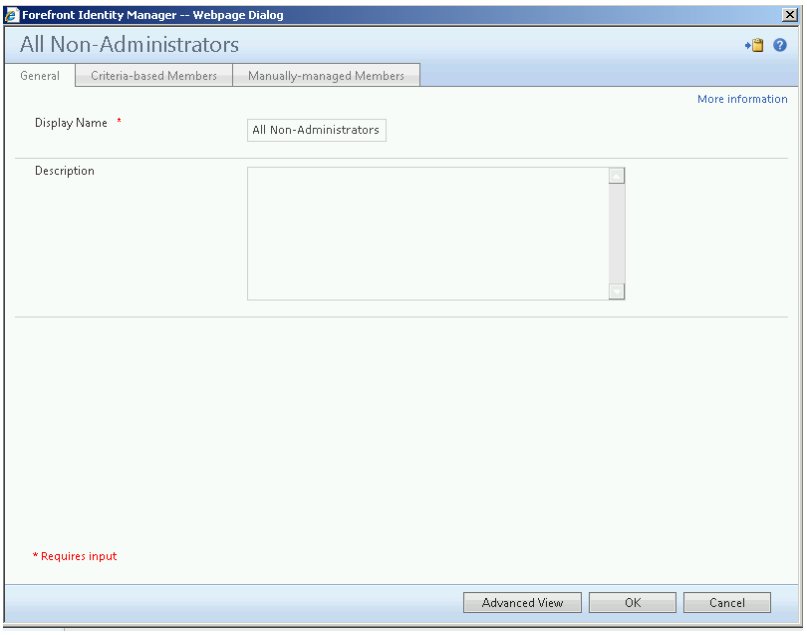

Kuva6: Käyttäjän lisääminen portaalista käsin



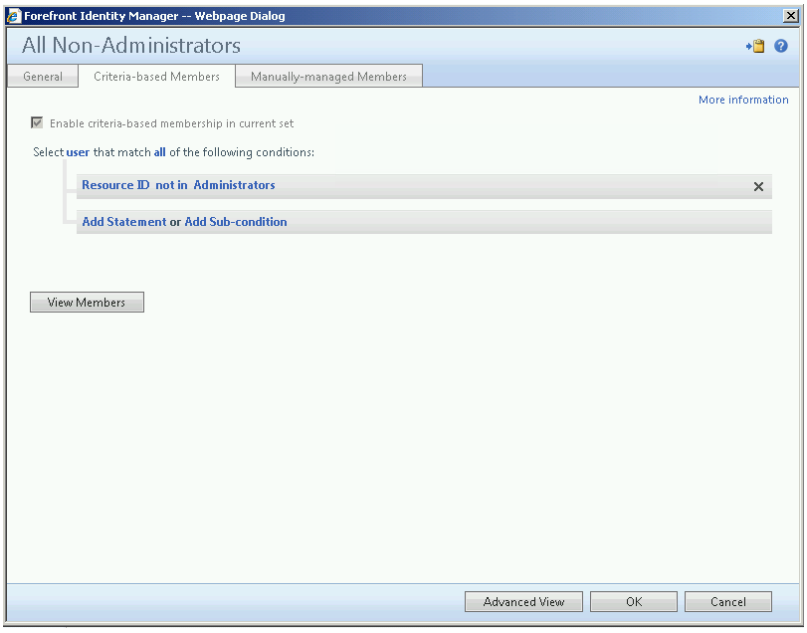

Kuva7: Portaalissa luotu käyttäjä ad:ssa

## FIM Set's

FIM organisoi objecteja seteiksi jotta hallintakäytännöt voidaan kohdistaa oikeisiin resursseihin. Yksi objecti voi kuulua niin moneen settiin kuin vaan on tarvetta. Katselin demossa muutamia valmiiksi rakennettuja settejä ja myöhemmässä testivaiheessa luon setin kaikista AD:käyttäjistä (AD-käyttäjien synkronointi osio)




Kuva8 :
Kuvassa näkyy setti johon kuuluu kaikki käyttäjät jotka eivät ole administraattoreita.



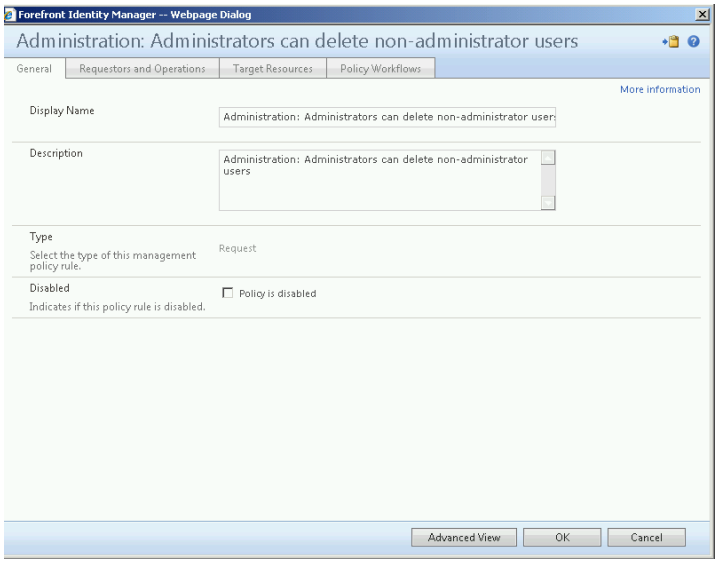

Kuva9: Kuvassa näkyy edellytykset joita käyttäjä tarvitsee kuuluakseen "All Non-Administator"-settiin

### Management Policy Rules (MPR)

MPR määrittelee tapahtuman ja siihen kuuluvat oikeudet ja työnkulut (workflows). MPR resurssia voidaan käyttää antamaan oikeuksia ja /tai iittämään yhtä tai useampaa työnkulkua johonkin tapahtumaan. On olemassa kahdenlaisia MPR:iä:

- Request MPR:
    - CRUD (Create, Read, Update ja Delete) komennot FIM:n tietokantaan kartoitetaan kaikkiin Request MPR resursseihin jotka ovat pyynnön kannalta oleellisia jolloin päätellään onko käyttäjällä oikeus suorittaa CRUD-komento, ja mitä ylimääräisiä työnkulkuja pitää suorittaa ennen tai jälkeen CRUD operaation luovuttamista FIM-servicen tietokantaan.
- Transition MPR
    - Tämän tyyppinen hallinta käytäntö kartoittaa mitä tapahtuu kun resurssi liikkuu setistä tai settiin mistätahansa syystä. Tämä voi tapahtua jonkin muun MPR:n seurauksena tai koska setti on määritelty pvm/aika (dateTime) arvolla.

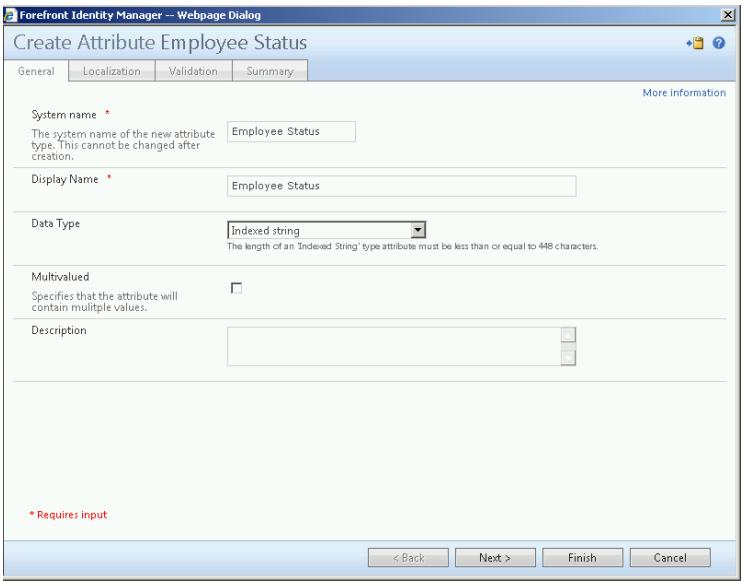
Tarkastelin demossa muutamia valmiita MPR:iä ja niiden toimintoja ja myöhemmin tulen luomaan ainakin yhden MPR:n AD-käyttäjien synkronointi osiossa.



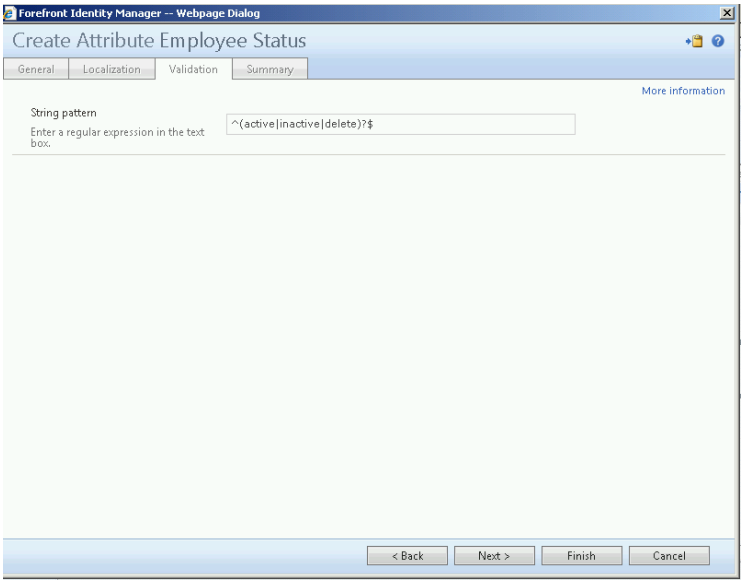

Kuva 10:
Esimerkki MPR jossa määritellään että administrator voi poistaa käyttäjiä jotka eivät ole administraattoreita

## Käyttäjän Scheman muokkaaminen

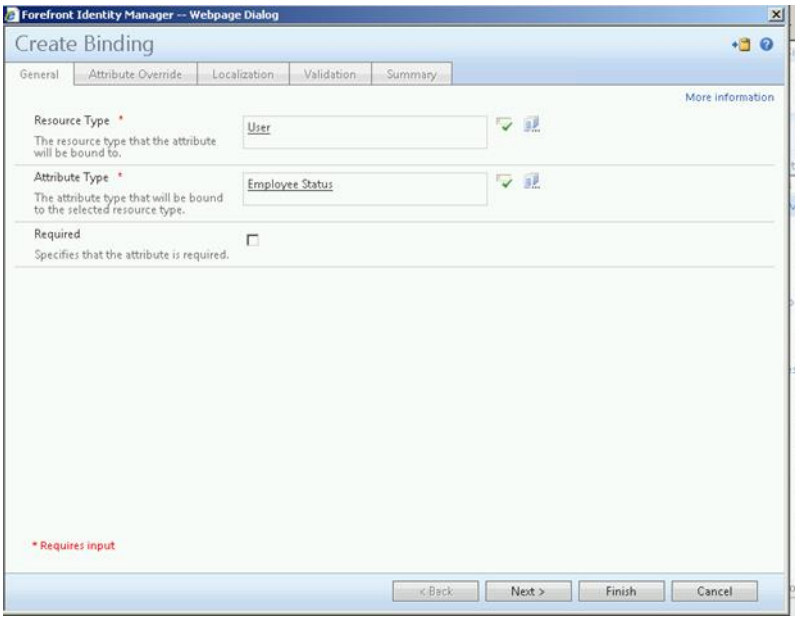
Tässä osiossa testaan  kuinka FIM-portaalin Scheman hallinnasta luodaan uusi atribuutti käyttäjälle ja kuinka uusi atribuutti otetaan käyttöön. Schemoja hallitaan FIM-portaalin administrator osiosta jossa on Schema Management osio. Osiossa voidaan luoda uusia atribuutteja ja  yhteyksiä atribuuttien ja resurssien välille.




Kuva 11:
Uuden atribuutin luominen FIM portaalissa. Atribuutti tulee olemaan ”Employee Status” joka kuvaa onko käyttäjä  aktiivinen tai  ei- aktiivinen.

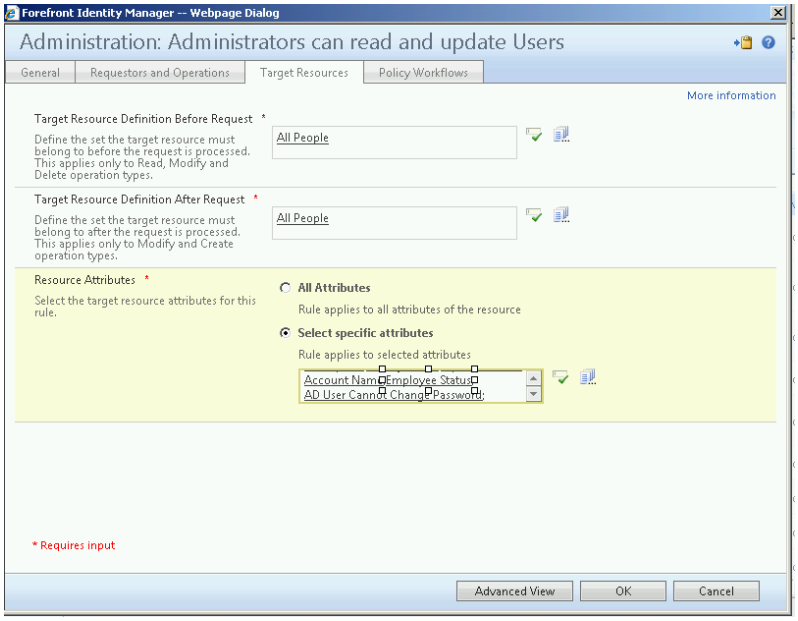



Kuva 12:
String pattern:in määrittäminen siten että  Employee Status voi olla joko active, inactice tai delete.

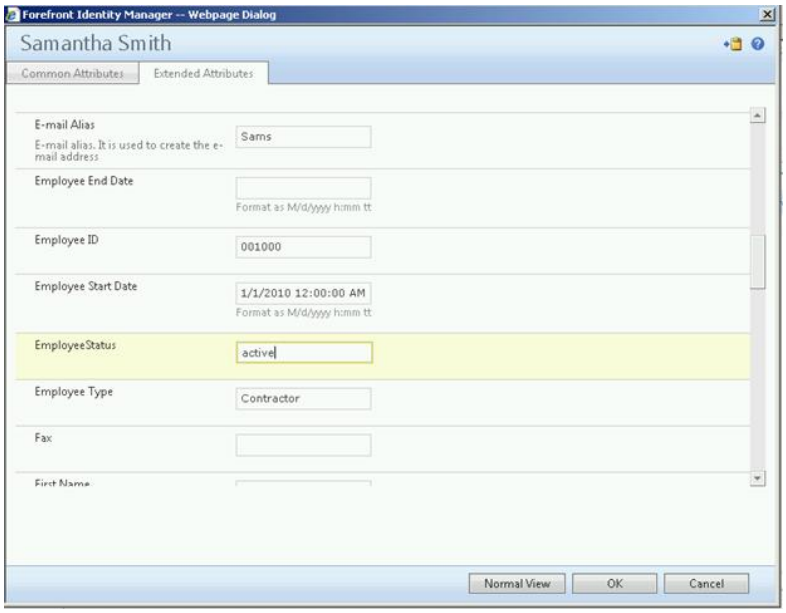



Kuva13:
Yhteyden luominen uuden atribuutin ja käyttäjät resurssin välille.

