LAMK
Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

SALASANANHALLINTAJÄRJESTELMÄ

LAHDEN AMMATTIKORKEAKOULU
Insinööri (AMK)
Tieto- ja viestintätekniikka
Kevät 2019
Topi Kokki

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Kokki, Topi	Opinnäytetyö, AMK	Kevät 2019
	Sivumäärä	
	34	

Työn nimi

Salasananhallintajärjestelmä

Tutkinto

Insinööri (AMK), Tietotekniikka

Tiivistelmä

Opinnäytetyön tavoitteena oli valita ja ottaa käyttöön keskitetty salasananhallintajärjestelmä. Työn toimeksiantajana oli Lahti Energia Oy.

Salasananhallintajärjestelmän tarkoituksena on lisätä tietoturvaa tarjoamalla helppokäyttöinen alusta käyttäjätunnusten ja salasanojen tallentamiseen. Usein tunnistetietoja erilaisia palveluja varten on niin paljon, että niiden muistaminen on mahdotonta. Tunnistetietojen säilyttäminen salaamattomassa muodossa on myös riskialtista, jolloin paras ratkaisu ongelmaan on salasananhallintajärjestelmä.

Salasananhallintajärjestelmä mahdollistaa arkaluontoisten tunnistetietojen tallentamisen ja jakamisen tietoturvan kannalta parhaalla tavalla. Keskitetyn järjestelmän hyötyjä ovat myös helppo hallittavuus ja ylläpito, jotka ovat tärkeitä etenkin suurissa organisaatioissa.

Vaatimuksia salasananhallintajärjestelmälle oli useita, kuten operoitavuus yhtiön omasta konesalista. Mahdollisia vaihtoehtoja kartoitettiin ja testattiin yhteistyössä kohdeyrityksen kanssa. Vaatimuksiin parhaiten soveltuva salasananhallintajärjestelmä otetaan lopulta tuotantokäyttöön.

Asiasanat

salasananhallinta, tietoturva

Abstract

Author(s)	Type of publication	Published
Kokki, Topi	Bachelor's thesis	Spring 2019
	Number of pages	
	34	

Title of publication

Password management system

Name of Degree

Bachelor of Engineering, Information Technology

Abstract

The main objective of this thesis was to choose and deploy a centralized password management system for Lahti Energia Oy.

The main purpose of a password management system is to enhance information security by offering an easy-to-use platform to store usernames and passwords. The amount of privileged credentials is often so high that it is impossible to remember them all. Storing the credentials in a plaintext form is also an insecure practice, therefore the best solution to the problem is a password management system.

A password management system allows to store and share privileged credentials in a secure environment. The benefits of a centralized system include easy management and maintenance, which are key features for large enterprises.

There were numerous requirements for the password management system, such as on-premise installation. Possible solutions were explored and tested in cooperation with the client company. A password management system that met the requirements in the best possible manner was chosen for deployment.

Keywords

password management, information security

SISÄLLYS

LYHENNELUETTELO

2FA	Two-Factor Authentication. Kaksivaiheinen todennus
AD	Active Directory. Käyttäjätietokanta ja hakemistopalvelu
AES	Advanced Encryption Standard. Lohkosalausmenetelmä
CPU	Central Processing Unit. Suoritin
IAM	Identity Access Management. Identiteetin hallinta
LDAP	Lightweight Directory Access Protocol. Verkkoprotokolla
PAM	Privileged Access Management. Ryhmä tietoturvaratkaisuja
RADIUS	Remote Authentication Dial In User Service. Verkkoprotokolla
SSO	Single Sign-On. Todennus useisiin sovelluksiin kerralla
TLS	Transport Layer Security. Salausprotokolla

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on ottaa käyttöön keskitetty salasananhallintajärjestelmä Lahti Energia Oy:lle. Konsernissa käytetään lukuisia omia sekä ulkopuolisten palveluntarjoajien palveluita, jotka vaativat käyttäjältä tunnistautumisen. Toistaiseksi ei ole ollut yhteistä linjaa siitä, miten käyttäjätunnuksia ja salasanoja tulisi säilyttää. Keskitetyn salasananhallintajärjestelmän tarkoituksena on lisätä tietoturvaa sekä tarjota helppokäyttöinen alusta arkaluontoisen tiedon säilyttämiseen.

Keskeinen tavoite on löytää ratkaisu, joka täyttää työn tilaajan vaatimukset mahdollisimman hyvin. Markkinoilla on paljon erilaisia salasananhallintajärjestelmiä, joiden avulla on mahdollista kattaa niin yksittäisten henkilöiden kuin suurien organisaatioidenkin tarpeet. Salasananhallintajärjestelmältä vaaditut ominaisuudet kartoitetaan, minkä jälkeen vertailuun otetaan tuotteita, jotka vaikuttavat parhailta vaihtoehdoilta vaatimuksia ajatellen. Salasananhallintajärjestelmien toimintaa tarkastellaan käytännönläheisesti.

Vertailussa keskitytään eri tuotteiden ominaisuuksiin yleisluontoisesti. Tietoturvan vuoksi tässä opinnäytetyössä ei käsitellä salasananhallintajärjestelmän varsinaista käyttöönottoa lainkaan. Sen sijaan valitusta salasananhallintajärjestelmästä käydään läpi käyttöönottoon liittyvät seikat, yksilöimättä konfiguraatioita ja toimintamalleja suoraan toimeksiantajan ympäristöön.

2 SALASANANHALLINTAJÄRJESTELMÄ

2.1 Salasananhallintajärjestelmän toiminta

Nykyään yhä useammat palvelut toimivat internetissä, ja aivan peruskäyttäjillekin kertyy käyttäjätunnuksia ja salasanoja enemmän kuin pystyy muistamaan. Ongelmaa voi yrittää ratkoa tai kiertää monin tavoin, mutta usein kaikkein yksinkertaisimmat ratkaisut eivät ole parhaita. Yhtä ja samaa salasanaa saatetaan käyttää useissa palveluissa, tai salasanoja kirjoittaa ylös muistioon joko tietokoneelle tai paperille. Tietoturvan kannalta nämä menetelmät eivät ole suositeltavia. Paras ratkaisu on käyttää salasananhallintajärjestelmää. (Zoho 2018.)

Perinteinen salasananhallintajärjestelmä on yksinkertaisimmillaan salattu tietokanta ja tätä käsittelevä asiakasohjelma. Yleinen toimintaperiaate on, että yhdellä todennuksella käyttäjä pääsee käsiksi tietokantaan, jossa on kaikki hänen tallentamansa käyttäjätunnukset ja salasanat. Usein myös muutakin tekstimuotoista dataa, kuten muistiinpanoja, on mahdollista tallentaa. (Techopedia 2018.)

On myös olemassa niin sanottuja tilattomia salasananhallintajärjestelmiä, jotka eivät vaadi minkäänlaista tietokantaa datan tallentamiseen. Kyseessä on algoritmi, jolle voidaan syöttää useita erilaisia lähtöarvoja, ja algoritmi palauttaa paluuarvona merkkijonon, jota voidaan käyttää salasanana. Yksi lähtöarvoista, yleensä oma pääsalasana, voidaan pitää vakiona. Vaihtuvia arvoja voivat olla esimerkiksi nettisivuston nimi tai oma nimimerkki. Kun ohjelmalle syötetään useita arvoja, joista osa on vaihtelevia, algoritmi laskee jokaiselle lähtöarvojen yhdistelmälle uniikin paluuarvon. Näin kaikki salasanat ovat käytettävissä missä tahansa, kunhan käyttäjä pääsee käsiksi laskennan suorittavaan sovellukseen. Menetelmässä on kuitenkin tiettyjä rajoituksia ja ongelmia, joiden takia menetelmä ei sovellu etenkään organisaatioon, jossa käyttäjätunnusten ja salasanojen hallinnan tulee olla keskitettyä. (Vincent 2016; Arcieri 2016.)

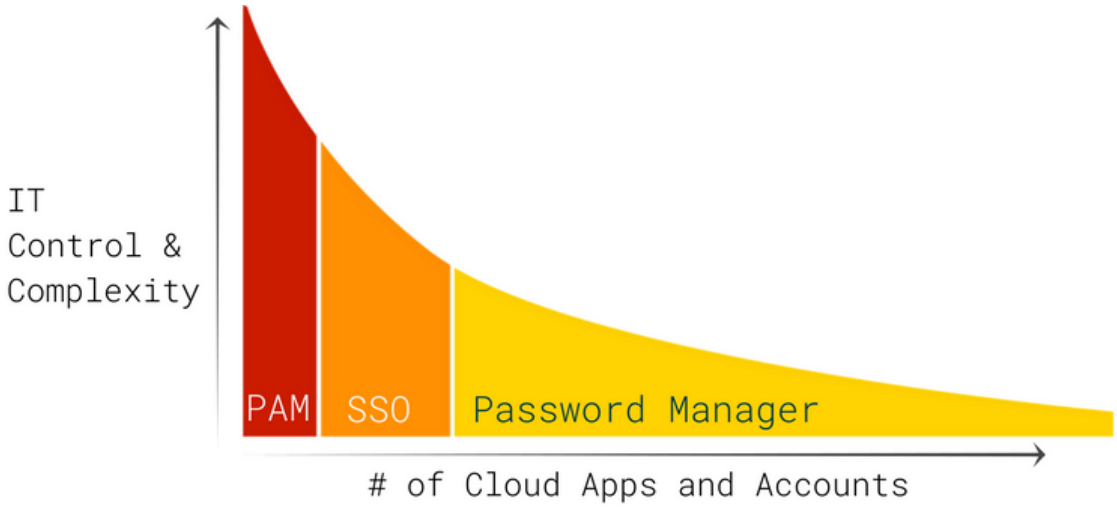
Perinteisiä salasananhallintajärjestelmiä on olemassa eri käyttötarkoituksia varten. Yksittäiselle henkilölle usein riittää yksinkertainen työpöytäsovellus tai pilvipalvelu. Yrityksille suunnatut keskitetyt salasananhallintajärjestelmät tarjoavat lukuisia muita ominaisuuksia, kuten Active Directory -integraation ja resurssien jakamisen käyttäjien kesken. Myös keskitetyt salasananhallintajärjestelmät voivat olla paikallisesti tuotettuja tai pohjautua pilvipalveluun. Ominaisuudet ja niiden toteutus vaihtelevat tuotekohtaisesti. (Allen 2018.)

2.2 Salasananhallintajärjestelmien lisäominaisuudet

Jotkin keskitetyt salasananhallintajärjestelmät tarjoavat Privileged Access Management (PAM) -ominaisuuden. PAM on joukko ratkaisuja, joiden avulla pyritään turvaamaan, hallitsemaan ja valvomaan pääsyä kriittisiin kohteisiin, esimerkiksi palvelimille. Tyypillisessä PAM-toteutuksessa halutun palvelimen käyttäjätunnustiedot tallennetaan ensin salattuun tietokantaan, aivan kuten tavallisessa salasananhallintajärjestelmässä. Kun pääsyä näihin käyttäjätunnustietoihin aletaan rajoittaa ja valvoa sovelluksen sisäisesti, voidaan puhua PAM:sta. Enää ei pidä tai tarvitse olla tekemisissä suoraan käyttäjätunnusten ja salasanojen kanssa, vaan kaikki määritellylle kohteelle tehtävät toimet hoidetaan salasananhallinta/PAM-järjestelmän kautta. Käyttäjällä voi olla esimerkiksi pääsy tietylle palvelimelle vain erikseen pyytämällä. Rajoitusten lisäksi PAM:iin kuuluu osaltaan myös käyttäjän toimien valvominen. Kun toiminta ikään kuin kierrätetään PAM-järjestelmän kautta, jää suoritetuista toimista myös aina jälki PAM-järjestelmään. (The Secret Security Wiki 2018.)

Termiä Single Sign-On (SSO) käytetään kuvaamaan palvelua, jonka avulla käyttäjä autentikoidaan yhdellä todennuksella useisiin sovelluksiin. Salasananhallintajärjestelmästä SSO eroaa siten, että sovellusten on tuettava tiettyä protokollaa autentikointiin, sillä käyttäjä autentikoidaan samalla kertaa jokaiseen määriteltyyn sovellukseen istunnon ajaksi. SSO-ominaisuuteen liittyy myös käyttäjän toimien valvonta. (Rouse 2018.)

Salasananhallintajärjestelmä, PAM- ja SSO-ominaisuudet voidaan käsittää osana suurempaa Identity Access Management (IAM) -strategiaa. Termit menevät helposti sekaisin, sillä niiden välillä on päällekkäisyyttä. Organisaation IAM-ratkaisun voi nähdä useina pienempinä komponentteina, jotka täydentävät toisiaan (kuvio 1). PAM-tyyppiset ratkaisut toimivat hyvin paikallisesti tuotettujen palveluiden yhteydessä ja tarjoavat hallittavuutta, kun taas lukuisat verkkopalvelut vaativat rinnalleen salasananhallintajärjestelmän. On täysin tapauskohtaista, millainen IAM-ratkaisu sopii millekin organisaatiolle. (Katz 2017; Thycotic 2018a.)



KUVIO 1. Kuvaaja termistöstä (Katz 2017)

Kaksivaiheista todennusta käytetään nykyään usein erilaisiin verkkopalveluihin kirjauduttaessa, ja ominaisuus on käytössä myös useissa keskitetyissä salasananhallintajärjestelmissä. Perusajatuksena on, että käyttäjätunnuksen ja salasanan lisäksi vaaditaan vielä toinen tunnistautuminen, joka on sidottu jollakin tavalla henkilön yksilökohtaisiin ominaisuuksiin tai resursseihin. Kyseessä voi olla jotain mitä henkilö tietää, mitä henkilöllä on hallussaan, tai henkilöön itseensä liittyvä fyysinen ominaisuus. Käytännössä vaihtoehtoina voivat olla esimerkiksi ylimääräinen turvakysymys tai salasana, mobiililaitteeseen lähetettävä vahvistusviesti tai biometrinen tunniste. Kaksivaiheisen todennuksen ansiosta hyökkääjä ei vielä pääse käsiksi käyttäjän tietoihin, vaikka toinen tunnistautumistapa murtuisikin. (Authy 2018.)

