Expertise
and insight
for the future

Jarrod Schafer

Unified Endpoint Management Software for a Small Company

Metropolia University of Applied Sciences

Master's Degree

Master of Engineering (Information Technology)

Master's Thesis

7.12.2021

Author(s) Title Number of Pages Date	Jarrod Schafer Unified Endpoint Management Software for a Small Company 44 pages + 4 appendices 13 November 2021
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Sami Sainio, Senior Lecturer Ville Jääskeläinen, Head of Information Technology Master's program

This thesis will cover the researching, comparing, and selecting of a Unified Endpoint Management software that satisfies the requirements set by small-sized companies. System Administrators, who do not use a Unified Endpoint Management software, are often required to create accounts and grant all the necessary permissions, across all of their company's infrastructure, manually. A Unified Endpoint Management software would make the creation of accounts and granting of permissions easier, while also offering better security, accountability, and transparency.

To find and recommend the best Unified Endpoint Management software available, interviews and questionnaires were used to gather the features that would become the list of basic requirements for the software. These requirements were discussed with technical experts to filter through the list of features obtained from the questionnaire. There was consideration to also develop a Unified Endpoint Management software to perfectly meet the wants and requirements. However, for this thesis it was chosen to use and compare existing cloud-based software.

Through writing this thesis, three suitable Unified Endpoint Management software were discovered, their features were explained, and how they met the requirements, while also discussing any limitations the software has. With one of the three software being recommended to small companies.

Keywords	Unified Endpoint Management, User Management, Device Management

Contents

List of Abbreviations

2FA	Two Factor Authentication
API	Application Programming Interface
BYOD	Bring Your Own Device
CMT	Client Management Tools
CSV	Comma Separated Values
EMM	Enterprise Mobility Management
GDPR	General Data Protection Regulation
HR	Human Resources
ID	Identification
IP	Intellectual Property
IT	Information Technology
LDAP	Lightweight Directory Access protocol
MAM	Mobile Application Management
MDM	Mobile Device Management
ME	ManageEngine
MFA	Multi-Factor Authentication
OS	Operating System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
SAML	Security Assertion Markup Language
SMS	Short Message Service
SSH	Secure Shell
SSO	Single Sign On
TFA	Two Factor Authentication
TOTP	Time-based One Time Password
UAM	User Access Management
UEM	Unified Endpoint Management
USB	Universal Serial Bus
VPN	Virtual Private Network

1 Introduction

Managing a computer system used to mean, creating an account in one place, and that was it. Now, computer systems have grown at an exponential level requiring IT administrators to find more tools. Computer administrators now need to manage multiple different user accounts, in multiple different websites, servers, computers, and mobile devices. (1) For administrators to oversee their computer systems, they need to start utilising software that helps control all user accounts and devices in a single place. (2)

Unified Endpoint Management (UEM) software is required as businesses are growing, and the number of devices their employees are using are growing too. Smart phones and tablets are now being used alongside desktop computers and laptops. Techniques used for manging computers cannot be used to manage new mobile devices. New techniques such as Mobile Device Management (MDM) are required to manage the mobile devices. If a company wants to manage both computers and mobile devices, they will need to adopt UEM software. UEM software provides all the necessary tools to support both computers and mobile devices in one place. Making managing everything consistent, faster, and less error prone. (2)

Currently, small companies are reaching a point where managing all their users and devices is becoming troublesome due to the high number of tasks and devices that need to be managed. IT Administrators can start to miss certain tasks, get delayed with others, to name a few, because of all the different tasks and devices they need to manage. In order to manage all their users and devices effectively, they need to implement UEM software. (3) To resolve this issue three UEM software were compared to find out which one meets the most requirements for a small company. Using a small company as a test case, the three software were analysed, and their features compared to a set of requirements that a small company might have. (2)

1.1 Aim of the Thesis

This thesis will cover deciding the most suitable Unified Endpoint Management (UEM) software for small businesses with between 15-50 employees. (4) In order to establish the most suitable software, the employees of a small company were surveyed on what they felt were difficulties with the existing systems, and what features of the software would be most important to them. With those results, the thesis compares three existing UEM software available today and will offer a recommendation on which of the three is more suitable for a small company.

This thesis will show to small business which software is right for them, and why. It will also explain the other software that was compared and outline their features so small companies could consider them too if the requirements used in this thesis do not exactly match their own. Small business will understand the selected UEM software so they can decide on a suitable software for them if their requirements differ to the ones mentioned in this thesis. Small companies will be able to better manage their users and devices via UEM software or have a better idea on what to start looking for when choosing UEM software for themselves.

1.2 Structure of Thesis

The thesis is broken up into six chapters covering different topics. This chapter introduces the thesis, providing context to the thesis and how it will be structured. Next is the Data Sources chapter, which covers all the necessary information required to properly understand the thesis. Following that is the Methods chapter, which outlines how the test data was acquired, to establish the requirements for the software. Once the method has been presented the Analysis chapter will introduce and discuss the three selected software, providing a brief overview of it, what features they offer, how it matches the idea of requirements obtained from the Methods chapter, and any limitations of that software. Afterwards is the Recommended Solution chapter, which compares all three of the chosen software and discusses which one meets the requirements the best. Finally, the Conclusion chapter will summarise what was achieved in the thesis.

2 Data Sources

In this chapter, important theory is outlined to give the reader the necessary knowledge to understand the analysis. Unified Endpoint Management is introduced and defined, alongside every feature that is mentioned in the thesis.

2.1 Background

UEM was born due to necessity of the growing market of new smart devices, such as smart phones and tablets, that were entering businesses rapidly. This led to an increase in employee happiness and productivity, at the cost of the security of the IT infrastructure, as these new smart devices operated on multiple different operating systems and getting access to business resources without the proper checks and balances that a normal computer would have. This created the term Bring Your Own Device (BYOD). (5)

BYOD can be described in two ways, according to Lunsford:

"BYOD can describe the process whereby employees are allowed to bring personal devices to the workplace for the purpose of conducting work-oriented activities. On the other hand, BYOD can also refer to the business strategy that governs the use of personnel devices in a business environment". (5)

This concept started developing itself as users decided to take it upon themselves to bring in their own devices to make their work-life easier. A new program had to be developed to ensure the integrity and security of the business' IT infrastructure. This program would allow businesses to enforce policies and procedures onto the new mobile devices that computers already had. (6)

These new BYOD programs were improved upon which created what is now called Mobile Device Management (MDM). MDM software allowed administrators to remotely wipe a device, in the event the device was stolen or if an employee left the business, limit access depending on where the device is currently located and enforce policies. (2)

As the technology industry continued to advance, MDM became more and more incapable of meeting the requirements of bigger companies. MDM started off as a system to manage devices and protect the IT infrastructure. However, now bigger companies require to be able to manage these devices at a deeper level. (5)

Bundled in with Enterprise Mobility Management (EMM) is Mobile Application Management, which allows administrators to manage only the applications on a device, not the device itself. This extends to prevent apps from being installed, prohibit apps from accessing company data, and removing specific apps without requiring to fully wipe the device. (7)

UEM is the advancement of EMM. Now administrators can easily manage both mobile devices and computers together in one place. “UEM solutions manage security, operating systems, patches, applications, and hardware for you, and they reduce the complexity of ever-expanding device diversity” (2)

2.2 Defining Unified Endpoint Management

UEM software can be defined under different names depending on the companies developing the software. For example, JumpCloud labels UEM software as Centralised User Management:

“Centralized user management allows IT the control and visibility over every device, application, or network across the organization, without dictating what resources are the right choice for each group. Central control over users ensures that digital assets stay within the organization. IT can provision access to the right people and terminate access across all resources when an employee or contractor leaves. Plus, central control over users is a critical audit point for compliance.” (8)

UEM is defined as “[…] an approach to securing and controlling desktop computers, laptops, smartphones and tablets in a connected, cohesive manner from a single console.” by Dr Phil Lunsford in his journal article titled The Road to Unified Endpoint Management (UEM). (5) UEM is the combination of Enterprise Mobility Management (EMM), Mobile Device Management (MDM), and client management solutions. (9)

Ivanov defines EMM as: “EMM solutions allow a business to remotely configure and manage devices through Mobile Device Management (MDM) and Mobile Application Management (MAM)” (10)

Ivanov continues by defining MDM as: “MDM platform enables tracking, managing, and securing an employee or corporate owned device. Each device and employee have a profile that is created for them and their specific tasks. An MDM solution means a business can configure network and storage access of mobile devices (Wi-Fi, Bluetooth, 3G/4G, GPS, etc.). MDM also enables the IT department can remotely lock and wipe a device if it’s lost or stolen” (10)

“Mobile Application Management (MAM) solution that limited the management and control of business applications. MAM helps in creating an enterprise application store and pushing or updating necessary applications on business devices remotely.” as defined by Ivanov (10)

Client Management tools (CMT) are used to automate endpoint management tasks. CMTs can perform the following functions: operating system deployments, create a hardware and software inventory, software distribution, patch management, configuration management, security configuration management, and remote control. (11)

2.3 Definition of Features

Every feature that is mentioned in this thesis will be defined in the groups of tables below. The tables are grouped by similar features, with a short introduction for each table. The first table will cover every feature that makes up device management. The second table will cover features related to user management, and the third table will be for features that are related to User and Device security.

Device Management allows the administrator to manage multiple computers to set them up for new users, clean them when a user leaves, and provide general maintenance when required. Device Management contains the following features: Mobile Device Management, Patch Management, Statistics on Devices, Run Commands Remotely, Software Deployment, Desktop Configurations, Remote Desktop Sharing, Multi-Platform, IT

Asset Management, USB Device Management, and Device Enrolment. All features that are related to device management are defined in Table 1.

Table 1 Device Management features and definitions

Feature	Definition
Mobile Device Management	MDM gives the administrators the ability to deploy and manage mobile devices such as smart phones and tablets. Policies can be created to restrict what an employee can install on their mobile device and to enforce any required security protocols. If an employee loses their device, an administrator has the ability to remotely delete all data stored on the device. (12)
Patch Management	Patch deployment related to operating systems and other applications to protect Windows and Macs from security threats. (13)
Statistics on Devices	Statistics on devices, also referred to as stats on devices, is a feature that allows the software to monitor and collect information about the device/computer it is installed on. This information is used to ensure everything is running smoothly on the device/computer.
Run Commands Remotely	Remote Commands can be used to execute commands on targeted devices to collect information on a device.
Software Deployment	Software deployment is the distribution of all software in a working environment without any to minimal intervention. (14)

Desktop Configurations	These configurations help administrators mange windows applications, system settings, desktop settings, and security policies. They are used to baseline systems and can be applied at the user or device level. (15)
Remote Desktop Sharing	Allows administrators to troubleshoot remote desktops with multiple users. Includes the ability to transfer files, record the remote desktop session, and chat with the other users in the remote desktop sharing session. (13)
Multi-Platform	Multi-platform means to be able to run on different operating systems.
IT Asset Management	IT Asset Management is a feature that manages and monitors any IT asset found in a network. It can track an asset over its entire time in the organisation. (16)
USB Device Management	Restrict and control the usage of USB Devices within the network both on the user level and at the computer level. (13)
Device Enrolment	The ability to enrol devices either in bulk or manually into the UEM software. Can also be done by users. (13)

User Access Management (UAM) is the ability for administrators in a system, whether it be for a company, a school, or a project, and others alike. to create, manage, and remove user accounts with a click of a button. (13) The features included in User Access Management are: Single Sign On, Sync with Google Workspace/Microsoft Azure/Active Directory, Strong Authentication or Multi-factor Authentication, Two Factor Authentication, and RADIUS. Every feature related to user access management is defined in Table 2 below.