Seuraavaksi juuri luotu atribuutti pitää lisätä MPR:ään jotta administraattorilla on oikeus muokata juuri luotua atribuuttia. Tämä tapahtuu siten että avataan FIM-portaalista Management Policy Rules ja avataan sieltä ”Administration: Administrator can read and update Users” ja lisätään luotu atribuutti kohdistettuihin resursseihin( ”Target resources”).




Kuva14:
Atribuutin lisääminen administtraattorien hallintaan.

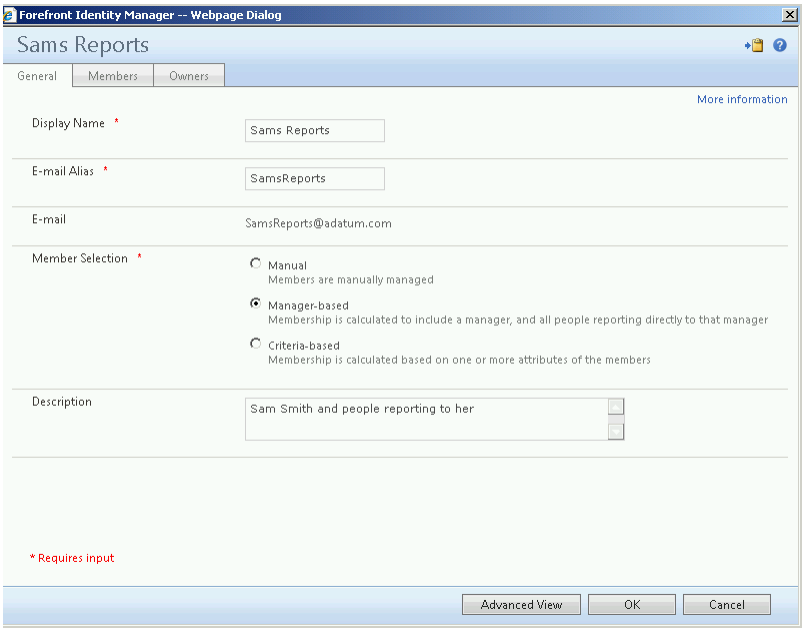



Kuva15:
Uusi atribuutti muokattavissa käyttäjätiedoissa.

## Ryhmien jäsenyyden hallinta:

Ryhmien jäsenyyden hallinnassa on kolme eri tapaa:

- Criteria Based
  - Ryhmän jäsenyys perustuu johonkin atribuuttiin
- Manager Based
  - Ryhmän jäsenyys koostuu ”Pomosta” ja kaikista ketkä vastaavat hänelle
- Manual
  - Ryhmän jäsenet määritellään manuaalisesti




Kuva16:
Esimerkki ryhmä jossa ”Manager Based ”-hallinta

## AD käyttäjien synkronointi

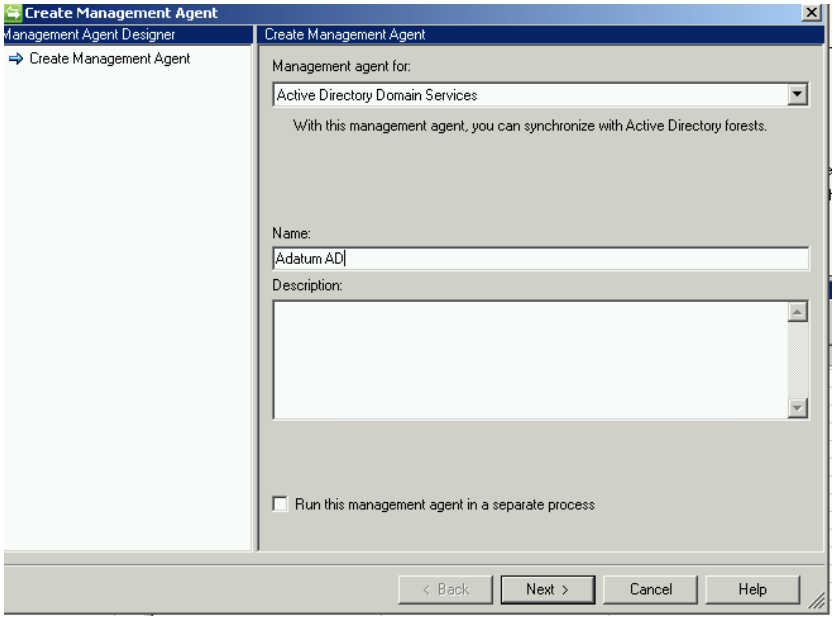
Tässä osiossa on tarkoitus testata kuinka AD tiedot synkronoidaan FIM:n käyttöön. Osiossa tullaan testamaan kuinka Management agentteja , suorita profiileja ( Run Profiles), ja syncronointi sääntöjä luodaan. Osiossa tehdään myös muutaman MPR ( Management Policy Rule) ja Setti käyttäjistä joille luotu synkronointi käytäntö kohdistetaan..

### Active directory management agentin (MA) luominen

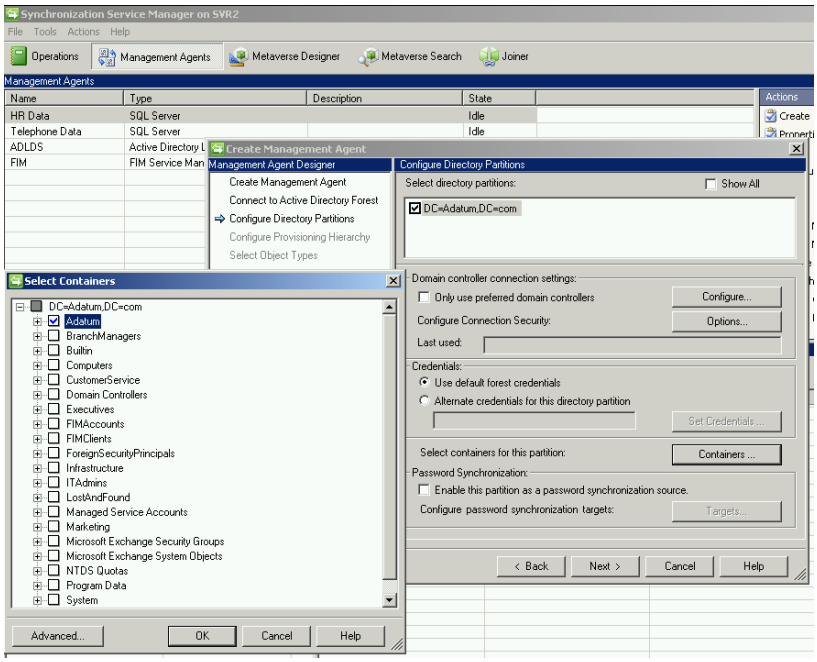
Management Agentteja luodaan FIM:n Syncronization Service Managerista. Uuden MA:n luominen aloitetaan valitsemalla kohde jolle MA luodaan, nimeämällä uusi MA ja j(Kuva17). Seuraavalla välilehdellä syötetään AD forestin tiedot jotka ovat: Forest name, Username,Password ja Domain. Seuraavaksi määritellään AD hakemiston osiot joita MA tulee tarvitsemaan (Kuva18). Seuraavassa välilehdessä määritellään varausten hierarkia (Provisioning Hierachy) jota ei käsitelty tässä demon osiossa.

Seuraavaksi valitaan objekti tyyppi ( esim: user, group jne.) jonka jälkeen valitaan atribuutit (esim: department, display name, employee id, mail, mobile , title jne.). Seuraavaksi skipataan Connection Filter, Join and Projenction säännöt ja Atribute Flow osiot koska demossa ei konfiguroida näitä osioita.

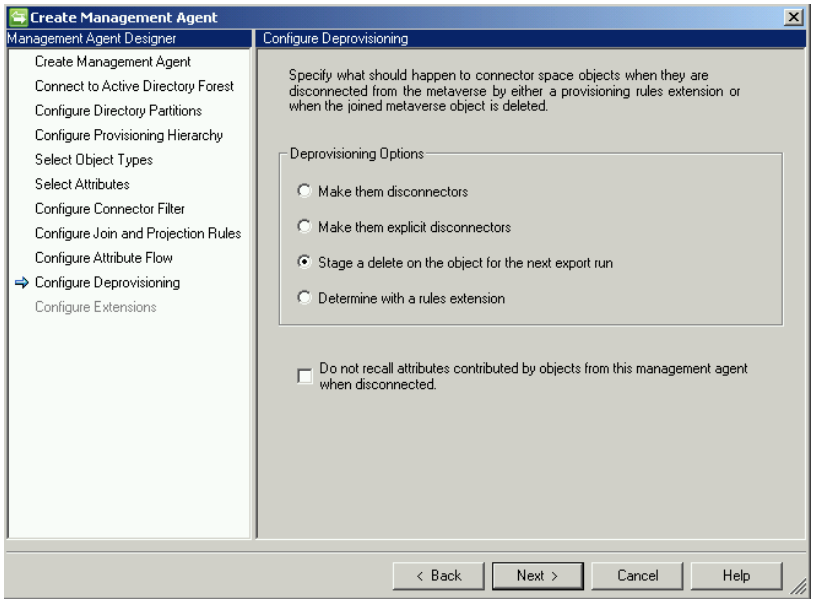
Seuraavaksi määritellään varausten poistaminen (Kuva19)jossa määritellään mitä tapahtuu yhdistetylle objectille jos yhteys katkeaa metaversumista(metaverse) koska esimerkiksi objecti poistetaan. MA:n luomisen viimeisessä välilehdessä määritellään laajennukset, demossa lisättiin Exchange 2010 laajennus joka lisättiin siten että valittiin Exhange 2010 pudotusvalikosta jonka jälkeen lisättiin Exchange 2010 RPS url: osoite .




Kuva17: Management Agentin nimen, kuvauksen ja käyttö kohteen määrittäminen.




Kuva18: Hakemiston osioiden määrittäminen.

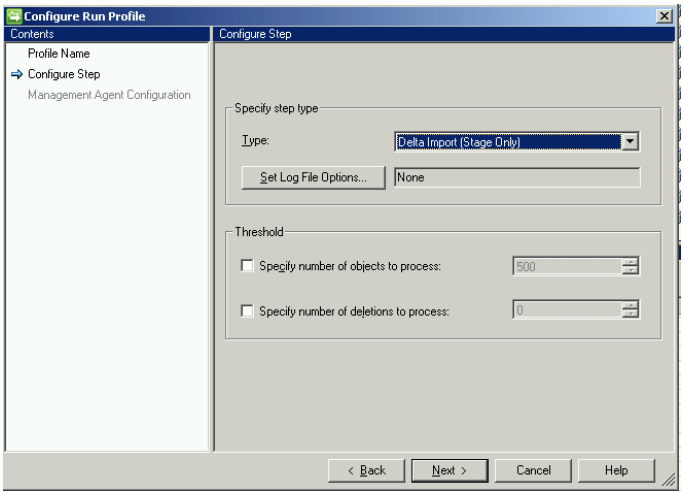



Kuva19: Deprovisioning toiminnon valinta neljästä vaihtoehdosta.

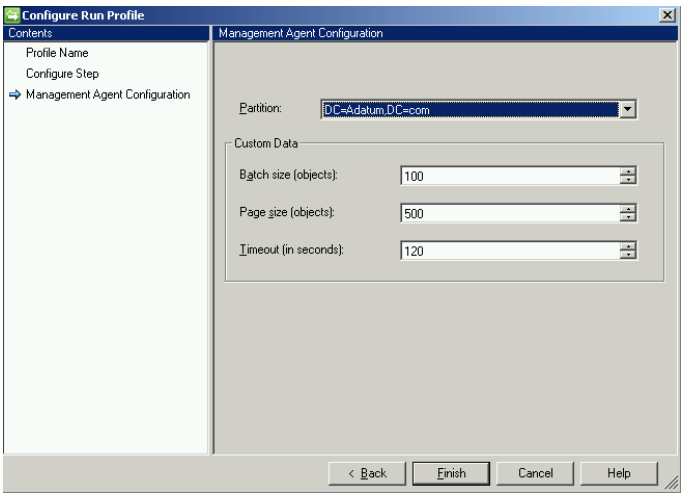
## Run profiles

Run profiileja käytetään Management Agenttien suorittamiseen. Tässä osiossa testaan muutaman Run profiilin luomista ja suorittamista. Run profiileja luodaan FIM sync managerista valitsemalla MA:n action työkalupalkista ”Configure Run Profiles”. Profiiileja luodessa ensimmäinen asia on nimetä profiili jonka jälkeen määritellään profiilin tyyppi ja kynnykset(threshold) jolla määritellään kuinka monta objectia ja poistoa prosessoidaan. Viimeinen vaihe on MA:n muokkaaminen valitsemalla domainin hakemisto/osio (partition) jota profiili käyttää suorittaessa MA:ta.

Tein demoympäristössä pari Run profiilia jotka olivat tyypeiltään Delta Synchronization, Export, Full Import ja Full Synchronization profiileja. Testasin myös profiilien suorittamista jonka lopputuloksena oli onnistunut syncronointi FIM:n ja AD:n välillä.




Kuva20: Run profiilin tyypin ja kynnyksien muokkaaminen.

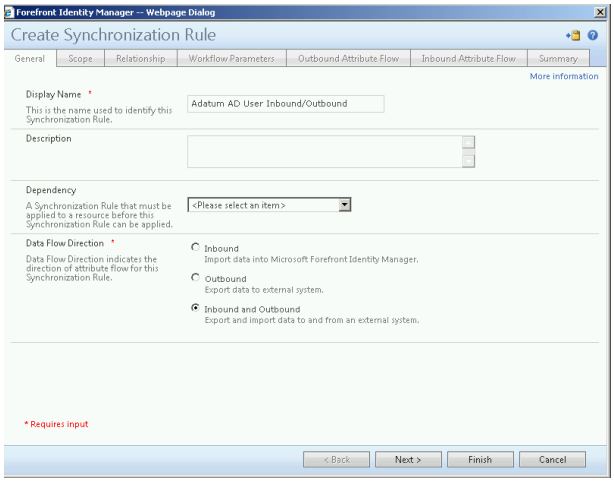



Kuva21: Run profiilin MA:n hakemiston valinta ja muokattavan datan määrittäminen.

