jamk

Leveraging JumpCloud for Zero Trust Architecture Implementation in Small and Medium-Sized Enterprises

Teemu Lampinen

Master's thesis
May 2024
Information and Communication Technology
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Lampinen, Teemu

Leveraging JumpCloud for Zero Trust Architecture Implementation in Small and Medium-sized Enterprises

Jyväskylä: Jamk University of Applied Sciences, May 2024, 89 pages.

Master's Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Small and medium-sized businesses have a high risk of being targeted by adversaries due to the lack of security controls and the inability to block access to company resources from unmanaged devices. This research explores the implementation of Zero Trust Architecture using JumpCloud. The primary objective is to evaluate how JumpCloud can enhance cybersecurity through its various features, including device management, Single Sign-On (SSO), and conditional access policies.

The research involves a detailed analysis of JumpCloud's technical capabilities, such as operating system support for Linux, Windows, macOS, Android, and iOS, password management, passwordless authentication, Zero Touch deployment, Multi-Factor Authentication, policy and patch management, and API services. The advantages and disadvantages of different SSO integration methods were evaluated with a cost-benefit analysis.

The results demonstrate that JumpCloud provides a comprehensive platform for managing and securing endpoints, identities, and SaaS application's SSO using different operating systems. By leveraging JumpCloud, organizations can enhance their security posture, streamline IT operations, and reduce the risk associated with unmanaged devices. By creating a Google Workspace SSO integration with JumpCloud and following best offboarding practices, SMEs can achieve significant cost savings compared to utilizing System for Cross-domain Identity Management (SCIM) with different applications.

The findings in this research are that utilizing many of JumpCloud's features improves SME's security significantly through conditional access policies, and Zero Trust's tenets can be achieved with a modern Endpoint Defence and Response (EDR) application. Overall, JumpCloud, if utilized and configured correctly, is an excellent Unified Endpoint Management (UEM) system that aligns with the latest cybersecurity standards, offering a robust solution for SMEs aiming to adopt the Zero Trust security initiative.

Keywords/tags (subjects)

Cyber security, Zero Trust, Unified Endpoint Management, Cloud Directory, Single Sign-on, SCIM, JumpCloud, Google Workspace, Mobile Device Management, Endpoint

Miscellaneous (Confidential information)

Work is public. It does not contain any confidential information.

Lampinen, Teemu

JumpCloudin hyödyntäminen Zero Trust -arkkitehtuurin toteuttamisessa pienissä ja keskisuurissa yrityksissä

Jyväskylä: Jyväskylän Ammattikorkeakoulu, Toukokuu 2024, 89 sivua.

Master's Degree Programme in Information Technology, Cyber Security. YAMK Opinnäytetyö

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Pienillä ja keskisuurilla yrityksillä on suuri riski joutua vastustajien kohteeksi puutteellisten tietoturva-asetusten vuoksi. Riskiä lisää yritysten kyvyttömyys estää hallitsemattomien laitteiden pääsy yrityksen resursseihin. Tässä tutkimuksessa esitellään kuinka JumpCloudia voidaan hyödyntää nollaluottamus-arkkitehtuurin toteutuksessa. Ensisijaisena tavoitteena on arvioida, kuinka JumpCloud voi parantaa kyberturvallisuutta eri ominaisuuksiensa, kuten laitehallinnan, kertakirjautumisen (SSO) ja ehdollisten käyttöoikeuskäytäntöjen kautta.

Tutkimus sisältää yksityiskohtaisen analyysin JumpCloudin teknisistä ominaisuuksista, kuten käyttöjärjestelmien tuesta Linuxille, Windowsille, macOS:lle, Androidille ja iOS:lle, salasanojen hallinnasta, salasanattomasta todennuksesta, automatisoidusta laitteen käyttöönotosta, monivaiheisesta todennuksesta, tietoturva-asetus- ja päivityshallinnasta sekä API-palveluista. Erilaisten SSO-integraatiomenetelmien etuja ja haittoja arvioitiin kustannus-hyötyanalyysin avulla.

Tulokset osoittavat, että JumpCloud tarjoaa kattavan alustan päätelaitteiden, identiteettien ja SaaS-sovellusten SSO-hallintaan ja turvaamiseen eri käyttöjärjestelmillä. Hyödyntämällä JumpCloudia organisaatiot voivat parantaa tietoturvatasoaan, tehostaa IT-toimintojaan ja vähentää hallitsemattomiin laitteisiin liittyviä riskejä. Luomalla SSO-integraation Google Workspacen ja JumpCloudin välille ja noudattamalla parhaita irtisanomiskäytäntöjä, PK-yritykset voivat saavuttaa merkittäviä kustannussäästöjä verrattuna ”System for Cross-domain Identity Management” -käyttäjähallinnan hyödyntämiseen eri sovelluksissa.

Tutkimuksen havainnot osoittavat, että useiden JumpCloudin ominaisuuksien hyödyntäminen parantaa PK-yritysten turvallisuutta merkittävästi ehdollisten käyttöoikeuskäytäntöjen avulla, ja nollaluottamuksen periaatteet voidaan saavuttaa hyödyntämällä lisäksi modernia päätelaitteiden tunnistus ja reagointisovellusta. Kokonaisuudessaan JumpCloud – oikein käytettynä ja konfiguroituna – on erinomainen keskitetty päätelaitteiden hallintajärjestelmä. Tuote mahdollistaa uusimpien kyberturvallisuusstandardien noudattamisen ja tarjoaa vankan ratkaisun PK-yrityksille, jotka pyrkivät ottamaan käyttöön nollaluottamusaloitteen.

Avainsanat (asiasanat)

Kyberturva, Nollaluottamus, Keskitetty päätelaitteiden hallinta, Pilvihakemisto, Kertakirjautuminen, SCIM, JumpCloud, Google Workspace, Mobiililaitteiden hallinta, Päätelaite

Muut tiedot (salassa pidettävät liitteet)

Työ on julkinen, eikä sisällä miltään osin salattavaa materiaalia

Contents

Figures

List of abbreviations

ABM	Apple Business Manager
ADE	Automated Device Enrollment
AI	Artificial intelligence
API	Application Programming Interface
BYOD	Bring Your Own Device
CBCM	Chrome Browser Cloud Management
CPU	Central Processing Unit
CSM	Customer Success Manager
DUNS	Data Universal Numbering System
EDR	Endpoint Detection and Response
EACS	Erase All Content and Settings
HRIS	Human Resource Information System
IDP	Identity Provider
IMEI	International Mobile Equipment Identity
IT	Information Technology
KB	Knowledge Base
LTS	Long-Term Support
MAC	Medium Access Control
MAID	Managed Apple ID
MB	Megabyte
MDM	Mobile Device Management

MFA	Multi-Factor Authentication
MSP	Managed Service Provider
OS	Operating System
PC	Personal Computer
PPPM	Per person / per month
QR	Quick-Response
RAAS	Radius-as-a-service
RADIUS	Remote Authentication Dial-In User Service
RE	Recovery Environment
SCIM	System for Cross-domain Identity Management
SSO	Single Sign-on
TOTP	Time-Based One-Time Password
TPM	Trusted Platform Module
TTL	Time-To-Live
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
VPP	Volume Purchasing Program
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language
ZTA	Zero Trust Architecture
ZFS	Zettabyte File System

1 Introduction

This thesis is a product-oriented research project that will give the reader a deep understanding of JumpCloud, its comprehensive features, and, most importantly, Zero Trust capabilities. The target audience for this thesis is everyone interested in the product, IT administrators who are already using JumpCloud and would like to deepen their knowledge about the tool, and decision-makers who are evaluating different Unified Endpoint Management (UEM) products.

JumpCloud can be used to protect the endpoints with various methods. In Chapter 3, the reader will learn how to use basic features, such as patch management to keep the operating systems' and browsers' versions up to date, how to erase the endpoint remotely, how to help users with the built-in remote assist tools, execute command and scripts remotely, and how to install and keep the applications up to date. Suppose the reader wants to master JumpCloud's device management capabilities fully. In that case, the thesis also offers more profound knowledge about JumpCloud's advanced features, such as the Windows MDM Lite Touch deployment, Apple Automated Device Enrollment (ADE), Managed Apple ID (MAID), and the Powershell module that leverages API.