Table 2 User Access Management features and definitions

Feature	Definition
Single Sign On (SSO)	SSO allows end users to use a single set of credentials to access all their applications. This helps users avoid being locked out from their applications and causing work delays because they forget their password as they only have one to remember. (17)
Sync with Google Workspace/Microsoft Azure/Active Directory	Allows administrators to synchronise their existing user directory in Google Workspace, Microsoft Azure, and Microsoft Active Directory. Any changes applied to the synchronised data, will be copied to the other user directory
Strong Authentication or Multi-Factor Authentication	Strong Authentication is defined by Stanislav as: "Authentication beyond simply a password. May be represented by the usage of 'security questions', or could be layered security like two-factor authentication." (18)
Two Factor Authentication	Stanislav also explains the definition of Two Factor Authentication as: "Use of two factor classes to provide authentication. This is also represented as '2FA' and 'TFA'." (18)
RADIUS (Remote Authentication Dial-In User Service)	RADIUS grants the ability to connect user identities stored in directories such as Active Directory, cloud directories, or even on a RADIUS server itself to networking infrastructure, which enables users to access the network or VPN with their own unique login details. (19)

User and Device security are made up by policies, rules, and procedures to ensure that no unauthorised users can get access to a user's account or their device. User and Device Security includes the Permission Groups, Policy Management and Application Control features. Table 3 covers all the features and definitions that make up User and Device security.

Table 3 User and Device Security features and definitions

Feature	Definition
Permission Groups	Permission groups allow administrators to group permissions together so they can be deployed all at the same time to multiple devices. (20)
Policy Management	Kandogan et al. defines policy management as: "In the computing or information technology (IT) domain, policies often describe rules of conduct and behavior for the management and use of computing resources, ensuring fair allocation, mutual understanding of responsibilities and liabilities, and proper and consistent handling of policy violations" (21)
Application Control	Control what applications users can install and use, either by blacklisting bad applications or whitelisting good applications. (13)

2.4 Scope of Company

The thesis is written for small businesses who operate inside Finland and are looking at improving their user and device management abilities. However, this thesis can also apply to other small companies within Europe. Small companies were chosen as most Finnish business are either micro or small businesses. (22) The size of a company is defined by the European Commission (EU) standards set in the EU guide titled User

guide to the SME Definition. These small companies have between 15 to 50 employees, and these employees each have around one to three devices to manage. (4) As companies very often utilise many different types of devices with different operating systems, the software selected for comparison must be multi-platform. (2)

EU defines a small company as a company with less than 50 employees, with less than 10 million euros annual turnover or less than 10 million euros annual balance sheet total. A micro company is a company with less than 10 employees that has either less than two million euros annual turnover or two million euros annual balance sheet total. Medium sized companies have less than 250 employees and have less than 50 million euro sin annual turnover or 43 million euros annual balance sheet total. (4) This is illustrated in Figure 1 below.

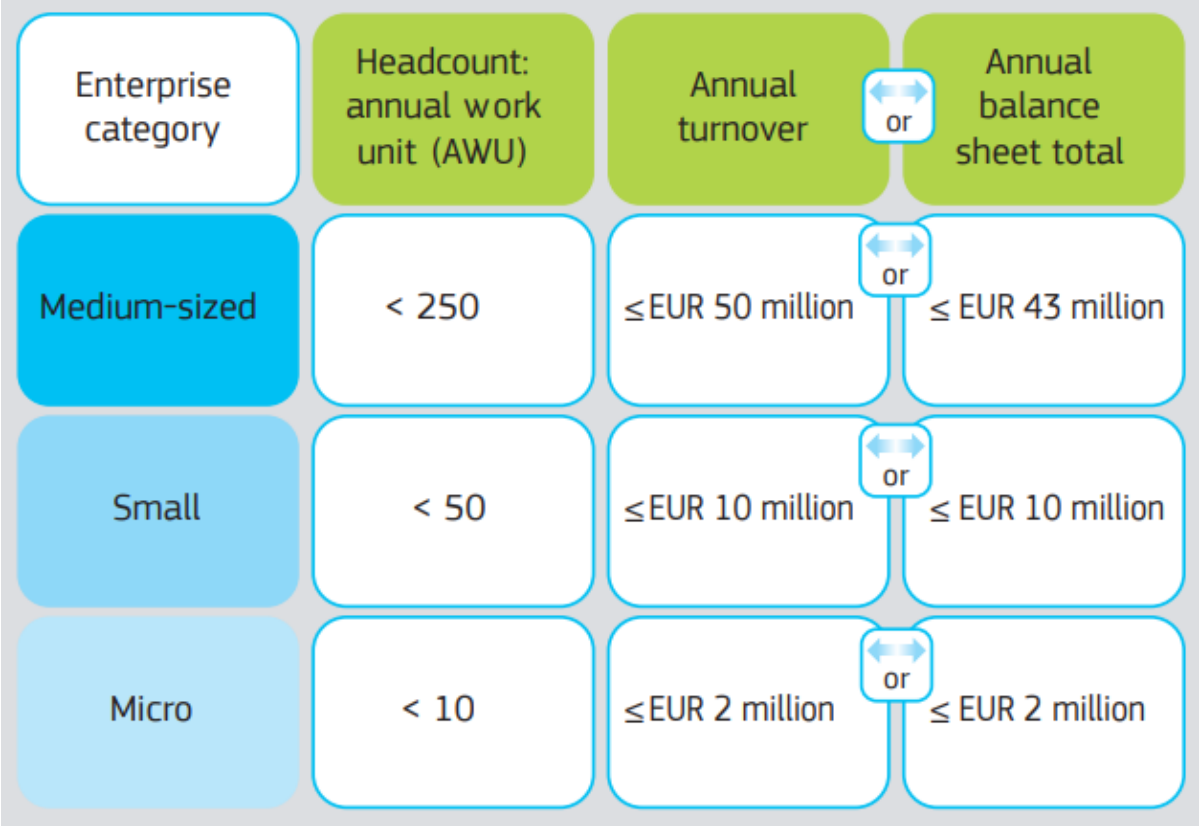


Figure 1 EU Definitions on Company Sizes (4)

3 Methods

This chapter of the thesis will cover the method and approach used throughout the analysis. It is important to think about how to get the information that solves the research question when finding the most appropriate research method. (23) This thesis uses a qualitative questionnaire to collect data on what features are most important to the respondents, and a discussion with technical experts to discuss the collected responses. A questionnaire was chosen as the most appropriate form of data collection for this thesis as questionnaires are a widely used and a highly valued means of data collection. (23) Figure 2 is a flow chart that was created to visually represent the methods process.

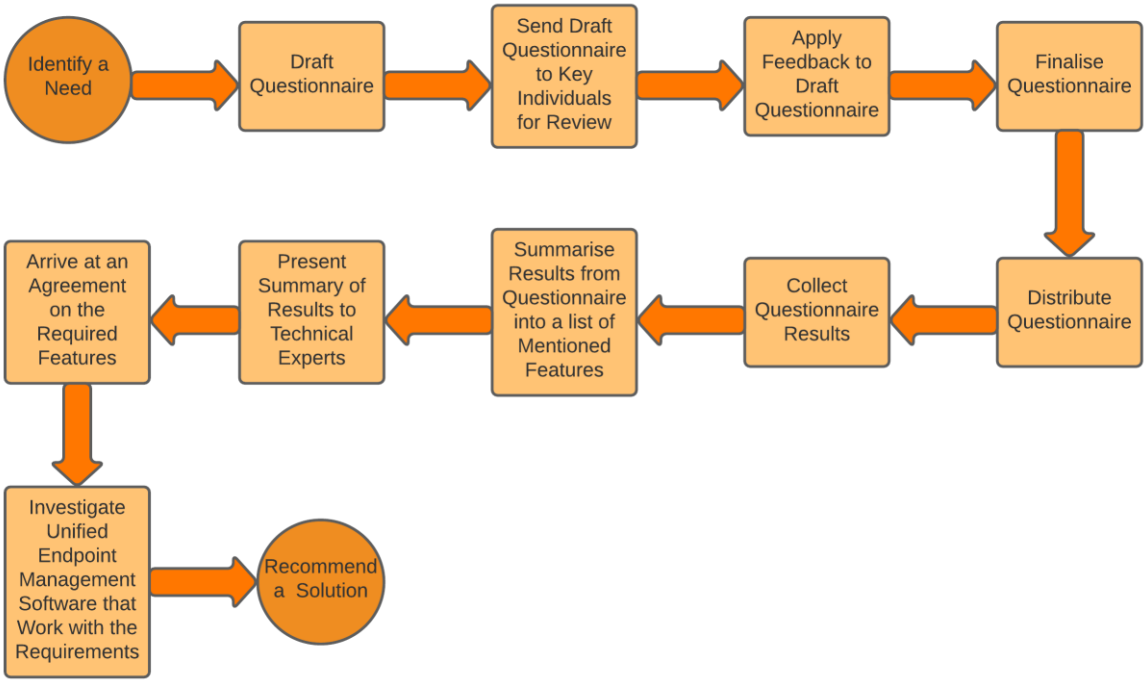


Figure 2 Process Flowchart

3.1 Questionnaire

In order to obtain the suitable requirements for the new unified endpoint management software, a questionnaire was created to collect qualitative data. One part of the survey uses a Likert scale to understand what employees feel are the more important and less

important features. (24) In order to get insight into how the new unified endpoint management software can make tasks easier and better, open-ended questions were also used to grab more detailed responses that can be used to determine if specific features are required or are simply desired. Open-ended questions can be extremely useful as they provide the respondent the ability to express their feelings freely and provide a deeper insight into the problem or problems being solved. (25)

A questionnaire was selected to collect this data as it allowed the sample group of twenty people the freedom to complete it in their own time. (26) The questionnaire was drafted and sent around to a small group of individuals for testing to ensure that the questions, layout, and appearance of a questionnaire were acceptable as they are of paramount importance in ensuring that good responses are received, and that respondents take the questionnaire seriously. (25) The questionnaire was created in a way to allow more technical minded individuals to provide answers for more technical questions, and the less technical people to answer more general questions. To do this, the questionnaire was broken down into the following sections: Introduction, Technical Features, Technical General, General, and Open Question.

In the Introduction section, one question asks the job title of the respondent to show or hide the more technical questions depending on their answer. To help get more information if a respondent's answer was vague, a question asking for their first name was added. The Technical Features section was constructed to allow the technically minded respondents to provide their thoughts on how important certain features were. These features were selected from a pool of general features a UEM software might have and were curated during the draft period to form the list of features in the questionnaire. The features were listed out, one by one, and had a small scale from one to five, where one was not at all important, three was if the respondent did not have an opinion on whether the feature was important or not, and five represented if the feature was very important. After the technical respondents finished the Technical Features, they were asked to answer more open-ended questions in the Technical General section. These were open-ended questions to get the respondents to provide additional information regarding what features they would like, what are some existing issues or problems that they would like to be resolved, and if they were aware of any existing software that they would like to recommend or mention.

The next section, General, was the first section for respondents who did not have a technical background. These were open-ended questions, asking them to talk about areas they felt could be improved, and if they had any personal requests for features of the software. As these questions were different to what the technical respondents answered, the technical respondents were also asked to answer these questions as well. The purpose of the General questions was to get insight into what other areas of an organisation might want or have issue with, as a technically minded respondent might overlook, or not be aware of them. The last section of the questionnaire was the Open Question, its purpose was to allow the respondents to provide any additional information they felt was required.

3.2 Semi-Structured Focus Group Interview with Technical Experts

When conducting a semi-structured interview, the interviewer does not use a set list of questions, instead, they use a list of topics to be discussed. A semi-structured format allows for a focused discussion about a set list of topics without limiting the possibility for any additional questions or discussions regarding the topics. (27) Focus groups are used to gather attitudes and dispositions. (28) Focus groups were chosen as they “draw out complexities, nuances, and contradictions with respect to whatever is being studied”. (28) A semi-structured focus group interview is an interview that has a limited amount of participants discussing a list of topics but have no structured list of questions.