Nykyään yleisin käytössä oleva symmetrinen salausmenetelmä on AES (Advanced Encryption Standard), joka kehitettiin korvaajaksi vanhentuneille standardeille. Symmetrisessä salausmenetelmässä salaukseen ja salauksen purkamiseen käytetään samaa avainta. Menetelmä on laskennallisesti kevyt ja nopea, mutta haittapuolena sama selkokielinen salausavain pitää jakaa kaikille osapuolille, joiden tulee päästä lukemaan salattua dataa. Ongelman ratkaisemiseksi on kehitetty epäsymmetrisiä salausmenetelmiä, joissa salaukseen ja salauksen purkamiseen käytetään eri avaimia. Käytössä on avainpari, joista toinen avain on julkinen ja toinen yksityinen. Julkinen avain on saatavilla vapaasti, ja sen avulla voidaan salata viesti, joka on avattavissa vain yksityisen ja salassa pidetyn avaimen avulla. Menetelmä toimii myös päinvastaisesti. Salaus toimii vain yhteen suuntaan kerrallaan, minkä ansiosta menetelmää voidaan hyödyntää salatun kommunikointikanavan muodostamiseen. Nykyaikainen TLS-protokolla (Transport Layer Security) yhdistelee sekä symmetrisiä että epäsymmetrisiä salausmenetelmiä. (SSL2BUY 2015.) Salasananhallintajärjestelmät käyttävät usein AES-salausmenetelmää, kun data kirjoitetaan

tallennusmedialle, minkä lisäksi keskitetyissä järjestelmissä palvelimen kanssa kommunikointi on salattu TLS-protokollaa hyödyntäen. Data voidaan myös salata useaan kertaan ja käyttää useita salausavaimia. Toteutukset vaihtelevat tuotekohtaisesti, mutta tietoturvaltaan kriittinen data säilötään ja siirretään aina salatussa muodossa.

3 VAATIMUKSET JA VAIHTOEHDOT JÄRJESTELMÄLLE

3.1 Tilaajan vaatimukset salasananhallintajärjestelmälle

Työn tilaaja, Lahti Energia Oy, asetti useita vaatimuksia salasananhallintajärjestelmälle. Vaatimukset käytiin läpi konsernin tietohallinnon ja tietoturvasta vastaavan henkilön kanssa.

Ensimmäinen ja ehdoton vaatimus on, että palvelua voidaan tuottaa konsernin omasta konesalista. Tämä karsii jo heti alussa pois pilvipalvelut. Päätökselle on perusteena käytettävyys, hallittavuus ja tietoturva. Paikallisesti tuotetuissa palveluissa voidaan esimerkiksi palveluun liikennöintiä rajoittaa omilla palomuurisäännöillä. Lisäksi palvelun data sijaitsee fyysisesti konsernin omilla palvelimilla ja on osa konsernin omaa infrastruktuuria, joten ulkopuoliset häiriöt ja riskitekijät on minimoitu.

Konsernissa käytetään käyttäjätietokantana Microsoftin AD (Active Directory) -tietokantajärjestelmää. Salasananhallintajärjestelmän AD-integraatio mahdollistaa sen, että jo olemassa olevasta käyttäjätietokannasta voidaan hyödyntää tietoja. Palveluun olisi esimerkiksi mahdollista kirjautua AD-tunnuksella ja hyödyntää valmiiksi hakemistosta löytyviä rakenteita. AD-integraatio on toinen vaadittu ominaisuus.

Salasananhallintajärjestelmään tallennettava data on luonteeltaan arkaluontoista, joten käyttäjän todennukseen on kiinnitettävä erityishuomiota. Tietoturvan kannalta on tärkeää, että palvelu tukee kaksivaiheista todennusta, joka on kolmas vaatimus salasananhallintajärjestelmälle.

Näiden vaatimusten lisäksi käytiin läpi useita muita toivottuja ominaisuuksia, jotka eivät ole niin yksiselitteisesti määriteltävissä. Salasananhallintajärjestelmän tulisi olla mahdollisimman helppokäyttöinen peruskäyttäjän näkökulmasta ajatellen, mikä voi tarkoittaa kompromissia helppokäyttöisyyden ja ominaisuuskirjon välillä. Suomenkielinen käyttöliittymä olisi hyödyllinen ominaisuus suurelle osalle käyttäjiä, mutta riittävällä ohjeistuksella ja käyttöliittymän helppokäyttöisyydellä myöskään englanninkielinen käyttöliittymä ei tuota ongelmia. Mahdollinen mobiilisovellus ja selaimeen tai työpöydälle asennettavat lisäosat eivät ole pakollisia, mutta nekin on hyvä käydä läpi ja tutkia, millaista lisäarvoa ne tuovat salasananahallintajärjestelmän käyttöön.

Erityinen pieni tutkimusprojekti liittyy PAM:iin. Konsernilla on käyttöä myös PAM-sovellukselle, joten tehtävänä on myös tutkia, miten hyvin salasananhallintajärjestelmien mahdolliset PAM-ominaisuudet toimivat käytännössä. Optimitilanteessa olisi vain yksi tuote, jota voisi hyödyntää molemmissa käyttötilanteissa.

PAM:n testausta varten kuvailtiin yksinkertainen käytännön tilanne, joka etenee seuraavalla tavalla: Yhtiön ulkopuolisen toimijan pitää päästä käsiksi johonkin Lahti Energian palvelimeen etätyöpöytäyhteyden avulla. Hän kirjautuu salasananhallinta/PAM-sovellukseen, ja pyytää käyttöoikeutta etätyöpöydälle. Tästä lähetetään ilmoitus IT-osastolle tai sovelluksen pääkäyttäjälle, joka päättää, hyväksytäänkö pyyntö vai ei. Kun pyyntö hyväksytään, ulkopuolinen toimija pääsee kirjautumaan etätyöpöydälle avaamalla yhteyden salasananhallinta/PAM-järjestelmän kautta. Etätyöpöytäyhteyden tunnistetiedot ovat tallennettuna salasananhallintajärjestelmässä. Käyttäjän ei tarvitse tietää salasanaa ja salasana voidaan piilottaa häneltä. Lisäksi koko istunto etätyöpöydällä voitaisiin tallentaa videomuodossa, jotta kaikesta palvelimelle tehdyistä muutoksista jäisi jälki järjestelmiin.

Viimeisenä seikkana palvelun tulisi olla mahdollisimman toimintavarma ja vaivaton ylläpitää. Palveluun tullaan tallentamaan tärkeää ja arkaluontoista dataa, joten toimintavarmuudesta ei haluta tinkiä. Käyttötarkoitukseen sopivaa salasananhallintajärjestelmää aletaan etsimään ensisijaisesti haluttujen ominaisuuksien perusteella. Hintoja vertaillaan eri tuotteiden kesken, jotta saadaan käsitys yleisestä hintatasosta.

3.2 Salasananhallintajärjestelmien vaihtoehtojen kartoitus

Vaatimuksiin soveltuvien salasananhallintajärjestelmien etsintä tapahtui yksinkertaisesti hakukoneen avulla. Vaatimuksiin kokonaan tai osittain sopivia vaihtoehtoja löytyi noin 20, ja kaikista niistä otettiin tärkeimmät ominaisuudet muistilistalle. Tämä listaus käytiin läpi IT-osaston palaverissa, jossa vaihtoehtoja arvioitiin. Tässä vaiheessa valintaperusteena oli esimääriteltyjen vaatimusten lisäksi ohjelmistotuottajien omat referenssit. Ohjelmistontuottajien laaja olemassa oleva asiakaskunta sekä auditoinnit ovat keinoja arvioida ohjelmistojen luotettavuutta, vaikka useissa kaupallisissa tuotteissa ohjelmistojen lähdekoodi ei olekaan avointa.

Vaihtoehtoja karsittiin, ja jäljelle jäi viisi vaihtoehtoa, jotka otettiin testiin. Valinnassa suosittiin pääosin alan tunnetuimpia ohjelmistontuottajia sekä painotettiin tuotteita, jotka on ensisijaisesti tarkoitettu salasananhallintaan. Lisäominaisuudet, kuten PAM, tulevat prioriteettilistalla vasta seuraavaksi. Vaihtoehdoiksi valikoitui neljä kaupallista tuotetta sekä yksi avoimeen lähdekoodiin perustuva ilmainen vaihtoehto.

4 SALASANANHALLINTAJÄRJESTELMIEN TESTAUS

4.1 Salasananhallintajärjestelmien testialusta

Resurssit kaikkien ohjelmistojen testaamiseen tarjosi kohdeyritys. Testialustana käytettiin pääasiassa Windows Server 2016 -käyttöjärjestelmää. Ohjelmistot ovat pääosin yksinkertaisia asentaa, joten jos asennuksessa ei tullut vastaan mitään huomionarviosta, ei siihen keskitytä sen suuremmin. Jokaista testattavaa tuotetta varten luotiin oma virtuaalikone, joita ajettiin VMware-virtualisointialustan päällä. Virtuaalikoneille määriteltiin kaksi gigatavua muistia, kaksi CPU-ydintä ja 40 gigatavua levytilaa levyjärjestelmän hitaalta osiolta. Resurssit riittävät testaukseen, ja lopulliselle salasananhallintajärjestelmälle voidaan määritellä enemmän resursseja, mikäli niin halutaan.

Testivaiheessa on tärkeintä saada yleiskuva tuotteista sekä vertailupohjaa lopullisen valinnan tueksi. Usein ominaisuuksia ja asetuksia on niin paljon, ettei jokaisen kohdan läpikäynti opinnäytetyössä ole mielekästä. Kun valinta on tehty, on helpompi keskittyä yhteen tuotteeseen hieman syvällisemmin. Maksullisten tuotteiden lisensointimallit ovat erilaisia ja hinta muodostuu usein monesta tekijästä, minkä vuoksi täsmällistä arviota hinnasta on vaikea antaa. Tuotantoympäristössä käyttäjien määräksi on arvioitu noin 200.

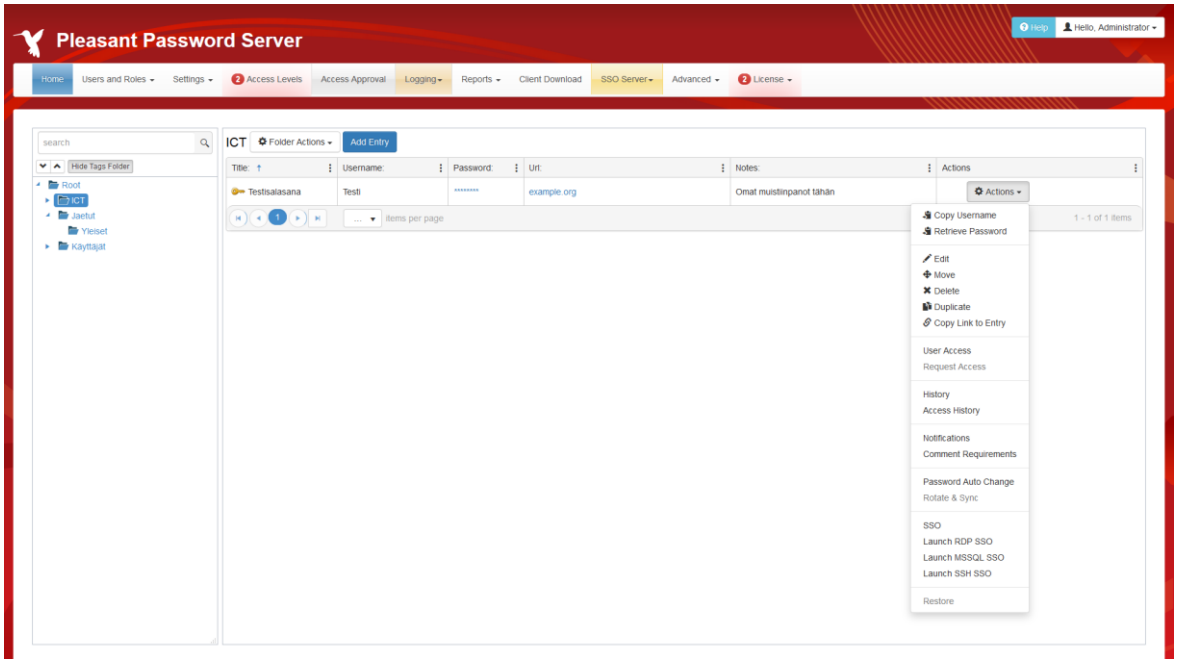
Kaikista tuotteista testataan ja arvioidaan vapaamuotoisesti seuraavat asiat:

- käyttäjätunnusten ja salasanojen tallentaminen, muokkaus ja poisto sekä muut vastaavat perusominaisuudet
- käyttäjätunnusten ja salasanojen ryhmittely, niiden jakaminen ryhmän kesken sekä tarvittavien käyttöoikeuksien määrittely
- käyttöliittymän arviointi yleisesti
- palvelun ylläpito ja hallinnointi
- kaksivaiheinen todentaminen
- PAM
- muut tuotekohtaiset ominaisuudet.

4.2 Pleasant Password Server

Pleasant Password Server (kuvio 2) on kanadalaisen Pleasant Solutions -yhtiön kehittämä salasananhallintajärjestelmä. Ominaisuuksiin kuuluu muun muassa AD-integrointi, käyttöoikeusien hallinta sekä monipuoliset asiakasohjelmat palvelun käyttöä varten. Saatavilla on 30 päivän ilmainen testiversio. Tuotteen hinta muodostuu valittujen ominaisuuksien ja

käyttäjämäärän mukaan. Kallein versio kahdellesadalle käyttäjälle kustantaa noin 13 000 dollaria vuodessa. (Pleasant Solutions 2018a; Pleasant Solutions 2018b.)



KUVIO 2. Kuvakaappaus Pleasant Password Server perusnäkymästä

Palvelun asennusprosessi on testatuista tuotteista kaikkein yksinkertaisin ja nopein. Oletusasetuksilla asennettaessa palvelu on pystyssä noin minuutissa, ja hallintanäkymään pääsee kirjautumaan paikallisella käyttäjätunnuksella.

Käyttöliittymän ulkoasu on selkeä ja loppuun asti mietitty. Aloitusnäkymässä ylhäällä on päävalikot ja vasemmalla on puumainen kansiorakenne salasanaryhmille. Käyttöliittymää ei juurikaan pääse muokkaamaan. Kaikille manuaalisesti luoduille tai AD:sta tuoduille käyttäjille luodaan automaattisesti oma kansio henkilökohtaisille salasanoille. Peruskäyttäjä näkee kansiorakenteessa vain ne kansiot, joihin hänellä on määritelty käyttöoikeudet. Oletuksena vain pääkäyttäjät voivat lisätä kansiota ja muokata käyttöoikeuksia, mutta näitäkin oikeuksia voidaan määritellä eteenpäin myös muille käyttäjille. Salasanojen hallinta ja jakaminen on helppoa eikä vaadi suurta perehtymistä.

AD-integraatiota hyödynnettäessä palvelun peruslogiikka toimii niin, että palveluun tuodaan ensin määritellyt käyttäjät ja ryhmät. Käyttäjien ja ryhmien keskinäiset suhteet ovat määritelty valmiiksi AD:ssa, ja niitä voidaan käyttää sellaisenaan palvelussa. Esimerkiksi jos palveluun tuodaan ICT-ryhmä, ryhmä sisältää kaikki käyttäjät, jotka ovat AD:ssa määritelty kyseiseen ryhmään. Tätä ryhmää voidaan käyttää suoraan palvelun omien käyttöoikeuksien määrittelyyn, eli esimerkiksi mihin salasanasanoihin ryhmällä on oikeudet.