In addition to the features focused on endpoint protection, the reader will also learn about JumpCloud's basic features of protecting the user's identity in Chapter 3 with the password manager and multi-factor authentication (MFA). In Chapters 4 and 5, the reader will learn advanced topics, such as creating Single Sign-on integrations with step-by-step instructions, conditional access policies, System for Cross-domain Identity Management (SCIM), and the differences between integrating JumpCloud to Google Workspace or directly to the service provider.

The motivation for writing this thesis is to make important information about JumpCloud and Zero Trust more accessible to everyone by collecting details about the topic from multiple sources into one document and sharing it with the online community and colleagues interested in the subject. An alternative motivation was to learn more about the product, especially the features I had no prior experience with, so I would be more prepared to pass the upcoming JumpCloud Expert level certification exam later this year when it comes out. Even though this thesis was written for a cy-

bersecurity master's degree program, it does not contain a long theoretical part about cybersecurity as a whole, as many other theses do. Zero Trust will also be addressed briefly and from the product perspective, as information on both popular topics can be easily fetched from books or the Internet.

I find this thesis important as some of JumpCloud's novel Zero Trust features were released during the writing of this thesis. Hence, it's unlikely that previous studies exist on the same topic. Some companies, especially those using mobile phones to access company resources, have not been able to implement all of JumpCloud's Zero Trust features in their companies. However, as the Mobile Device Trust feature is behind the corner, all JumpCloud customers with the Platform Prime license can soon prohibit access from unmanaged devices to its resources and mitigate two significant risks: employees using unsafe personal devices and adversaries exploiting compromised credentials. According to Okta (n.d.), 61 percent of the companies have already adopted a Zero Trust security initiative in 2023, and 35 percent are planning to implement it within the next 18 months, so it's safe to say that 2024 will be remembered as the year of Zero Trust, at least for JumpCloud customers.

2 Research Methodology

2.1 Research Questions

The main research question in this thesis is to define the answer to the following question: "What are the key benefits for small and medium-sized enterprises of leveraging JumpCloud for Zero Trust architecture implementation?" The question focuses on JumpCloud's features, a real-life test involving conditional access, and what risks the company can mitigate using it.

The secondary research question in this thesis is to define the answer to the following question: "What are the advantages and disadvantages of Google Workspace SSO integration compared to the SCIM-supported SSO integrations for small and medium-sized enterprises?" The question focuses on the cost-benefit analysis of popular SaaS applications' SSO features, pricing, and how the company can save money using an alternative solution if willing to accept the risks involved with fewer features.

2.2 Research Ethics and Methods

This research followed Jamk's ethical guidelines and principles. The text was written solely by me; no artificial intelligence (AI) was used for the thesis, and no text was copied from other sources. All software used during the thesis was licensed, and no deliberate damage or harm was done to any parties. All the tests were conducted, and the material was collected within the IPRally Technology's private environments. Users' privacy was protected by removing all personal or identifiable information from the screenshots.

All the source materials were cited according to the American Psychological Association's 7th edition style, and credit was given to the original authors. The security controls and policies were explicitly created for this thesis and do not reflect the current status of IPRally's security posture. All mentioned SaaS applications are used as an example and are not necessarily used at IPRally Technologies. All confidential information was removed from the screenshots to protect the company. It's worth mentioning that JumpCloud is evolving rapidly, and some features might have changed dramatically or even be missing altogether a few months after this thesis has been published. For

this reason, if this thesis is being used as a manual for implementing some of JumpCloud's features, remember to verify if the documentation has been changed and follow Zero Trust's primary principle: "Never trust, always verify."

The qualitative research method was used in this thesis, as it does not contain any numerical data for statistical analysis, except when JumpCloud's and SaaS application's licensing prices were compared. The quantitative research method could not be used for three reasons. Firstly, JumpCloud and its features were not compared with other tools. Secondly, no questionnaire about user satisfaction or ease of use scores was created. Lastly, the endpoint's current state and possible vulnerabilities and misconfigurations were not evaluated against the common security frameworks, such as NIST Cybersecurity Framework and the CIS Critical Security Controls, as the feature does not exist in JumpCloud and requires an XDR product, such as CrowdStrike.

3 JumpCloud & UEM

JumpCloud was founded in 2013 in Louisville, Colorado, United States, by Rajat Bhargava and Larry Middle. Rajat has been managing the company as a CEO for the whole duration of the company's history. Larry was acting as a CFO and senior vice president of operations until 2021 before leaving the company. The company has offices in five locations: Louisville - USA, Denver – USA, San José - Costa Rica, Hyderabad - India, and Medellín - Colombia. The company is privately owned and has raised over $400 million in six funding rounds. It has over 5000 paying customers in over 160 countries, valued at $2,56 Billion three years ago (JumpCloud, 2021). JumpCloud has won numerous awards, and the 2024 award list includes but is not limited to the Cybersecurity Excellence Award for Best Passwordless Solution, Global InfoSec Award for Best Identity and Access Management Solution, and Globee Cybersecurity Award for Passwordless Authentication (JumpCloud, n.d.-e).

JumpCloud has only one product named after the company, and the future JumpCloud references are for the product, not the company. The business idea for JumpCloud is to be a cloud directory platform built for managed service providers that are outsourcing services to various companies and for in-house IT administrators. JumpCloud can manage and secure multiple operating systems and integrations and simplify IT staff's lives. It's a centralized, unified management system for passwords and software updates and all the usual IT-related acronyms that will be opened later in this thesis: MDM, API, MFA, SSO, SCIM, IAM, RADIUS, and ADE. JumpCloud can manage, configure, secure, and support identities, devices, IT resources, connections, and events. Endpoint management, onboarding, and offboarding can be made simple for any user and IT administrator anywhere in the world. In a nutshell, JumpCloud takes care of the identity synchronized from an identity provider, handles access to various services, such as Wi-Fi or a SaaS application, and takes care of the user's managed device during the whole lifecycle.

In the big picture, Jumpcloud improves efficiency, refines control, and strengthens security. JumpCloud improves agility and can eliminate the need for Active Directory and on-premises infrastructure. JumpCloud streamlines the IT, and the company can generate cost savings by having fewer members in the IT team. According to JumpCloud (n.d.-as), Cabify can support 1,500 employees in 11 countries with an IT team of only seven members. The IT team's cost savings should be considered when evaluating different tools and their pricing.

JumpCloud's current pricing can be found in Figure 1. The prices at the bottom of the picture are United States Dollars per user per month (PPPM). The prices are valid if a company wants to commit to the product for 12 months. If a company does not want to commit and wants to pay one month at a time, the prices are 18% higher. Like any other application, the most precious features can be seen in the most expensive license level. This thesis strongly relates to device management, so the SSO and Core Directory licensing levels are not included in the following comparison.

The 9$ Device Management licensing level is sufficient for small companies to manage and collect detailed information from the devices and import user accounts from an external identity provider. Additionally, it can be used to keep the operating systems, applications, and browsers up to date. Helpdesk functionality is also available with Remote Access features. The next 13$ licensing level, Device Identity, will upgrade the experience by enabling the passwordless login mechanism, multi-factor authentication (MFA), and synchronizing accounts and passwords with other cloud directories, such as Google Workspace or HRIS systems.

Platform licensing level, which is priced at $19 PPPM, adds heaps of advanced features, such as Single Sign-on, provisioning, and de-provisioning of user accounts with SAML, JIT, and SCIM. Additionally, it allows the company to use JumpCloud's password manager, which can save money on other applications' licensing costs. Auditing features include viewing users' activity with Directory Insights for security and compliance purposes. Platform licenses also add the Cloud LDAP & Radius services for authenticating to wireless networks, file servers, applications, and other on-premises resources.

The $24 Platform Prime is the most exciting licensing level, as it adds the Zero Trust capability to the product, which addresses the main research question in this thesis. The most expensive licensing level also allows JumpCloud administrators to implement all future features as soon as they are released. Suppose a company is interested in the Zero Trust feature but doesn't need some features they already have in their company, such as password manager, LDAP, and Remote Access. In that case, they can customize the product and select features they only need from the A La Carte pricing options in the upper left corner of the pricing list. (JumpCloud, n.a.-r.)