An online meeting was held with a focus group of technical experts. They had a technical background and provided insight into what parts of the requirement list generated by the questionnaire results should stay in the requirements list and what should be considered a desirable feature instead. From the meeting, the list of ideal requirements was refined, moving similar features together, changing features from being a requirement to being a desirable, and adding brand new features to the desirable list. One of the technical experts suggested that the password management feature is added to the desirables list. Another brought up the point that permission management will be challenging due to the scattered permissions in a typical IT infrastructure, but would be greatly appreciated if possible, so they suggested that the permission management feature be moved from the requirement list to the desirable list. The table of features in the Analysis chapter represents the outcomes of the questionnaire and this meeting with the technical experts.

3.3 Selecting of UEM Software to Compare

These three UEM software were selected as all of them have multi-platform support and are suitable for a small company. The three software were discovered by searching the internet for all UEM software that supported Windows, Mac, and Linux devices. If a software did not support all of these three operating systems, then they were disregarded. The three selected software are: JumpCloud, ManageEngine Desktop Central, and Okta.

During the selection process, four UEM software were discovered and considered for the comparison, however, when researching and testing these software, it was discovered that one of them only operated in the United States, as this thesis is for small companies operating in Finland, it was decided to not include it in the comparison as it could not be used. The software was called Rippling, and it allowed a company to integrate their Human Resources (HR) tasks within their UEM software. Allowing a HR person to create a basic user account and use that to send the necessary paperwork the new employee needs to sign before joining the company. It also allows the billing team to purchase devices through the software and deliver the device straight to an employee pre-configured, while also meeting the other UEM requirements.

3.4 Software Testing

Where possible, the software selected for comparison were tested to determine if they were appropriate or not for a small company's needs. Software testing was done to get an understanding of how the software worked and to try and discover any usability problems. (29) This testing focused on usability problems because first impressions are important. (29) JumpCloud and ManageEngine offer free trails that offer access to all their features. Okta offer a free trial for their entire range of packages for 30 days.

In order to test these software properly a testing strategy was developed. The testing strategy involved enrolling all of the test devices into each of the software and go through each of the features and confirm if it accomplishes what it says it does. Figure 3 illustrates this testing strategy with the test devices.

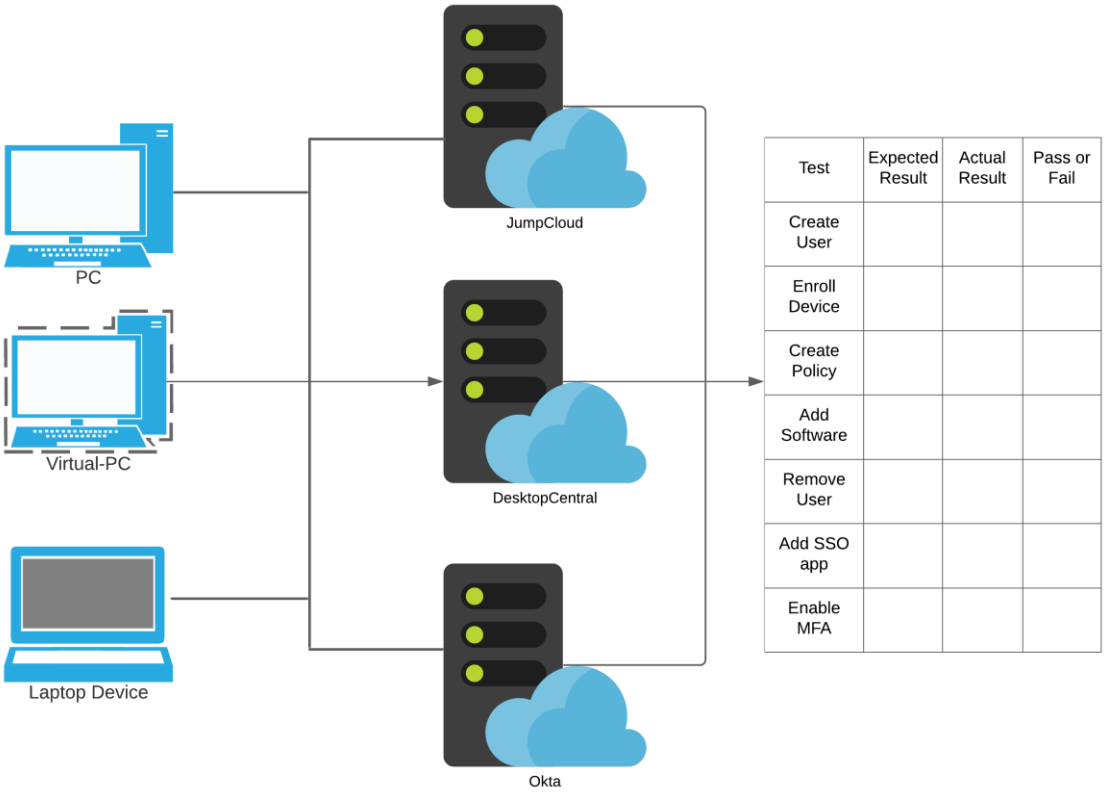


Figure 3 Software testing strategy

Some features of the selected software could not be tested entirely due to the lack of resources. For example, testing how each software handled syncing users from Google Workspace wasn't possible as there was no access to a test Google Workspace account with test users.

If testing features was not possible, information about the feature and how it operated was obtained from the developer of the software's website if available. Different types of information were used, blog posts, demonstration videos, articles, to name a few, were all consulted to gather knowledge on how a feature worked.

Test devices were set up in order to properly test the features that were testable. These test devices were personal devices. Two Windows devices, one with the Windows Server 2022, and the other with the Windows 10 Pro, one MacBook Pro with macOS, and one Linux server running Ubuntu 20.04.

3.5 Ethical Considerations

The study was conducted ethically, and respondents voluntarily answered the questionnaire. The responses from the questionnaire will also be treated anonymously. Any data that was stored for the purpose of the questionnaire was stored according to GDPR regulations. Data stored for the questionnaire was removed after the completion of the thesis.

4 Analysis

This chapter covers the discussion of the results from the questionnaire and how they were discussed with the technical experts. The three selected UEM software will be discussed, detailing basic information about each software, what features they provide, how those features compare against the requirements obtained during the Methods chapter, and finally listing any limitations the software may have.

4.1 Results of Questionnaire

The questionnaire was sent out to employees via email, however there were some who did not respond to the questionnaire. From the responses that were received, it was clear that the respondents appeared welcoming of the change, however, some respondents were apprehensive as they fear they might lose some control of their own device which they had previously, others were excited to implement the changes, as they saw how it would benefit their work.

In the Technical Features part of the questionnaire, technical respondents were given a list of potential features for the UEM software, and, using a Likert scale, asked to rate each feature for how important it was to them. The results show that most of the respondents who answered the questionnaire, feel the Single Sign On feature is the most important one, followed by Device Management, and Sync with Google Workspace/Microsoft Azure/Active Directory. A few respondents, however, felt like Single Sign On was

not an important feature to have. From these results, the features were added to the Requirements list to be discussed with technical experts.

4.1.1 Features

Summarising the results of the questionnaire, any feature that was mentioned is listed below in addition to the curated list of features that respondents had to rank. Some of the responses required interpretation in order to establish what feature could solve the problem or weakness they identified. Certain features were mentioned multiple times, and some of the mentioned features were closely related to each other, so the related features have been grouped together. For example, a Software Library feature, can include the option to update the software, which can include the ability to schedule the update to a convenient time. See the features below in Figure 4.

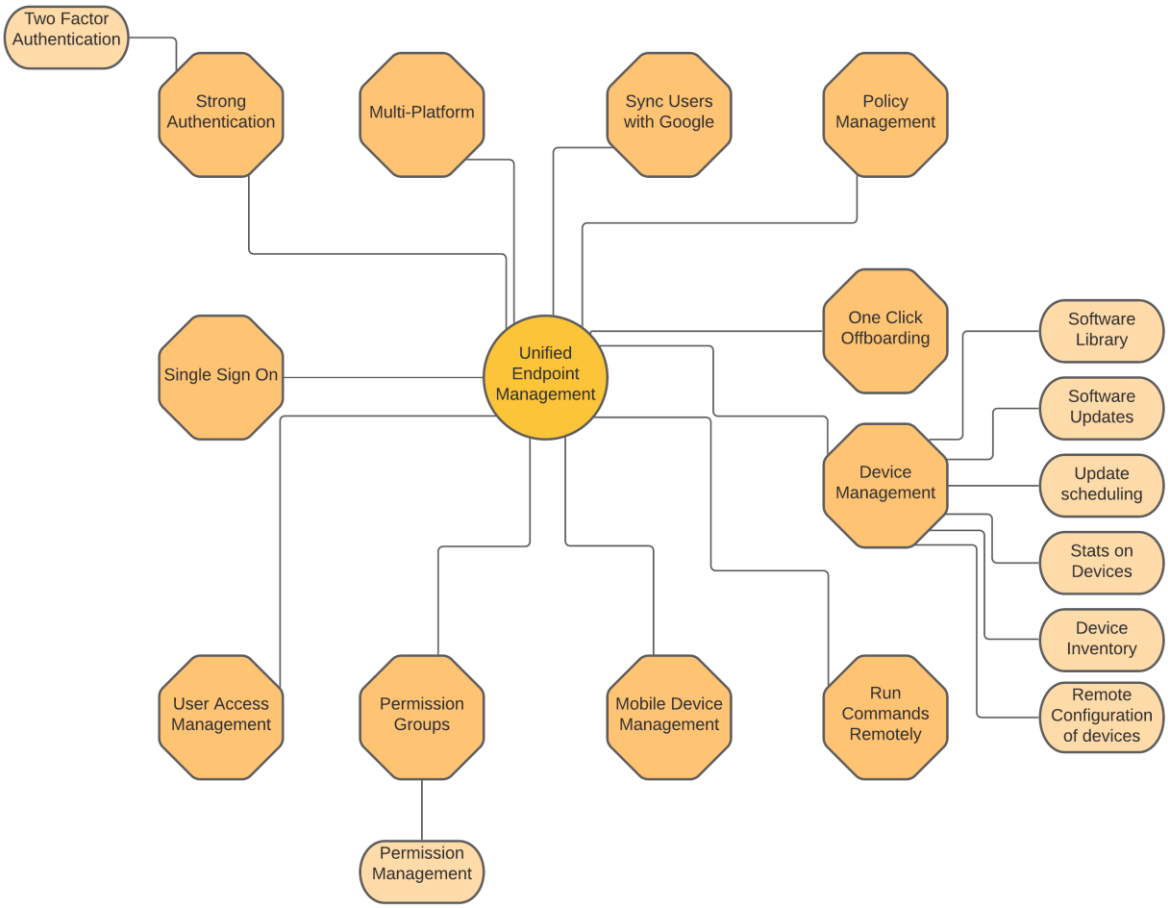


Figure 4 The features collected from the questionnaire

4.2 Results of Technical Experts Discussion

After the results of the questionnaire were summarized and all mentioned features were extracted into a Requirements list, a meeting was held with technical experts to decide on which of the mentioned features should be a requirement for the new UEM software, and which should become a desirable feature instead. The following sections will cover, the features that were mentioned in the questionnaire responses, the requirements that were chosen by the technical experts, and the features that were determined to be desirable instead of a requirement.

4.2.1 Requirements

After analysing the results of the questionnaire and discussing these results with experts, the requirements of the UEM software was agreed upon, and they are displayed in Table 4.

Table 4 The required features of the unified endpoint management software

Feature	Sub-feature
Strong Authentication	Two-Factor Authentication
SSO	
Device Management	Software Updates and scheduling
	Device Inventory
	Remote Configuration
One Click Offboarding	
Sync Users with Google	
Multi Platform	

SSO is required as the respondents considered this feature to be the most important one out of all the other features in the list. Multiple respondents also mentioned that having to juggle all their different usernames and passwords was getting tricky to handle, which SSO can resolve by replacing all of the different usernames and passwords with one.

Device Management, is required as many of the required features, like software updates, device inventory, and remote configuration require the devices to be managed by the software. Respondents also expressed many improvements for the current computer deployment process that involved things such as automatic software updates, remotely

configuring new devices, and controlling when updates are deployed. Device Management was also voted as the second most important feature.