Palveluun tuodulle tiedoille voidaan määritellä säännöllinen synkronointi AD-palvelimen kanssa, jotta tiedot pysyvät ajan tasalla.

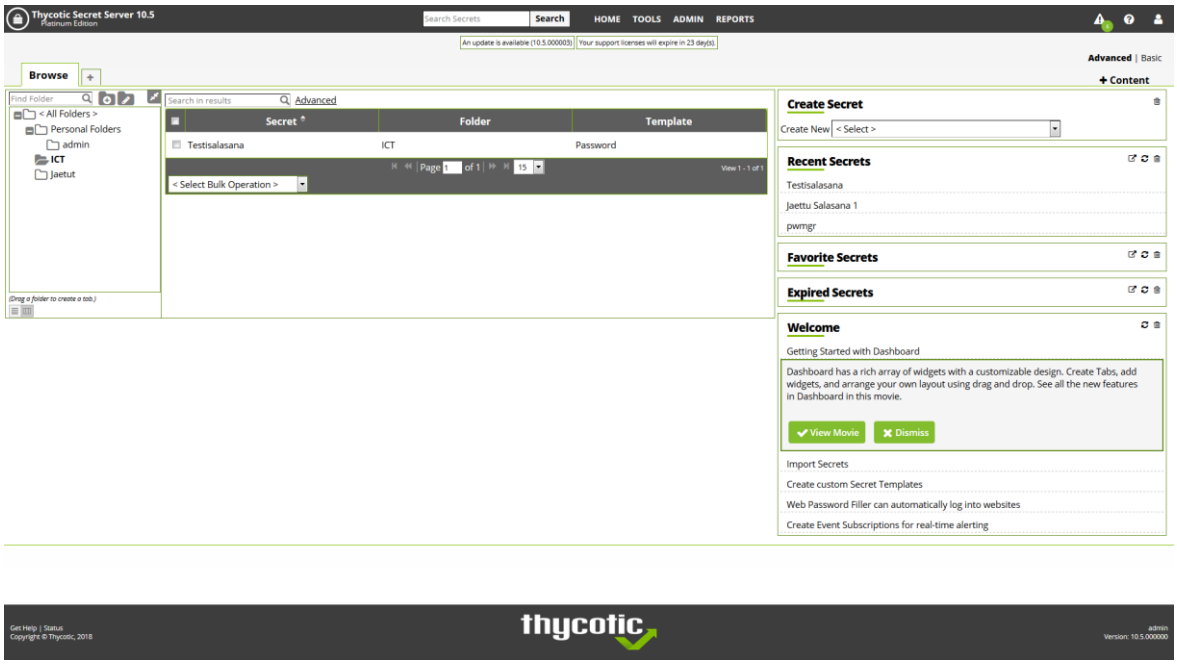
Pleasant Password Server tarjoaa selainkäyttöliittymän ja mobiilisovelluksen lisäksi erillisen KeePass-työpöytäsovelluksen palvelun käyttöä varten. Kyseessä on jonkin verran muokattu versio alkuperäisestä KeePass-työpöytäsovelluksesta. Muokattu versio toimii muuten samalla tavalla, mutta hyödyntää palvelimen tietokantaa paikallisen sijasta. Suurin hyöty tästä on peruskäyttäjille, koska KeePass-sovelluksen kielen saa vaihdettua suomeksi ja ohjelma on yksinkertainen käyttää. Kaikkia toimintoja, kuten käyttöoikeuksien hallintaa, ei työpöytäsovelluksesta kuitenkaan löydy, joten vastaavat toimenpiteet pitää tehdä web-käyttöliittymän kautta.

Kaksivaiheinen todentaminen Duo Securityn avulla vaatii paikallisen RADIUS-palvelimen, joka toimii välityspalvelimena Pleasant Password Serverin ja Duon palvelimien välillä. Eräs paikallinen RADIUS-palvelin oli jo yhtiöllä käytössä jo ennestään, joten sitä pääsi hyödyntämään suoraan. Kaksivaiheinen todentaminen toimii kuten pitää.

PAM-ominaisuutena Pleasant Password Server tarjoaa erillisen SSO-moduulin, joka sisältyy kaikkein kalleimpaan versioon ohjelmistosta. Sen avulla on mahdollista toteuttaa aiemmin kuvailtu tilanne, jossa käyttäjä pyytää oikeutta päästä käsiksi etätyöpöydälle. Käyttöoikeuden pyytäminen ja myöntäminen tapahtuu salasananhallintajärjestelmän sisällä, ja lopulta käyttäjä pääsee avaamaan linkin, jonka protokolla on kytketty paikalliseen etätyöpöytäsovellukseen. Tämän sovelluksen saa ladattua web-käyttöliittymän kautta, mutta sen asennukseen tarvitaan työaseman pääkäyttäjän oikeudet. Tämä saattaa olla ongelmallista esimerkiksi ulkopuolisten käyttäjien kannalta, sillä heille ei mahdollisesti ole myönnetty oikeuksia asentaa ohjelmia itsenäisesti työasemalleen. Etätyöpöytäyhteys vaatii toimiakseen myös voimassa olevan turvallisuusvarmenteen liikenteen salaamista varten.

4.3 Thycotic Secret Server

Thycotic on yhdysvaltalainen tietoturvaratkaisuihin erikoistunut yritys. Tuoteperheeseen kuuluu useita ohjelmistoja, joista Secret Server (kuvio 3) yhdistelee salasananhallinta- ja PAM-järjestelmän yhdeksi kokonaisuudeksi. Hinta muodostuu haluttujen ominaisuuksien mukaan, ja hintatietoja varten on aina pyydettävä tarjous myyntiosastolta. (Thycotic 2018b.) Jostakin syystä vastausta ei saatu, vaikka hintaa kyseltiin pariin otteeseen. Kuukauden voimassa oleva testiversio on kuitenkin ladattavissa vapaasti.



KUVIO 3. Kuvakaappaus Thycotic Secret Server perusnäkymästä

Thycotic Secret Server oli testatuista tuotteista kaikkein hitain asentaa. Tuote vaatii toimiakseen Microsoftin SQL-palvelimen, IIS-palvelut ja .NET Frameworkin, mutta asennusohjelma osaa asentaa nämä myös itse, mikäli ne puuttuvat. Asennus oli helppoa, mutta siinä kesti lähes tunnin verran, vaikka vaaditut lisäohjelmistot olivat jo valmiiksi asennettu.

Aloitusnäkymä on oletuksena hieman sekava, mutta toisin kuin muissa tuotteissa, ulkoasua saa muokattua itse. Kiinteänä osana käyttöliittymässä on vasemmalla oleva kansiorakenne ja sen vierellä oleva listaus kansioon tallennetusta datasta. Lisäksi saatavilla on vapaasti liikuteltavia elementtejä, esimerkiksi listaus viimeksi käytetyistä salasanoista. Salasanojen hallinta on helppoa, ja perusominaisuudet kuten salasanojen lisäys, muokkaus, jakaminen ja poisto toimivat hyvin.

AD-integraatio toimii samalla tavalla kuten Pleasant Password Serverissä. Käyttäjät ja ryhmät tuodaan ensin palveluun, ja palvelun omia käyttöoikeuksia voidaan suoraan määritellä AD-ryhmien perusteella. Kaksivaiheinen todentaminen Duon kautta on tuettu suoraan, eli erillistä välityspalvelinta ei tarvita. Thycotic Secret Server kommunikoi suoraan Duon palvelinten kanssa, ja kaksivaiheinen todentaminen toimii kuten pitää.

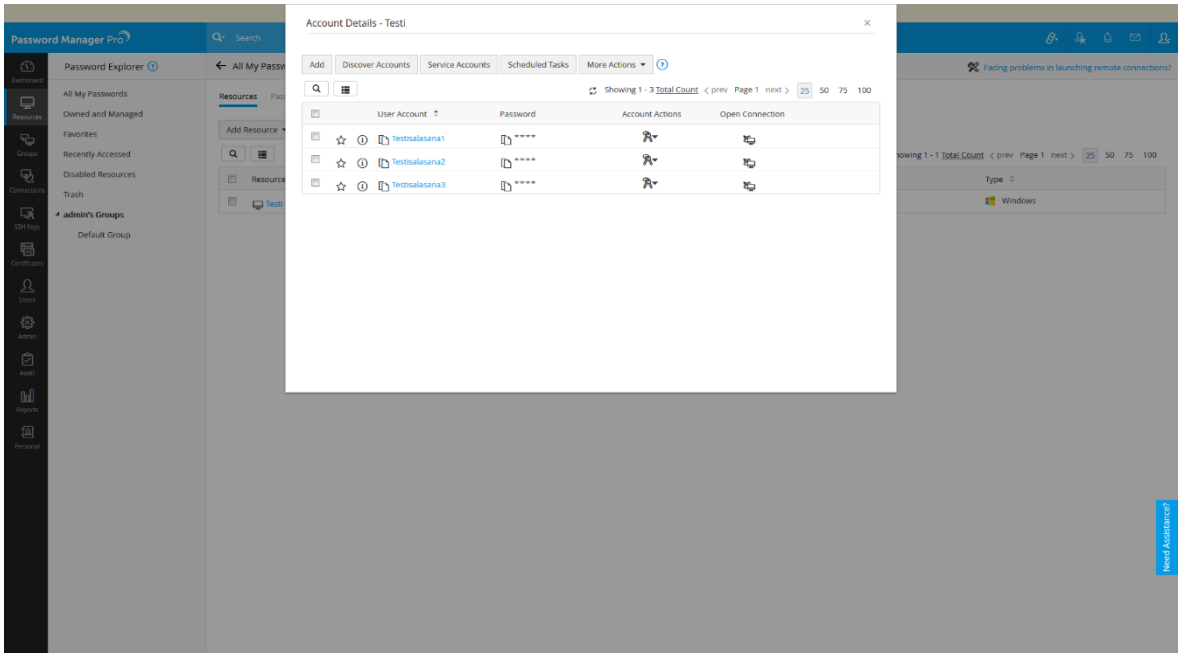
Thycotic Secret Server vaikutti muihin tuotteisiin verrattuna paljon raskaammalta. Välillä valikoiden avaamisessa oli jopa minuutin viiveitä. Resurssienhallinnassa ei näkynyt mitään poikkeavaa eikä resurssien lisääminen virtuaalipalvelimelle vaikuttanut suorituskykyyn. Asennuksen yhteydessä tuli selväksi, että ohjelmisto hyödyntää useita Microsoftin omia ohjelmistokomponentteja, joten vika voi olla yhtä lailla niissäkin. Kyseessä on

todennäköisesti bugi eikä asiaa alettu sen kummemmin tutkimaan. Ongelma saattaisi olla kohtuullisen helposti ratkaistavissa ottamalla yhteyttä tekniseen tukeen.

PAM-ominaisuuden puolesta Thycotic Secret Server toimii identtisesti Pleasant Password Serverin kanssa. Käyttöoikeus pyydetään ja myönnetään sovelluksen sisällä, jonka jälkeen käyttäjä pääsee käsiksi linkkiin, jonka protokolla on kytketty paikalliseen työpöytäsovellukseen. Ratkaisuun liittyy myös tiedossa oleva huono puoli: paikallinen työpöytäsovellus on asennettava jokaiselle työasemalle erikseen, mikäli PAM-ominaisuutta halutaan käyttää. Myös turvallisuusvarmenne pitää olla kunnossa, kuten edellisessäkin tapauksessa.

4.4 ManageEngine Password Manager Pro

ManageEngine on osa intialaista Zoho-yhtiötä. ManageEnginen valikoimiin kuuluu yli 90 yritysten IT-osastoille suunniteltua hallinta- ja ylläpitosovellusta. Password Manager Pro (kuvio 4) on ManageEnginen monipuolinen salasananhallintajärjestelmä. (Zoho 2018.)



KUVIO 4. Kuvakaappaus ManageEngine Password Manager Pro resurssivalikosta

Tuotteesta on saatavilla sekä Windows- että Linux-versiot. Testikäyttöä varten asennettiin Windows-versio. Asennus oli vaivatonta ja vei vain hetken.

Käyttöliittymä on miellyttävä. Vasemmalla on useita päätason valikoita, joiden avulla navigoidaan syvemmälle käyttöliittymään. Valikot on tehty niin, että kaikki asetukset löytyvät intuitiivisesti sieltä mistä niiden olettaisikin löytyvän, ilman turhaa etsimistä. AD-integraatio toimii kuten edellisissäkin tuotteissa. Käyttäjiä voidaan tuoda järjestelmään esimerkiksi

ryhmän perusteella sekä määritellä synkronointiaikataulu AD-palvelimen kanssa, jotta tiedot pysyvät ajan tasalla. Kaksivaiheinen todentaminen toimii Duon kanssa kuten pitää.

Password Manager Pro:n käyttölogiikka toimii hieman eri tavalla kuin muissa tuotteissa. Käyttäjätunnusten ja salasanojen tallennus on jaettu kahteen osioon, joilla on eri käyttötarkoitus. Käyttäjän omille salasanoille on ”Personal” -osio, jonka voi tarvittaessa vielä erikseen suojata salasanalla. Tälle osiolle voi tallentaa käyttäjätunnuksia ja salasanoja eikä osio tarjoa muuta toiminnallisuutta. Henkilökohtaisen osion lisäksi on olemassa ”Resources” -osio, johon voidaan yhtä lailla tallentaa tunnistetietoja, mutta jonka toiminnallisuus liittyy etäyhteyksien hallintaan ja PAM-ominaisuuteen.