Features See À La Carte Pricing >	Device Management	Device Identity	SSO	Core Directory	Platform	Platform Prime
MDM/Device Management	✓	✓			✓	✓
System Insights™	✓	✓			✓	✓
Patch Management	✓	✓			✓	✓
Remote Access™	✓	✓			✓	✓
External Identity Federation	✓	✓			✓	✓
Identity Management for Devices		✓			✓	✓
Multi-Factor Authentication (MFA)		✓	✓	✓	✓	✓
Cloud Directory		✓	✓	✓	✓	✓
Single Sign-On (SSO)			✓	✓	✓	✓
User Lifecycle Management			✓	✓	✓	✓
Password Management			✓	✓	✓	✓
Directory Insights™			✓	✓	✓	✓
Cloud LDAP				✓	✓	✓
Cloud RADIUS				✓	✓	✓
Passwordless Authentication (JumpCloud Go™)					✓	✓
Conditional Access / Zero Trust						✓
Prime Pass						✓
JumpCloud Support	Standard	Standard	Standard	Standard	Standard	Premium
	Device Management $9	Device Identity $13 /user/mo	SSO $11 /user/mo	Core Directory $13 /user/mo	Platform $19 /user/mo	Platform Prime $24 /user/mo

Figure 1 JumpCloud licenses and prices as of May 2024

Unified Endpoint Management (UEM)

Today, there are tens of different device management tools in the market. Some companies sell their products as UEM (Unified Endpoint Management) solutions and not as MDM (Mobile Device Management) solutions anymore, which have been around for a long time. Generally speaking, UEM means that IT can use a single console to secure, manage, and deploy corporate applications and resources (Broadcom, n.d.). MDM solutions are nowadays considered device-centric tools, whereas UEM has a user-centric approach, as it also protects the user's identity and not just the device like an MDM (IBM, n.d.). An alternative definition for a UEM is Linux support. Most MDM tools do not support Linux, making it a non-unified solution, as the Linux devices need to be managed with another solution. All UEMs are MDMs, but not all MDMs are UEMs. I will refer to JumpCloud as a UEM in this thesis, even though the MDM acronym will be widely used to refer to device management capabilities. UEM and MDM products should not be mixed up with remote monitoring and management (RMM) tools, which might have network and server management and asset and inventory scanning features but lack some crucial device management capabilities, such as Apple's automated device enrollment feature. (Atera, 2024.)

3.1 Operating system support

3.1.1 Linux

Many MDMs support macOS, Windows, iOS, and Android operating systems but cannot support the most common Linux distributions, such as RHEL (Red Hat Enterprise Linux), Debian, Ubuntu, Linux Mint, and Fedora. Nowadays, lacking the capability to support Linux is a big issue if an SME (Small and Medium-sized Enterprises) would like to use only one tool to manage all operating systems used in the company. Linux market share passed 4% for the first time in February 2024 in global usage (Harding, 2024). In the Stack Overflow 2023 survey, Debian and Ubuntu combined were more popular operating systems than macOS in professional use: 34.78% vs. 33% (Stack Overflow, n.d.). The trend is clear: Linux is not going away and will become increasingly popular among developers. MDM companies with endpoint management solutions without Linux support, e.g., Hexnode, IBM MaaS360, and Miradore, should look into these numbers and start supporting Linux or risk losing customers.

JumpCloud supports a wide range of Linux operating systems. In addition to the previously mentioned usual distributions, JumpCloud supports Amazon Linux, CentOS, Pop!_OS, and Rocky Linux

(JumpCloud, n.d.-ac). Some of JumpCloud's features won't work in all distributions, such as Patch Management, which works only in Ubuntu. JumpCloud's policy management has 19 built-in policies but doesn't have a custom policy template like Windows and macOS policy management. If the policy list lacks a specific security control, it must be configured with a different mechanism, like executing a Bash script with the Commands feature.

Unlike other computer operating systems, JumpCloud doesn't have an agent the user would see in their operating system's menubar. Agentless solution means that if the user wants to change the password, they must log in to JumpCloud's user console and change it from there. The agent running in the background can be installed in several ways. One of the most used methods is to get the Install Command in JumpCloud admin console -> Devices -> Plus-icon -> Linux and email it to the user. The Install Command looks like this, and the connect key is unique for each JumpCloud customer:

> *curl --tlsv1.2 --silent --show-error --header 'x-connect-key: [connect key]' https://kickstart.jumpcloud.com/Kickstart | sudo bash*

Not all Linux operating systems have curl application preinstalled. If the Install Command returns an error mentioning that curl is missing, it can be installed with the following command:

> *sudo apt update && sudo apt install curl*

If the users have been enabled to install the agent by themselves, the agent can also be installed in the User portal -> Security -> JumpCloud Device Enrollment. Users must select the Generate Command, and enter the command into the terminal application. Unlike the admin console's install command, the user portal's install command must be used within one hour. After that, it will expire. The user portal's expiring install command is a great security feature. In the worst-case scenario, the non-expiring admin console's Install Command can leak, and an adversary can enroll their device and access company resources.

Additionally, the agent can be installed with Puppet, Chef, and Ansible. Instructions on how to use these can be found in JumpCloud's support documentation. After the agent has been successfully installed, the device must be bound to the correct user in the admin console. After that, the JumpCloud password will sync to the device, and all scoped policies and commands will be enforced and executed. (JumpCloud, n.d.-ag.)

3.1.2 Windows

Windows dominates the enterprise's operating system market share; thus, its extensive support is crucial in UEMs. All JumpCloud's features work with Windows, and 59 built-in policies can be deployed to the devices. Due to how Windows operating systems work with different manufacturers' devices, it lacks one crucial feature compared to macOS. Unlike macOS devices, Windows devices can't be remotely locked on the device level. Additionally, JumpCloud doesn't support IT administrators in enabling Windows Autopilot, which can be used in ZeroTouch deployment scenarios, similar to macOS, which uses Automated Device Enrollment. Windows Autopilot uses multiple technologies, requires expensive licenses, and needs in-depth knowledge about Microsoft products and services. Understandably, JumpCloud lacks Autopilot support, as it's used more in SMEs than in large enterprises. On the other hand, having Autopilot in a UEM is not unheard of, as VMware's Workspace ONE supports it.

JumpCloud supports Windows 10 (64 bit) and 11 desktop operating systems. For servers, 2012 R2, 2016 (64 bit), 2019 and 2022 are supported. JumpCloud requires Windows Professional or Enterprise licenses; otherwise, the conditional access, policies, security commands, and agent might not work. Microsoft Accounts are not supported, as only one online account can simultaneously be in the operating system. (JumpCloud, n.d.-ac.)

Windows devices can be enrolled in four different ways. The first method is selecting the MDM Enrollment in the user console if the feature has been enabled for users. The process is straightforward and the easiest method for users to use. The second method is to download the MSI installer and the Connect Key from the admin console and share them with the user. The third method is to share the Powershell script from the admin console with the user. The Connect Key is included in

the Powershell script, which creates a security risk if the key gets leaked. For security reasons, using the user portal to enroll Windows devices is best. (JumpCloud, n.d.-ah.)

The last enrollment method is the Windows Lite-Touch Deployment via Provision Package, which is as close to ZeroTouch and Windows Autopilot as possible with JumpCloud. The process starts with downloading a configuration file from the JumpCloud admin console -> Devices -> Plus-icon -> Windows -> Create Provisioning Package, as seen in Figure 2. This file must be opened with a Windows Configuration Designer application, which is only available for Windows operating systems. After the configuration file has been modified with company-specific information, such as the Wi-Fi password, it must be saved to a USB drive.

When the new device is ready to be enrolled, the USB drive needs to be connected to the device during the location selection screen. If the enrollment does not start automatically, the user must press the Windows key five times. After a few minutes, the user will see the Sign in with JumpCloud icon in the lower left corner. When the user signs in successfully for the first time, the user will be automatically bound to the device in the admin console, saving this step from the administrator if the laptop had been enrolled differently. The enrollment requires an active internet connection. Adding an Ethernet cable to the parcel is recommended if the laptop and USB drive are shipped to the user's home address. The user's home Wi-Fi password could be added to the configuration file, removing the need for the Ethernet cable. For security purposes, this is not recommended. (Deepak, 2024.)