Sync Users with Google Workspace/Microsoft Azure/Microsoft Active Directory is required as it allows businesses to utilise their existing user directories instead of having to create every user again on the new service. Syncing also ensures that all changes are replicated in the necessary areas. Many small businesses use Google Workspace so future references to this specific feature will only say “Sync Users with Google”.

Device Inventory is required as one respondent brought up that this could be utilised to document any existing compatibility issues with the devices and provide solutions or workarounds to them to remove any work interruptions.

Software Updates and the ability to schedule them started as two separate features, however, were combined after the discussion with experts due to their similarity. This is required as many respondents mentioned that software updates should be managed so that reminders can be set to install them later or install them automatically, and to schedule them outside of business hours to avoid interruptions.

Multi-platform is required as many companies utilise devices with different operating systems. One respondent also mentioned this specific feature when answering the question Personal Feature Requests for the Software.

One Click Offboarding is required as one respondent mentioned that it is very difficult to remove every account an employee had when they leave a company.

Remote Configuration of devices is required as many companies have shifted into a working from home model, and because of this, new devices are mailed directly to the new employee’s address. This feature will allow administrators to remotely install everything that is required for the new employee to do their work without requiring physical access to the device. Another respondent also mentioned that a new employee does not always get every permission they need to do their work.

Strong Authentication is required as one respondent mentioned this in the additional information section of the questionnaire. Strong Authentication utilises MFA to provide extra security for users.

4.2.2 Desirables

Any feature in the desirables list will, if any UEM software has it, grant extra consideration to that software during the Recommended Solution chapter. However, it will not stop one of the three software from being chosen as the best if it does not contain any of the features mentioned in this section.

Permission Management was on the initial list of requirements; however, it was moved to a desirable feature as it might be a challenging feature to implement for current IT infrastructures. The expert who brought up this feature detailed how they would like to see this feature implemented, providing the software does contain this feature, saying, in their ideal world, they would like to see from one interface, every permission granted to every user in the system. If this feature is available in any of the software being compared it will be considered during the comparison as many respondents have mentioned that necessary permissions for new employees are not always granted automatically and need to be requested. They also mentioned that some permissions appear to vanish.

Password Management was suggested to be added as a Desirable feature during the meeting with experts, as this feature could be used to compliment SSO for the applications or managed devices that do not support SSO. This feature could also force users to reset their passwords after a specified amount of time to ensure the security of the organisation’s computer system is not compromised.

4.3 JumpCloud

JumpCloud “understood that IT administrators needed a comprehensive platform to manage a growing number of cloud infrastructure and storage solutions, macOS and Linux devices, web applications, WiFi and VPN networks, and remote employees”. (30) JumpCloud offers several features in its unified endpoint management software that are outlined in the Features section below, and comes in many different packages. JumpCloud has five different kinds of packages and plans. They are: SSO Package, Core Directory Package, JumpCloud Platform, and Platform Plus. SSO Package includes cloud directory and standard support, cloud MFA, JumpCloud Protect Authenticator App,

single sign on, and user lifecycle management. If required, an organisation can also purchase the device management bundle. Core Directory Package includes all the same things the SSO Package includes as well as: Cloud LDAP, Directory Insights, and Cloud RADIUS. JumpCloud Platform contains everything in the Core Director Package, and includes Device and Server Management, MDM, and System Insights. The final package, Platform Plus, contains all the other features listed plus Zero Trust features, such as Conditional Access Policies, Device Trust, and Network Trust. Every package but the Platform Plus one, has the option to purchase premium support, Platform Plus already includes premium support. If an organisation does not want or need every feature listed in JumpCloud's packages, then they can build their own package using the A La Carte plan. This allows the organisation to only pay for the features that they need. Figure 6 shows the costs for each of JumpCloud's packages, and Figure 7 covers the A La Carte package if an organisation would select annual pricing.

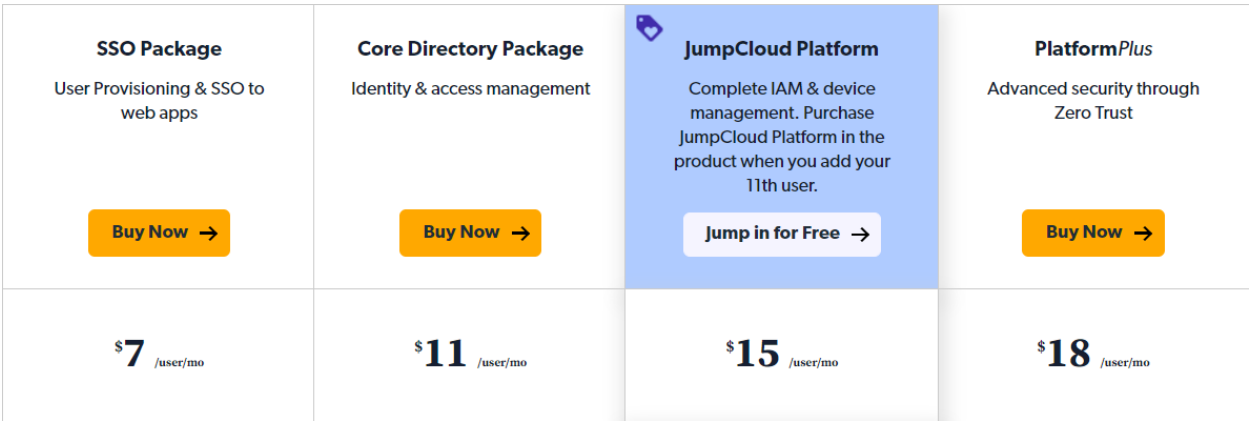


Figure 5: JumpCloud Features and Pricing from https://jumpcloud.com/pricing

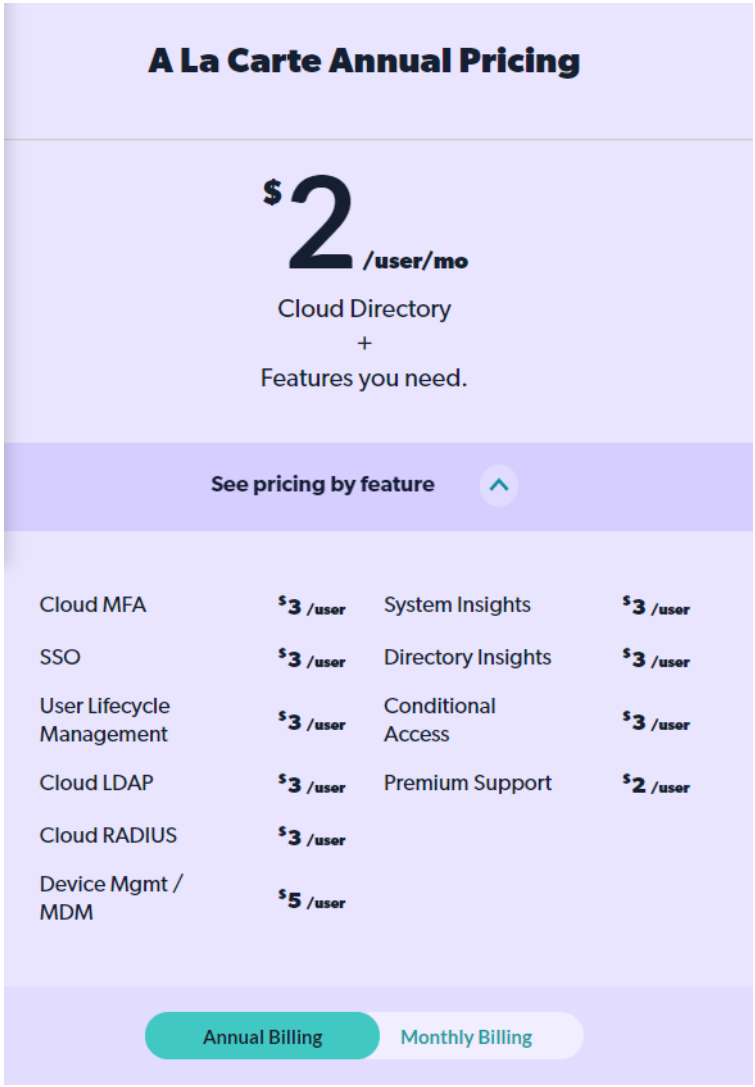


Figure 6: JumpCloud Features and Pricing from https://jumpcloud.com/pricing

JumpCloud requires an agent to be installed on every device an administrator wishes to manage. However, administrators are not required to install any additional software themselves to manage the devices, they can log into the administrator portal, and run all their tasks from there. Users also have access to an online portal which allows them to access any SSO applications that have been configured, modify information on their JumpCloud profile, reset their password, add SSH keys, and configure multi-factor authentication. Appendix 2 shows what an Administrator sees when they log into the administrator portal, and Figure 8 shows what a user sees when they log into the user portal.

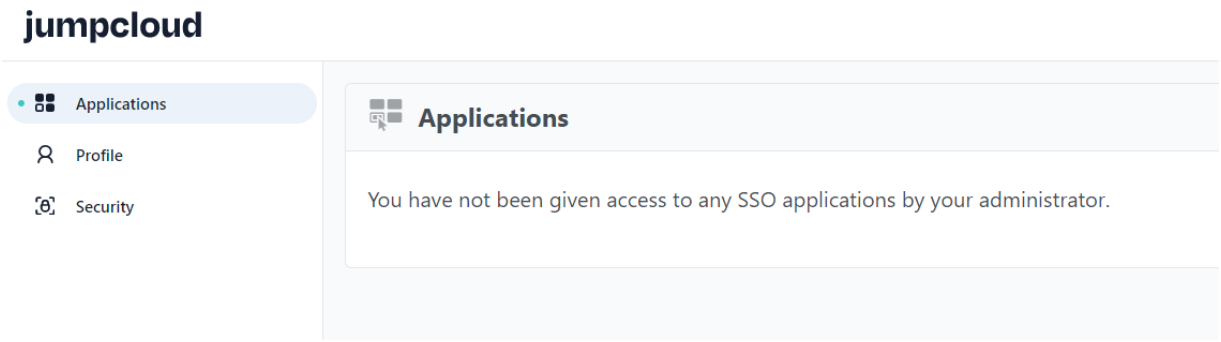


Figure 7 JumpCloud User Portal Screen

4.3.1 Features

This section covers all the major features JumpCloud provides and explains how they operate. Features will not be analysed in this section, only described. The analysis of JumpCloud's features and how they match the requirements will be in the Features vs. Requirements section.

To add users to JumpCloud, there are many different integration methods available. Administrators can import users from Google Workspace, Microsoft 365, Microsoft Azure Active Directory, or via a comma separated value (CSV) file. JumpCloud also offers a slightly similar feature in its Directory Integrations section. The features in the Directory Integrations section allow administrators to synchronise users and their information between the two directories. This should be used if an organisation requires the existing user directory but would also like to start using JumpCloud's one as well.

Users are created either manually via an administrator, or synchronised/bulk imported from other user directories. Once the user account has been created, an administrator can assign them to a user group, which might be a team in an organisation, so that the user receives access to applications that team has. If there are devices already added to JumpCloud, an administrator can assign a user to a device, which will trigger JumpCloud to create the user's account on the assigned device. The user's password can be managed here. If the organisation is enforcing MFA, the administrator will set a time period to give the new user time to download an MFA application and configure it. For every user, a Directory Activity is available which provides a brief history of events that the user has done. Administrators also can suspend a user or schedule when their account will be suspended.

To help authenticate users online with different applications, JumpCloud offers three separate ways to implement a form of single sign on. The three ways are Single Sign On (SSO), Remote Authentication Dial-In User Service (RADIUS), and Lightweight Directory Access protocol (LDAP).

JumpCloud allows administrators to manage the devices of the users in the company. Administrators can register new devices, these new devices can be Windows, Linux, or Mac. Administrators can even add servers managed with Puppet or Chef. Puppet and Chef are software configuration management tools, that help manage and automate configuration of servers. (31) (32) Once a device has been registered, an administrator can assign it to a new user and add it to a device group. Figure 9 displays this process. The device group will allow the administrator to push out certain tasks to specific devices within the group. JumpCloud displays the managed devices in a list format, with default columns such as: Status, Device Name, OS, Primary Adapter IP, MFA Status. and Last Contact. These columns are customisable if an administrator requires less or additional information about the managed devices.