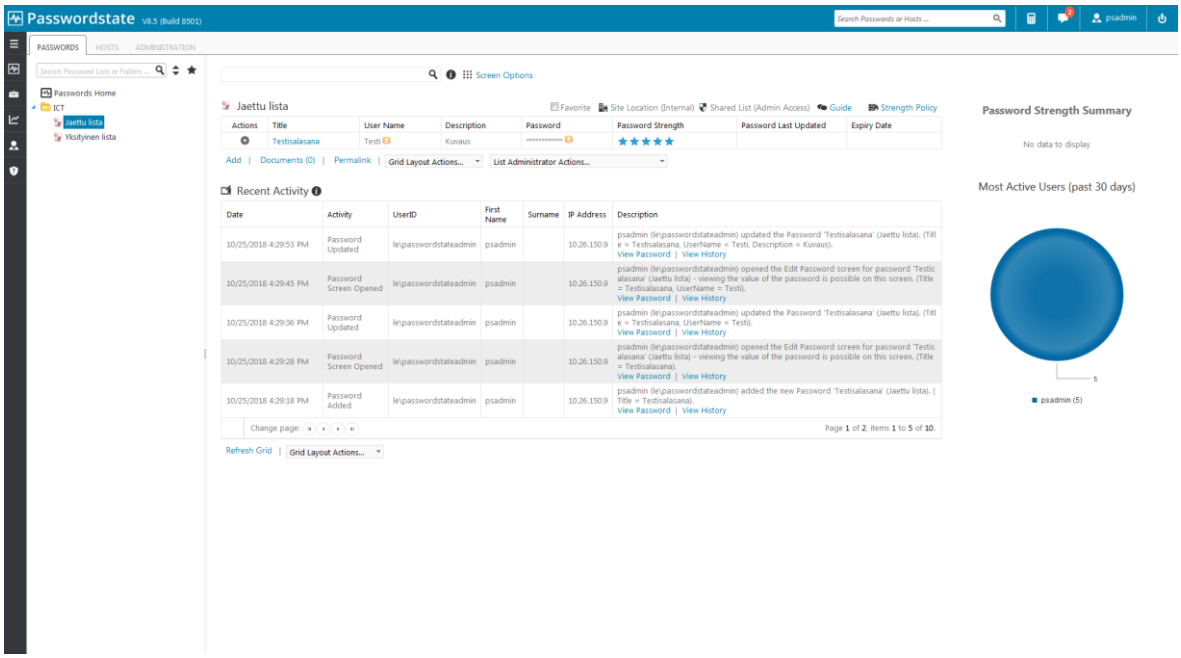
Resurssit-osio ei tarjoa perinteistä kansiorakennetta, vaan kaksitasoisen mallin tietojen tallentamiseen. Aluksi luodaan pohjalle Resurssi, jonka voi käsittää eräänlaisena kansiona. Sille voidaan määritellä esimerkiksi palvelimen osoite ja muita parametreja. Resurssin sisälle voidaan lisätä sitten varsinaiset käyttäjätunnukset, joita käytetään kyseiselle palvelimelle kirjautuessa. Näistä tiedoista luodaan pikakuvakkeen tapainen käyttöliittymäelementti, jota klikkaamalla esimerkiksi etätyöpöytäyhteyksiä pääsee käyttämään suoraan selainkäyttöliittymän kautta. Ominaisuuksiin kuuluu myös monipuolinen käyttöoikeuksien hallintaominaisuus, jonka avulla pääsyä tunnistetietoihin pääsee rajoittamaan esimerkiksi pyyntöjen perusteella. Tuloksena on testatuista tuotteista parhaiten toteutettu PAM-ominaisuus.

Password Manager Pro:n lisensointimalli on erilainen muihin tuotteisiin verrattuna. Hinta koostuu kolmesta osasta: ylläpitäjien lukumäärästä, valitusta ominaisuuskirjosta sekä valinnaisesta SSH-avainten ja SSL-varmenteiden uusimiseen tarkoitetun palvelun kustannuksista. (ManageEngine 2018a.) Tärkein yksittäinen tekijä on tässä tapauksessa ylläpitäjien lukumäärä. Jokaiselle palvelun käyttäjälle on määritelty rooli, jonka mukaan käyttäjä saa valtuuksia suorittaa toimintoja. Toimintoja on suuri määrä, ja ne on jaettu kahteen kategoriaan: peruskäyttäjän toiminnot ja ylläpitäjän toiminnot. Esimerkiksi resurssien jakaminen muille käyttäjille on ylläpitotoimi, joten kyseinen käyttäjä kuluttaa yhden ylläpitäjän lisenssin, mikäli resurssien jako-oikeus on hänelle määritelty. (ManageEngine 2018b.) Tämän vuoksi palvelun kustannukset voivat vaihdella rajusti muutamista tuhansista kymmeniintuhansiin dollareihin vuodessa, käyttötavasta riippuen.

4.5 Passwordstate

Passwordsate (kuvio 5) on australialaisen Click Studios -yhtiön kehittämä salasananhallintajärjestelmä ja samalla yhtiön ainoa tuote. Hinnan perustana on kertamaksu, jonka lisäksi ohjelmistopäivityksistä ja teknisestä tuesta sekä erillisistä lisämoduuleista veloitetaan

vuosimaksu. (Click Studios 2018.) Passwordstate on halvin kaikista vertailluista kaupallisista tuotteista, sillä kertaoston jälkeen palvelun vuosikustannukset ovat edullisimmillaan vain noin tuhat dollaria vuodessa.



KUVIO 5. Kuvakaappaus Passwordstate perusnäkymästä

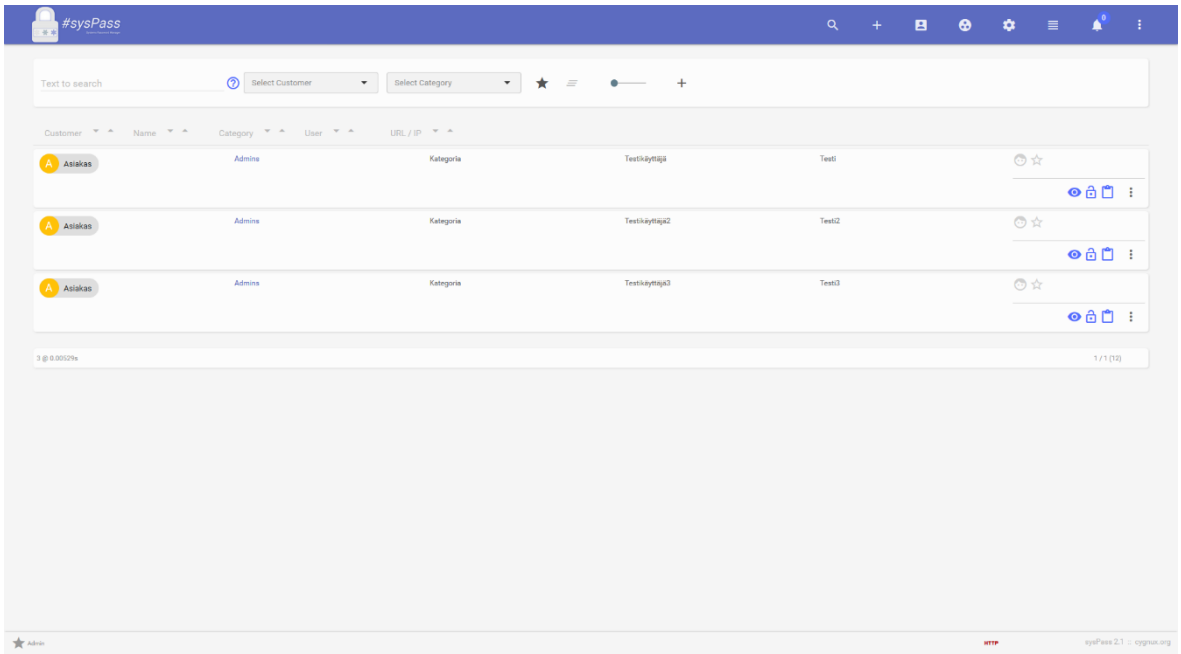
Passwordstaten perusasennus on nopeaa ja helppoa, asennuksen jälkeen web-käyttöliittymään kirjautuessa pyydetään määrittämään asetuksia ennen käyttöönottoa. Muista kaupallisista tuotteista poiketen palvelu vaatii tietokantapalvelimen määrittelyn manuaalisesti. Esimääriteltyjä vaihtoehtoja on joustavasti: tietokanta voi sijaita esimerkiksi omalla paikallisella palvelimella tai vaikkapa Amazonin pilvipalvelussa. Testiä varten asennettiin samalle palvelimelle Microsoftin SQL Express -tietokantapalvelu, johon piti määritellä useita käyttöoikeusasetuksia, jotta Passwordstate kykeni käyttämään tätä tietokantaa. Tietokannan määrityksen jälkeen piti valita, miten palveluun kirjaudutaan: paikallisilla käyttäjätunnuksella vai AD-tunnuksella. On tärkeää huomata, että tätä valintaa ei pysty myöhemmin muuttamaan, joten päätös pitää tehdä heti alussa. Tässä ympäristössä valittiin AD-tunnistautuminen.

Käyttöliittymä noudattelee samaa linjaa kuin ManageEnginen Password Manager Pro, mutta on jonkin verran sekavampi. Käyttöliittymässä käytetään paljon vaaleita värejä, jolloin eri elementit ikään kuin sulautuvat toisiinsa. Kuten useissa muissakin tuotteissa, perusnäkymässä vasemmalla on kansiorakenne ja sen vierellä listaus kansion datasta. Oletuksena näkymässä on myös reaaliaikainen loki, joka näyttää myös käyttäjälle jokaisen hänen tekemänsä muutoksen. Salasanojen hallinta ja jakaminen toimivat helposti, mutta peruskäyttäjälle tuotteen ulkoasu saattaa olla hieman sekava.

AD-integraatio toimii kuten muissakin tuotteissa. Kaksivaiheiselle todennukselle on kattava tuki, ja Passwordstate toimii suoraan Duon kanssa. Passwordstaten PAM-ominaisuudet ovat halutun toiminnallisuuden osalta puutteelliset. Hyvänä puolena etätyöpöytäyhteydet saa avautumaan suoraan selaimessa, mutta käyttöoikeuksien määrittelymahdollisuudet eivät ole niin laajat kuin muissa tuotteissa. Käyttäjälle voidaan jakaa tunnistetietoja etätyöpöytäyhteyksien käyttämistä varten pysyvästi tai tiettyyn kellonaikaan, mutta ei pyyntöjen perusteella. Asiaa tiedusteltiin tuotteen teknisestä tuesta ja vastauksena oli, että kyseinen ominaisuus on vasta kehitteillä.

4.6 sysPass

Avoimeen lähdekoodiin perustuva sysPass (kuvio 6) otettiin testiin, jotta nähtäisiin miten sen ominaisuudet vertautuvat kaupallisiin tuotteisiin. Käyttöjärjestelmistä tuettuina ovat CentOS ja Debian, joista käyttöön valikoitui jälkimmäinen. Asennusdokumentaatio on puuttellinen, ja joitakin puuttuvia php-moduuleja piti etsiä virheviestien perusteella, ennen kuin web-käyttöliittymän sai toimimaan. Myös MariaDB-tietokannan alkumääritykset piti tehdä manuaalisesti.



KUVIO 6. Kuvakaappaus sysPass perusnäkymästä

Käyttöliittymä on perusrakenteeltaan toimiva, mutta graafinen ilme ei yllä muiden vertailussa olleiden tuotteiden tasolle. Tekstien sijaan valikoissa käytetään ikoneja, mikä hieman vaikeuttaa navigointia. Kansiorakennetta tietojen organisointiin ei ole, vaan kaikki tallennetut salasanat menevät yhteen pitkään listaan, josta niitä on tarkoitus etsiä haun avulla. Kun käyttäjätunnuksia ja salasanoja alkaa tallentamaan järjestelmään, kaikkien

kohdalla on pakollista täyttää myös ylimääräiset kentät ”Customer” ja ”Category”, mikä hieman hidastaa käyttöä. Kyseessä on käytännössä kaksi ylimääristä muuttujaa, joita voidaan käyttää halutulosten suodattamisessa. Käyttäjätunnusten ja salasanojen jakaminen onnistuu, mutta ominaisuus on toteutettu vähemmän intuitiivisesti kuin muissa vertailluissa tuoteissa. Hyvänä puolena itse sovellus toimii erittäin nopeasti.

AD-integraatio on tuettuna LDAP-protokollan kautta. Palveluun tuotavien ryhmien polut on kirjoitettava täydellisenä, jotta järjestelmä ymmärtää ne, mutta muuten suurempia käytännön eroja Windows-pohjaiseen järjestelmään ei ole. Kaksivaiheinen todennuksen saa mobiililaitteelle Google Authenticatorin avulla. PAM-ominaisuuksia ei ole.

5 JÄRJESTELMÄN KÄYTTÖÖNOTTO

5.1 Salasananhallintajärjestelmien vertailu ja valinta

Joka ohjelmistontuottajalla on oma tapansa esitellä ja markkinoida tuotettaan, ja pelkästään listattujen ominaisuuksien perusteella olisi mahdotonta tehdä arviointia. Kaikki testatut tuotteet ovat ominaisuuksiensa puolesta jonkinlaisia hybridejä, joissa yhdistyy erilaisia salasananhallinta-, SSO- ja PAM-ominaisuuksia. Jokaista tuotetta pitää käsitellä yksilönä eikä kaikilta ominaisuuksiltaan täydellistä ratkaisua löytynyt, mutta melko lähelle silti päästiin.

Ohjelmistojen keskinäinen vertailu on koottu taulukkoon (taulukko 1). Vihreä väri kuvastaa positiivista ominaisuutta tai toteutusta, ja punainen, negatiivista. Jokaista kohtaa arvioitaessa vertailupohjana on käytetty vain vertailun muita tuotteita, joten taulukko kuvastaa vain valittujen ohjelmistojen keskinäisiä suhteita eikä absoluuttista totuutta.

TAULUKKO 1. Salasananhallintajärjestelmien ominaisuuksien vertailu

	Pleasant Password Server	Thycotic Secret Server	ManageEngine Password Manager Pro	Passwordstate	sysPass
Käyttöliittymä					
AD-integrointi					
2FA-tuki					
Mobiilisovellus ja selainlisäosa					
PAM					
Logitus ja raportointi					

Ylläpito ja hallinnonti					
Hinta					
Lähdekoodin avoimuus					

Pelkästään salasanojen keskitettyyn hallintaan ja jakamiseen on oikeastaan samantekevää, minkä tuotteista valitsisi. Käyttöliittymän osalta eroja löytyy jonkin verran, mutta pääasiassa kaikissa tuotteissa on toteutettuna samat perusominaisuudet, usein vielä samalla tavalla. Lisäominaisuudet, kuten mobiilisovellukset ja selainlisäosat, toimivat kaikissa tuotteissa vähintään kohtuullisesti. Ylläpitäjän näkökulmasta minkään vertailussa olleen salasananhallintajärjestelmän käyttö ei tuota ongelmia, mutta asian voi kääntää myös toisinpäin: jos ajatellaan asiaa peruskäyttäjän näkökulmasta, on olemassa tietty määrä toimintoja, jotka pitää opetella joka tapauksessa, jotta salasananhallintajärjestelmän käyttö olisi tarkoituksenmukaista ja tehokasta. Tässä suhteessa kaikki tuotteet ovat edelleen suhteellisen samalla viivalla.