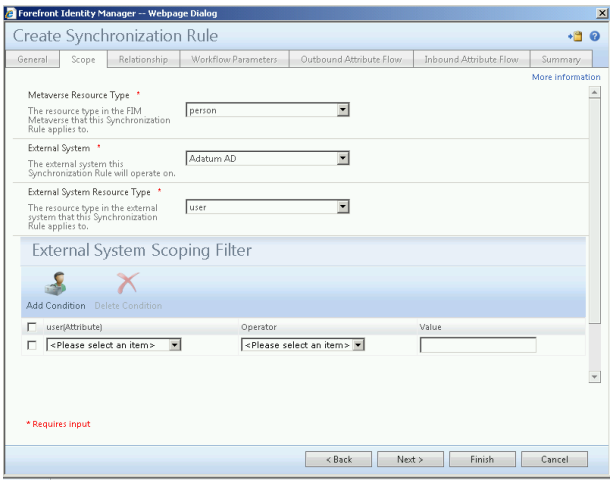
## Synkronointi säännöt ( Synchronization Rule)

Synkronointi säännöillä hallitaan synkronointia määrittämällä esimerkiksi datan liikkumis suunta (inbound ja outbound), mihin resurssi tyyppiin synkronointi kohdistuu jne. Tässä osiossa on tarkoitus käydä läpi synkronointi säännön luominen.

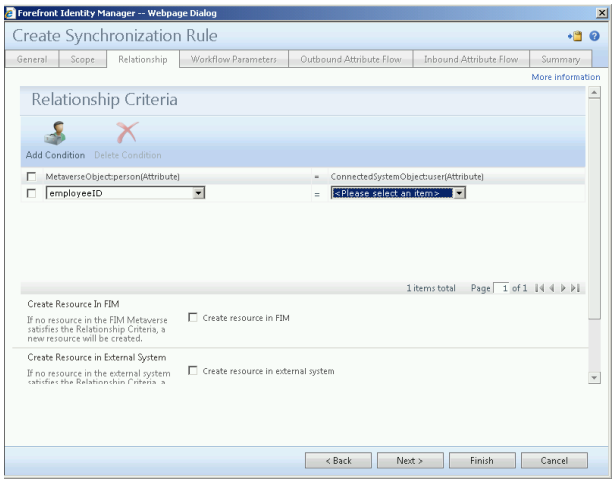
Synkronointi sääntöjä luodaan FIM:portaalin Synchronization Rules sivustosta joka löytyy Administration osion alta.




Kuva22: Ensimmäinen asia synkronointi sääntöä luodessa on nimetä sääntö ja muokata mahdollinen kuvaus säännölle jonka jälkeen valitaan riippuvuus johonkin toiseen synkronointi sääntöön ja valitaan datan liikkumis suunta(inbound ja outbound).

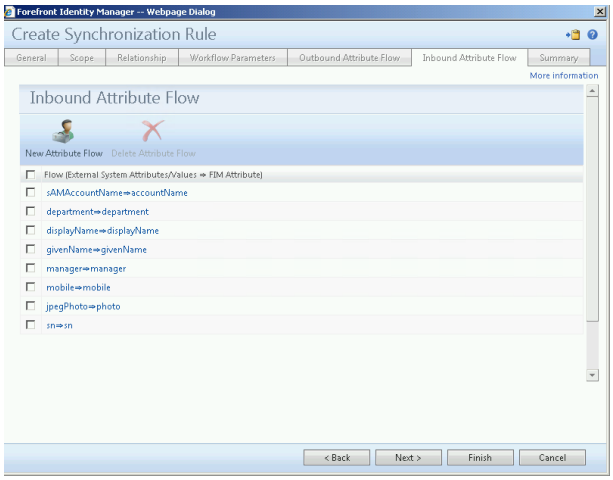



Kuva 23: Seuraavaksi määritellään synkronointi säännön laajuus valitsemalla kohteet säännölle. Tässä kohdassa määritellään meteverse resurssin tyyppi, ulkoinen kohde johon synkronointi kohdistuu ja resurssi tyyppi ulkoisessa kohteessa johon synkronointi kohdistuu. Tässä kohdassa on myös mahdollista määritellä ulkoiseen järjestelmään kohdistetut rajaukset.

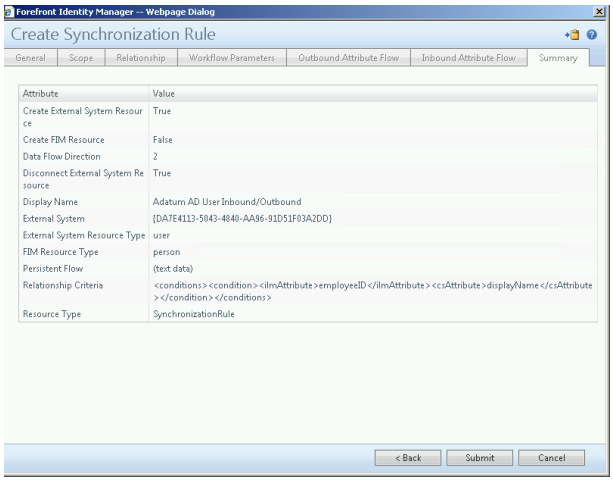



Kuva24: Seuraavaksi määritellään yhteydet atribuuttien välille jotta FIM osaa yhdistää oikean metaverse atribuutin ulkoisen systeemin vastaavaan atribuuttiin. Osiossa voidaan myös valita luoko FIM tai ulkoinen järjestelmä resurssin jos resurssi ei tyydytä suhde kriterioita.

Seuraavassa välilehdessä olisi työnkulkujen parametrien (workflow parametres) määrittely mutta tässä demossa ei käsitelty asiaa.




Kuva 25: Viimeiseksi määritellään saapuvien ja lähtevien ominaisuuksien kulku jossa määritellään saapuvien/lähtevien atribuuttien yhdistäminen FIM:n atribuutteihin. Esimerkki saapuva atribuutti ”sAMAccountName” yhdistetään FIM:n atribuuttiin ”accountName”.

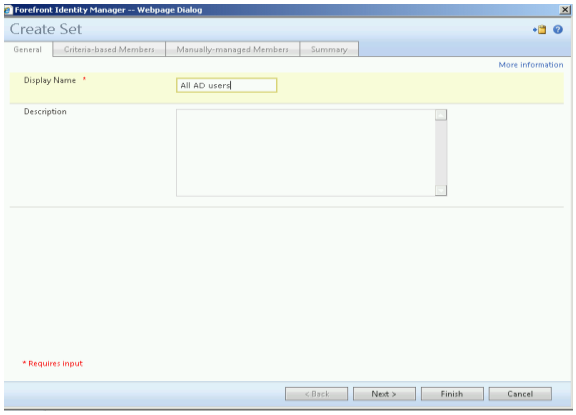



Kuva 26: Lopuksi tulee yhteenveto luodusta synkronointi säännöstä jonka jälkeen sääntö tallennetaan painamalla ”Submit” painiketta.

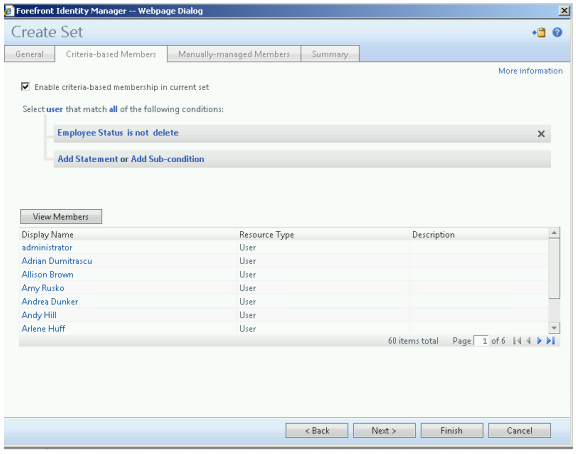
Lopputulos demosta oli synkronointi sääntö jonka tarkoituksena on hakea käyttäjä tietoja AD:sta. Atribuutteja otettiin AD:sta ja myös Exchange palvelimelta(mailNickname). Osa atribuuteista vaati osoitteita tai muita tietoja joita piti kalastella demokoneelta ADSI edit- työkalulla.

## Kohde setin luominen uudelle säännölle

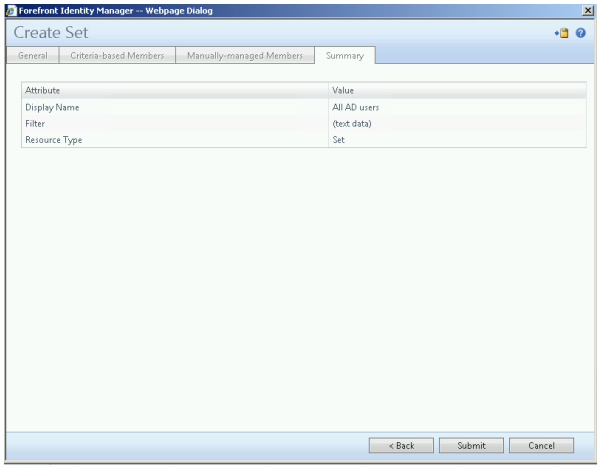
Tässä osiossa luodaan setti jotta juuri luotu sääntö saadaan kohdistettua käyttäjille. Settiin tulee kuulumaan kaikki AD-käyttäjät




Kuva 27: Setin luomisessa ensimmäinen asia on nimetä setti ja antaa sille kuvaus.

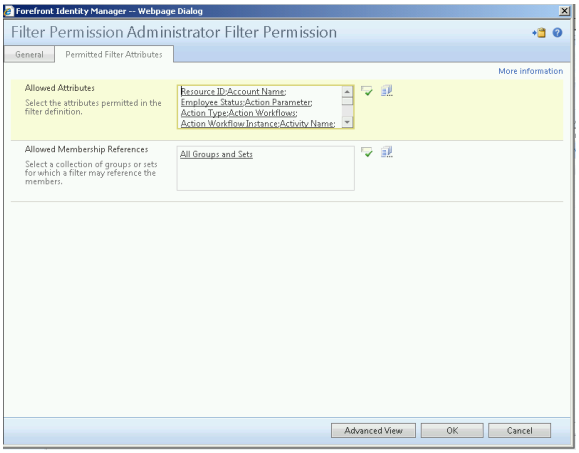



Kuva 28: Seuraavaksi määritellään kriteerit joilla FIM päättelee kuuluko käyttäjä/resurssi kyseiseen settiin. Tähän kyseiseen settiin kuuluminen vaattii että käyttäjän ”Employee Status” ei ole delete eli toisinsanoen kaikki AD-käyttäjät kuuluvat tähän settiin. Tässä kohdassa voi myös tarkistaa settiin kuuluvat käyttäjät.




Kuva 29: Viimeiseksi on lyhyt yhteenveto luodusta setistä jonka jälkeen setti tallentuu painamalla ”Submit” painiketta.

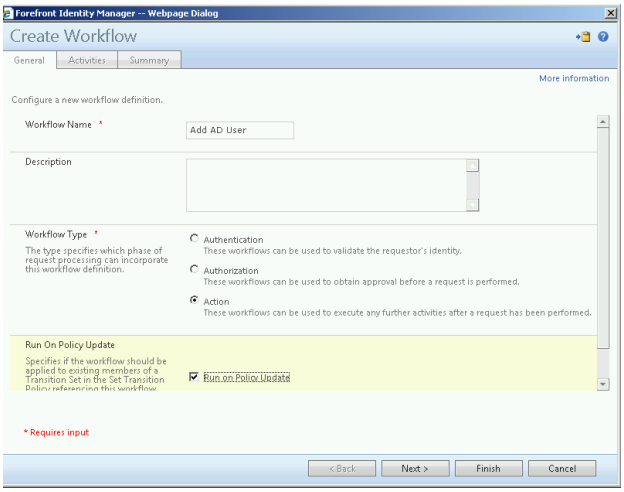
Seuraavaksi demossa piti lisätä ”Employee Status” atribuutti administraattorien hallintaan jotta juuri luotu setti osaa käyttää sitä kriteerinä oikein. Lisääminen tapahtuu FIM-portaalista  administration navigointipalkin alta josta valitaan All Resources →Filter Permissions→ Administrator Filter Permissions ja sieltä Permitted Filter Attributes välilehti.



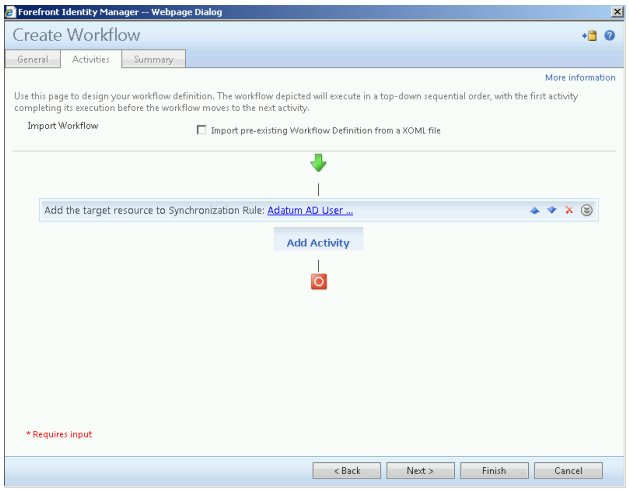

Kuva 30: Kuvassa Employee Statuksen lisääminen sallittuihin atribuutteihin.

## Työnkulun (Workflown )luominen joka lisää tai poistaa synkronointi säännön

Tässä osiossa luodaan työnkulkuja joiden tarkoituksena on lisätä ja poistaa AD käyttäjiä käyttämällä vasta luotua synkronointi sääntöä.

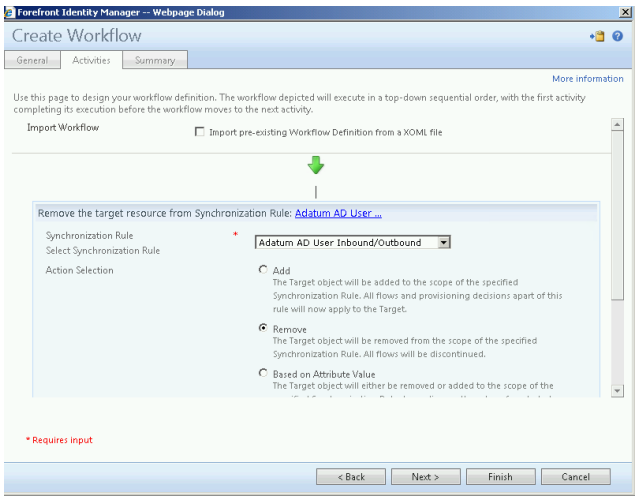



Kuva 31: Ensimmäissessä välilehdessä nimetään uusi workflow ja valitaan workflow tyyppi. Workflow tyyppejä on kolme erilaista. Ensimmäinen on Authentication joka tarkoittaa että workflow:ta voidaan käyttää käyttäjän tunnistaumiseen. Toinen on Authorization jota käytetään pyyntöjen valtuuttamiseen. Kolmas vaihtoehto on Action jota voidaan käyttämään eri aktiviteettien suorittamisessa pyynnön jälkeen. Seuraavaksi määritellään suoritetaanko workflow käytäntö päivityksien yhteydessä , tämä tarkoittaa että workflow kohdistuu jo olemassa oleviin käyttäjiin.