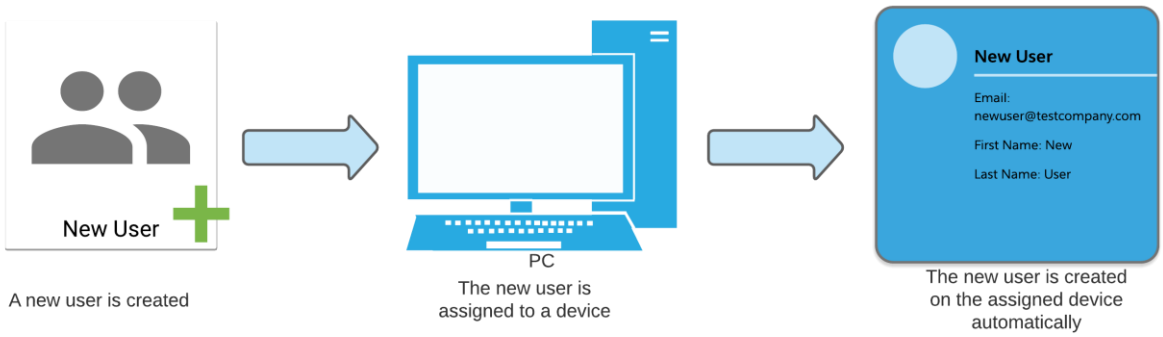


Figure 8 User creation and device assignment process

These devices can have security policies assigned to them to enforce company policies automatically. Policies can then be grouped into separate policy groups to push out multiple policies at once to different devices. JumpCloud recommends certain policies it feels are the most beneficial to an organisation here, however, you are not required to use them. After creating the new policy and assigning it to devices, you can select the policy in the list and click on the Status tab to show how many of the assigned devices now have this new policy, or if any devices failed to receive the policy.

If there are Apple devices in the organisation, JumpCloud can manage these devices via its MDM solution. This allows administrators to "…securely install, configure, and deploy devices to your users without ever touching the device" (33) This integration can also create customised policies with MDM to automate device enrolment, manage settings remotely, disable any unwanted user accounts, and manage any other security considerations. To aid administrators in configuring this feature, JumpCloud have a video tutorial available to explain the setup process step by step.

For Security Management, JumpCloud offers administrators the ability to configure Conditional Policies. These conditional policies are used to control how users authenticate themselves in order to get access to the user portal or specified SSO applications. When adding a new conditional policy, an administrator needs to provide the policy name, whether this policy targets every user or just specific ones, if any conditions are necessary, and most importantly, whether the user is allowed to authenticate into the selected resource or if they are denied. The ability to select specific conditions for a conditional policy, is a Platform Plus feature. Administrators can specify that certain policies only apply when the user is or is not in a list of pre-defined countries, when the user is trying to authenticate from a list of pre-defined IP addresses, or if they are trying to authenticate from a specific device.

If an administrator wants to set a policy to only apply when a user is authenticating from a particular device, then they will need to configure device certificates. Device certificates allow authentication mechanisms to tell if it is coming from a device that is being managed by JumpCloud.

JumpCloud includes four different methods of implementing MFA. These methods are JumpCloud Protect Mobile Push, Time-based One Time Password (TOTP), WebAuthn, and Duo Security. JumpCloud Protect Mobile Push is a mobile application that can be download from the iOS App Store and the Google Play Store. This can be used to protect a user's device by requiring them to confirm their login action via the app.

4.3.2 Features vs. Requirements

This section covers how the features of JumpCloud matches the requirements established at the beginning of this chapter. Table 5 provides a simplified view of the requirements and how JumpCloud meets them. For any feature that is marked as Limited, it will be discussed in the Limitations section.

Table 5 Outlining which of the requirements JumpCloud has

Requirements	JumpCloud's Features
SSO	Yes
Sync Users with Google	Yes
Device Inventory	Yes
Software Updates and scheduling	Limited
Multi-Platform	Yes
One Click Offboarding	Yes
Remote Configuration of Devices	Limited
Strong Authentication	Limited

JumpCloud's SSO feature offers 731 easy configuration templates for different applications. However, if an organisation is using a custom SAML application, they can add it via the Custom SAML App button.

JumpCloud meets the requirement for Device Management. How JumpCloud handles device management is detailed in the Feature section above. As JumpCloud displays every managed device in a list in the Administrator portal, it also meets the Device Inventory requirement.

Administrators have the ability of syncing their current user directories from places such as Microsoft Azure, Active Directory, Google Workspace, and Workday. This allows administrators to bulk import users from the current user directory into JumpCloud's user directory. This integration also means that administrators or users only need to update information in one place only, with the updated information copied to the other directory.

JumpCloud allows easy offboarding when an employee leaves an organisation. All an administrator needs to do is unassign the user from the device, and their user account on the device will be removed. However, this does take time as the user will not be removed until the JumpCloud agent on the device contacts the server and notices that the user has been unassigned.

Most of JumpCloud's features are multi-platform, only two of them are not. These two features are MDM, which is only for Apple devices, and Software Management, which is only available for Windows and Mac computers. This will be covered more in the Limitations section.

4.3.3 Limitations

While JumpCloud does support multiple platforms, not every feature works the same across all operating systems. For example, managing software on Windows devices requires the use of a package manager called Chocolatey, whereas Mac devices require administrators to create and host their own .pkg files or using links to .pkg files hosted by third parties. Linux devices do not have this feature at all.

Requiring the use of the Chocolatey package manager for Windows devices does pose some security concerns, as the Chocolatey package manager receives its applications from volunteers. Chocolatey does provide information on who the package maintainers are and also includes security checks, such as validation testing and scan testing. However, there is still a possibility that a bad actor could upload malware or a virus. There should be an option to allow JumpCloud to manage either self-hosted windows applications, either in exe or msi format, or provide a cloud database so administrators can upload safe and trusted versions of the applications they wish to install.

If a user has an issue with their device and is requesting assistance in resolving the problem, administrators will need to utilise other software to facilitate the remote session. If JumpCloud had this feature in built with their own software, it will save Administrator's time having to jump back and forth between an external remote desktop application and JumpCloud's administrator portal.

There are only a set list of policies to implement and no way to add a custom one. Windows has by far the greatest number of policies to implement, Mac has the next biggest amount, and Linux only has six. This feature would be greatly improved if administrators could add their own custom policies

4.4 ManageEngine Desktop Central

Desktop Central is defined on their website as:

"a Unified Endpoint Management (UEM) and security software that comprehensively addresses the requirements of IT administrators. Desktop Central helps IT administrators to perform patch management, software deployment, mobile device management, OS Deployment and take Remote Control to troubleshoot devices. And with the help of Endpoint Security Add-on, which includes vulnerability assessment, application control, device control, BitLocker Management and browser security, IT administrators can safeguard their network endpoints. Furthermore, Desktop Central integrates seamlessly with ManageEngine and other third-party solutions" (13)

ManageEngine is the IT Management division of the Zoho Corporation since 2002. They started business in 1996 as AdventNet. ManageEngine have offices in US, India, Japan, China, Netherlands, and Australia. Desktop Central comes in four different versions, the free version, professional version, enterprise version, and UEM version. The free version offers administrators the ability to manage up to 25 computers and 25 mobile devices, deploy software, create a hardware inventory, remote control devices, and deploy patches. The professional edition includes everything that is available in the free edition without the 25 computers and 25 mobile device restriction, with the ability to add on mobile device management, OS deployment, and endpoint security. The enterprise version includes everything in the professional version and adds a self-service portal, the

ability to prohibit and block specific exe files, controlling software licenses, recording remote sessions, and two factor authentication. Mobile device management, OS deployment and endpoint security can be added on if the company requests. The final version is the UEM version, which includes everything in the enterprise version plus mobile device management, management of Mac and Windows computers, and OS deployment, a company can also pay extra to get endpoint security as an add-on. Desktop Central supports the following platforms: Windows, Linux, Android, iOS, macOS, tvOS, Chrome OS and iPadOS. Desktop Central can be integrated with other ManageEngine products such as Servicedesk Plus, ServiceDesk Plus On-Demand, OS Deployer, Asset Explorer, and Analytics Plus.

As ManageEngine Desktop Central has four different versions, a table has been constructed to outline the price differences between each version. Company X has outlined its preference towards cloud-based solutions, so only those prices have been listed in Table 6 below.

Table 6: Data obtained from https://www.manageengine.com/products/desktop-central/pricing.html

Endpoint Range (with 1 technician)	Professional Version		Enterprise Version		UEM Version	
	Monthly	Annual	Monthly	Annual	Monthly	Annual
50	$104	$1045	$124	$1245	$129	$1295
100	$189	$1895	$234	$2345	$249	$2495
250	$374	$3745	$469	$4695	$494	$4945
500	$654	$6545	$824	$8245	$874	$8745

ManageEngine Desktop Central requires an agent to be downloaded and installed onto all the devices that will be managed by Desktop Central. Administrators can log into the online portal to manage the devices and the users assigned to them. Appendix 4 illustrates what an administrator sees when they log into the online portal.

4.4.1 Features

Desktop Central includes a robust selection of features, so not all features will be listed here. Only the relevant features have been mentioned below.

Patch Management allows administrators to track the status of patches on every managed device. This allows Desktop Central to see if some devices are missing any patches, and if these patches are critical or not. Within the Patch Management section is a dashboard that provides graphs on the system health, network health, information on what patches are missing, and the managed computers by their operating system. It also has a section dedicated to showing the latest security news. Patches can be deployed from the Patches section. The administrator can select all the patches they want to install, click on install and then create the configuration. During the configuration creation process, administrators can schedule when the patches are deployed based on a selected deployment policy. This is where an administrator also selects which devices they want the patches to be deployed to. Patches can also be automated. Administrators can create an automatic task to install patches, third party updates, anti-virus updates, and driver updates. These automatic patches can be delayed if necessary, by specifying the amount of days to wait either from the release of the patch, or from the approval date.

Software Management controls what software can and cannot be installed on the managed devices. It can also create a list of every software installed on the device. An administrator can automate the deployment of software via the templates that have been pre-configured in Desktop Central. These software templates, promote fast software package creation and deployment by supplying all the required software information for the administrator. Once all the required software have been added to the Packages, the administrator can trigger the installation process by creating a new configuration. These packages can also be uninstalled following the same process above and changing install to uninstall. Figure 10 illustrates the software deployment process.