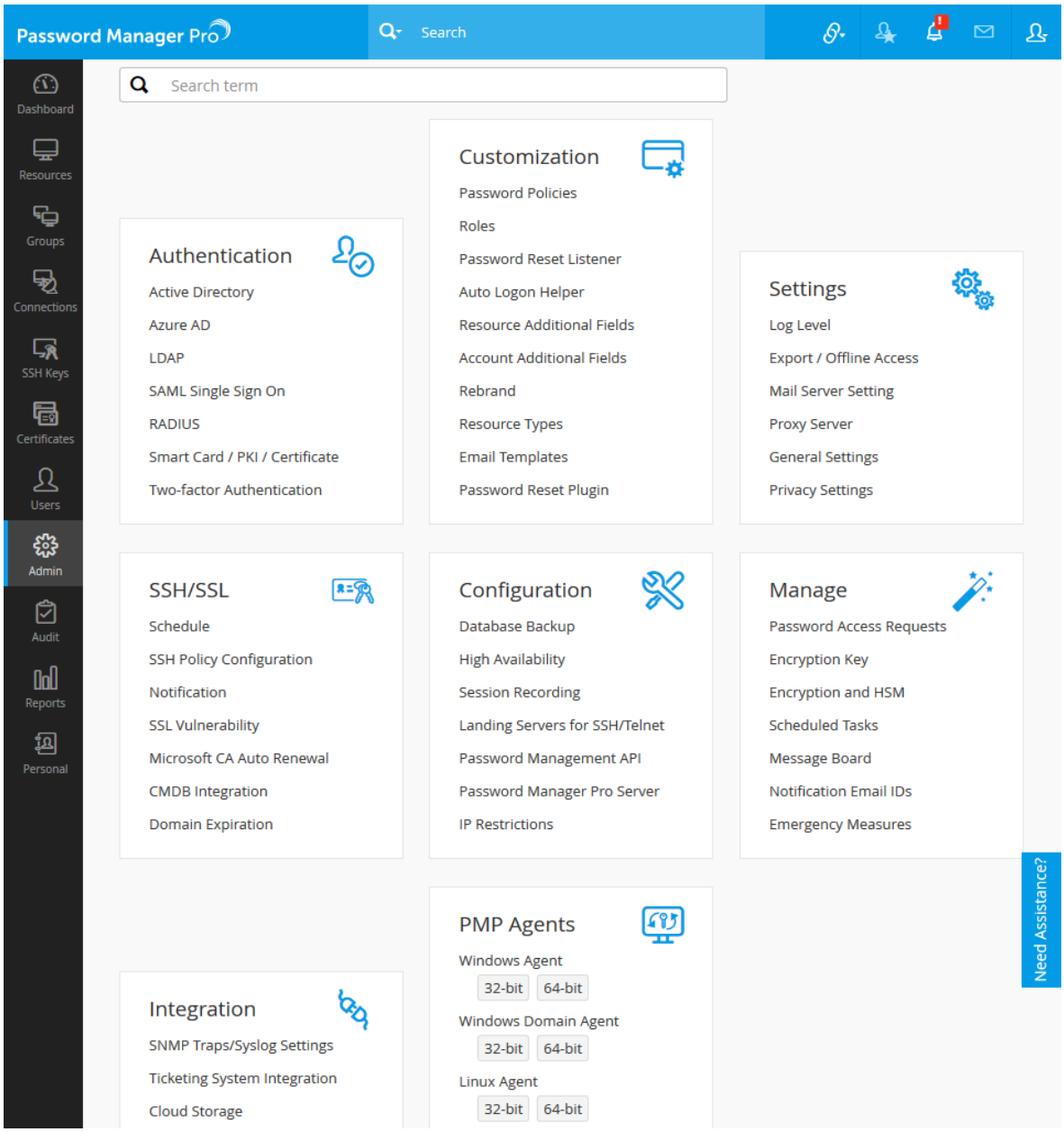
Erot tulevat selkeämmin esiin, kun vertaillaan PAM-ominaisuuksia. PAM-ominaisuuksien toteutus vaihtelee tuotekohtaisesti. Esimerkiksi Passwordstate ei tue resurssien käyttöoikeuden myöntämistä pyyntöjen perusteella, mikä taas oli toimeksiantajan toiveiden listalla PAM-ominaisuuteen liittyen. ManageEnginen tuote suoriutui vertailluista tuotteista kaikkein parhaiten. Ohjelmisto täytti vaatimukset hyvin, minkä lisäksi etätyöpöytäyhteyksiä voidaan käyttää suoraan selaimen kautta. sysPass ei tukenut PAM:ia lainkaan, joten ohjelmisto jätettiin pois laskuista.

Kaikki vertailussa olevat tuotteet käytiin läpi yhteistyössä kohdeyrityksen kanssa. Valituksi tuli ManageEngine Password Manager Pro. Ohjelmisto havaittiin käytännössä hyvin toimivaksi ja käyttöliittymältään selkeäksi, minkä lisäksi PAM-ominaisuus on hyvin toteutettu. Erilaista muihin tuotteisiin verrattuna on kuitenkin Password Manager Pro:n lisensointimalli, joka pohjautuu suurelta osin palvelun omiin ylläpitäjän rooleihin. Organisaation rakenteesta ja vaatimuksista riippuen tuote saattaa olla verrattain edullinen, mutta ylläpitäjien lukumäärää kasvattamalla hinta nousee nopeasti.

5.2 Salasananhallintajärjestelmän käyttöönotto

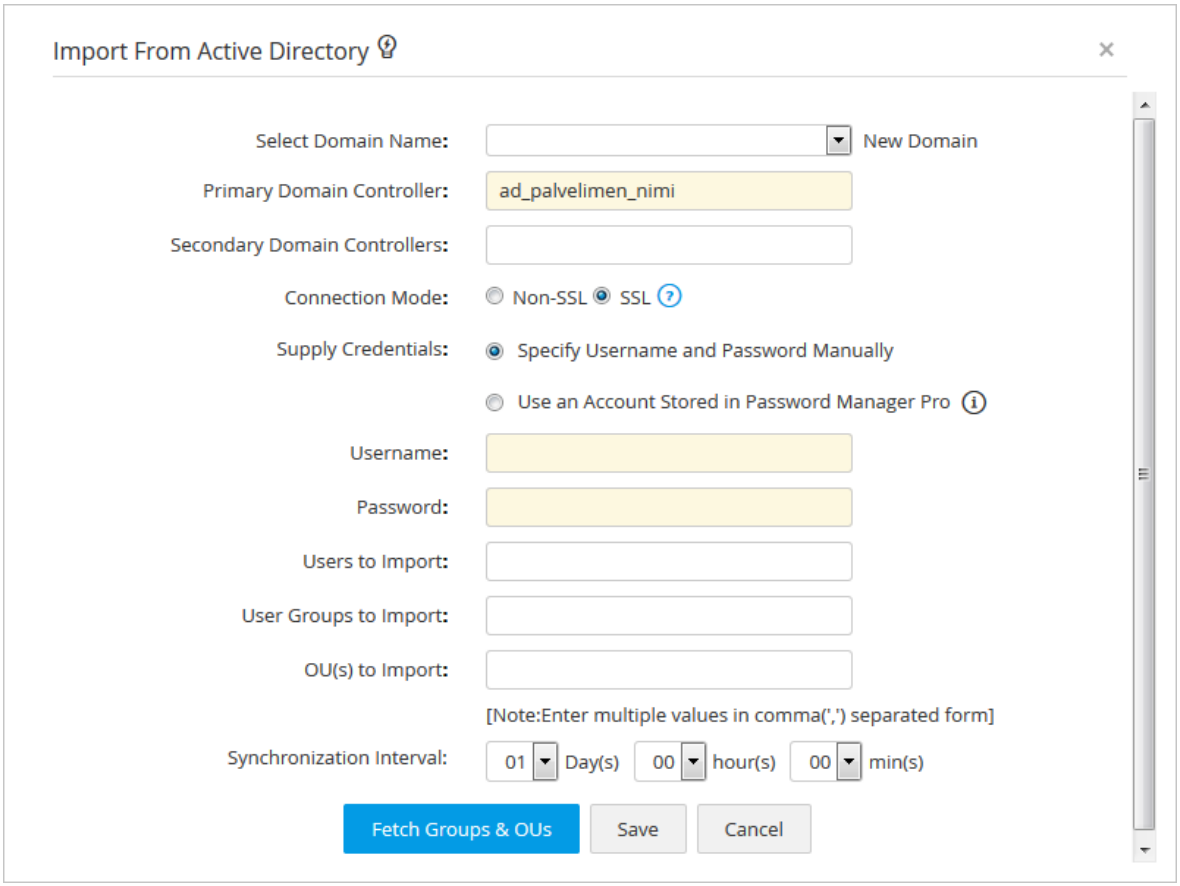
ManageEngine Password Manager Pro:n varsinainen käyttöönotto tapahtuu Lahti Energian omien prosessien mukaisesti, ja tietoturvan vuoksi aihetta ei käsitellä tässä opinnäytetyössä. Itse sovellus ja sen käyttö on kuitenkin yleistasolla selitettävissä, ja seuraavaksi käydään läpi Password Manager Pro:n tärkeimmät käyttöönottoon liittyvät ominaisuudet. Kuvakaappauksissa mahdolliset yksilöivät tunnisteet, kuten nimet ja IP-osoitteet, on peitetty punaisella värillä.

Password Manager Pro:n käyttöliittymä on selkeästi jaoteltu eri osioihin, jolloin kaikki tarpeellinen löytyy nopeasti. Ominaisuuksia on runsaasti, ja ne kattavat myös vaativimpiin ympäristöihin tarvittavat asetukset (kuvio 7).



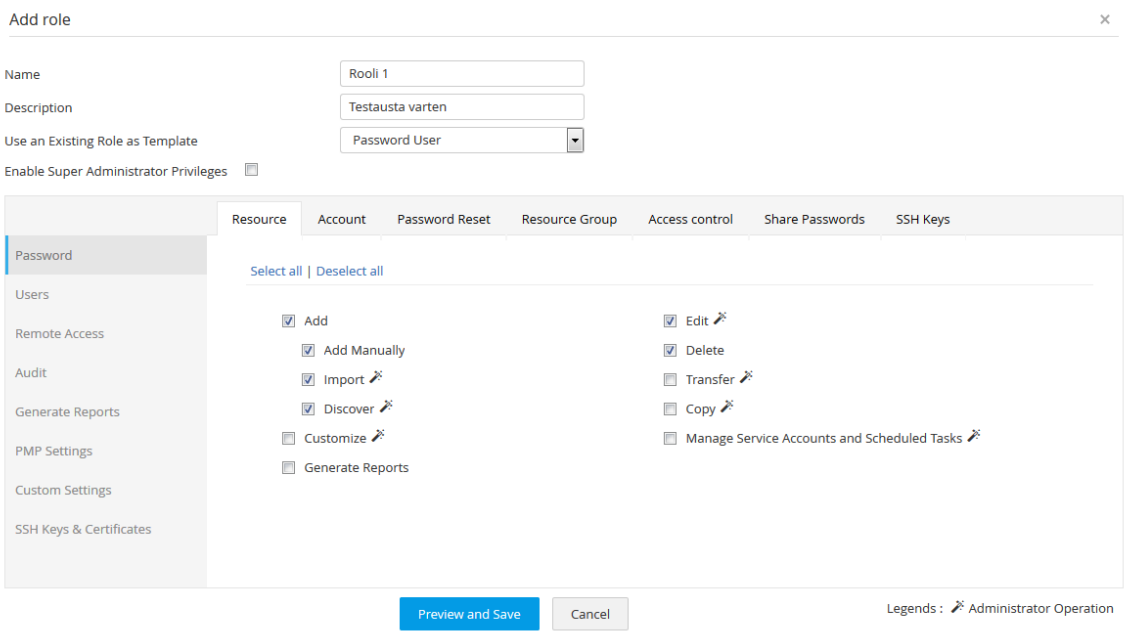
KUVIO 7. Kuvakaappaus Admin-valikosta

AD-käyttäjien tuonti järjestelmään on helppoa. Laajassa toimialueessa on järkevää syöttää ensimmäiseen valikkoon (kuvio 8) vain toimialueen perustiedot sekä käyttäjä, jolla on ainakin lukuoikeus koko hakemistoon. Sovellus lukee koko AD-hakemiston ja avaa seuraavassa valikossa listan, josta on kätevä poimia esimerkiksi yksittäisiä ryhmiä järjestelmään tuontia varten.



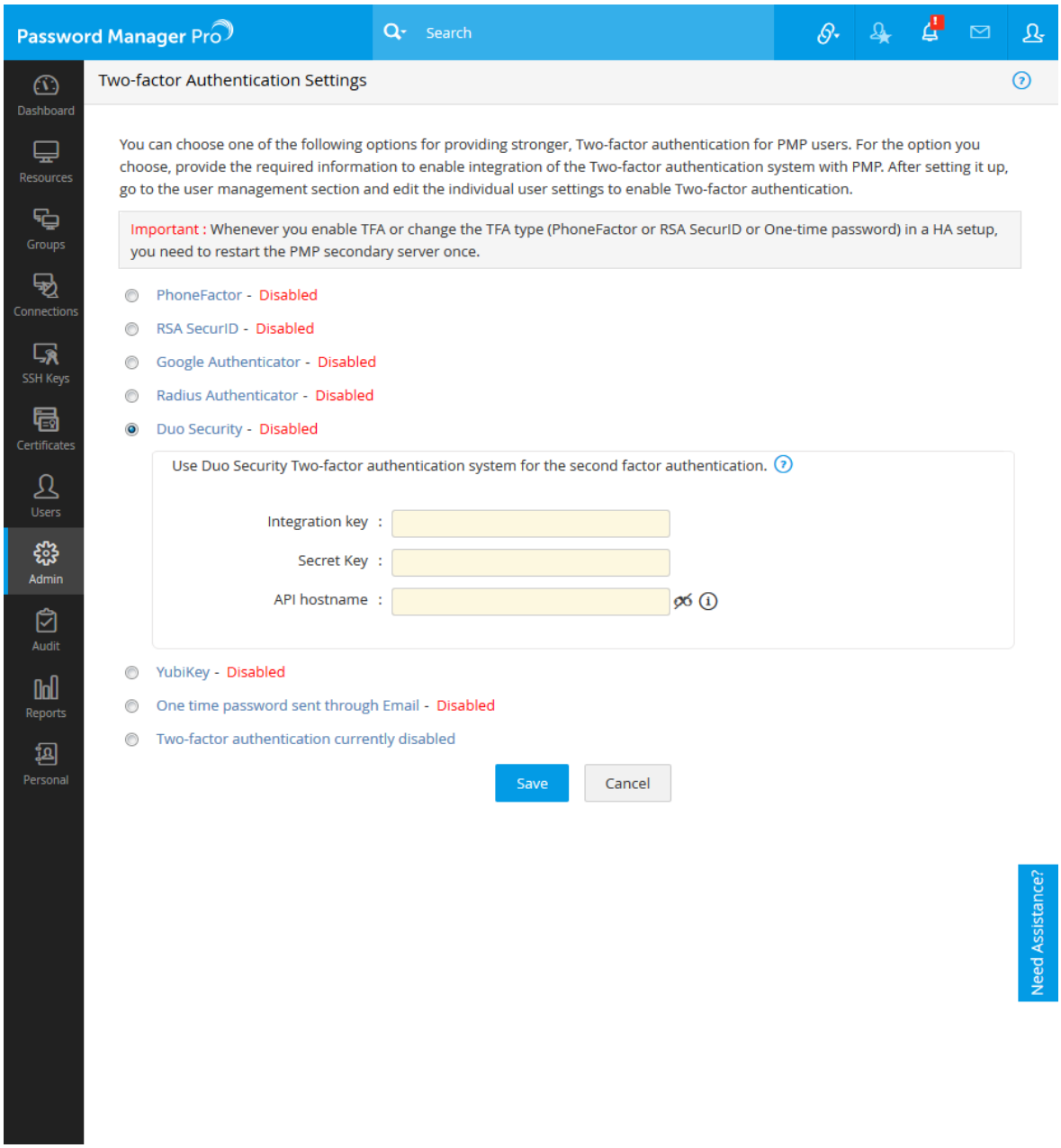
KUVIO 8. Kuvakaappaus AD-käyttäjien tuonnista järjestelmään

Käyttäjiin olennaisesti liittyvä asia on, millaiset oikeudet heillä on suorittaa mitäkin toimia. Sovelluksen sisäisten käyttöoikeuksien määrittelyyn on olemassa oma valikkonsa, nimeltään roolit (kuvio 9). Perusajatuksena on, että ensin luodaan rooli tietyillä käyttöoikeusasetuksilla, jonka jälkeen kyseinen rooli sidotaan tiettyihin käyttäjiin tai ryhmiin. Asetuksia on suuri määrä, ja niiden avulla voidaan määritellä tarkasti käyttäjille sallitut toimet. Roolit liittyvät myös Password Manager Pro:n lisensointimalliin, sillä osa toimista on määritelty ylläpitäjien tehtäviksi. Tällöin käyttäjä, jolle on määritelty yksi tai useampi ylläpitäjän toimi, kuluttaa yhden ylläpitokäyttäjän lisenssin.