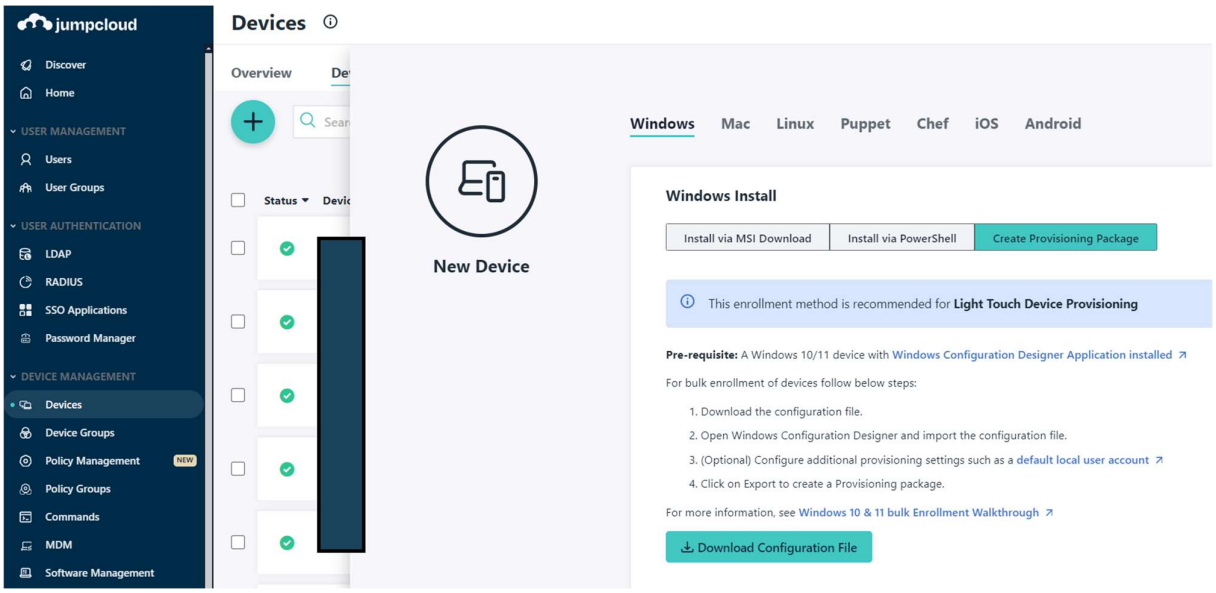

Figure 2 Windows Lite-Touch Deployment provision package download location

3.1.3 macOS

macOS is the most supported operating system in JumpCloud, at least when comparing the number of built-in policies to other operating systems. With 69 built-in policies for macOS, it's easy to customize the devices to comply with the company's security policies. The policies list includes configuration profiles for the most used EDR solutions, such as CrowdStrike Falcon, Malwarebytes, and SentinelOne. These pre-configured profiles help administrators with the initial EDR deployment. If the EDR vendor changes the configuration profile, JumpCloud is responsible for keeping it up to date, similar to the built-in commands.

macOS devices can be enrolled in JumpCloud in three different ways. Auto-enrollment is the first and most popular enrollment style, also known as Automated Device Enrollment (ADE). ADE requires the company to sign up to the Apple Business Manager. Verifying the company with Apple requires the company's Data Universal Numbering System (DUNS) number. Apple also needs the contact information of a person with the company's signature rights. This person is usually a CEO, CFO, or CTO. During the review process, Apple will make a verification call to this person (Apple, 2023). Vendors can start adding macOS devices to the ABM after the company has been verified.

To enable the ADE for old Macs, IT staff can add them to ABM with the Apple Configurator iOS application during the Setup Assistant (Apple, n.d.). All devices added to the ABM will show an enrollment screen during the Setup Assistant every time the laptop has been wiped. The enrollment screen can't be skipped, so if the device is stolen, it can't be used by an unauthorized person.

The auto-enrollment method is also known as Zero-Touch onboarding, as the device can be shipped directly to the employee's home address, and the IT doesn't need to touch the device physically. This enrollment style is the most secure and convenient way to manage macOS devices, as the policies and applications will get installed automatically during the first login. macOS devices must be restarted after the setup assistant has been completed so that JumpCloud's service account can be configured appropriately. The forced restart can be easily automated with the Baseline open-source project, which can also be used for installing applications and running scripts (GitHub, n.d-a). A common issue for many international organizations is that they have employees in countries where the authorized vendor can't ship the devices. For this reason, some of the macOS devices must be procured locally and enrolled using a different method.

The second enrollment mechanism is the MDM Enrollment Profile. As seen in Figure 3, the profile can be downloaded from the admin console, or the download link can be copied. Like the iOS device enrollment's QR code or URL, the enrollment link will expire after one hour. However, the downloaded profile won't expire. Hence, the file can be added to the company's internal documentation or shared with users via Email. The Mac will be enrolled into JumpCloud after installing the enrolment profile. Enrolling the macOS device manually with the enrollment profile will have the same outcome as auto-enrollment. However, it will be impossible to customize the Setup Assistant and disable some of its features. Suppose the Migration Assistant is not disabled, and the user transfers all files and settings from an old personal device to the new company-owned device before the JumpCloud enrolment. In that case, the user might violate the security policy with some files, and some applications might degrade the device's performance.

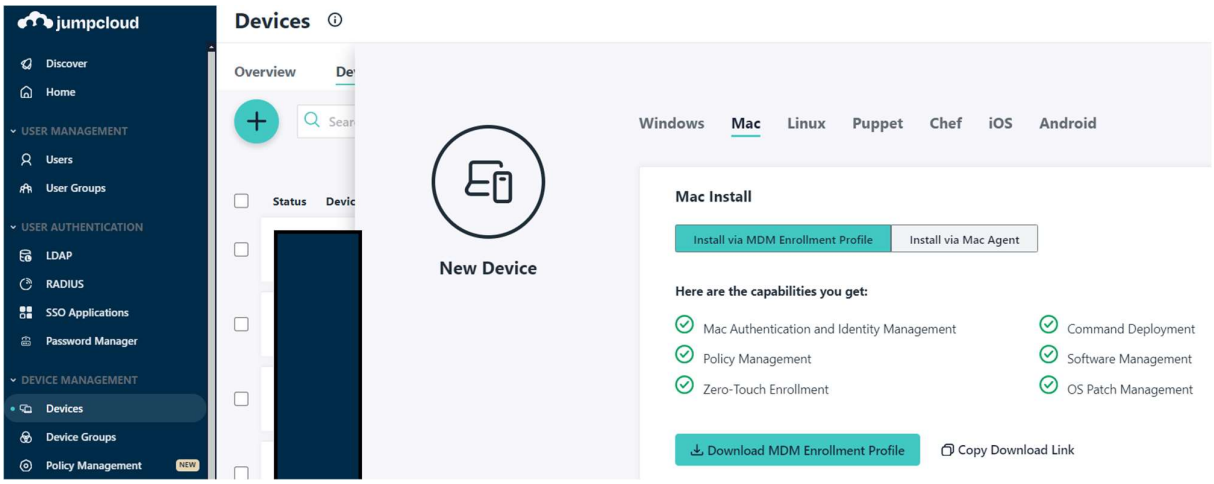

Figure 3 MDM Enrollment Profile download location

The third enrollment method is manually installing the JumpCloud Mac Agent and entering the Connect Key during installation. After the installation, the JumpCloud application will ask to complete the enrollment by installing the MDM profile if the enrollment policy is scoped accordingly in the Policy Management. This enrollment method is convenient for companies migrating from other UEM or MDM to JumpCloud. The agent supports commands, so once the JumpCloud agent has been remotely installed on all macOS devices with the current management solution, the commands can be used to delete files and applications and enroll the device into JumpCloud with a profile that can also be used to remove existing non-JumpCloud MDM enrollment profiles. (JumpCloud, n.d.-h.)

If a computer operating system is enrolled in JumpCloud manually, without auto-enrollment, there is one critical consideration to understand and remember for each new device. The local user account was created for the device before enrollment, so the account's name must be added to the admin console before enrollment. This way, JumpCloud knows which account will be managed so that the password can be changed or the account can be locked if necessary. If there is a mismatch between the local user accounts, some of JumpCloud's features won't work, and JumpCloud will create an additional user account for the device, confusing the user. (JumpCloud, n.d.-aa.)

JumpCloud supports Intel and Apple Silicon CPUs and the following macOS versions: Monterey 12, Ventura 13, and Sonoma 14. macOS Big Sur 11 support ended in December 2023, and Monterey's

support will end in December 2024. JumpCloud allows companies a few months to upgrade their oldest operating systems if they follow the N-2 policy, as Apple launches new macOS versions every fall. The N-2 policy means the IT department supports the three newest operating systems. The best practice is always to use the latest operating system, as Apple does not patch all vulnerabilities to older operating systems, e.g., CVE-2023-40424 (Fitzl, 2024). Upgrading macOS devices to the newest operating system is usually a big project in giant corporations, as they need to do lots of testing with the managed applications, profiles, commands, etc. (JumpCloud, n.d.-ac.)