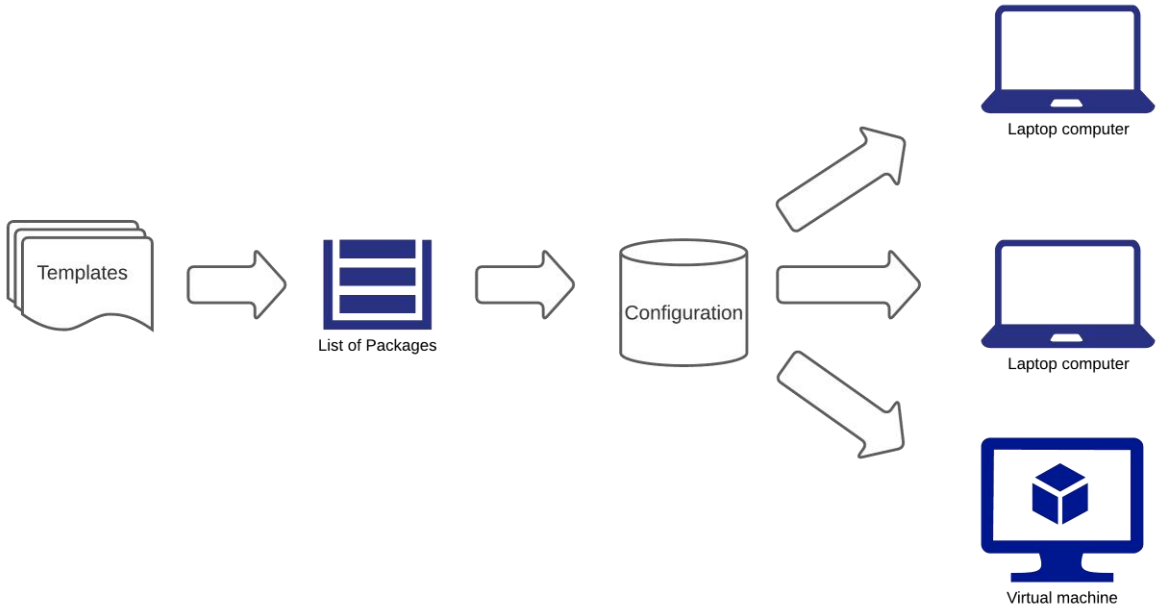


Figure 9 Desktop Central software deployment process

Inventory provides an overview of every device you are managing. It has many different sections covering computers, hardware, software, alerts, and reports. Computers contains every computer managed by Device Central. From this section you can view currently managed computers, add new computers, and modify data about the computers. Clicking on one of the computers in the list will open a window displaying detailed information about the selected computer. The detailed information is broken down into many different tabs. These tabs are Summary, System, Hardware, and Software. The Summary tab gives a detailed overview of the computer. The System tab lists all services, users, groups, and drivers that are on the computer. The Hardware tab provides all the hardware details about the selected computer. The Software tab lists all the installed software on the device.

Mobile Device Management allows administrators to enrol and manage computer and mobile devices. The Mobile Device Management section also manages any mobile device applications an organisation chooses to use. Administrators can set up managed access to their application store accounts to automatically add applications, or manually add them themselves by using Desktop Central's built-in application search feature. These applications can then be assigned to any mobile device managed by Desktop Central. Applications for Windows and Macs can also be managed in this same way.

Documentation can be uploaded to Desktop Central if an organisation wishes to distribute it across their managed devices. The users need to install the ManageEngine (ME) MDM application in order to view any of the shared documents.

Desktop Central offers administrators the ability to remotely control any device in the system. To get the remote control to work, an Administrator needs to select the device and click Remote Control. Once that is clicked, the remote session will begin with no additional downloads or installations required on the admin's side or on the user's side. Remote Control also allows both administrators and users to communicate to each other via the in-built chat feature and send files to and from each other.

4.4.2 Features vs. Requirements

This section details how Desktop Central meets the requirements that were outlined at the start of the chapter. Table 7 outlines which of the requirements are met by Desktop Central.

Table 7 Shows which features Desktop Central has that match the requirements

Requirements	Desktop Central's Features
SSO	No
Sync with Users Google	Limited
Device Inventory	Yes
Software Updates and scheduling	Yes
Multi-Platform	Yes
One Click Offboarding	No
Remote Configuration of Devices	Yes
Strong Authentication	No

Desktop Central only meets half of the requirements, with two features meeting the requirements in a limited way. Inventory is its own category in Desktop Central and it allows administrators to store information related the organisation's IT infrastructure. Desktop Central even allows you to manage software licenses from the Inventory section. There is a separate device inventory within the Mobile Device Management section, which keeps track of both computer and mobile devices, displaying them all together in one place.

The Patch Management meets the requirements as it gives administrators the ability to find unprotected devices, and schedule automatic patch deployments that will not inhibit the employee's ability to work on that machine. Patches can also be approved before they are deployed by creating a test plan. The test plan is applied to specific test machines chosen by the administrator, and once the test plan passes, the patches are marked for approval and can deployed to the rest of the managed devices.

Desktop Central supports Windows, Mac, and Linux devices. However, there are some features that do not have Linux support. For example, MDM does not support managing Linux devices, only Windows, Apple, Samsung, and Google.

Desktop Central through its patch management, software deployment, remote desktop features, meets the requirement for remote configuration, as administrators will not require physical access to the device to install and set up everything that is required.

4.4.3 Limitations

Desktop Central uses configurations to trigger most of its tasks. While the configurations offer many areas to customise, every single action requires a configuration, from deploying patches as a once off, to installing software to one device. To make this experience easier for new organisations, it would be better to keep configurations only for repeating tasks and actions.

Mobile Device Management can link an account with a device; however, nothing happens on the device after it is linked. The software should create the user account on the device and manage the account on its own. This would make configuring computers for new employees incredibly easy as the software does most of the work for you, as well as allowing easy offboarding when an employee leaves the organisation.

4.5 Okta

Okta started in 2009 and was co-founded by Todd McKinnon and Frederic Kerrest, who had both previously worked together in another company called Salesforce. Okta is a general technology company that offer many products and solutions. They currently offer the following 11 products: Single Sign-On, Universal Directory, Authentication, Advanced Server Access, API Access Management, Multi-factor Authentication, User Management, B2B integration, Lifecycle Management, Access Gateway, and Workflows. Okta also offers two solutions, they are Workforce Identity, and Customer Identity. Workforce Identity includes the following features: Securely Enable Remote Work, Adopt a Zero Trust Security Model, Improve M&A Agility, Reduce IT Friction, Move to the Cloud, Collaborate with Partners, and Adopt Office 365. Customer Identity includes the following

features: Transform into a Digital Platform, Cultivate User Trust, Modernize Infrastructure, Build Highly Scalable Apps, Secure Access to APIs, Protect Against Account Takeover, and Integrate Apps. Figure 11 shows what a user sees when they log into their Okta account and appendix 4 displays what an administrator sees when accessing the administrator portal.

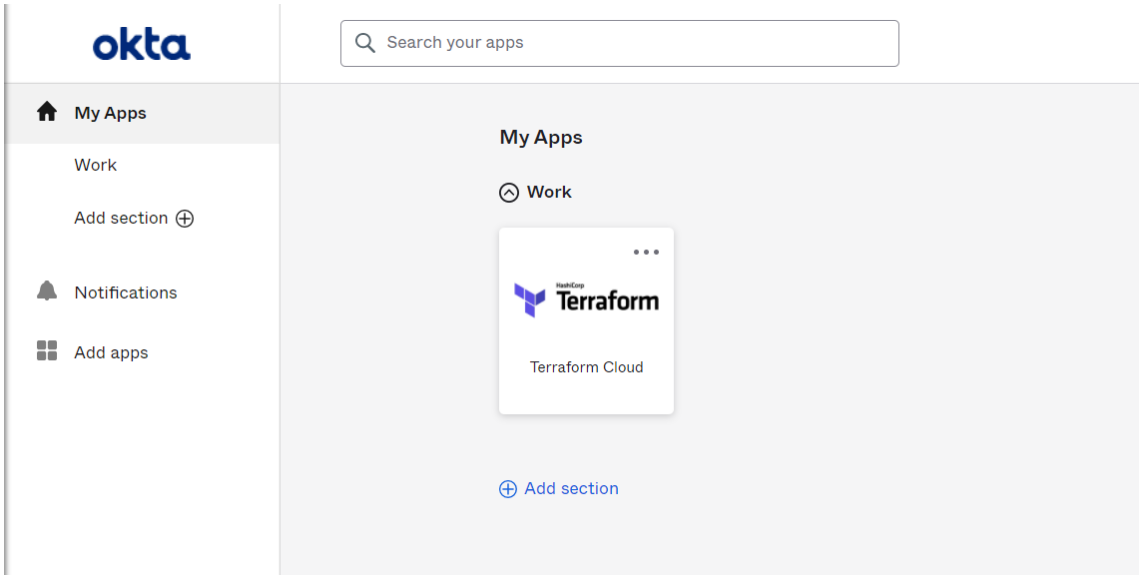


Figure 10 Okta User Account Screen

4.5.1 Features

To achieve the company's goals, three separate products are required. These are Single Sign-on, Multi-factor Authentication, and Advanced Server Access. As Advanced Server Access can provide centralised permission management for an organisation's servers, which is a desirable feature, it will be discussed in this section alongside the other products.

Single sign-on costs two dollars per user per month and includes the following features: Desktop and mobile SSO, Email as a factor, third party MFA integration, Group and app access policies, RADIUS authentication, PIV card authentication, and IdP discovery. It allows directory integrations with Active Directory and LDAP. Another tier of this feature exists for five dollars per user per month, which includes extra features such as: Location context, Device context, Network context, and Risk-based Authentication. These extra features allow administrators to provide contextual access when required.

To allow for multi-factor authentication with Okta, a company will need to purchase the Multi-factor Authentication package. It costs three dollars per user per month and includes the following features: Security questions, confirming possession, and biometric verification. The confirming possession feature works by allowing users to prove they are the holders of the device via, SMS, voice, and email. For the biometric verification feature, Okta allows users to verify their identity via Windows Hello, and Apple TouchID.

Advanced Server Access aims at providing centralised access to servers that can scale with an organisation's servers. It supports both Linux and Windows servers. It grants users access to an organisation's servers without the need of a username and password. This package authenticates the user to the server using a one-time access key that expires the moment the user logs out of the server. This also allows new users to be onboarded and offboarded quickly. Figure 12 illustrates how advanced server access works.

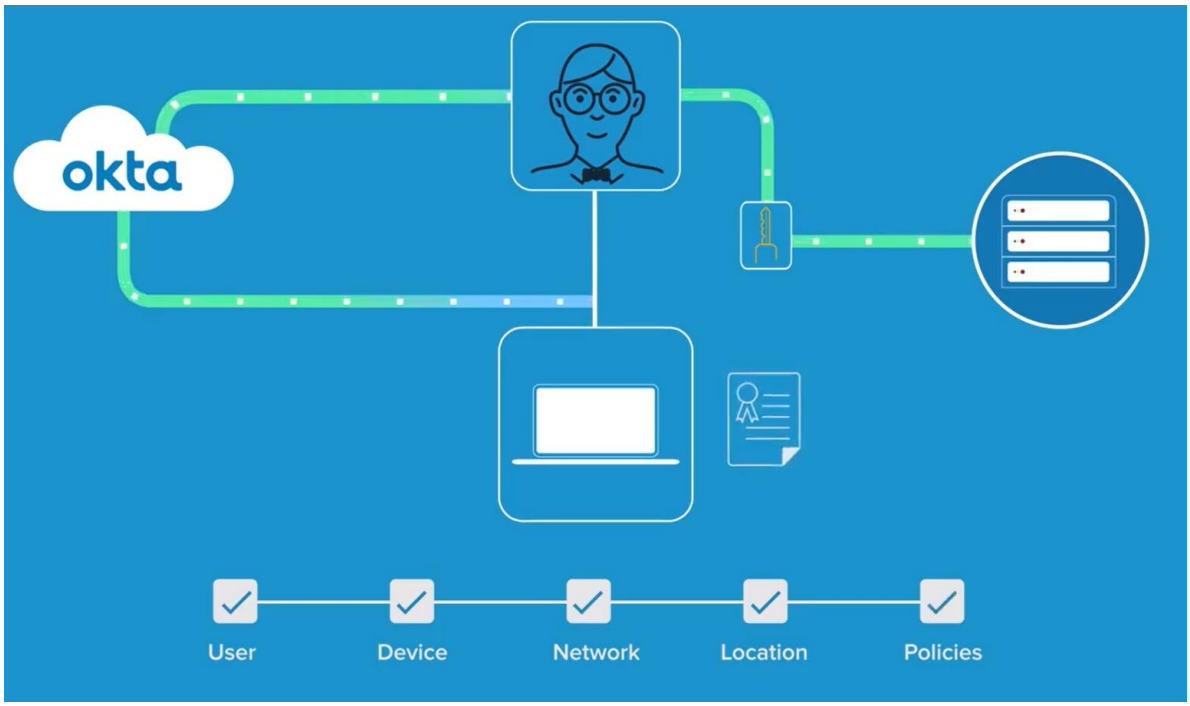


Figure 11 Okta's Advanced Server Access process diagram. (34)

4.5.2 Features vs. Requirements

In this section, the UEM software requirements will be compared to the features that are included in the three Okta packages. Table 8 shows a list of the requirements, whether Okta meets that requirement, and which of the three Okta packages meets the requirement.