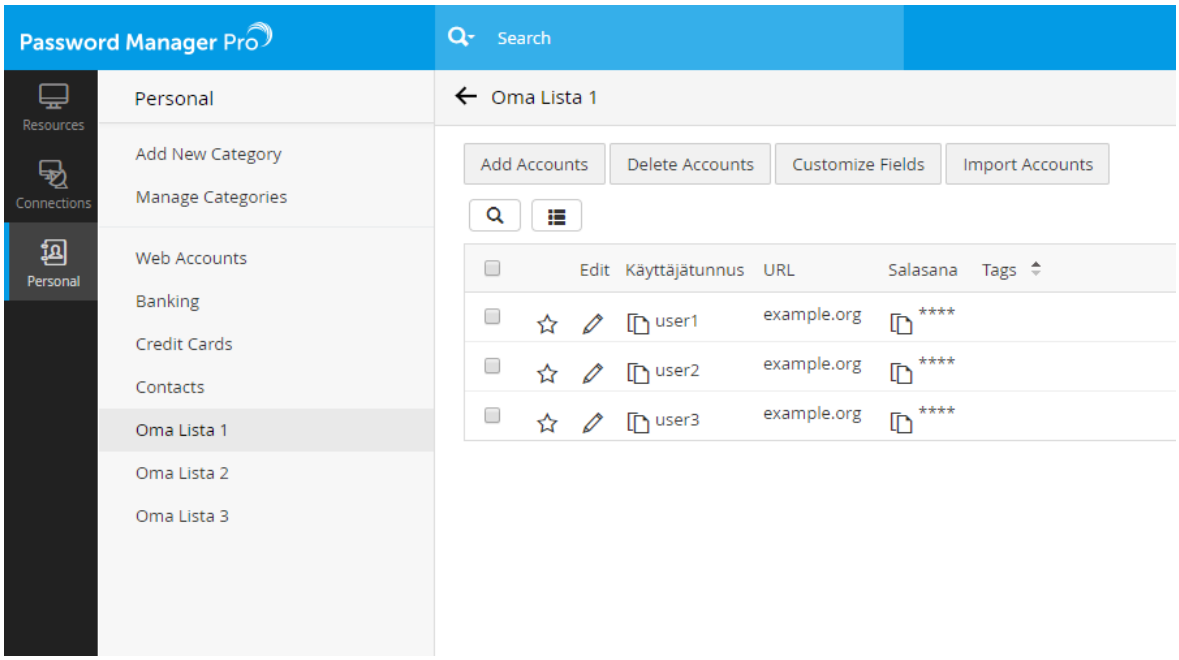
KUVIO 9. Kuvakaappaus käyttäjien roolien määrittelystä

Kaksivaiheinen todennus on laajasti tuettuna Password Manager Pro:ssa. Valittavana on useita vaihtoehtoja, jotka ovat pääosin helppoja konfiguroida. Esimerkiksi Duo Securityn tarjoama kaksivaiheinen todennus toimii, kun täyttää kolmeen kenttään organisaatiokohtaiset tiedot (kuvio 10) ja määrittelee käyttäjille kaksivaiheisen todennuksen käyttöön. Huonona puolena kaksivaiheisia todennusvaihtoehtoja ei voi käyttää sekaisin, eli vain yksi vaihtoehdoista voi olla käytössä kerrallaan.



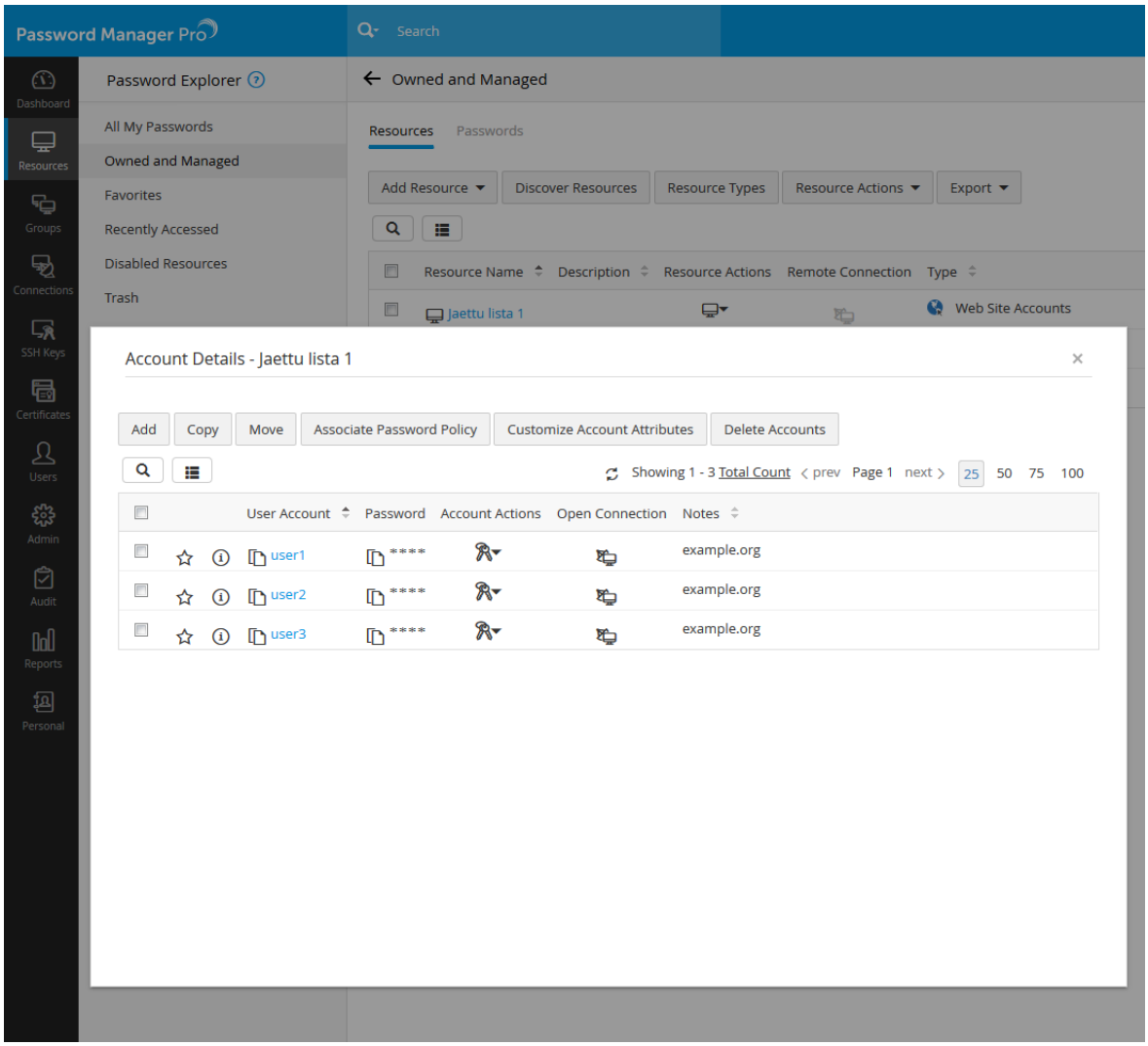
KUVIO 10. Kuvakaappaus kaksivaiheisen todennuksen määrittelystä

Henkilökohtaisille salasanoille tarkoitettu osio (kuvio 11) on selkeä. Vapaamuotoista itse luotavaa kansiorakennetta ei ole, mutta salasanat voidaan ryhmitellä yksitasoisten kategorioiden mukaan. Tarvittaessa henkilökohtainen osio voidaan suojata ylimääräisellä salasanalla, jolloin tietoturva paranee entisestään. Tämä asetus on ylläpitäjien määriteltävissä, eli käyttäjä voidaan myös velvoittaa määrittämään oma ylimääräinen salasanansa, ennen kuin tunnistetietoja voi alkaa tallentamaan järjestelmään. Toisaalta, jos tämä ylimääräinen salasana unohtuu tai katoaa, tietoja ei voi palauttaa mitenkään.



KUVIO 11. Kuvakaappaus salasanalistauksesta

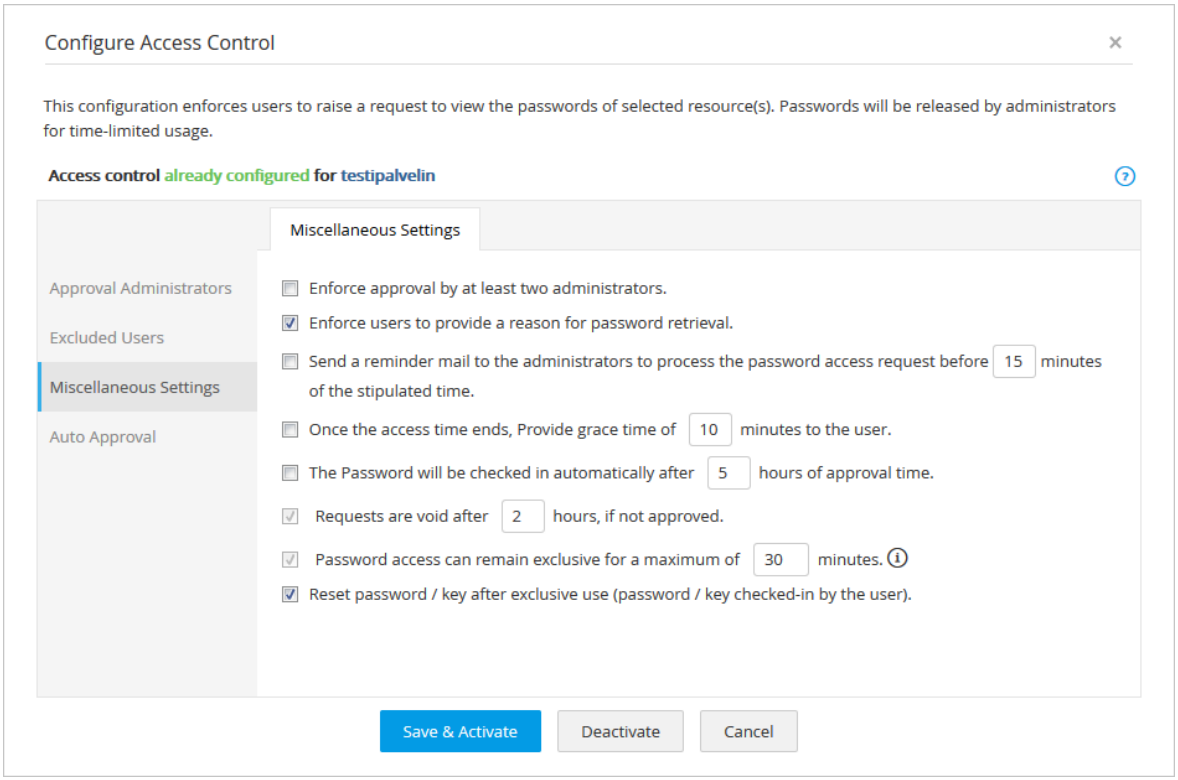
Resurssit-osio (kuvio 12) on ulkoisesti saman tyyppinen kuin henkilökohtainen osio, mutta sisältää toiminnallisuutta ja asetuksia muun muassa PAM:iin liittyen. Resurssien luontivaiheessa on valittavana useita erilaisia pohjia, jotka määrittelevät, minkä tyyppisiä yhteys- ja tunnistetietoja on tarkoitus tallentaa. Esimerkiksi Windows- ja Linux-palvelimille sekä useille valmistajakohtaisille laitteille ja sovelluksille on olemassa omat yksilöidyt pohjat.



KUVIO 12. Kuvakaappaus Resurssit-osiosta

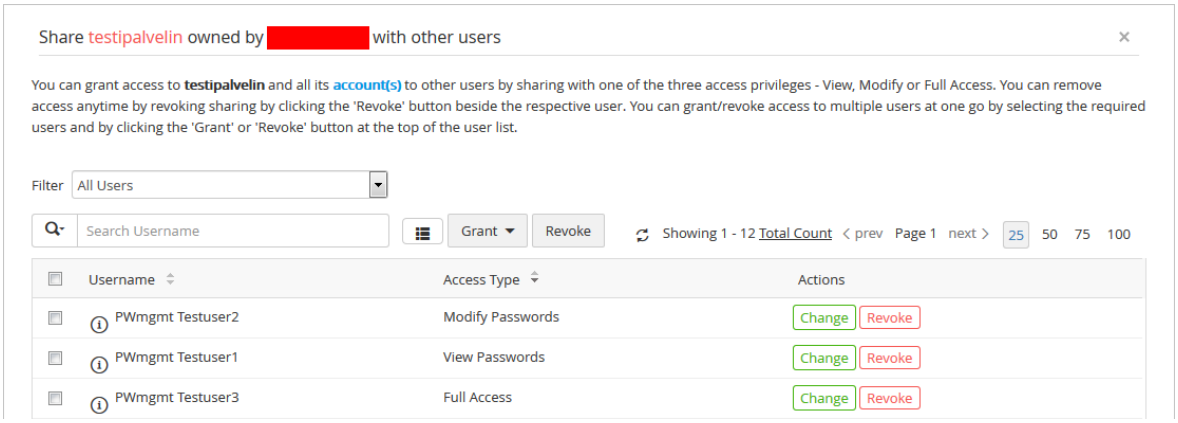
PAM:n hyödyntäminen alussa kuvatulla tavalla on helppoa. Ensin luodaan resurssi, johon määritellään palvelimen tyyppi, osoite ja muita parametreja. Resurssin sisälle tallennetaan käyttäjätunnukset, joita käytetään palvelimelle kirjautuessa.