Kuva 32: Toisessa välilehdessä määritellään mitä toimintoja workflow suorittaa. Tässä määritellään se että luotu resurssi ( eli käyttäjä) liitetään synkronointi säännön näkyvyysalueelle (scope) . Tämä tapahtuu valitsemalla toiminnoksi Synchronization Rule Activity jonka jälkeen valitaan luotu synkronointi sääntö.

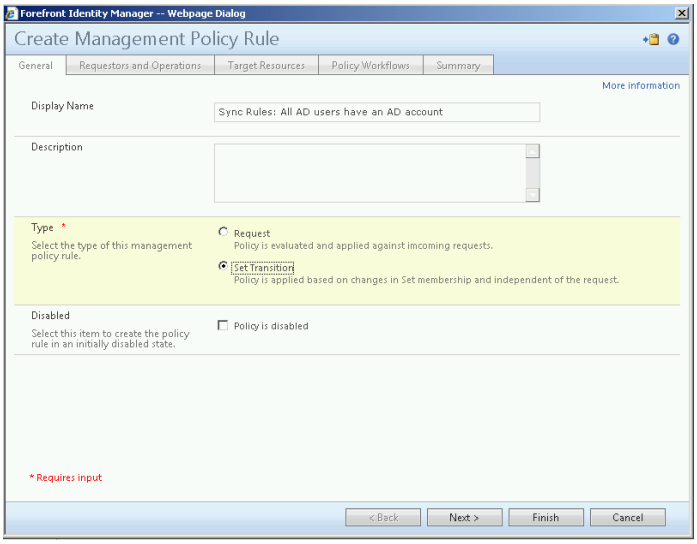
Tämän jälkeen käyttäjän lisäämiseen tarkoitettu workflow on valmis.




Kuva 33: Käyttäjän poistamiseen tarkoitettu workflow tehdään melkein täysin samalla tavalla kuin käyttäjän lisääminenkin sillä erollla että synkronointi säännön lisäämisen jälkeen määritellään toiminnoksi remove joka poistaa resurssin synkronointi säännön näkyvyys alueelta.

## Management Policy Rule (MPR) luominen käyttämään työnkulkuja (workflow)

Tässä osiossa luon kaksi MPR:ää joista toinen käyttää Add AD User työnkulkua ja toinen käyttää Remove AD User työnkulkua.

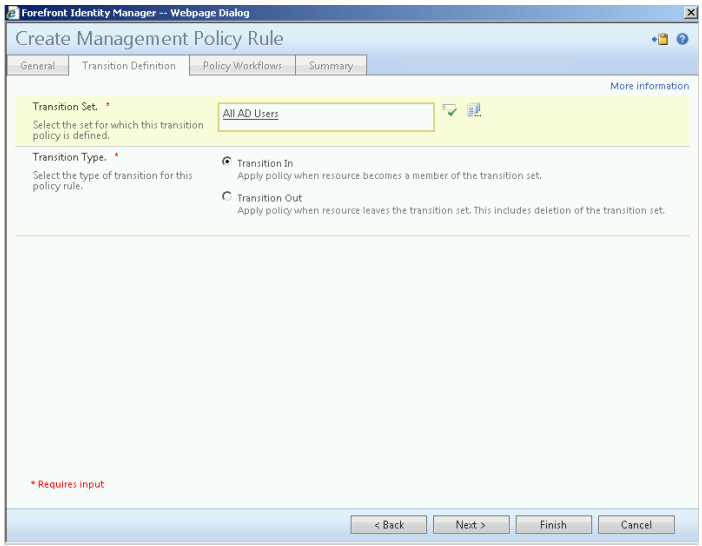



Kuva 34: Ensimmäisessä välilehdessä määritellään Nimi, kuvaus, tyyppi ja onko uusi MPR oletuksena pois käytöstä.

MPR tyypeissä on kaksi eri vaihtoehtoa:

- Ensimmäinen vaihtoehto on Request joka tarkoittaa että käytäntö arvioidaan ja sovelletaan saapuviin pyyntöihin.

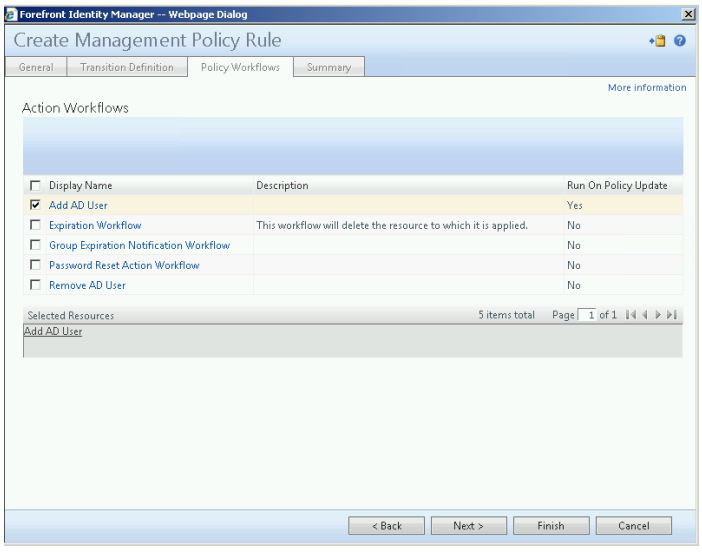
- Toinen vaihtoehto on Set Transition joka tarkoittaa että käytännön soveltaminen perustuu muutokseen setin jäsenyydessä ja riippumaattomissa pyynnöissä.




Kuva 35: Toisessa välilehdessä määritellään setti johon MPR kohdistetaan ja koska tämä MPR on Set Transition tyyppinen niin määritellään Transition tyyppi.

Transition tyyppeissä on kaksi eri vaihtoehtoa:

- Ensimmäinen vaihtoehto on Transition in joka tarkoittaa että käytäntö otetaan käyttöön kun resurssi liittyy kohde settiin.
- Toinen vaihtoehto on Transition out joka tarkoittaa että käytäntö tulee käyttöön kun resurssi poistuu kohde setistä.



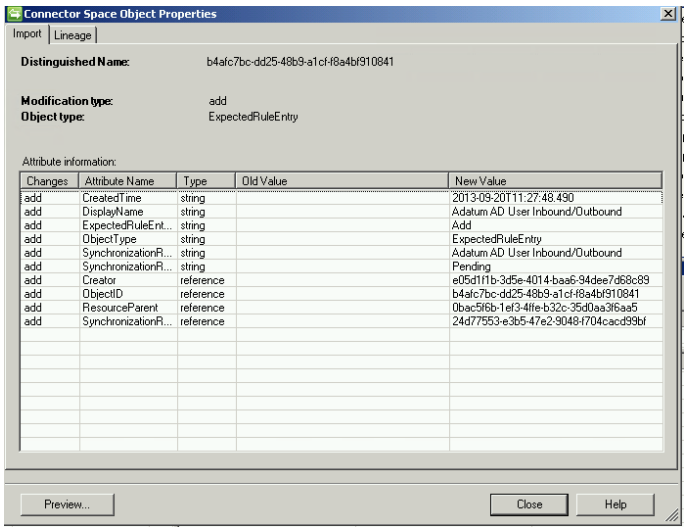

Kuva 36: Kolmannessa välilehdessä valitaan workflowt jota käytäntö tulee käyttämään. Tämän jälkeen MPR on valmis.

Käyttäjän poistamiseen tarkoitettu MPR luotiin samalla tavalla kuin edellinenki mutta workflowksi valittiin Remove AD-user workflow.

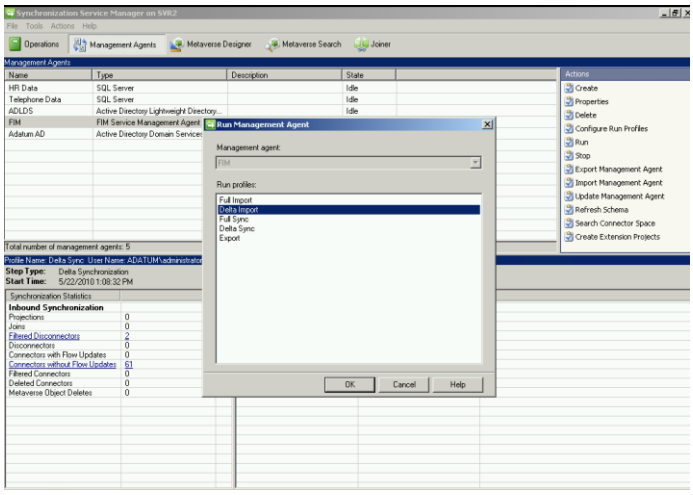
## Uuden säännön tuonti ja itse synkronointi

Tässä osiossa on tarkoitus testata synkronointia käyttämällä edellisissä osioissa säädettyjä asetuksia ja sääntöjä. Synkronointi tapahtuu FIM:n Syncronization Managerissa.

Demossa synkronointi operaatio aloitetaan ajamalla delta import suorita profiili FIM management agentilla, tämä tuottaa paljon lisäyksiä (adds) uuden synkronointi säännön vuoksi. Tämän jälkeen ajetaan delta sync suorita profiili joka synkronoi kaikki edellisessä importilla tulleet lisäykset ja FIM:stä saapuvat GUID tiedot. Uusia AD tilejä ei synny vielä tässä vaiheessa. Seuraavaksi demossa määritellään asetuksista ”Enable Syncronization Rule Provisioning”. Tämän jälkeen ajetaan Full Sync suorita profiili jonka jälkeen AD tilit luodaan ja ne ovat valmiina exporttaamiseen. Seuraavaksi valitaan Adatum AD Ma (AD:n Management agentti) ja ajetaan export profiili , tämän jälkeen käyttäjät ovat Adatum domainin Adatum OU:ssa. Tämän jälkeen ajetaan Delta Import ja Delta sync profiilit, kun kummatkin profiilit on ajettu syntyy tärkeitä atribuutti vienti virtauksia (flows) FIM:iin ( esim email ja objectSID tiedot). Viimeiseksi ajetaan Delta import ja delta sync FIM management agentilla.




Kuva 37: Delta import profiililla suoritetut lisäykset.

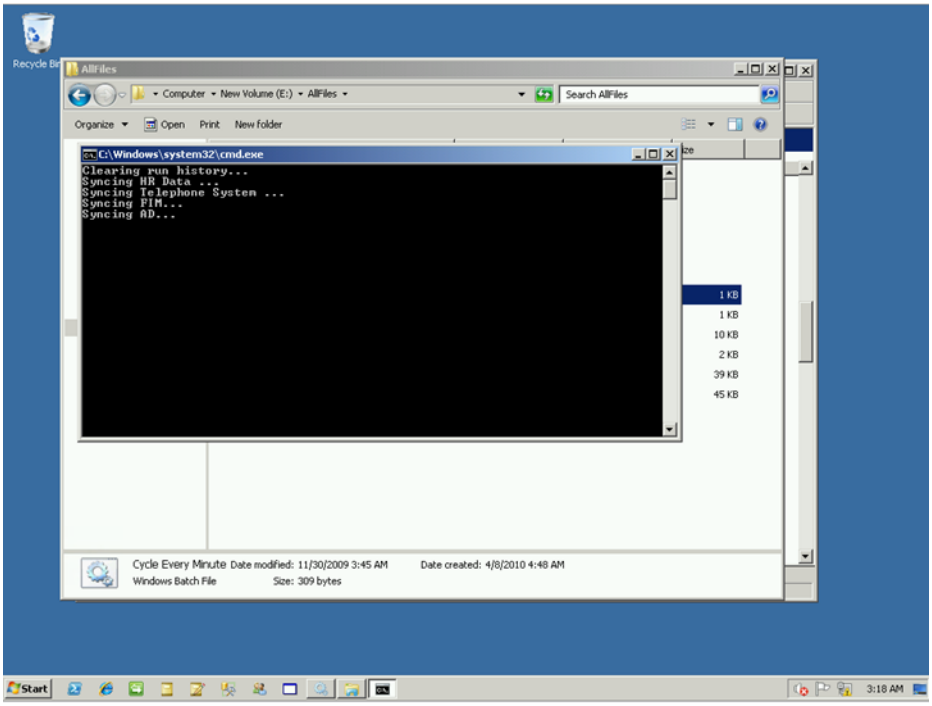



Kuva 38: Suoritettavan profiilin valinta.

## Käyttäjätietojen automaattinen synkronointi

Testasin automaattista synkronointia testauksen alussa FIM experience Virtual Labsissa

Käyttäjätiedot synkronoituvat tietyin väliajoin ( demossa synkronointi väli on minuutti) jos esimerkiksi FIM:n portaalista muutetaan jonkin käyttäjän tietoja niin minuutin jälkeen tiedot päivittyvät AD:seen. Synkronointi ottaa huomioon kaikki muutetut atribuutit ja lähettää muutetun tiedon AD:seen. Testasin demossa erilaisia käyttäjätietojen muutoksia kuten puhelinnumeron muuttamista, työ nimikkeen muuttamista, tilin poistamista ja tilin ottamista pois käytöstä. Kaikki tekemäni muutokset päivittyivät minuutin kuluessa.




Kuva 39: Synkronointi cmd näkymässä,

## FIM:n salasanan uusiminen itsepalvelu työkalulla

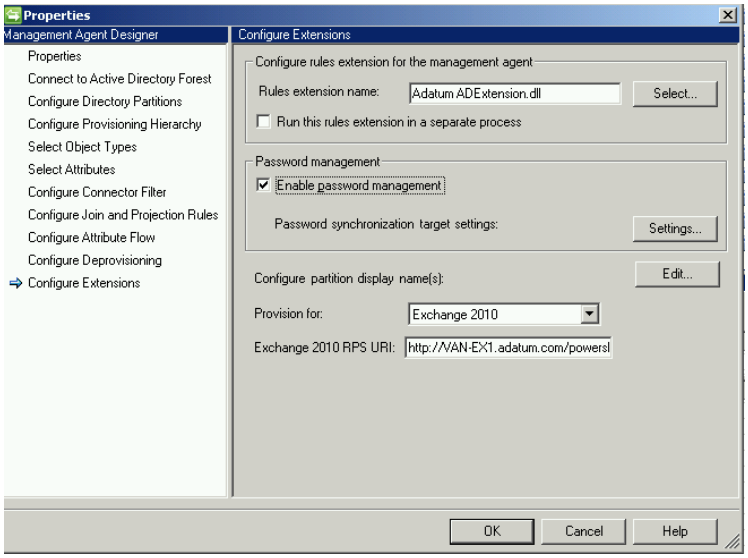
Tässä osiossa testaan miten salasanan uusiminen tapahtuu FIM:n työkaluilla. Osiossa muokkaan salasanan rekisteröimisen ja resetoinnin asetuksia jonka jälkeen testaan miten salasanan resetointi toimii käyttäjän näkökulmasta. Testaan myös miten käyttäjäntunnuksen lukitus toimii jos käyttäjä antaa vääriä tietoja nollatessaan salasanaansa. Lopuksi testaan miten PCNS:n (Password Change Notification Service) määritäminen tapahtuu.

### Ympäristön tarkistus ja muokkaus

Demo tehtävä aloitetaan tarkistamalla FIM serverin palomuurin Inbound säännöt siten, että katsotaan onko FIM:ä koskevat säännöt määritelty oikein (portit).