Table 8 Compares the features and packages Okta have and the requirements they meet

Requirements	Okta's Features	From Which Okta Package?
SSO	Yes	SSO
Sync Users with Google	No	
Device Inventory	No	
Software Updates and scheduling	No	
Multi-Platform	Yes	SSO, MFA, Advanced Server Access
One Click Offboarding	Limited	Advanced Server Access
Remote Configuration of Devices	No	
Strong Authentication	Yes	MFA

Okta's MFA package grants the ability to force users to use a second authentication factor. By default, Okta enables Okta Verify, which is a mobile application that users are required to have in order to obtain the six-digit code to allow them to log into their account. If desired, the Okta Verify app can be configured to require a user to pass through Apple's Face ID or Touch ID before getting access to the six-digit code. Applications can

be modified to also require the user to use MFA. Okta also allow administrators to configure many other types of MFA tokens, such as: SMS authentication, Google authenticator, Duo Security, RSA SecurID, and an On-Prem (on premise) MFA.

The SSO package allows organisations to either use the existing application templates to implement SSO or they can create a custom SSO integration either via OpenID Connect, SAML 2.0, Secure Web Authentication, and API Services. Administrators can configure Okta to allow users to add their own personal applications, however, administrators can remove this permission and be the only ones responsible for adding applications.

Advanced Server Access allows quick onboarding and offboarding of users. Their user accounts are created when they are attempting to connect to the server using credentials that are generated for that session and will be removed the moment the user logouts of the server. Audit logs are created every time a user connects to a server and logs everything the user accesses, so administrators can track any file or system modifications that have been made. However, this is only for servers, and cannot be used to onboard or offboard users from computers.

4.5.3 Limitations

Okta only meets three of the eight requirements. These requirements are only met by purchasing additional packages. Okta does not provide any way for administrators to manage devices, synchronise users from Google, create a device inventory, update software, or remotely configure devices. Okta is more designed to allow organizations to easily access the applications they use in a protected and secure way, instead of managing devices. While Okta offer an Advanced Server Access package, they do not offer user device management with their packages so user devices will continue to be managed manually. If an organisation wants to utilise Okta, and bring across their users from Google Workspace, they will need to export the users into a CSV file and then bulk import them into Okta, whereas Active Directory users can be easily imported via the Active Directory integration. Okta should allow for more user directory integrations like JumpCloud and Desktop Central.

5 Recommended Solution

This chapter covers the comparison of the three selected Unified Endpoint Management software, detailing how well they have met the requirements or how they have not. If any of the selected software included any of the desirables, they will also be discussed here. To clearly illustrate how each of the selected software went in meeting the requirements, Table 9 includes both the requirements and desirables and shows which software provides which of the requirements.

Table 9 Comparison table to see which software matched what requirement

Feature	JumpCloud	Desktop Central	Okta
SSO	Yes	No	Yes
Sync Users with Google	Yes	Limited	No
Device Inventory	Yes	Yes	No
Software updates and scheduling	Limited	Yes	No
Multi-platform	Yes	Yes	Yes
Onboarding and Offboarding	Yes	Limited	Limited
Remote Configuration of devices	Limited	Yes	No
Strong authentication	Limited	No	Yes
Password Management	No	No	No
Permission Management	Limited	Limited	Limited

JumpCloud had five out of eight of the requirements, however, it does provide a limited version of the rest of the required features. Desktop Central has four of the eight requirements, while also providing a limited version of most of the other features, it does not provide any form of strong authentication or single sign on functionality. Okta had only three out of the eight features, and these were spread out in three separate packages.

However, Okta was the only software to offer strong authentication completely and not a limited version like JumpCloud does.

Comparing the software against each other, JumpCloud better manages user and devices by allowing user accounts to be created and removed automatically when the user is assigned or unassigned from the device. Greatly allowing fast onboarding and offboarding of new and old employees. However, Desktop Central allows for better management of software and updates, with its ability to create test plans for new updates, and ease of deploying new software to the required devices. Okta's implementation of SSO and MFA, allows for greater number of applications to be connected and a higher degree of protection for users.

When it comes to pricing, in order to meet the requirements, a company needs to purchase JumpCloud's Platform package which costs 15 dollars per user per month. For Desktop Central, the company will require the Professional package with the Mobile Device Management Add-on. This costs 129 dollars per month for 50 endpoints. Across all three of Okta's packages, the monthly cost to meet the requirements are 11 dollars per user per month plus 15 dollars per server per month. So for a hypothetical company with 30 users, 50 computers and mobile devices, and 5 servers, they would need to pay Okta 4860 dollars per year (4307 euros). For Desktop Central they would need to pay 1548 dollars per year (1372 euros) plus an additional cost if they want to purchase additional technicians, refer to Figure 13 for the prices of additional technicians. For JumpCloud they would need to pay 5400 dollars per year (4786 euros).

Additional technician(s)	Monthly	Annual
1	$44	$445
2	$79	$795
5	$154	$1,545
10	$254	$2,545
25	$499	$4,995
50	$779	$7,795

Figure 12 Price of additional technicians for Desktop Central from: https://www.manageengine.com/products/desktop-central/pricing.html

For the Desirables, all of the selected software offer a limited permission management feature, and none of them offer any sort of password management, so no extra considerations will be provided when deciding on the software to recommend as a solution.

JumpCloud utilises permission management by implementing policies dictating if a user can connect to a resource on a certain device or in a certain location, with or without MFA. Desktop Central implements permission management via its ability to control what applications users can run or not. Okta uses permission management to control which specific SSO applications users can run, and whether they are required to verify their identity via MFA.

As JumpCloud meets five of the eight requirements while also providing a limited version of the other requirements, the recommendation in this thesis is that a small business should implement JumpCloud to improve how it handles user and device management the best out of the three selected software, despite its high cost. If a small company does not want to pay such a high price, the next best software would be Desktop Central, as it offers almost all the same features JumpCloud does while being more than half the

price of JumpCloud. Do take note though that JumpCloud does not charge for extra technicians, while Desktop Central does, so the cost of Desktop Central might increase.

6 Conclusion

This thesis, using a small company as a test case, showed how user and device management can be improved using Unified Endpoint Management software. The employees of a case company were used to obtain a list of requirements, which were then used to discover three appropriate UEM software for comparison. Three different software were introduced, features outlined and compared with the requirements, and closing by outlining any limitations the software has. The three software were then compared to each other and JumpCloud was selected as the best UEM software as it met almost every requirement.

All of the software chosen for this thesis are excellent software that provide an expansive set of features for companies to manage their users and devices. Desktop Central allows for better software and update management. For companies that value patching their devices and easily deploying software, Desktop Central is a better choice. If a company only wants to manage their servers, then Okta's Advanced Server Access is the better choice.

The solution outlined in the Recommended Solution chapter allows small organisations to manage their users and devices efficiently. It allows users to be added automatically from synchronised user directories and have those added users automatically added to managed devices. These devices can now be managed to help deploy software, manage permissions, and be protected by multi-factor authentication. SSO will allow users to easily access all their needed web applications and services via a single login and can also be protected by multi-factor authentication.

This solution is catered towards a small-sized company, larger companies should do more research to conclude what software is best for them. This solution might not apply for micro companies, as micro companies only consist of 10 or less employees, so managing the devices for a low amount of users should not be difficult for IT administrators, as well as the fact that paying for UEM software is expensive, and it will not be worthwhile

for a micro company to spend money to manage a small amount of devices. For this comparison only cloud-based software were selected; however, the possibility still exists for a self-developed solution if the recommended solution does not meet small businesses' needs, and the small business is happy to spend money on the development costs.

6.1 Future Research

This thesis only covers the requirements for a small company, so further research can be done to understand if there are any different requirements that a bigger company requires. Also, further research into developing a new UEM software should be considered as businesses can have very unique needs.

References

1. Insight. Insight. [Online]. [cited 2021 November 17. Available from: https://ca.insight.com/en_CA/content-and-resources/2017/07312017-4-reasons-need-end-user-device-management-policy.html.
2. Hess K. Unified Endpoint Management for Dummies Hoboken: John Wiley & Sons Inc.; 2017.
3. Blanton S. What is User Management. [Online].; 2021 [cited 2021 November 29. Available from: https://jumpcloud.com/blog/what-is-user-management.
4. European Commission. User guide to the SME Definition. Luxembourg:; 2015.
5. Lunsford P. The Road to Unified Endpoint Management. Emerging Technology. 2019 July.
6. Laird J. LifeHacker. [Online].; 2014 [cited 2021 November 18. Available from: https://web.archive.org/web/20141110000156/http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore.
7. Citrix. Unified Endpoint Management. [Online]. [cited 2021 November 2021. Available from: https://www.citrix.com/fi-fi/solutions/unified-endpoint-management/enterprise-mobility-management-emm.html.
8. Keller G. Why Centralized User Management is Important. [Online].; 2015 [cited 2021 October 30. Available from: https://jumpcloud.com/blog/why-centralized-user-management-is-important.
9. ManageEngine. The What Why and How of Unified Endpoint Management. [Online].; 2019 [cited 2021 November 6. Available from: https://blogs.manageengine.com/desktop-mobile/desktopcentral/2019/03/11/the-what-why-and-how-of-unified-endpoint-management.html.
10. Ivanov V. Analysis and Problems Using Enterprise Mobility. In 7th International Conference on Application of Information and Communication Technology and Statistics in Economy and Eduation; 2017; Sofia. p. 5.
11. Gartner. What are CMTs (client management tools)? [Online].; 2016 [cited 2021 November 6. Available from: https://www.gartner.com/reviews/market/client-management-tools.
12. Hayes D, Cappa F, An Le-Khac N. An effective approach to mobile device management:Security and privacy issues associated with mobile applications. Digital Business. 2020 September; 1.

13. ManageEngine. DesktopCentral Features. [Online]. [cited 2021 November 9. Available from: https://www.manageengine.com/products/desktop-central/features.html.
14. ManageEngine. Automate Software Deployment for Windows, Mac, & Linux. [Online]. [cited 2021 November 11. Available from: https://www.manageengine.com/products/desktop-central/software-deployment.html#features.
15. ManageEngine. Windows Configuration. [Online]. [cited 2021 November 2021. Available from: https://www.manageengine.com/products/desktop-central/windows-configurations.html.
16. ManageEngine. IT Asset Management (ITAM) Software. [Online]. [cited 2021 November 11. Available from: https://www.manageengine.com/products/desktop-central/it-asset-management.html#features.
17. JumpCloud. An Overview of Applications. [Online]. [cited 2021 10 29. Available from: https://support.jumpcloud.com/support/s/article/An-Overview-of-Applications.
18. Stanislav M. Two-Factor Authentication: IT Governance Publishing; 2015.
19. JumpCloud. The Definitive Guide to RADIUS. [Online]. [cited 2021 November 11. Available from: https://jumpcloud.com/resources/radius-guide.
20. JumpCloud. Getting Started: Policies. [Online]. [cited 2021 November 13. Available from: https://support.jumpcloud.com/support/s/article/getting-started-policies-2019-08-21-10-36-47.
21. Kandogan E, Magilo PP, Haber E, Bailey J. On the roles of policies in computer systems management. International Journal of Human-Computer Studies. 2011 June; 69(6).
22. European Commission. 2019 SBA Fact Sheet. ; 2019.
23. Lancaster G. Research Methods in Management : A Concise Introduction to Research in Management and Business Consultancy: Taylor & Francis Group; 2005.
24. Joshi A, Kale S, Chandel S, Pal DK. Likert Scale: Explored and Explained. British Journal of Applied Science & Technology. 2015 February.
25. Bajpai N. Business Research Methods: Pearson Education India; 2018.
26. Bryman A, Bell E. Business research methods. 3rd ed.: Oxford University Press; 2011.
27. Bryman A. Social Research Methods New York: Oxford University Press Inc; 2012.