3.1.4 Android

JumpCloud supports Android devices. Usually, in SMEs, these mobile phones run the latest or second-latest Android (13 or 14) operating system that is refreshed every 2-3 years and used for personal matters. Still, it's not unusual to have older Android tablets used at the office as a display next to a conference room or as a digital visitor book. JumpCloud uses Android Enterprise Mobility Management (EMM), which is not confused with MDM, the technology used with other operating systems. Once the company has registered the organization with the EMM, the devices can be enrolled in four methods. Registration with EMM is a straightforward process outside this thesis's scope. Full instructions on how to set Android management in JumpCloud can be found at this link: https://jumpcloud.com/support/set-up-android-emm

JumpCloud features 22 built-in policies for Android, and the first four can be seen in Figure 4. A Custom Payload is also present, so admins can configure and enforce missing policies using JSON format. When selecting the configure button of some of the built-in policies, the left pane shows which minimum Android operating system is supported. The pane also mentions the supported enrollment type. Most policies require a company-owned device, and only some are supported by a personal device. The enrolment types are categorized as the following:

Personal devices: Work profile and personal profile are separated. This enrolment type is also known as an employee-owned device. This enrolment type has been supported by Android 5.1 operating system version and later. Suppose this method has been enabled in the JumpCloud settings. In that case, users will enroll the device in the user portal using the Android Device Policy

application, which needs to be downloaded to the mobile phone before scanning the QR code. This enrollment method requires the least effort from administrators.

Company-owned devices: There are three different enrollment types, and they all have different use cases. Android 8.0 operating system is the minimum version for these enrollment types in JumpCloud, but it's best practice always to use the latest available version. The most significant difference with the enrollment is that the device needs to be new or erased to factory settings because the enrollment starts with tapping the screen six times after the device has been turned on. The first enrollment type is Work Profile (Company-owned device), which is a very similar setup to personal enrollment, as two different profiles work side by side. However, this enrollment method allows JumpCloud to enforce device-wide policies, such as blocking USB file transfers or configuring Wi-Fi settings).

The second Company-owned enrollment method is Fully Managed. This enrollment method is usually selected for phones used for work purposes only, as it lacks the support for a personal profile. The third enrollment method is called Dedicated, which is traditionally used for kiosk-type devices. This method enables the device to be locked down to a single application for a particular use case, such as managing inventory or printing tickets. Either of these methods does not support a work profile.

Zero-Touch Enrollment method also exists for Android, which is a very similar enrolment method to Automatic Device Enrollment for iOS & macOS and requires a vendor that supports it. Some security commands are available only for company-owned devices, such as Erase Device, which will erase all data from the device. Only work profiles can be removed from personal devices. If the device has a work profile, the Reset Passcode and Lock Device commands will only affect the work profile, not the personal one, meaning the work profile will be locked down, its passcode will be changed, and the personal profile will not be affected. (JumpCloud, n.d.-af.)

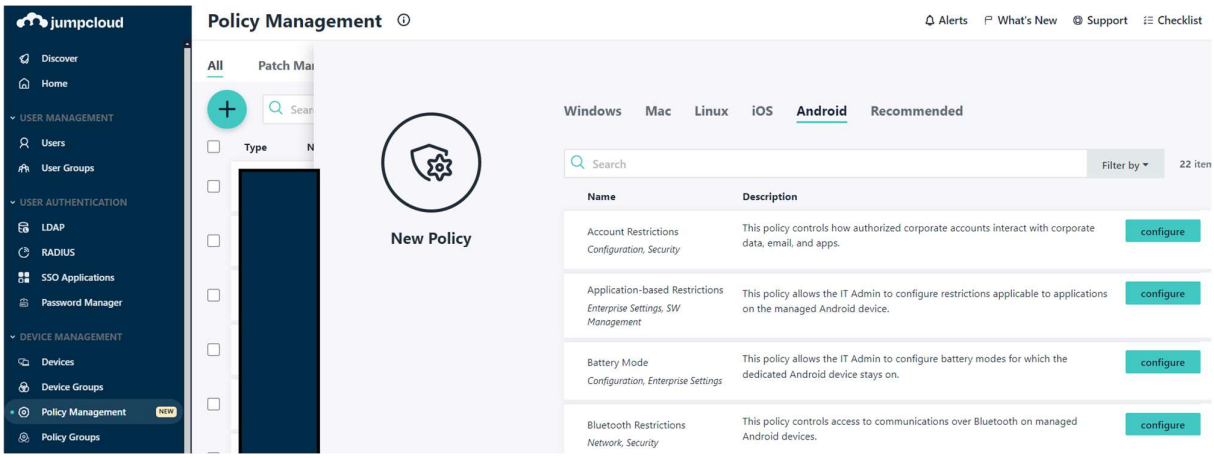

Figure 4 First four Android policies sorted by name

3.1.5 iOS & iPadOS

iOS and iPadOS (later iOS) operating systems can also be managed with JumpCloud. The company-owned iOS devices, usually iPhones, are typically enrolled with device-enrollment or auto-enrollment methods. The device enrollment link and QR code can be accessed via the admin console, so it's meant to be used by the IT department before giving the iOS device to the user. The auto-enrollment method is the most convenient way to enroll the devices, as the vendor adds the device to the ABM, and the iOS devices get enrolled to JumpCloud automatically during the initial setup, similar to macOS devices. According to my experience, auto-enrolment for macOS devices is more popular in enterprises than iOS devices, as the security requirements vary for different operating systems. iOS devices are secure and out-of-the-box if they are kept up to date. They are also heavily used for private matters outside working hours. Employees are usually against policies that disable some operating system features, like AirDrop, which worsens the user experience.

iOS devices can be locked, erased, or unenrolled with JumpCloud. The amount of collected information is significantly smaller compared to computer operating systems. The most important information about the devices is the operating system version, last contact, passcode status, storage usage and capacity, serial number, and International Mobile Equipment Identity (IMEI). iOS devices can be managed with different built-in policies, as seen on this web page: https://jumpcloud.com/support/configure-settings-for-ios-policies. Custom configuration profiles can be deployed to devices, just like with macOS. The Apple Business Manager's Volume Purchasing

Program can be used for application deployment. After the application has been purchased in the ABM, it can't be removed from the JumpCloud console.

Suppose the iOS devices have been bought from an unauthorized vendor that doesn't support the auto-enrolment. In that case, the devices can be added manually to ABM with the Apple Configurator macOS application. Having the iOS devices in the ABM and auto-enrolling them puts them in supervised mode. A supervised device gives the most control over the devices. The complete list of settings that require a supervised iOS device can be found on this website: https://developer.apple.com/documentation/devicemanagement/restrictions (Apple, 2023). If a user has an Apple Watch, some policies also affect that, as the iOS device controls the watch. A good example is the passcode policy, which must also be set to the watch.

User enrollment is an alternative and the newest method for enrolling iOS devices in JumpCloud. User enrolment is meant for personal devices, usually Bring Your Own Devices (BYOD). BYOD means the user owns the device, so user management is built around privacy and does not give the company access to all settings. The device needs to have at least iOS 13 or later installed. Compared to the device enrollment, many details, such as the device's serial number, carrier, or MAC address, are not visible in the admin console. In addition, many policies can't be deployed to user-enrolled devices. The supported enrollment type is shown in each JumpCloud policy. A few examples of non-supported policies are blocking applications, application notification settings, disabling FaceTime, and custom fonts. Additionally, the user-enrolled devices can't be wiped remotely, unlike those enrolled using a different method.

User enrollment can be allowed in JumpCloud's MDM settings. After enabling it, users can log in to the user portal and select "Enroll Your iOS Device" from the Security settings, as seen in Figure 5. After that, the user must scan the QR (Quick-Response) code with their iOS device and follow the instructions. Choosing this enrollment method over device enrollment is beneficial for the IT department, as the users can enroll themselves without contacting anyone or asking for help, and the device enrollment URL or QR code is only valid for one hour. (JumpCloud, n.d.-y.)