Kuva 40: Palomuurin säännöt

Palomuuri sääntöjen tarkastelun jälkeen varmistetaan AD:sta , että FIM service account kuuluu FIMSyncPassworSet:iin. Seuraavaksi otetaan käyttöön salasanojen hallinta AD:n management agentista.

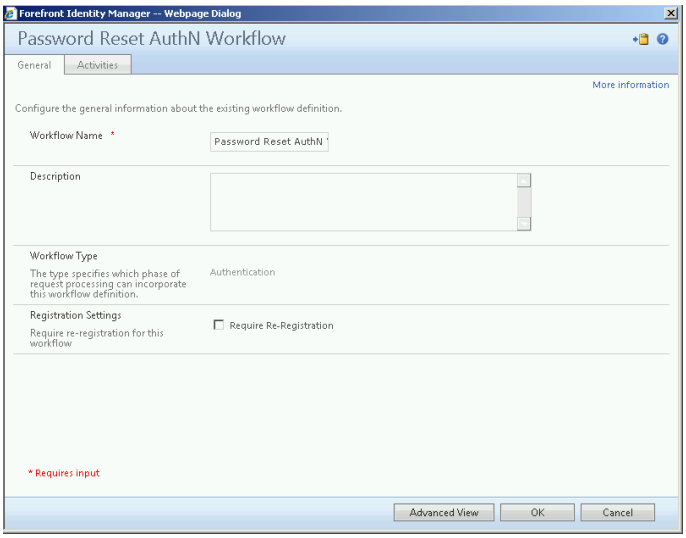



Kuva 41: Salasanojen hallinnan käyttöön ottaminen AD:n management agentista.

## Salasanan rekisteröinnin ja resetoinnin asetusten muokkaaminen

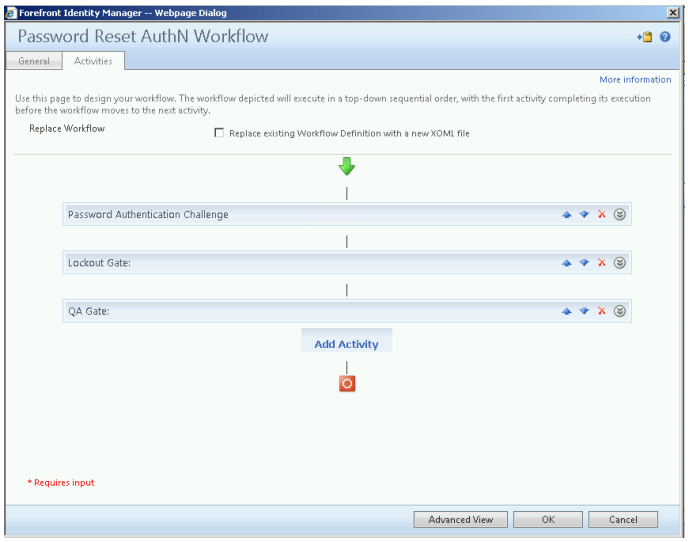
### *Työnkulut (workflows)*

Asetusten muokkaaminen aloitetaan muokkaamalla salasanan resetointiin tarkoitettuja työnkulkuja(workflow).



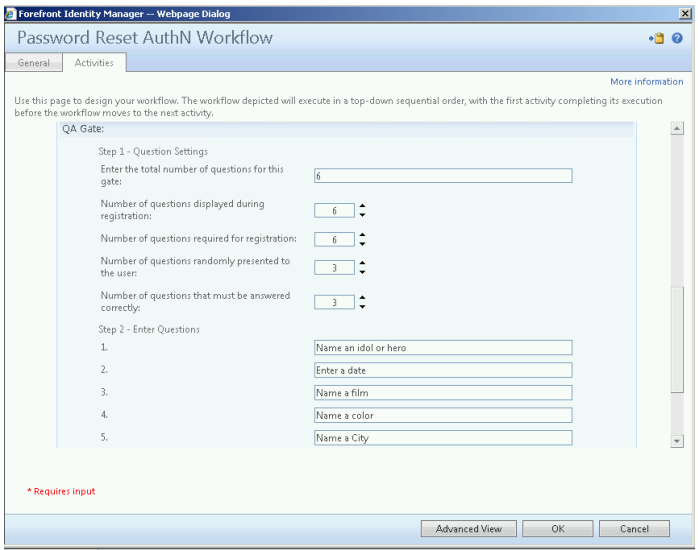

Kuva 42: Työnkulkujen muokkaaminen

Password reset AuthN workflow:n ensimmäisessä välilehdessä määritellään käyttäjät rekisteröimään salasanan rekisteröimis tiedot uudelleen valitsemalla ”Reguire Re-Registeration” ( tämä tehdään siksi jotta rekisteröimis omiaisuutta voidaan testata myöhemmässä vaiheessa.



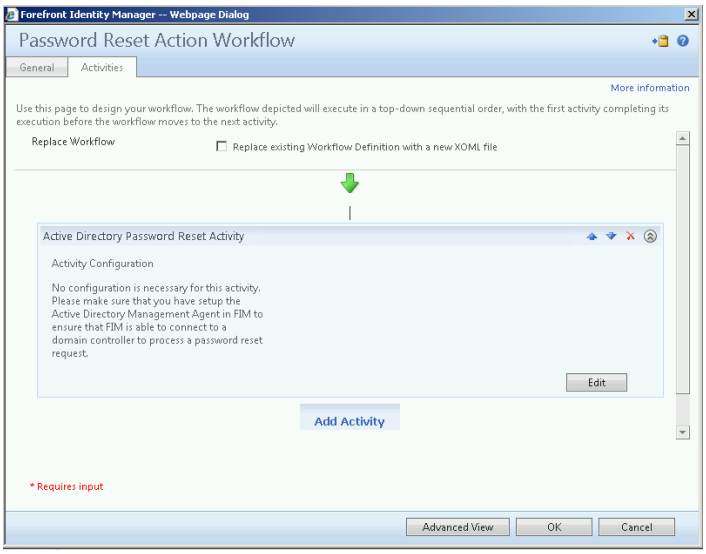

Kuva 43: Työnkulkujen muokkaaminen

Toisessa välilehdessä määritellään mitä aktiviteetteja tapahtuu kun salasanaa resetoidaan . Ensimmäisessä aktiviteetissa tunnistetaan käyttäjä, toisessa aktiviteetissa määritellään lukitus siinätapauksessa jos käyttäjä antaa väärät tunniste tiedot.




Kuva 44: Työnkulkujen muokkaaminen

Kolmannessa aktiviteetissa määritellään turva kysymykset joihin käyttäjä vastaa ja joiden avulla käyttäjä pystyy resetoimaan salasanan.

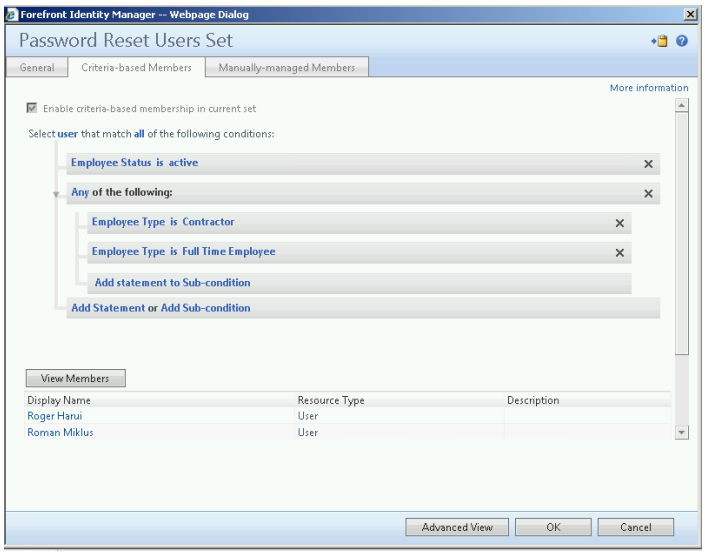



Kuva 45: Työnkulkujen muokkaaminen

Seuraavaksi tarkastelin Password Reset Action Workflow:ta jossa ei ollut muokattavia aktiviteetteja.

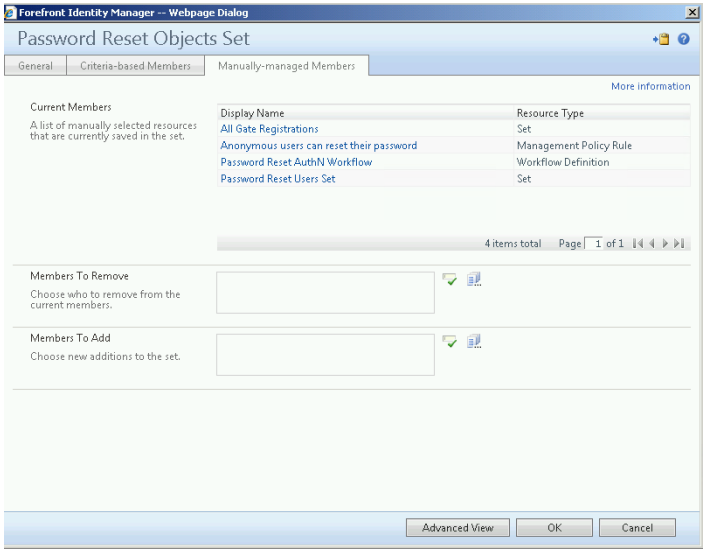
### *Resetoinnin  settien muokkaaminen.*

Seuraavassa osiossa muokataan settiä johon salasanan resetoinnin piiriin kuuluvat käyttäjät kuuluvat.




Kuva 46: Setin muokkaus

Setin toisessa välilehdessä määritellään millä perusteella käyttäjä kuuluu kyseiseen settiin. Tässä tapauksessa  settiin kuuluvuus määriteltiin siten että käyttäjän  Employee statuksen pitää olla active ja ali ehtona on että käyttäjä on  täysipäiväinen työntekijä (Full Time employee) tai käyttäjä on urakoitsija (contractor).

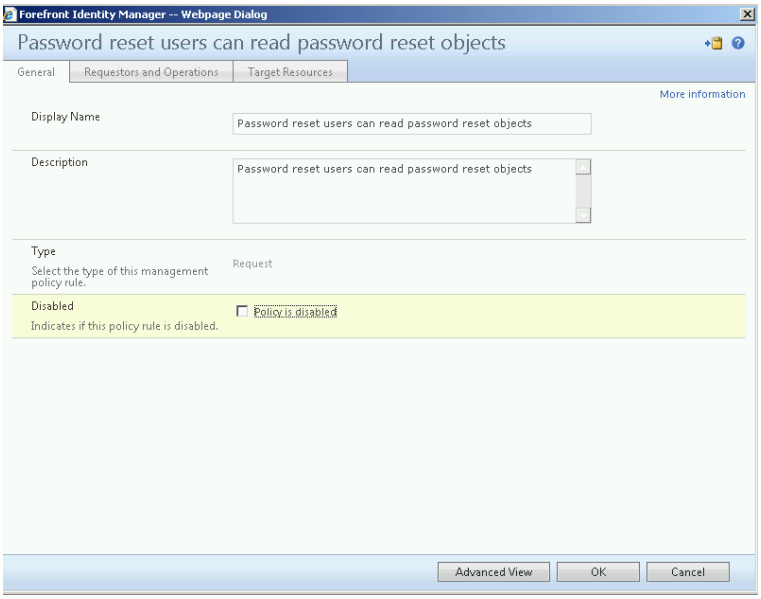



Kuva 47: Setin muokkaus

Seuraavaksi tarkastelin Password Reset Objects Set:iä. Tämän setin manuaalisesti määritellyissä jäsenissä on määritelty kaikki resurssit joita Password Reset User setti vaatii päästäkseen käsiksi tallennettuihin kysymyksiin ja vastauksiin jne.

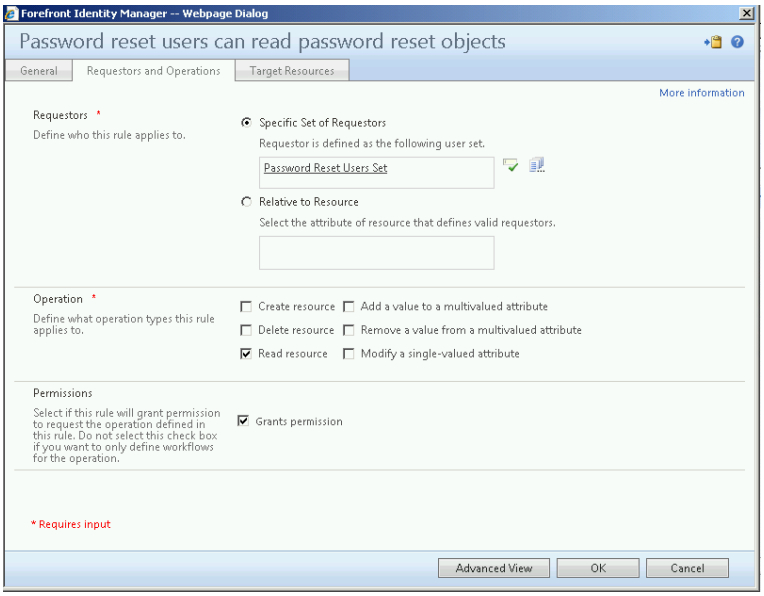
## *MPR:ien muokkaaminen*

Tässä osiossa muokataan ja otetaan käyttöön Management Policy sääntöjä siten että käyttäjällä on oikeus lukea atribuutteja joita hän tarvitsee salasanan resetointiin ja että tuntemattomilla käyttäjillä on oikeus salanan resetointiin.




Kuva 48: MPR:n muokkaaminen

Ensimmäiseksi avataan “Password reset users can read password reset objects” MPR ja otetaan se käyttöön poistamalla täppä Policy is disabled kohdasta.




Kuva 49: MPR:n muokkaaminen

Seuraavassa välilehdessä tarkastistetaan, että tämä MPR antaa luku oikeudet Password Reset Users settiin.

Viimeiseksi tarkastellaan target recources välilehteä ja tarkistetaan, että kohde resurssi on ”Password”.

Seuraavaksi otetaan seuraavat MPR:t käyttöön ottamalla jokaisesta Disabled täppä pois, nämä MPR:t ovat: Click Anonymous users can reset their password, Click Password reset users can update the lockout attributes of themselves, Users can create registration objects for themselves, User management: Users can read attributes of their own ja Click General: Users can read non-administrative configuration resources. Viimeiseksi otetaan General workflow: Registration initiation for authentication activity MPR käyttöön.

## Salasanan resetoinnin testaus käyttäjällä

Tässä osiossa on tarkoitus testata salasanan resetointia edellisissä osioissa muokatuilla asetuksilla. Testaus alkaa kirjatumalla normaalilla käyttäjällä sisään toimialueelle.