28. Kamberelis G, Dimitriadis G. Focus Groups : From Structured Interviews to Collective Conversations. 1st ed.: Taylor & Francis Group; 2013.
29. Myers GJ, Sandler C, Badgett T. The Art of Software Testing. 3rd ed.: John Wiley & Sons, Incorporated; 2011.
30. JumpCloud. About Us. [Online]. [cited 2021 October 30. Available from: https://jumpcloud.com/about-us.
31. Carty D. TechTarget. [Online]. [cited 2021 November 13. Available from: https://searchitoperations.techtarget.com/definition/Chef-software.
32. Puppet. Puppet Docs. [Online]. [cited 2021 November 13. Available from: https://puppet.com/docs/puppet/6/puppet_overview.html.
33. JumpCloud. Getting Started: MDM. [Online]. [cited 2021 November 7. Available from: https://support.jumpcloud.com/support/s/article/Getting-Started-MDM.
34. Okta. [Video].; 2019 [cited 2021 November 20. Available from: https://www.youtube.com/watch?v=PlYXNeBKhBI.

Questionnaire Questions

Features for Centralised Account Management Software

* Required

What is your first name? *

The purpose of this question is to allow me to follow up on results that require more information

What team are you a member of? *

This survey changes depending on what team you are in. If you are in Analytics or IT, you will get more technical based questions. Everyone else will skip these questions, and get more general questions.

Team 1	Team 2	Team 3	Team 4	Other:

Which Features Do You Feel are Important?

1 being Not at all Important
3 being Neutral
5 being Very Important

Single Sign On (SSO) *

Allows you to log into multiple different services with a single account

Not at all Important	1	2	3	4	5	Very Important

Mobile Device Management (MDM) *

Mainly for our Macbooks, it allows us to easily deploy new Macbooks with the same settings and applications, as well as remotely deploying applications and updates.

Not at all Important	1	2	3	4	5	Very Important

Device Management *

Gives the IT team the ability to view stats of devices, add users, change settings, etc. For example when setting up a new computer.

Not at all Important	1	2	3	4	5	Very Important

Stats on Devices *

Gives the IT team the ability to view statistics on devices like amount of free space on a hard drive, total amount of RAM being used, etc. For example when troubleshooting if a computer has enough resources for a task

Not at all Important	1	2	3	4	5	Very Important

Software Library *

The ability for IT to have a list of applications that can be remotely installed to computers when requested. For example to be to install a new antivirus solution to every computer at once, instead of installing it one computer at a time.

Not at all Important	1	2	3	4	5	Very Important

Run Commands Remotely *

The ability for IT to execute commands on computers without needing to connect to it first. Can be used for troubleshooting purposes, like changing a setting from the command line.

Not at all Important	1	2	3	4	5	Very Important

Policy Management *

Ensure certain settings are pushed out to all applicable devices. Settings such as resetting your password every 90 days.

Not at all Important	1	2	3	4	5	Very Important

Sync with Google Workspace/Microsoft Azure/Microsoft Active Directory *

Allow the software to connect to Google Workspace, Microsoft Azure, Active Directory, and synchronise users, devices, etc. To ensure one change is automatically copied to another.

Not at all Important	1	2	3	4	5	Very Important

Discussion Time!

This section is to allow more detailed responses from the technical teams

What do you feel are the current weaknesses in our account creation/management process? *

Do you think the computers can be better managed? If so, in what way? *

Is there something that IT can improve on already without new software? If so, what and how? *

Do you know of any Centralised Account Management software that you want to recommend? *

What Would Make Everyone's Lives Easier?

Centralised Account Management doesn't just impact the work of the IT team, it can also impact people outside of the IT Team. So this section of the questionnaire is dedicated to understanding what things or features that would make lives easier, for say, requesting new accounts to be created, specific permissions to be granted, etc.

Centralised Account Management software is used to make account organisation, access rights management, and device management and setup way easier

Do you have any personal requests for the centralised account management software? *

Are there any issues with the current process of requesting accounts to be created by IT? *

What improvements would you like in the deployment of new computers and/or computer/software updates? *

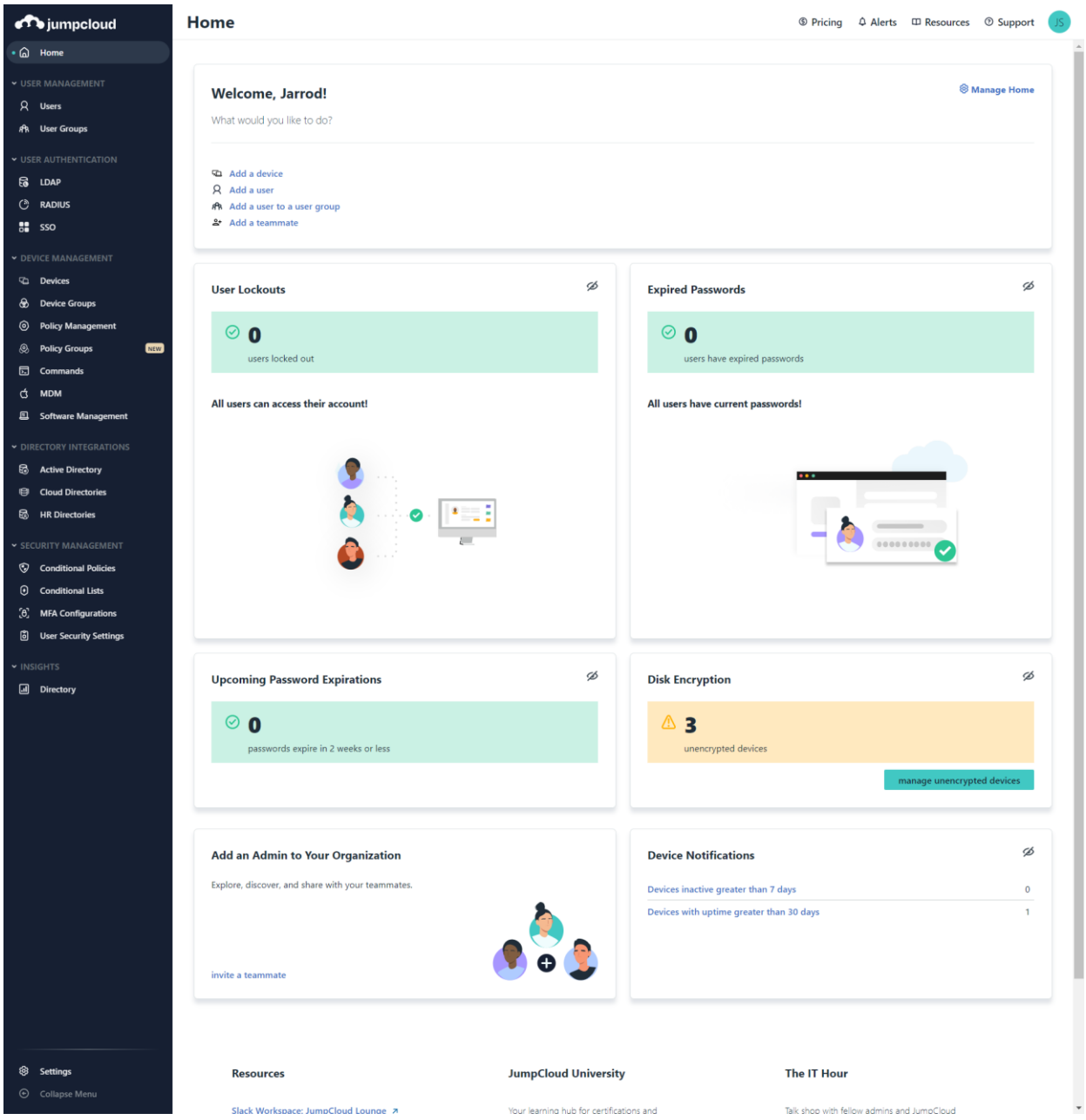
How do you feel about the IT team being able to remotely, without needing anything from you, install applications, install updates or modify permissions? *

This would allow both the IT Team and the team member requesting changes to work without interruption or delay

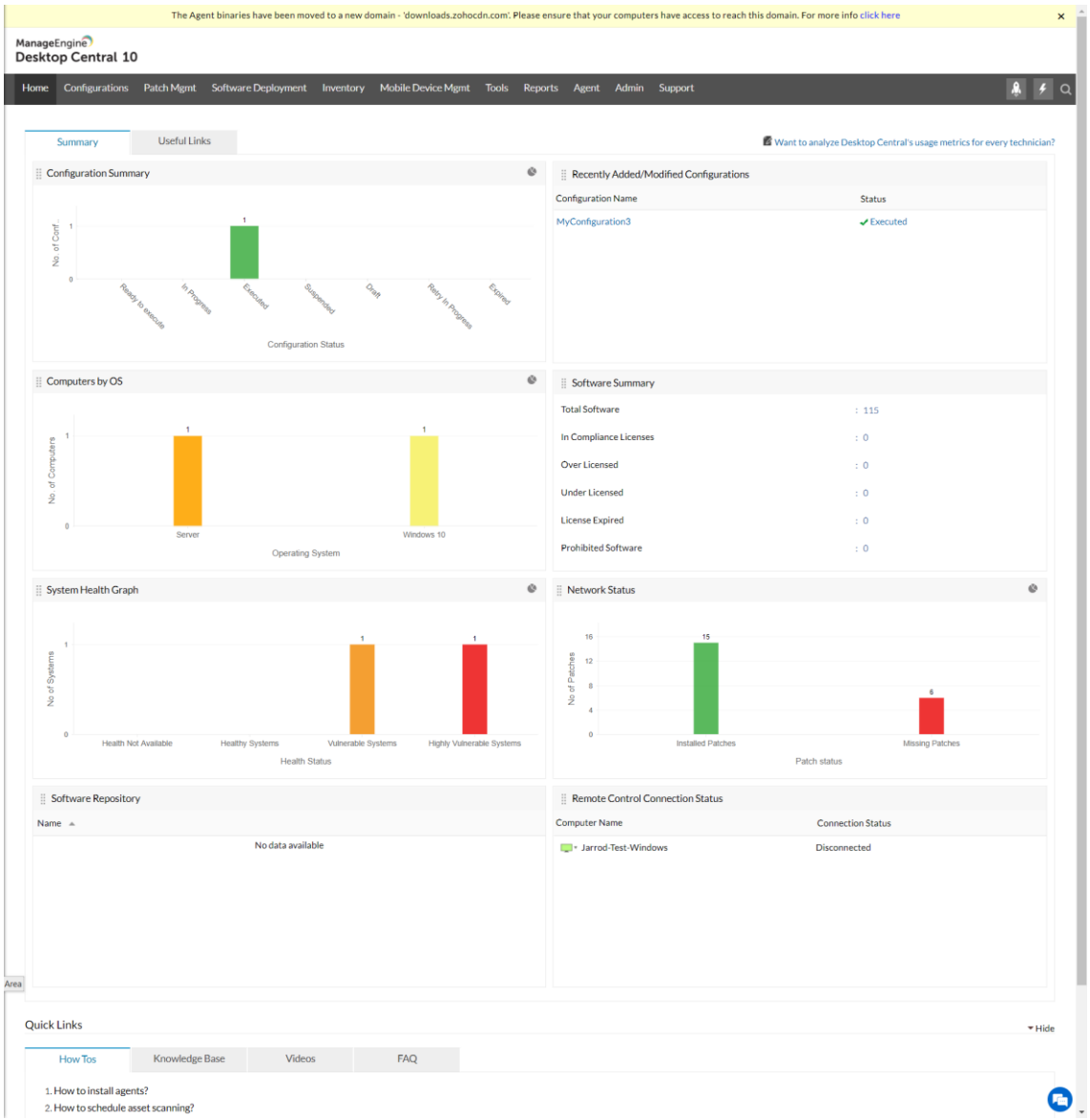
Have I Missed Anything?

Do you want to say something that wasn't asked in the previous questions?

JumpCloud Administrator Portal Screenshot



ManageEngine Desktop Central Administrator Portal Screenshot



Okta Administrator Portal Screenshot