Oletuksena resurssin luoja on ainoa, jolla on käyttöoikeudet kyseiseen resurssiin. Käyttöoikeusasetuksia voidaan määritellä joustavasti, jotta voidaan hallita muiden pääsyä resurssiin tapauskohtaisesti (kuvio 13). Valittavana on muun muassa kuka käyttöoikeuksia saa myöntää ja kuinka kauan käyttöoikeudet ovat voimassa.



KUVIO 13. Kuvakaappaus käyttöoikeuksien hallinnasta

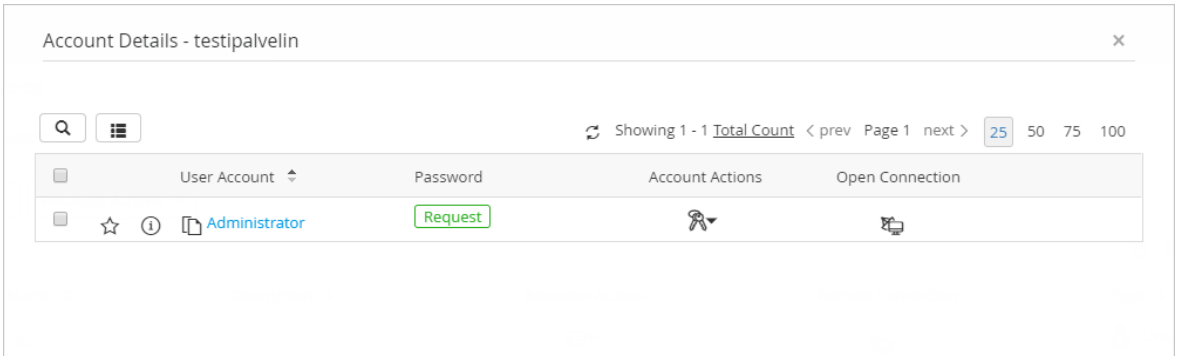
Resurssin jakaminen on erillinen toimenpide. Listalta (kuvio 14) valitaan käyttäjä, jolle resurssi jaetaan, ja määritellään mahdolliset muokkausoikeudet. Tyypillisessä tapauksessa pelkkä katseluoikeus on riittävä.



KUVIO 14. Kuvankaappaus resurssin jakamisesta

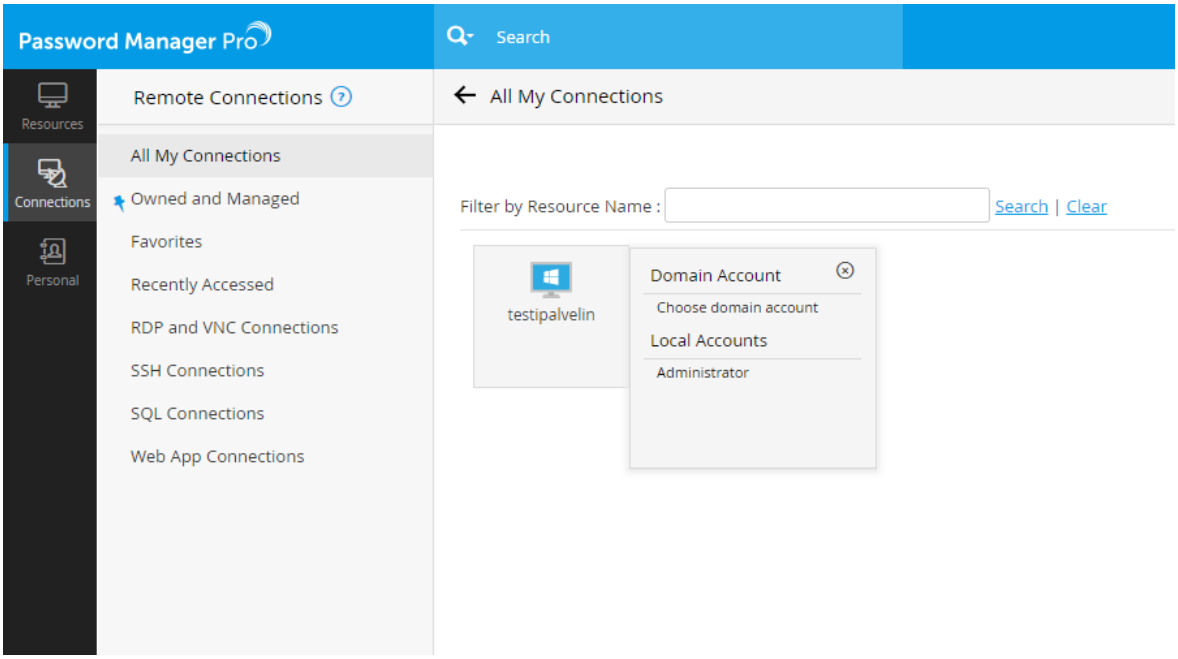
Nyt PAM on määritelty käyttöä varten. Resurssin voisi toki pelkästään jakaa käyttäjälle, jolloin hän pääsee käsiksi resurssiin, milloin tahansa. Käyttöoikeuksien määrittelyn jälkeen toiminnallisuus kuitenkin muuttuu hiukan. Enää salasana ei ole vapaasti nähtävissä, vaan sen tilalle on painike, josta tilapäisen käyttöoikeuden saa pyydettyä (kuvio 15). Käyttäjälle avautuu ikkuna, jossa vahvistetaan pyyntö, ja johon voi tarvittaessa kirjoittaa viestin

ylläpitäjälle. Ylläpitäjä saa tästä ilmoituksen, ja joko hyväksyy tai hylkää pyynnön. Kun pyyntö on hyväksytty, saa käyttäjä puolestaan ilmoituksen käyttöoikeuden myöntämisestä. Ilmoitukset ovat sovelluksen sisäisiä, mutta ne saa ohjattua halutessaan samaan aikaan myös sähköpostiin.



KUVIO 15. Kuvakaappaus käyttöoikeuden rajoituksesta

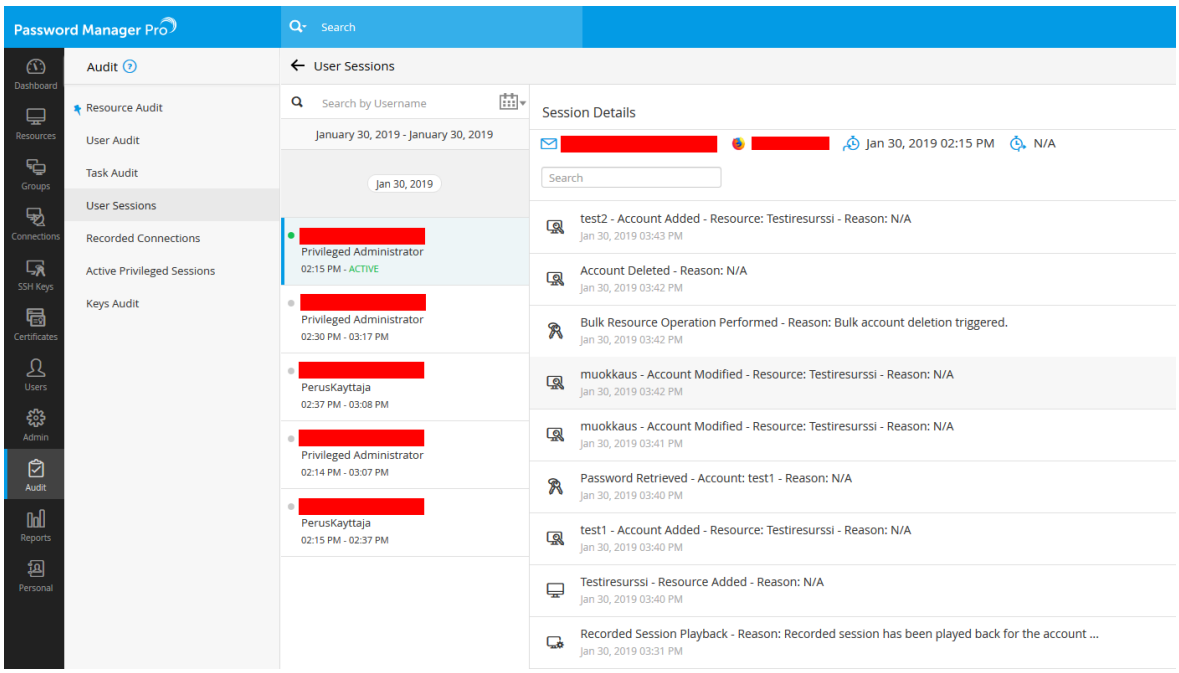
Lopulta käyttäjä näkee etäyhteydet-valikon alla kuvakkeen, jota klikkaamalla aukeaa pieni valikko käyttäjätunnuksen valintaa varten (kuvio 16). Käyttäjätunnusta klikkaamalla etätyöpöytäyhteys avautuu selaimen uuteen välilehteen. Jos resurssi olisi pelkästään jaettu ilman käyttöoikeuksien määrittelyä, käyttäjä pääsisi avaamaan etätyöpöytäyhteyden, milloin vain.



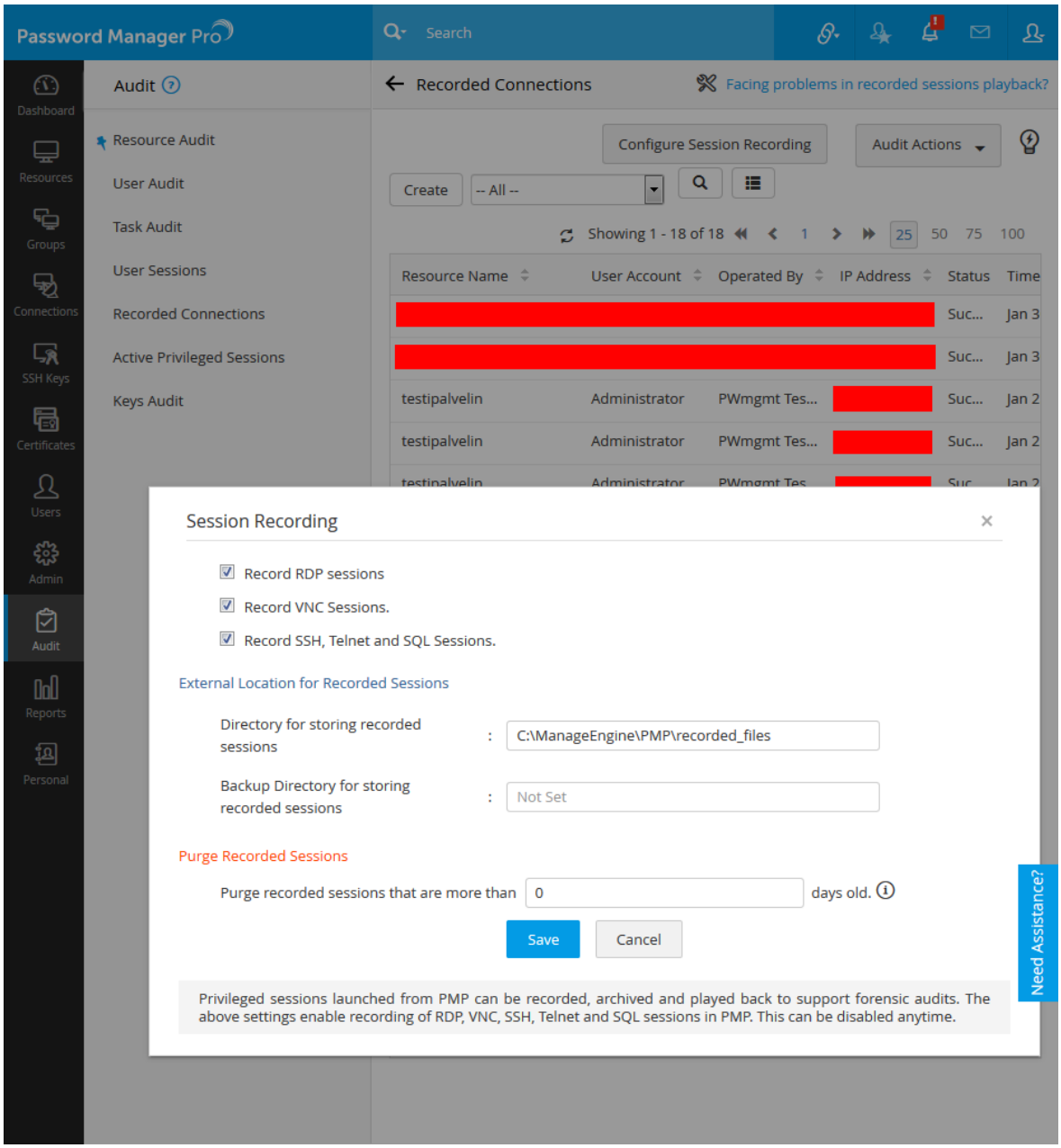
KUVIO 16. Kuvakaappaus etätyöpöytäyhteyden avauksesta

Suuri osa kaikista sovelluksen sisäisistä tapahtumista kirjataan lokiin, ja portaittaisen valikkorakenteen ansiosta on helppo etsiä ja tarkastella yksittäisiä tapahtumia (kuvio 17). Esimerkiksi resursseihin kohdistuneet muokkaukset jäävät lokiin, jolloin vaikkapa

tietoturvarikkomusten selvitys on helpompaa. Käytönvalvontaan ja PAM:iin liittyen saatavilla on myös istuntojen nauhoitusominaisuus. Sovellus voi tallentaa koko istunnon videomuodossa, ja istuntoa voidaan tarkastella jälkikäteen myöhemmin (kuvio 18).