### *Resetointi toiminnon käyttöönottaminen*


Kuva 50: Resetointi toiminnon käyttöönottaminen

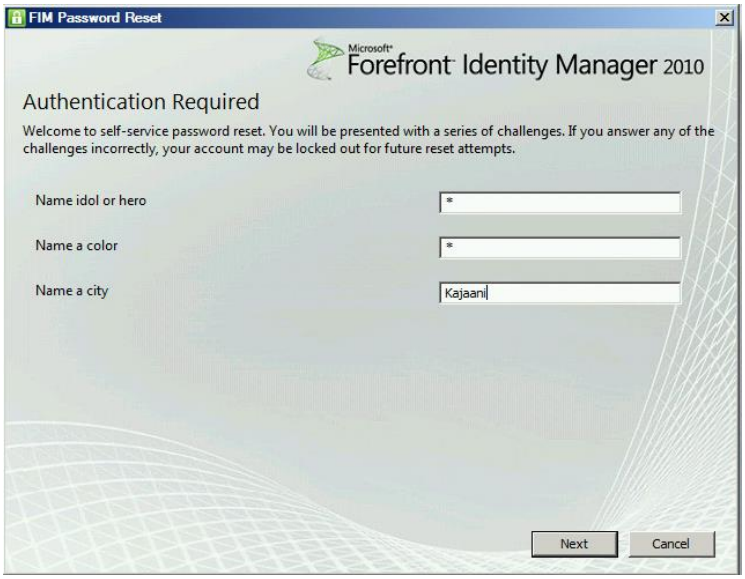
Työpöydällä tullessa ruudulle tulee ikkuna jossa alkaa salasanan resetoinnin rekisteröityminen. Tervehdys ikkunan jälkeen ohjelma kysyy nykyisen salasanan jotta ulkopuoliset ei pääse muokkaamaan salasanan resetointi tietoja.


Kuva 51: Turva kysymykset

Seuraavaksi annetaan vastaukset turvakysymyksiin jotka määriteltiin PassResetAuthn workflowssa. Tämän jälkeen salasanan resetoinnnin rekisteröityminen on valmis.

### *Resetoinnin testaus*

Resetoinnin testaus tapahtuu kirjautumalla ulos työpöydältä ja klikkaamalla windowsin kirjautumis ikkunasta reset password kohtaa.




Kuva 52: Salasanan vaihto

Salasanan resetonnin ensimmäinen kohta on vastata kolmeen kysymykseen joihin käyttäjä on vastannut rekisteröitymisen yhteydessä.


Kuva 53: Salasanan vaihto

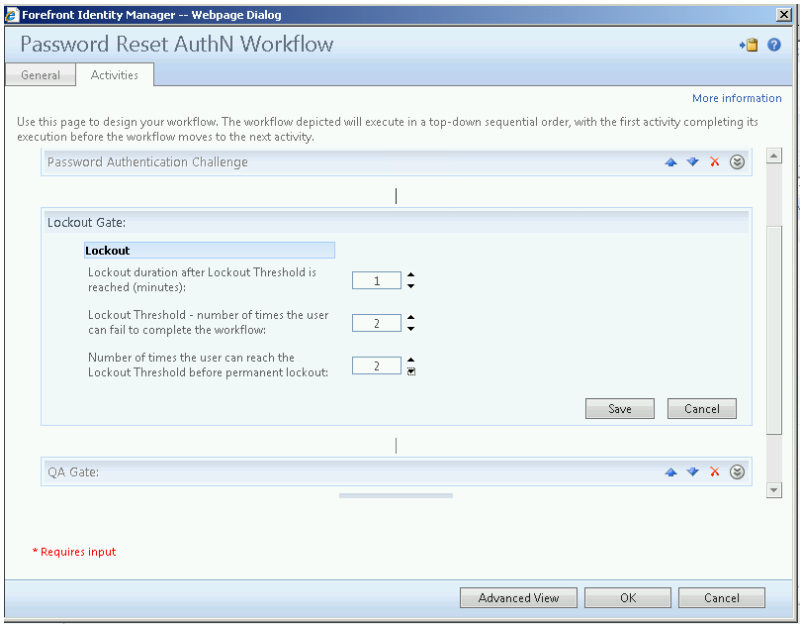
Kysymyksiin vastaamisen jälkeen käyttäjältä kysytään uusi salasana jonka jälkeen salasana on resetoitu.

Salasanan resetointi toimii myös portaalin kautta sillä erolla että salasanan resetointi aloitetaan antamalla käyttäjä johon resetointi kohdistetaan,

Jos käyttäjän halutaan uusivan salasanan resetoinnin tiedot niin se tapahtuu menemällä portaaliin ja valitsemalla ”Reguire Re-Registration” käyttäjän Password Reset AuthN Workflow:sta.

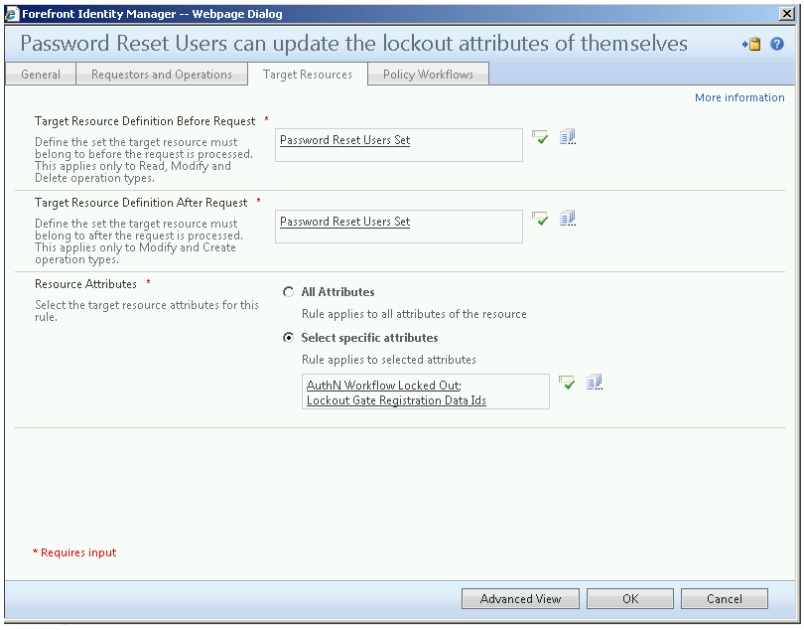
## Salasanan resetoinnin lukituksen muokkaaminen ja testaus

Tässä osiossa on tarkoitus testata miten resetoinnin lukitus toimii muokkaamalla asetuksia ja testaamalla mitä tapahtuu kun käyttäjä lukitaan.




Kuva 54: Lukituksen asetusten muokkaaminen

Ensiksi avataan portaalista Password Reset AuthN Workflow jonka Activities välilehdestä valitaan Lockout Gate. Tästä voidaan määritellä muutamia lukituksen asetuksia kuten esimerkiksi lukituksen kesto ja yritysten määrä ennen kuin lukko menee päälle.




Kuva 55: Lukituksen asetusten muokkaaminen

Seuraavaksi tarkastellaan MPR:ää joka määrittää että käyttäjät voivat päivittää lukitus atribuutteja itse.

Targer resources välilehdeltä tarkistetaan että kohteiksi on määritelty Password Reset Users Set ja että atribuuteiksi on määritelty AuthN Workflow Locked Out aja Lockout Gate Registration Data Ids atribuutit.

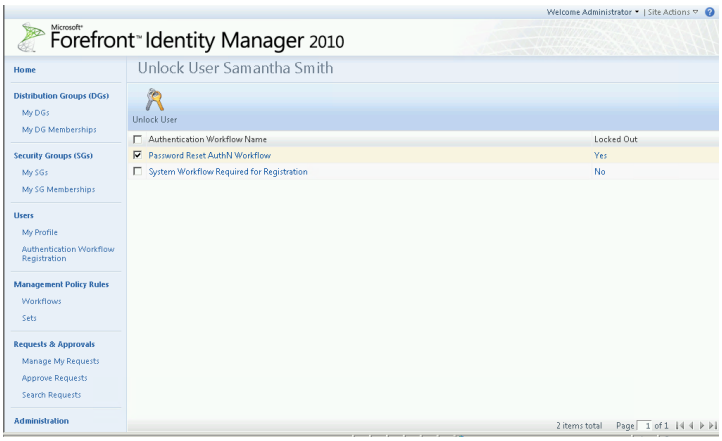
Requestors and Operations välilehdeltä tarkastetaan että ”Resource ID” on määritelty pyytäjäksi (Requestor), tämä määrittää sen että käyttäjällä on oikeus muokatava hänen omaa objektiaan portaalissa.

### *Lukituksen testaus*


Kuva 56: Käyttäjän lukitus

Lukitusta testataan käynnistämällä salasanan resetointi kirjautumis ikkunasta ja vastaamalla turvakysymyksiin väärin. Kolmen yrityksen jälkeen käyttäjätili lukitaan minuutiksi. Minuutin jälkeen resetointia voi yrittää uudelleen mutta muutaman virheellisen yrityksen jälkeen käyttäjätili lukkiutuu pysyvästi.

### *Lukituksen avaus*




Kuva 57: Lukituksen avaus

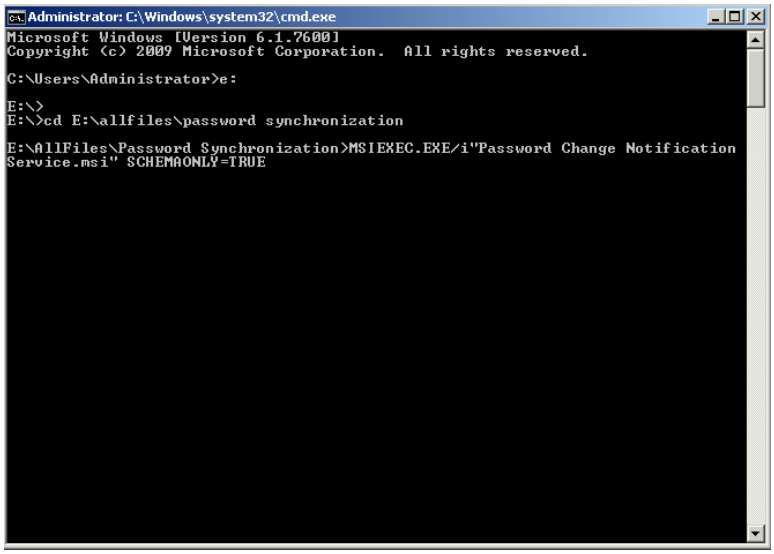
Lukituksen avaus tehdään portaalista Unlock Users admin työkalun avulla. Ensiksi etsitään lukittu käyttäjä jonka jälkeen valitaan Password Reset AuthN Workflow ja klikataan Unlock User painiketta.

Lukituksen avaus ei onnistu jos admineille ei ole annettu oikeuksia avata lukkoa. Oikeudet annetaan luomalla MPR jossa määritellää että admin voi avata lukkoja. MPR:ään määritellään pyytäjäksi (requestor) administrator, kohteeksi määritellään ”All Gate Registrations” ja atribuutiksi laitetaan ”Gate data”.

## PCNS:n Määrittäminen (Password Change Notification Service)

Tässä osiossa määritellään PCNS asetukset domainiin. Työ järjestys on seuraava: AD scheman laajentaminen PCNS:lle, PCNS:n asennus DC:lle, palvelun spn:n (service principal name) määrittäminen, PCNS:n määrittäminen domainille, FIM:n konfigurointi salasanojen synkronointia varten ja lopuksi salasana synkronoinnin testaus.

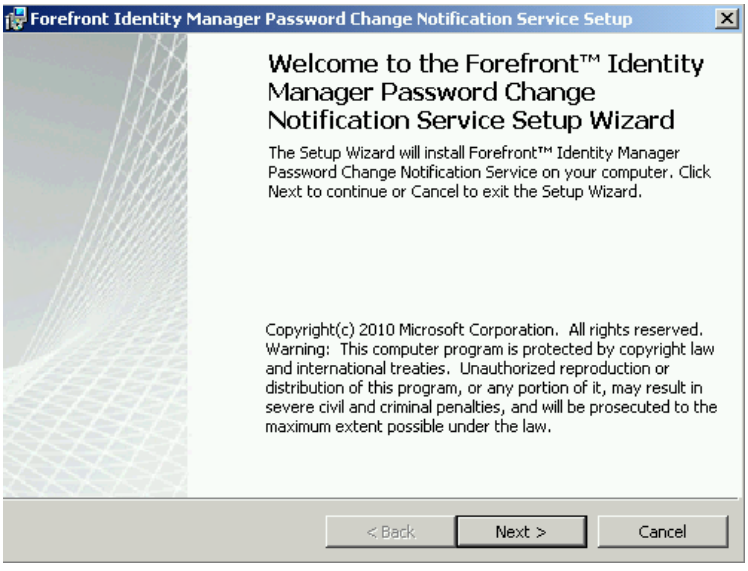
### *AD scheman laajentaminen PCNS:lle*




Laajentaminen tehdään command prompt:issa. Ensiksi paikannetaan asennus tiedoston sijainti cmd:ssä jonka jälkeen suoritetaan seuraava komento:" MSIEXEC.EXE /i "Password Change Notification Service.msi" SCHEMAONLY=TRUE". Tämän jälkeen asennus velho käynnistyy ja asennuksesta selviää next/ok painikkeilla.

Kuva58: AD scheman laajentaminen

### *PCNS:n asennus DC:lle*




Asennus aloitetaan paikantamalla koneelta PCNS:n asennus tiedosto (Password Change Notification Service.msi). Asennuksessa ei ole mitään muokattavia asetuksia vaan asennus on valmis muutaman next painalluksen jälkeen.

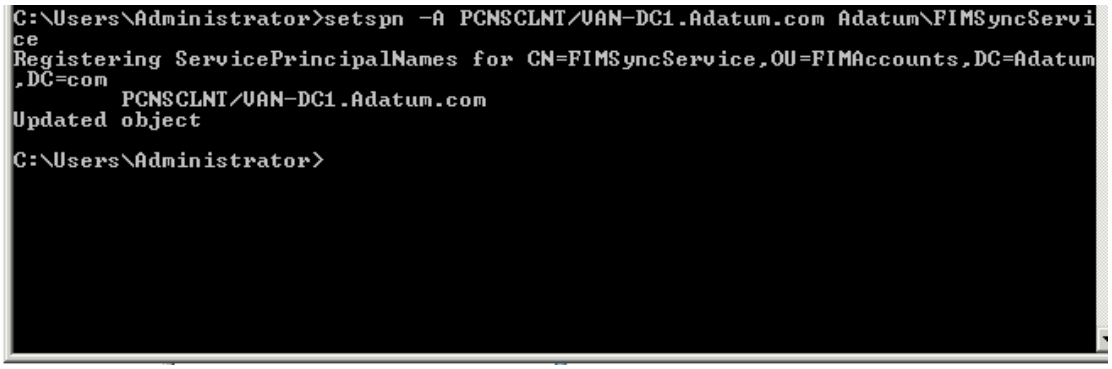
Tämä ohjelma täytyy suorittaa kaikissa domain controllereissa jotka osallistuvat salasanojen synkronointi prosessiin. Tämä asennus ohjelma asentaa seuraavat komponentit: Password change

Kuva 59: PCNS asentaminen

notification service (Pcnssvc.exe), Password change notification configuration utility (Pcnscfg.exe) ja Password change notification filter (Pcnsflt.dll)

### *Palvelun spn:n määrittäminen*

Palvelun nimi määritellään cmd:ssä komennolla : ”setspn -A PCNSCLNT/VAN-DC1.Adatum.com Adatum\FIMSyncService”.