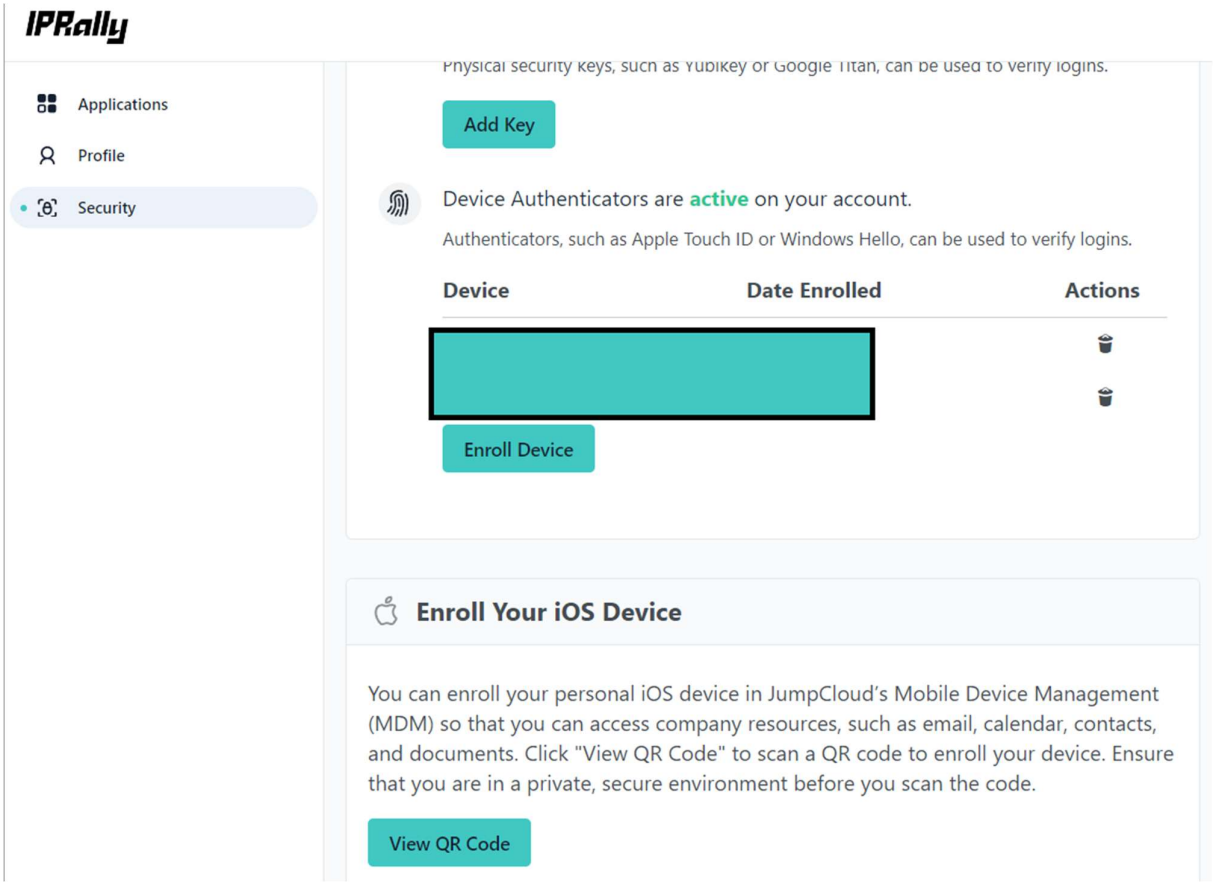

Figure 5 QR code for iOS user enrollment in the user portal

MAID (Managed Apple ID) is required for user enrollment. If the MAID is missing from the user's details, the user enrolment feature is missing from the user portal. MAID can be manually created in the Apple Business Manager or enabling the federation from the IdP, such as Google Workspace or Azure AD. If the federation has been enabled, the MAID will be the same as the user's primary email address. If someone had created a personal Apple ID to the company's email address, the federation would give the user 60 days to change the Apple ID's email address to something else. If the user does not change it, Apple will change it automatically to firstname.lastname-company.com@temporary.appleid.com. MAIDs can be easily added to the user's details with JumpCloud's MAID Import Script, as this information is not automatically imported from the IdP or the HRIS system. MAID must be manually filled out for all new joiners, or the Powershell script must be automated to run recurringly. (JumpCloud, n.d.-w.)

MAIDs can also be used with the iCloud services. However, Apple has restricted access to some iCloud services for privacy reasons. The blocked services include but are not limited to Find My, Health, Journal, iCloud Family Sharing, iCloud Mail, and iCloud+ services (Apple, 2024). The most significant limitation of using MAID with the iCloud services is not being able to purchase applications. For this reason, all work-related applications must be added to JumpCloud via Apple Business Manager and deployed to devices if employees refuse to install the applications with their personal Apple IDs. Otherwise, users need to use applications, such as Slack or Gmail, with the browser, which has a worse user experience than native applications. (JumpCloud, n.d.-x.)

3.2 Technical Features

3.2.1 Password Manager

Even though Single Sign-on is becoming increasingly popular, there is still room for a password manager in the corporate world, especially for SMEs that can't afford SSO licenses for all applications. Companies should offer a password manager license to anyone who requests it so that employees wouldn't store passwords in unsafe locations or applications. The best scenario is that employees can do all their work tasks with tools that use SSO as the login method. Unfortunately, this is not always the case, and people need to log in with their email addresses and passwords to some services that lack the SSO. There are usually two different reasons why SSO can't be used. Sometimes, the IT department needs to login to routers, firewalls, and other networking equipment. Usually, these are used with local accounts configured directly to the device. The other reason is the cost of licenses. Typically, the vendor has a few different license models for their application, and the cheapest might lack the SSO functionality entirely. Upgrading the licenses will often enable the SSO and other valuable features, such as SCIM and session timeouts.

Password manager, similarly to Remote Access, is one of the features in JumpCloud that are not needed for the core functions. Many companies choose to use a different tool for storing passwords. One of the reasons could be that the 3rd party password manager was being used already before the company started using JumpCloud. The password manager is included in all JumpCloud's packages except the cheapest Device Management package. If a company is a JumpCloud customer, using the password manager can generate significant cost savings. If a 50-employee

company would use 1Password or Dashlane as their password manager solution, it would cost 4800e annually.

JumpCloud password manager is working similarly to other password managers. It can store passwords, credit card information, secure notes, 2FA tokens, etc. The password generator can create strong passwords, and all saved items can be shared with other users. Browser extensions can be installed for the most used browsers, such as Chrome, Firefox, Safari, and Edge. Users tend to use the password manager more as a browser extension, as the passwords are very convenient to fill automatically into the password fields in the browser. If someone wants to use the password manager outside the browser, a native application can be installed on macOS, Linux, and Windows, as shown in Figure 6. Mobile phone users are not forgotten; the application can be downloaded to iOS and Android.