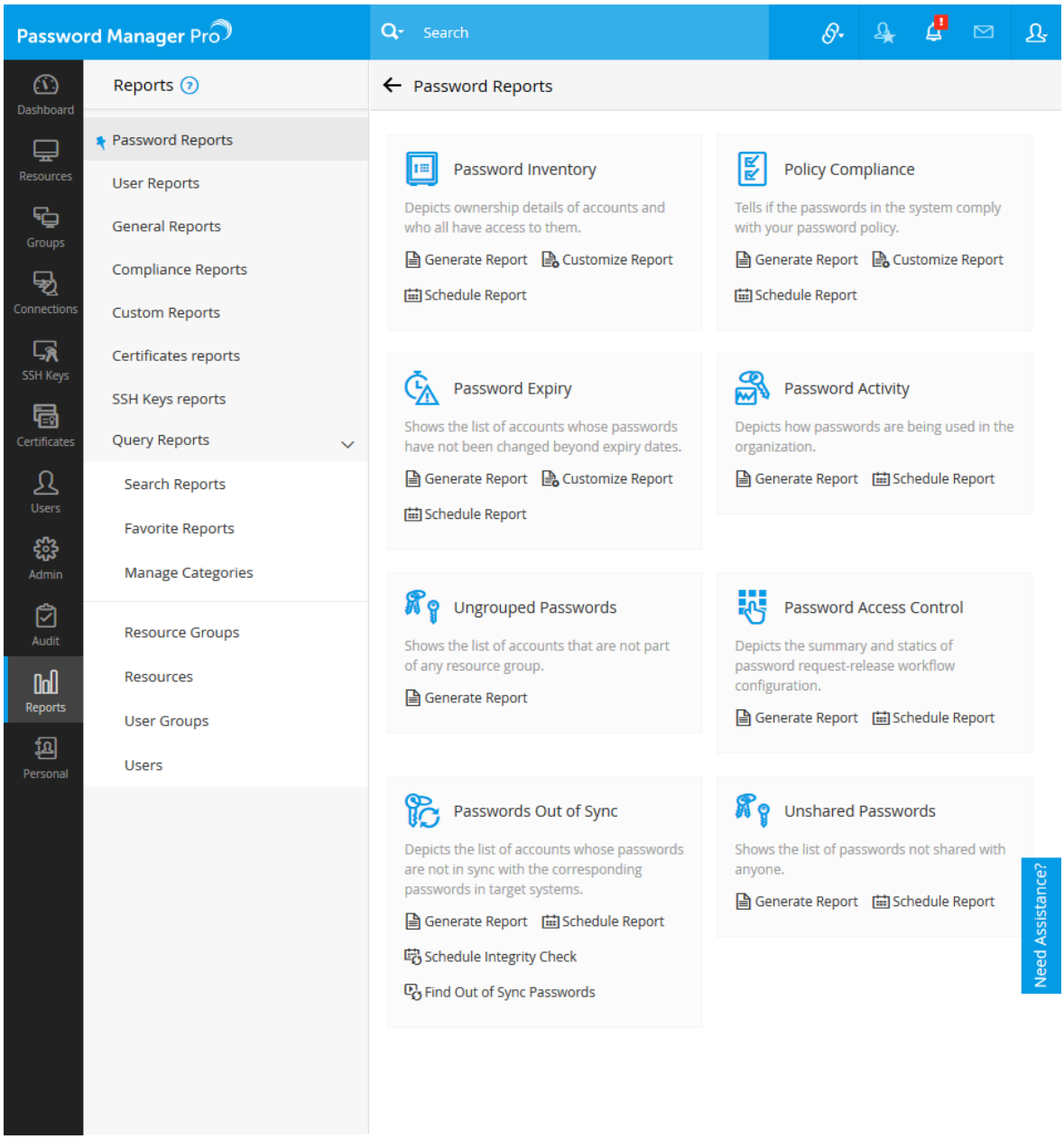


KUVIO 17. Kuvakaappaus Audit-valikosta



KUVIO 18. Kuvakaappaus istunnon nauhoituksen määrityksestä

Kerätystä datasta voidaan muodostaa myös automaattisia raportteja esimerkiksi ylläpitäjien tai johtoryhmän tarkasteltaviksi. Valittavana on useita rapottityyppejä alakategorioineen (kuvio). Raportteihin kerättävien tietojen määrää on mahdollista muokata tarpeiden mukaan, jotta vain olennaisimmat asiat päätyvät raporttiin.



KUVIO 19. Kuvakaapaus raportointiosiosta

ManageEngine Password Manager Pro täyttää salasananhallintajärjestelmältä vaaditut ominaisuudet hyvin. Jaottelu henkilökohtaisten salasanojen ja jaettavien resurssien välillä on muihin tuotteisiin verrattuna uniikki ratkaisu, mutta silti toimiva. Henkilökohtaisille salasanoille tarkoitettu osio on yllättävän pieni osa kokonaisuutta, ja suuri osa ohjelmiston toiminnallisuudesta liittyy nimenomaan PAM:n hyödyntämiseen. Vaikuttaisi siltä, että Password Manager Pro on ensisijaisesti tarkoitettu IT-henkilöstön käyttöön, ei niinkään loppukäyttäjien yleismalliseksi salasananhallintajärjestelmäksi. Tämä ei kuitenkaan ole ongelma, sillä odotettavissa oli, että salasananhallintajärjestelmä ja muu infrastruktuuri sekä toimintatavat pitää sovittaa toisiinsa joka tapauksessa.

6 YHTEENVETO

Opinnäytetyön tavoitteena oli valita ja ottaa käyttöön keskitetty salasananhallintajärjestelmä Lahti Energia Oy:n tarpeet huomioiden. Ensisijaisesti tarve oli keskitetylle järjestelmälle, johon on turvallista tallentaa kaikki työasioihin liittyvät käyttäjätunnukset ja salasanat. Lisätoiveena oli, että sama järjestelmä voisi toimia myös PAM-sovelluksena.

Aluksi käytiin läpi salasananhallintajärjestelmältä vaaditut ominaisuudet, minkä jälkeen tutkittiin yleisluontoisesti saatavilla olevia vaihtoehtoja ja niiden ominaisuuksia. Erilaisia salasananhallintaan tarkoitettuja keskitettyjä järjestelmiä on saatavilla yllättävän suuri määrä, ja kaikkien niiden testaaminen olisi aikataulun ja käytännöllisyyden kannalta mahdotonta. Testaukseen valittiin viisi vaihtoehtoa, jotka vaikuttivat parhailta vaatimuksia ajatellen.

Kaikkia testattavia tuotteita varten asennettiin kullekin oma virtuaalipalvelin. Jokaisesta tuotteesta käytiin läpi vaatimuslistalla olevat ominaisuudet sekä arvioitiin järjestelmäkohtaisia eroja ja ominaisuuksia. Toimintalogiikka kaikissa tuotteissa on sama, ja usein myös tärkeimmät ominaisuudet on toteutettu samalla tavalla. Pienempiä tuotekohtaisia eroja löytyi myös, mutta niiden merkitys kokonaiskuvan kannalta on vähäinen.

Vertailun loppuvaihetta kohti valintaperusteet muuttuivat hieman. Testattujen salasananhallintajärjestelmien keskitetty luonne mahdollisti myös sen, että useisiin tuotteisiin sisältyi myös PAM-ominaisuuksia. Sovellusten ollessa muuten hyvin samankaltaisia, eri tavalla toteutetut PAM-ominaisuudet olivat lopulta merkittävässä osassa salasananhallintajärjestelmää valitessa. Markkinoilla on myös ensisijaisesti PAM-sovelluksiksi tarkoitettuja tuotteita, ja jälkikäteen ajateltuna myös niiden ottaminen vertailuun olisi ollut järkevää.

Identiteetinhallinta kokonaisuudessaan koostuu niin teknisistä ratkaisuista kuin toimintamalleista. Tekninen ratkaisu on tässä tapauksessa salasananhallinta/PAM -järjestelmä, ja toimintamallit ovat osaltaan kytköksissä siihen, miten kyseisellä järjestelmällä voidaan toteuttaa halutut asiat. Tämän vuoksi lähestymistapa parhaan ratkaisun löytämiseen on käytännönläheinen. Salasananhallintajärjestelmän käyttöönotossa ratkaisevaa on tutkia, miten eri ohjelmistojen ominaisuudet on toteutettu ja miten ne sopivat juuri tiettyyn käyttöympäristöön. Vertailun tekeminen oli pääosin helppoa, kun alussa on määritelty asiat, joista testattavien ohjelmistojen tulee ainakin suoriutua.

Tietoturvastrategiassa perustason salasananhallintajärjestelmä on tärkeä, mutta ei kuitenkaan kokonaisuutta hallitseva osa. Kun mukaan otetaan PAM, asia muuttuu hieman monimutkaisemmaksi. PAM-sovellus voidaan integroida laajasti olemassa oleviin järjestelmiin, jolloin sen merkitys korostuu. PAM-sovelluksen vikaantuessa siihen integroituihin järjestelmiin pääsy häiriintyy, mutta itse järjestelmien toimintaan PAM-sovelluksen vikaantuminen

ei vaikuta. Järjestelmiin pääsee käsiksi samalla tavalla kuin ennen PAM-sovelluksen käyttöönottoa, olettaen ettei verkkoinfrastruktuuriin ole tehty muutoksia ja että tunnistetiedot ovat saatavilla muualla. PAM-sovellusta saatetaan hyödyntää kaikissa mahdollisissa etäyhteyksissä, ja oikeaoppisessa toteutuksessa vikatilanteiden katastrofaaliset vaikutukset on minimoitu. Pahimmassa tapauksessa tärkeitä tietoja voi vuotaa ulkopuolisille ja vikoja saatetaan joutua korjaamaan pitkään. Tämän vuoksi PAM:n käyttöönotossa tulee noudattaa harkintaa. PAM ei tarkoita yleisluontoista tietoturvaratkaisua, ja sen käyttöönotto vaatii, että myös muut tietoturvan tasot ovat kunnossa.

Salasananhallintajärjestelmältä vaaditut ominaisuudet vaihtelevat käyttöympäristön mukaan. Ratkaisu, joka sopii hyvin Lahti Energialle, ei välttämättä ole optimaalinen vaihtoehto jollekin muulle yhtiölle. Täysin mahdollinen skenaario on, että salasananhallintaan ei tietyissä yhtiöissä saateta kelpuuttaa muita kuin avoimen lähdekoodin vaihtoehtoja. Pienemmissä yhtiöissä, joilla ei ole käytössään kattavaa IT-infrastruktuuria, ratkaisuksi saatetaan kelpuuttaa vain pilvipalveluja. Nämä ovat esimerkkejä suurista jakolinjoista, jotka määrittelevät jo varhaisessa vaiheessa, millaisen salasananhallintajärjestelmän käyttöönottoa yleensä ruvetaan harkitsemaan. Ohjelmistoja myös kehitetään jatkuvasti, minkä vuoksi puuttuvia ominaisuuksia on voitu jo lisätä ja vikoja korjata. Näiden syiden perusteella opinnäytetyössä läpi käyty vertailu ei ole yleispätevä, vaan kuvaa salasananhallintajärjestelmän valintaprosessia ja käyttöönottoa lähinnä yksittäisen yhtiön näkökulmasta, ottaen huomioon tapauskohtaiset vaatimukset.

Salasananhallintajärjestelmän tärkeys korostuu nykymaailmassa, jossa hyödynnetään yhä enemmän todennusta vaativia verkkopalveluja. Salasananhallintajärjestelmä on oikeastaan vain korjaustoimenpide, jolla pyritään paikkailemaan salasanaan perustuvan todennuksen huonoja puolia. Salasanaan perustuva todentaminen on vain rajapinta ihmisen ja tietojärjestelmien välillä, ja tämä rajapinta voidaan tulevaisuudessa korvata esimerkiksi biometrisillä tunnisteilla. Salasana on todennuksen välineenä standardi ja käytössä lähes kaikkialla, ja niin kauan kuin teknologialle ei ole yhtä laajamittaista korvaajaa, pysyy salasananhallintajärjestelmä olennaisena osana digitaalisen maailman tietoturvaa.

LÄHTEET

Allen, C. 2016. 11 Enterprise Password Management Solutions For Cybersecurity [viitattu 22.11.2018]. Saatavissa: https://phoenixnap.com/blog/enterprise-password-management-solutions

Arcieri, T. 2016. 4 fatal flaws in deterministic password managers [viitattu 25.10.2018]. Saatavissa: https://tonyarcieri.com/4-fatal-flaws-in-deterministic-password-managers

Authy 2018. What Is Two-Factor Authentication (2FA)? [viitattu 3.12.2018]. Saatavissa: https://authy.com/what-is-2fa/

ClickStudios 2018. Purchase Passwordstate [viitattu 5.11.2018]. Saatavissa: https://www.clickstudios.com.au/buy-now.aspx

Katz, E. 2017. PAM vs SSO vs Password Manager: Which is Best for Your Business? [viitattu 22.11.2018]. Saatavissa: https://blog.dashlane.com/pam-sso-password-manager-comparison/

ManageEngine 2018a. Licensing Details [viitattu 31.10.2018]. Saatavissa: https://www.manageengine.com/products/passwordmanagerpro/download.html#licensing

ManageEngine 2018b. User Management [viitattu 31.10.2018]. Saatavissa: https://www.manageengine.com/products/passwordmanagerpro/help/user_management.html

Pleasant Solutions 2018a. Features – Pleasant Password Server [viitattu 29.10.2018]. Saatavissa: https://pleasantsolutions.com/passwordserver/details/features/

Pleasant Solutions 2018b. Purchase – Pleasant Password Server [viitattu 29.10.2018]. Saatavissa: http://www.pleasantsolutions.com/passwordserver/purchase/?users=200

Rouse, M. 2018. What is single sign-on (SSO)? [viitattu 22.11.2018]. Saatavissa: https://searchsecurity.techtarget.com/definition/single-sign-on

SSL2BUY 2015. Symmetric vs. Asymmetric Encryption – What are differences? [viitattu 20.2.2019]. Saatavissa: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Techopedia 2018. What is a Password Manager? - Definition from Techopedia [viitattu 15.10.2018]. Saatavissa: https://www.techopedia.com/definition/31435/password-manager

The Secret Security Wiki 2018. Privileged Access Management (PAM) [viitattu 22.11.2018]. Saatavissa: https://doubleoctopus.com/security-wiki/authentication/privileged-access-management/

Thycotic 2018a. IAM, PIM and PAM: Here's what those cyber security acronyms mean. [viitattu 22.11.2018]. Saatavissa: https://thycotic.com/resources/iam-pim-pam-privileged-identity-access-management-terminology/

Thycotic 2018b. Secret Server Features Chart [viitattu 31.10.2018]. Saatavissa: https://thycotic.com/products/secret-server/features/

Vincent, G. 2016. LessPass How Does It Works? [viitattu 25.10.2018]. Saatavissa: https://blog.lesspass.com/lesspass-how-it-works-dde742dd18a4

Zoho 2018. What is password management? [viitattu 15.10.2018]. Saatavissa: https://www.zoho.com/vault/educational-content/what-is-password-management.html

Zoho Corporation 2018. Fact Sheet [viitattu 31.10.2018]. Saatavissa: https://download.manageengine.com/pdf/factsheet.pdf