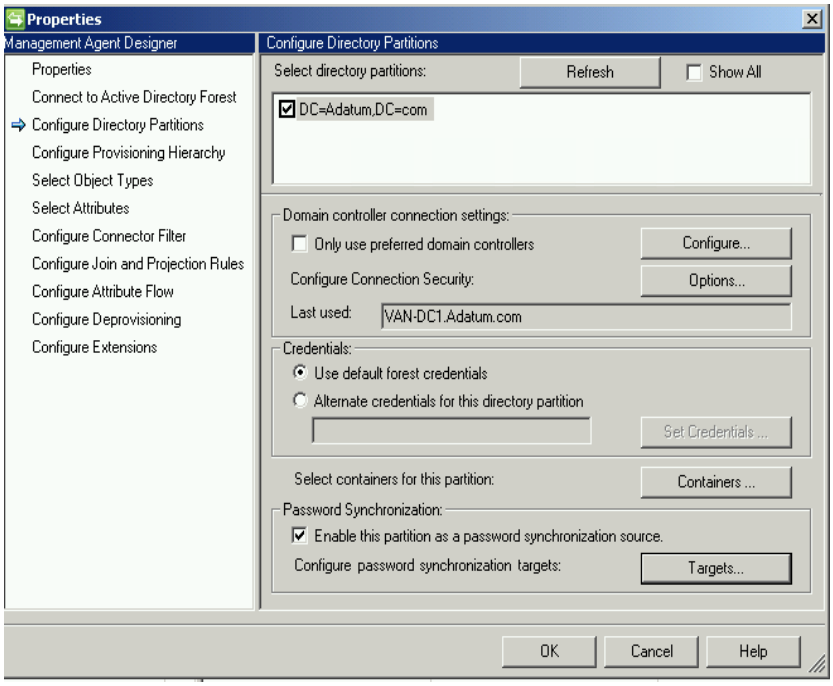

Kuva 60: spn:n määrittäminen

### *PCNS:n määrittäminen domainille*

PCNS:n määrittäminen tapahtuu cmd:ssä. Ensiksi paikannetaan PCNS:n asennus kansio ( esim : “cd C:\Program Files\Microsoft Password Change Notification”) jonka jälkeen luodaan kohde seuraavalla komennolla: ”pcnscfg.exe ADDTARGET /N:FIMServer /A:SVR2.Adatum.com /S:PCNSCLNT/VAN-DC1.adatum.com /FI:"Domain Users" /FE:"Domain Admins" /f:3”. PCNS parametreja voi hallita pcnscfg.exe työkalulla ja hallintaa voi käyttää myös etänä.


Kuva 61: PCNS:n määrittäminen domainille

## *FIM:n konfigurointi salasanojen synkronointia varten*

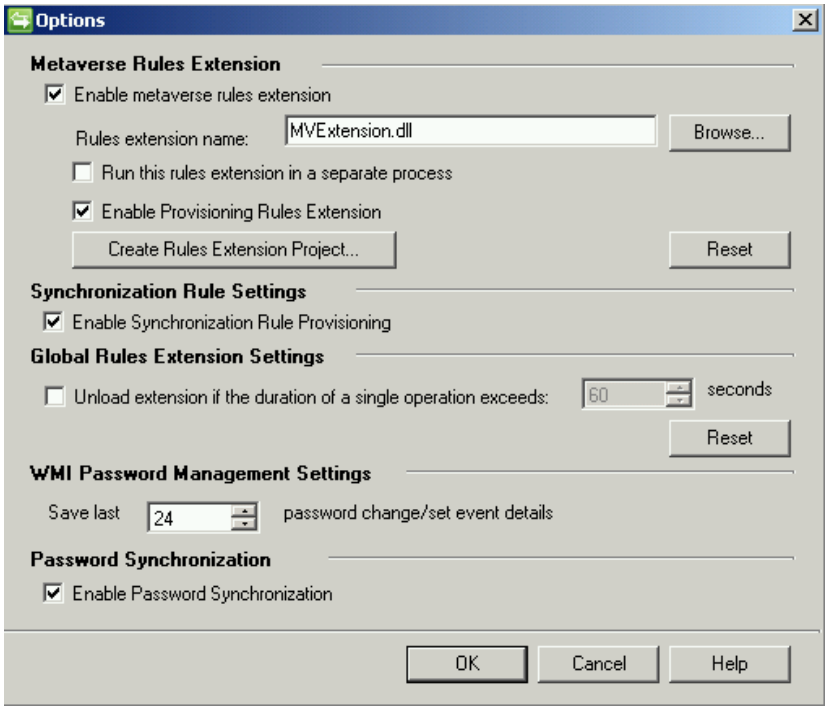



Kuva 62: FIM konfigurointi

FIM:n konfigurointi aloitetaan avaamalla Synchronization Service Manager ja avaamalla sieltä AD:n management agentin.

Configure Directory Partitions välilehdessä laitetaan täppä kohtaan “Enable this partition as a password synchronization source” jonka jälkeen painetaan targets painiketta ja valitaan ”ADLDS” vaihtoehto.

Seuraavaksi laitetaan Configure Extensions välilehdeltä täppä kohtaan ”Enable password management”



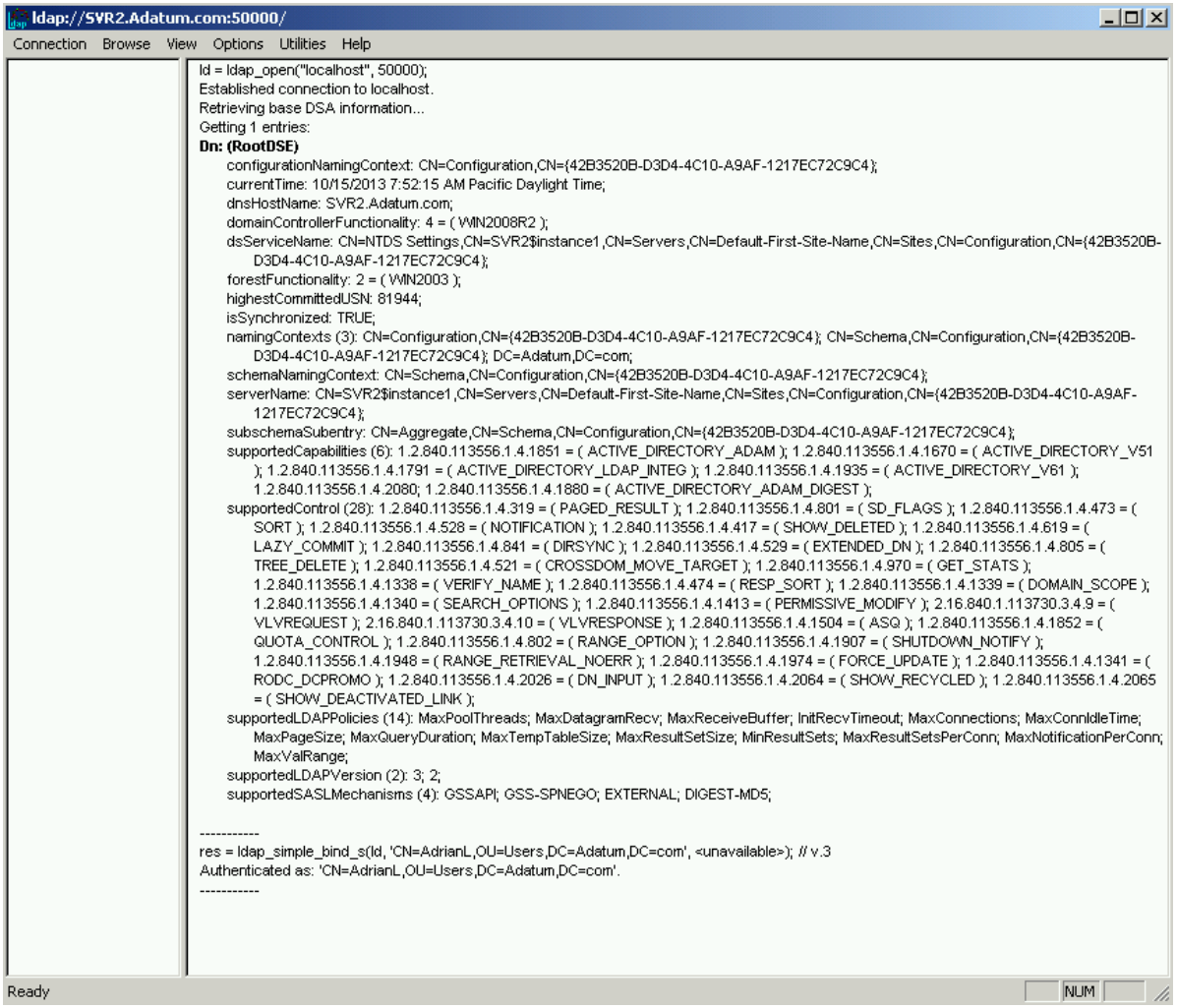

Kuva 63: FIM konfigurointi

Viimeiseksi avataan options valikko työkalupalkista ja laitetaan täppä kohtaan ” Enable Password Synchronization”

### *Salasana synkronoinnin testaus*

Synkronoinnin testaus tapahtuu muuttamalla käyttäjän ( tässä tapauksessa Adrian L) salasanaa jonka jälkeen käytetää LDP työkalua selvittämään toimiiko PCNS oikein.

LDP työkalussa valitaan ensimmäiseksi connect painike joka sijaitsee connection menun alla, avautuvaan konfigurointi ikkunaan laitetaan server kohtaan tyypiksi localhost ja portiksi 50000. Seuraavaksi avataan Bind menu joka sijaitsee myös connection menun alla, tässä konfigurointi ikkunassa valitaan ensin Simple Bind ja sen jälkeen kirjoitetaan User kohtaan käyttäjän tiedot (esim.”CN=AdrianL,OU=Users,DC=adatum,DC=com”). Tämän jälkeen annetaan salasana ja painetaan OK painiketta, jos syntynyt raportti on onnistunut niin PCNS toimii oikein.




Kuva 64: Kuvassa testauksen lopputuloksena tullut raportti.

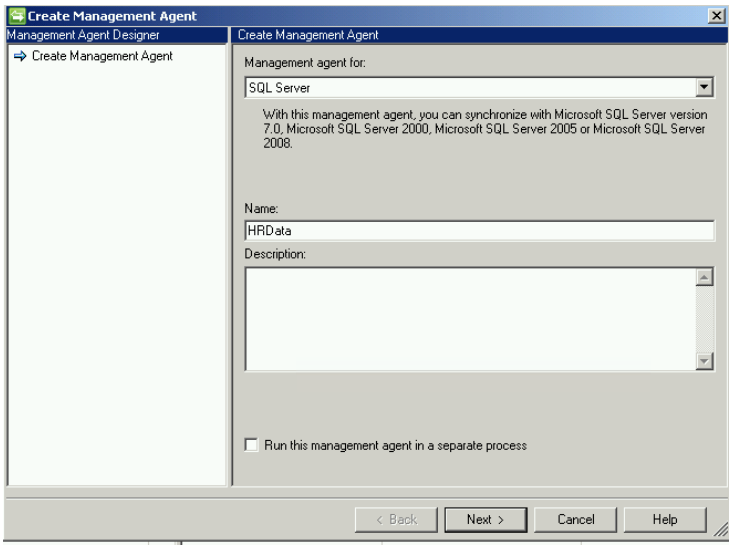
# Tietojen tuominen ja synkronointi

Tässä osiossa määritellään Forefront identity manageria siten että identiteettitiedot tuodaan HR (human resources) järjestelmästä metaversumiin. Osiossa varmistetaan myös se että, muutokset joita tehdään HR sovelluksella synkronoidaan  metaversumiin.

## HR tietojärjestelmään yhdistäminen ja identiteetti tietojen tuominen

Tässä osiossa luodaan management agentti (MA) jotta HR:n SQL tietokanta saadaan yhdistettyä FIM:iin . Osiossa myös luodaan ja ajetaan suorita profiileja.

### *MA:n luominen*

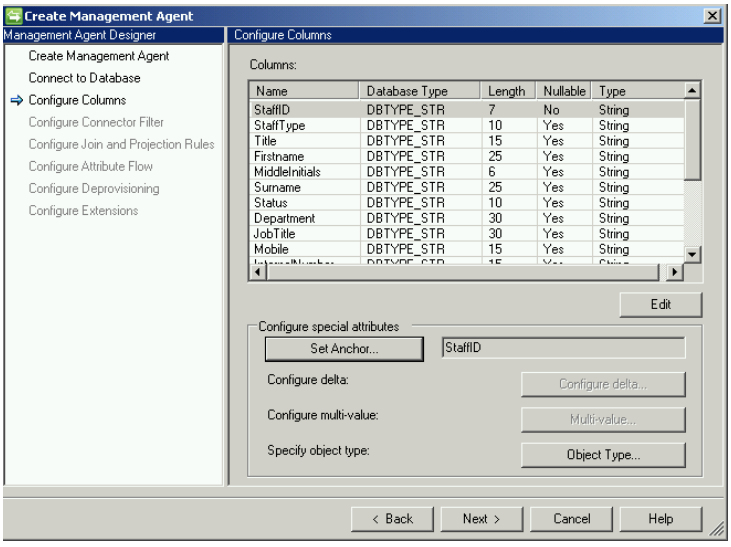



Kuva 65: MA:n luominen

MA:n luominen aloitetaan FIM sync managerin Management Agents välilehdeltä.

Ensimmäiseksi määritellään MA:n kohteeksi SQL server jonka jälkeen annetaan nimi ja kuvaus.

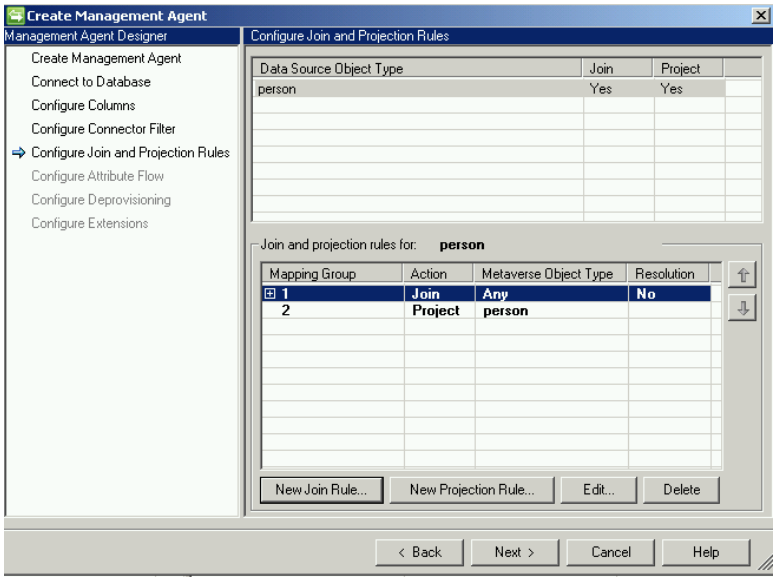
Seuraavassa välilehdessä määritellään yhteys SQL tietokantaan antamalla  tiedot serverin nimestä, tietokannasta ja taulukosta/näkymästä (table/view) ja antamalla autentikointitiedot kyseiseen tietokantaan.