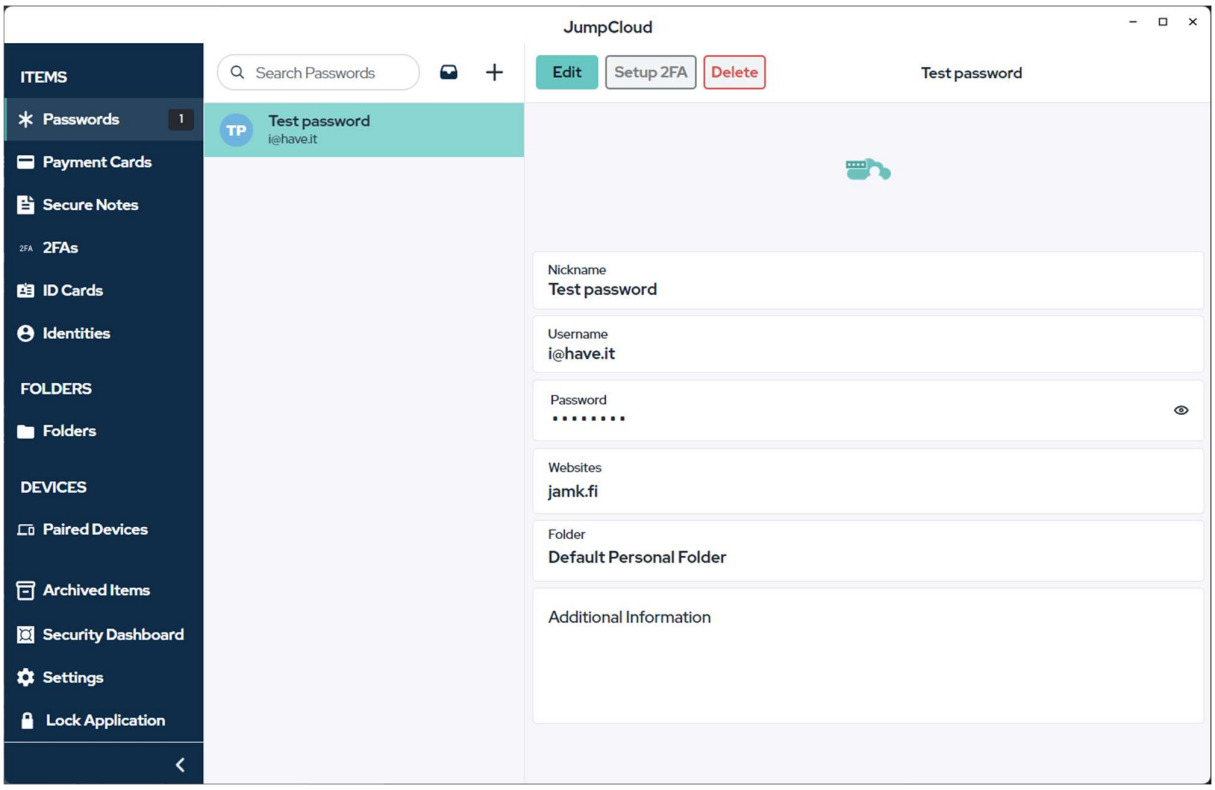

Figure 6 Password Manager for Windows

The most significant difference between the JumpCloud password manager and other solutions is that the passwords are saved locally to the device by default. If a user uses the password manager only with one device, which gets stolen or breaks down, the passwords are gone. To tackle the issue, using at least two different devices is recommended so the passwords are syncing between them. It's also possible to turn on the backups for the passwords, but storing the passwords in JumpCloud's servers creates an additional attack vector for adversaries. (Lake & Worthington, 2023.)

3.2.2 Policy & Patch Management

When it comes to endpoint security, there are usually two different reasons why UEMs are used in the enterprise and have all endpoints enrolled in it. The first reason is to have the ability to see the endpoint's current settings, details, operating system, and application versions. Usually, most of the operating system's default security settings are set correctly, such as the automatic updates. Still, companies want to be able to verify that the settings are not tampered with. This periodically occurring review is called an audit. The second reason is having the ability to enforce security settings, operating system updates, application updates, disable unsafe features, and block connected devices, such as external USB mass storage devices.

JumpCloud's policy management is rich with features and supports all computer and mobile operating systems. Almost two hundred pre-built policies combined for all operating systems can be easily selected and scoped to individual devices or device groups (JumpCloud, n.d.-a). If other teams require different policies, policy groups can be created to bundle policies together and scope them accordingly. When a pre-built policy is selected, some policies can be customized in the Details tab, e.g., text can be added to the Login Window Text policy, or the number of seconds can be added to the Lock Screen policy. After the policy is customized, scoped to the correct devices, and saved, the Status tab will show the policy's status. The policy has been successfully applied to the endpoint if the status symbol is green. Deploying a new policy might take a few minutes, or if multiple policies are published simultaneously, it might take a few hours. If the policy is not applied and the endpoint is active, rebooting the device might fix the issue. Windows policies are based on group policies, and the policy deployment can be fastened with a "gpupdate /force" command, similar to the devices connected to an Active Directory. (JumpCloud, n.d.-c.)

Some policies have a Minimum Supported Version in the left pane. The policy won't work if the device's operating system is older than the one mentioned in the policy. Some policies also mention the Supported Enrollment Type, which means the policy doesn't get applied to the device if it's enrolled in a way unsupported by the policy. All other operating systems than Linux support custom settings. For Windows, Custom Registry Keys can be configured. macOS and iOS can be configured with an MDM Custom Configuration Profile. The iMazing Profile Editor application or Jamf Compliance Editor can be utilized for profile creation, which can then be uploaded to custom profiles, for establishing compliance baselines, such as CIS Level 1 (Klaassen 2024). For Android, a Custom Payload can be configured in JSON format.

JumpCloud has created Policy Group Templates that can be very helpful, especially for junior IT administrators. The templates are a combination of different policies, and they are named Light, Standard, and Enhanced Security. Some of these templates can be seen in Figure 7. These three Policy Groups are available for all computer operating systems, and evaluating and applying even some of the Light Security bundle's profiles to devices is highly recommended. Depending on the operating system, this will enable the disk encryption, firewall, screen lock, and disable the guest account, among other settings. Only one template should be used for each operating system so there wouldn't be any duplicate policies, as the Standard Security group includes the Light Security group policies, and the Enhanced Security group includes Light and Standard Security group policies. (JumpCloud, n.d.-b.)

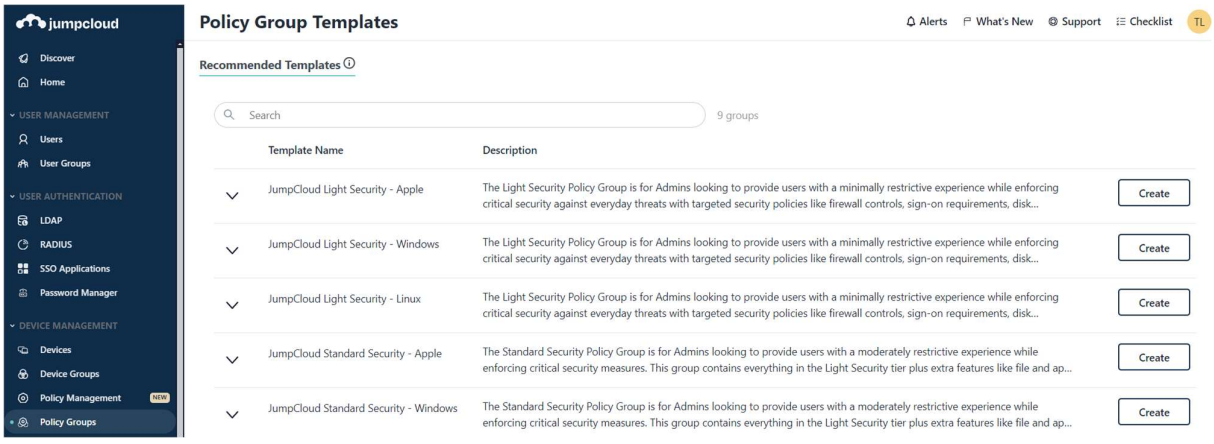

Figure 7 Policy group templates

Patch Management

JumpCloud's Patch Management consists of two different elements: OS and Browser. OS is an acronym for operating system, and it can be used to keep Windows, macOS, and Linux operating systems up to date. For Linux operating systems, Ubuntu is the only supported distribution. In the Patch Management's OS tab, the Update History and Release Trains are shown, as seen in Figure 8. It's essential to visit this tab often to see when the latest updates have been released so these two panes can be cross-referenced. Something might be wrong if a new patch was released a while ago and the devices are not automatically updated.

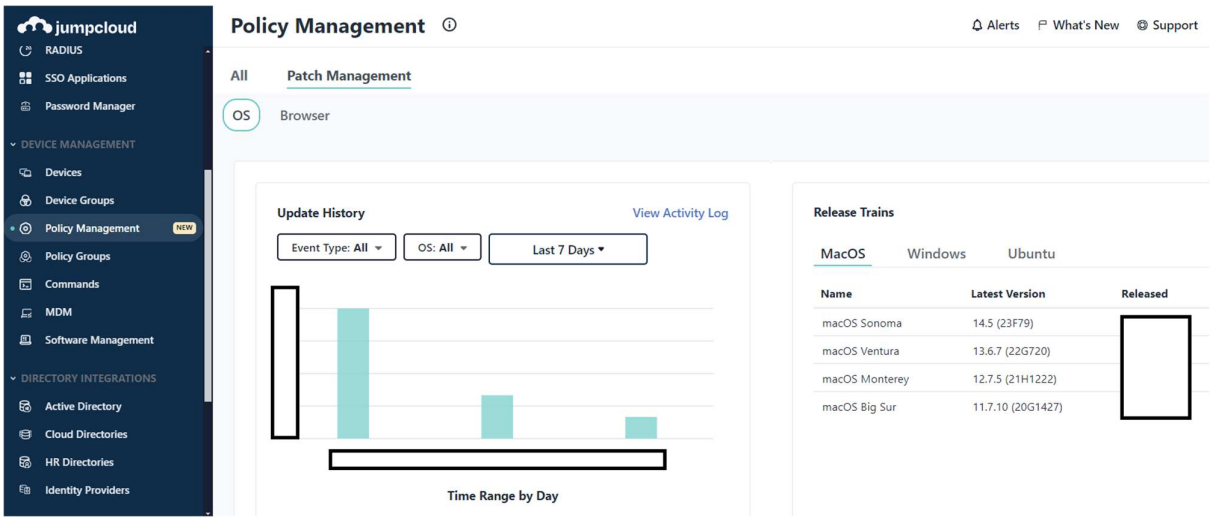

Figure 8 Update History and Release trains

Different policies for supported operating systems can be found at the bottom of the page. Policies consist of four deployment rings: Vanguard, Early Adoption, General Adoption, and Late Adoption. These 12 pre-built policies have unique settings and can be scoped to different device groups. Vanguard is the strictest ring; it doesn't have update deferrals for any operating system, and they must be installed within a few days. Vanguard is the best ring for the IT department's devices to test the updates before they become available in other endpoints. It's highly recommended that other policies be scoped for the rest of the devices. New policies can also be created from scratch, which will help companies if the pre-built settings do not match their security requirements.