Kuva 66: MA:n luominen

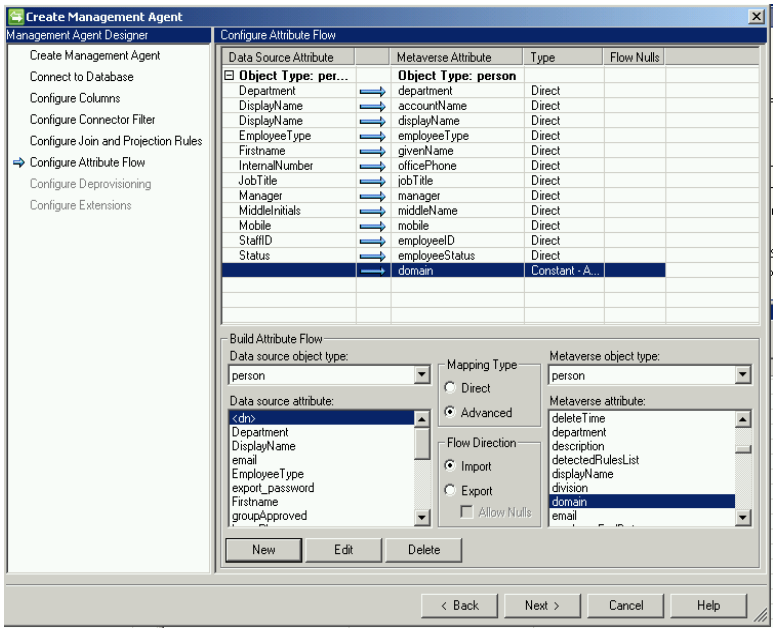
Configure Columns välilehdellä määrititellään ankkuri atribuutiksi StaffID atribuutti ja tarkastetaan että objecti tyypiksi on määritelty henkilö (person). Seuraavaksi etsitään sarake listalta manager atribuutti ja avataan se  ja laitetaan täppä kohtaan ”Reference (DN)”. Tämä tehdään siksi koska manager sarakkeessa on viittauksia StaffID atribuuttiin.

Seuraavassa välilehdessä määritellään suodattimet mutta tässä demossa siihen ei ollut tarvetta.




Kuva 67: MA:n luominen

Seuraavalla välilehdellä määritellään liittymisen ja projektion säännöt (Join and Projection Rules). Ensiksi määritellään uusi projektio sääntö painamalla ”New Projection Rule” painiketta ja määrittämällä objecti tyypiksi henkilön (person). Seuraavaksi määritellään uusi liittymisen sääntö ”New Join Rule” painikkeesta ja määritellään StaffID tietolähteen atribuutiksi ja employeeID metaverse atribuutiksi.




Kuva 68: MA:n luominen

Configure attribute flow välilehdellä määritellään yhteydet tietolähde atribuuttien ja metaverse atribuuttien välille. Yhteyksien luominen tapahtuu valitsemalla kummastakin lähteestä vastaavat atribuutit jonka jälkeen valitaan kartoitus tyyppi ja virtaus suunta ja lopuksi painetaan ”New” painiketta.

Lopuksi valitaan metaverse atribuuteista domain atribuutti ja valitaan advanced kartoitustyyppi ja painetaan ”New ” painiketta jonka jälkeen avautuun ikkuna johon laitetaan Constant kohtaan arvoksi domainin nimi.

Lopuksi hypätään yli välilehdet configure deprovisioning ja configure extensions koska niitä asetuksia ei tarvinnut muokata tässä demo scenaariossa.

### *Suorita profiilien luonti ja profliilien suorittaminen*

Suorita profiilien luominen aloitetaan FIM sync managerista. Ohjelmiston actions paneelista valitaan configure run profiles ja sieltä valitaan new profile. Tein demossa kaksi suorita proifiilia jotka olivat Full Import ja Delta Sync, suorita profiilit on kohdistettu edellisessä osiossa tehtyyn management agenttiin. Seuraavaksi suoritetaan profiilit ja tarkastellaan tuloksia.

| Synchronization Statistics | |
|---|---|
| **Staging** | |
| Unchanged | 0 |
| Adds | 62 |
| Updates | 0 |
| Renames | 0 |
| Deletes | 0 |

Kuva 69: Synkronoinnin statistiikkaa

Ensimmäiseksi suoritetaan Full Import profiili jonka lopputuloksena on 62 lisäystä henkilöstön tietokannasta.

| Synchronization Statistics | |
|---|---|
| **Inbound Synchronization** | |
| Projections | 0 |
| Joins | 62 |
| Filtered Disconnectors | 0 |
| Disconnectors | 0 |
| Connectors with Flow Updates | 62 |
| Connectors without Flow Updates | 0 |
| Filtered Connectors | 0 |
| Deleted Connectors | 0 |
| Metaverse Object Deletes | 0 |
| | |
| **Outbound Synchronization** | **FIM** |
| Export Attribute Flow | 62 |
| | |
| **Outbound Synchronization** | **Adatum AD** |
| Export Attribute Flow | 58 |
| | |
| **Outbound Synchronization** | **ADLDS** |
| Export Attribute Flow | 3 |

Kuva70: Synkronoinnin statistiikkaa

Seuraavaksi suoritetaan Delta Sync profiili jonka lopputuloksena on että kaikki edellisen Full importin 62 lisäystä on synkronoitu onnistuneesti.

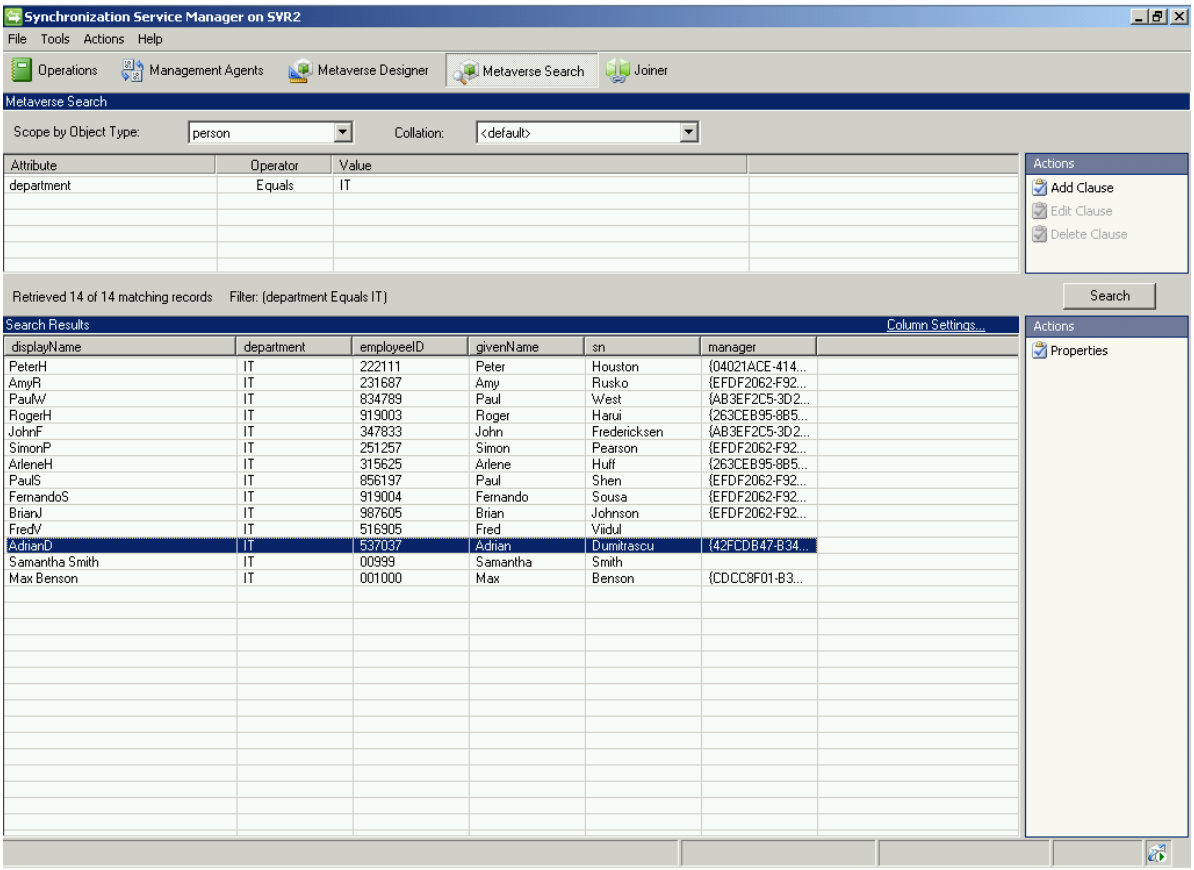
## Metaversumin tarkastelu

Tässä osiossa tarkastellaan metaversumia FIM sync:in metaverse search ja metaverse designer työkaluilla. Osiossa käydään läpi miten metaverse tietoa haetaan, miten haku asetuksia muokataan ja lopuksi indeksoidaan employee id atribuutti.

Tarkastelu aloitetaan valitsemalla metaverse search työkalu ja painamalla sieltä search painiketta. Tämä palauttaa kaikki 62 objektia koska suodattimia ei määritelty. Seuraavaksi määritellään suodattimia valisemalla sivun ylälaidasta Scope by object type ja valitsemalla pudotusvalikosta tyypin person (henkilö). Tämän jälkee lisätään ehto/lauseke painamalla Actions työkalupalkista Add Clause painiketta,. Lausekkeeseen määritellään atribuutiksi department , operaattoriksi equals ja arvoksi(value) määritellään IT, tämä tarkoittaa sitä että haku hakee nyt ne ihmiset joiden osasto on IT.

Seuraavaksi määritellään mitä sarakkeita haun tuloksessa näkyy. Sarakkeiden määritys tapahtuu column settings painikkeesta josta avautuu Search Results Column Setting sivu. Sivun Available Columns kohdasta etsitään haluttu sarake ja painetaan Add painiketta jolloin kyseinen sarake tulee näkyviin hakutuloksien yhteydessä. Määrittelin employeeID, givenName, sn ja manager sarakkeet näkyväksi.

Lopuksi indeksoidaan employeeID atribuutti avaamalla metaverse designer työkalu ja valitsemalla sieltä objektiksi person jonka jälkeen kyseisen objektin atribuutit tulevat näkyviin. Atribuutti listalta tupla klikataan employeeID atribuuttia ja laitetaan täppä kohtaan Indexed ja painetaan ok painiketta,

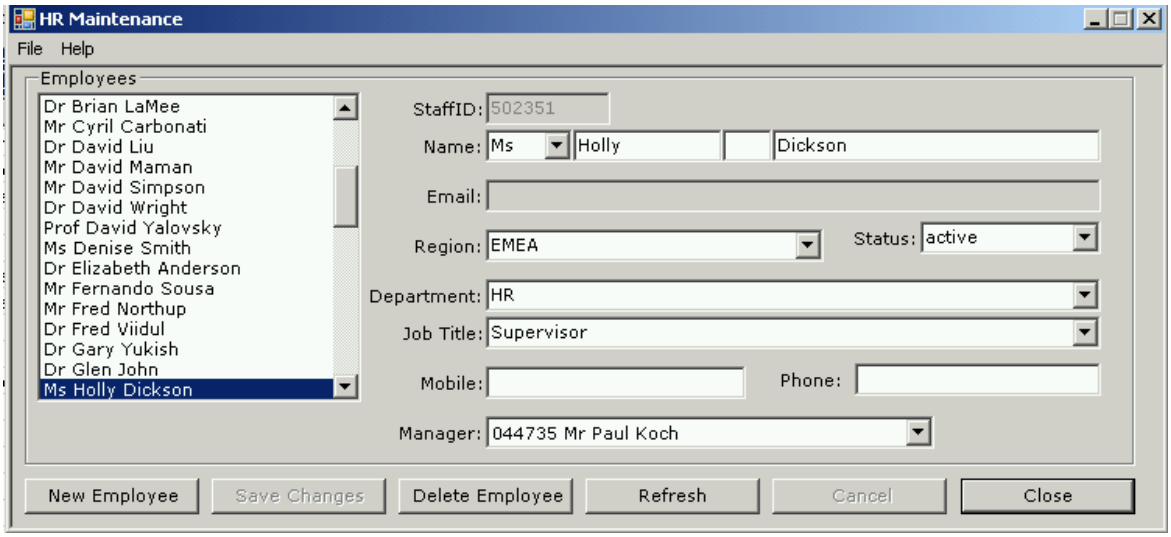



Kuva 71:Kuvassa suodatetun haun lopputulos ja määritellyt sarakkeet ovat näkyvissä.

## Muutoksien tuonti

Tässä osiossa on tarkoitus testata miten muutoksien tuonti tapahtuu käyttämällä FIM:ä. Muutoksia testataan siten että HR maintenance ohjelmassa muokataan,poistetaan ja lisätään käyttäjä jonka jälkeen ajetaan full import ja delta sync suorita profiilit FIM syncronization managerissa.

Ensimmäiseksi muokataan käyttäjätietoja siten että yhdeltä käyttäjältä vaihdetaan osasto, kaksi käyttäjää poistetaan ja lopuksi lisätään yksi käyttäjä.




Kuva72: Kuvassa HR Maintenance henkilöstön hallinta ohjelma.

Seuraavaksi avataan FIM synchronization manager ja valitaan HRData MA ja suoritetaan Full import suorita profiili ja tarkastellaan tuloksia.

| Synchronization Statistics | |
|---|---|
| **Staging** | |
| Unchanged | 59 |
| Adds | 1 |
| Updates | 1 |
| Renames | 0 |
| Deletes | 2 |

Tuloksista näkyy että Full Importin mukana tulleet tiedot ovat juuri ne mitä muokkasin. Tuloksissa näkyy yksi käyttäjän lisäys, yksi tietojen päivitys ja kaksi poistoa. Hyperlinkkejä painamalla aukeaa lisätietoja lisäyksistä tai päivityksistä.

Kuva 73: Synkronoinnin statistiikkaa

Lopuksi ajetaan delta sync suorita profiilit jonka jälkeen muutokset ovat tulleet voimaan pysyvästi. FIM syncronization managerin Operations työkalulla voi tarkastella jo suoritettuja suorita profiileja ja tarkastella niiden statistiikkaa.