JumpCloud utilizes Windows' built-in updating and notification system, and macOS uses the Nudge open-source project to nudge users to update their operating system. However, Ubuntu lacks the installation deadline or restart grace period feature, which means the updates are installed automatically every week. Still, no forced reboot will ever occur, leaving some updates pending. Not rebooting the device might negatively affect the performance and user experience, eventually making the endpoint vulnerable. The option to gracefully restart the laptop periodically is one of the most significant security-related drawbacks of JumpCloud for companies with many Ubuntu devices. (JumpCloud, (n.d.-d.)

The second tab of Patch Management is the Browser tab. This feature will update the Chrome browsers for Windows, macOS, and Ubuntu, while the operating system patching updates Safari and Edge for Windows. The tab contains four policies that can be seen in Figure 9: Chrome Day Zero, Chrome Early Adoption Ring, Chrome General Adoption Ring, and Chrome Late Adoption Ring. Like OS policies, they all have different settings: automatic updates and component updates are enabled, and the relaunch grace period varies from 1 day to 14 days. The policies also have a setting for the Browser Sign-in Settings, which can be set as Enable, Disable, or Force. Enable is the default setting, and users can sign into their Chrome to use features such as Google Chrome Sync. Disable prevents the browser sign-in, and many of the browser's features will be unavailable. The force option will require users to sign in to Chrome. For all these features to work, the Chrome Browser Cloud Management must be enabled in the Google Workspace, and the Enrollment token must be added to each policy. Browser patch management is also supported for Debian, Fedora, and Rocky Linux distributions. (JumpCloud, n.d.-f.)

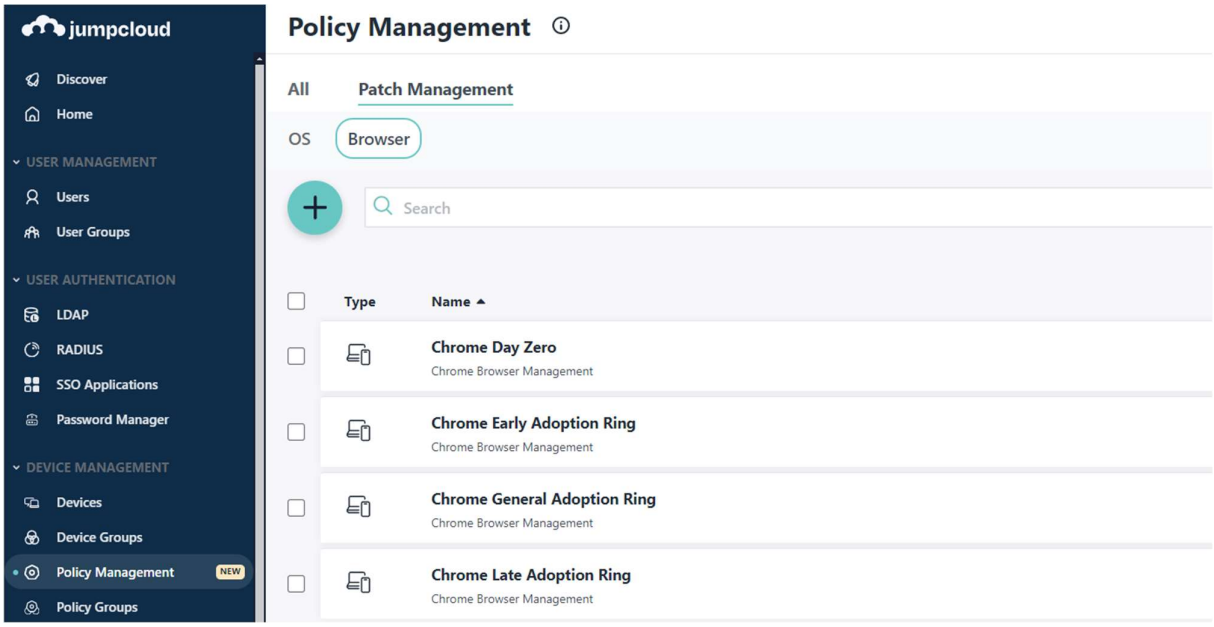

Figure 9 Preconfigured Google Chrome update policies

3.2.3 Security & MDM commands

IT administrators must be able to send security commands to the endpoints if something is wrong with the device. These commands are known as MDM (Mobile Device Management) commands for Apple devices. The reason for sending security commands to the endpoint varies. The device might be compromised, which means stolen, hacked, or used by someone else. It's best practice to deploy a modern EDR (Endpoint Detection and Response) tool to the endpoints, keep them up to date, and apply essential security controls to the device, such as screen lock, firewall, and disk encryption, so that the endpoint wouldn't get compromised. Security commands can also be leveraged to help users with slow or stuck endpoints.

Security commands consist of four different commands: Lock device, Restart device, Shut Down Device, and Erase Device. The first three commands can be issued in the device list view to minimize the accidental erasure of the device. As seen in Figure 10, the rest of the commands, such as the Erase Device, can be found under the Actions button in the device details view.

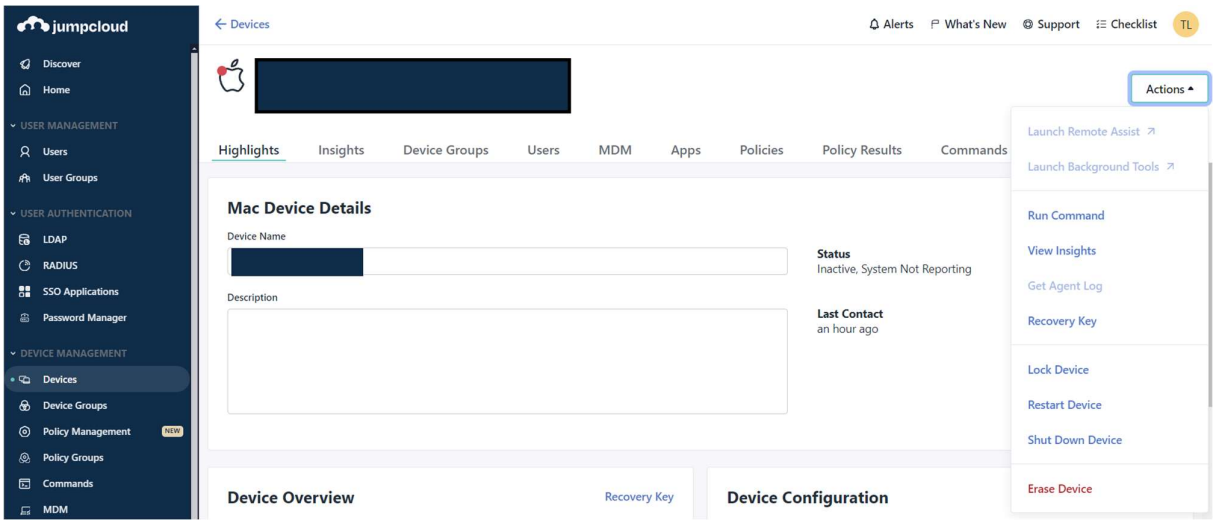

Figure 10 Security commands for a macOS device

The lock command for macOS is meant to lock a device remotely and can be used in many scenarios. The device might be lost, or an employee won't return the endpoint to the company on their last day. The console will ask for an unlock PIN when the lock command is issued. When the PIN is entered, the endpoint restarts and asks for the unlock PIN. Unlock PIN is also known as firmware PIN, which means it can't be bypassed, and the endpoint can't even be erased. The only way to unlock the device is to enter a correct PIN or contact Apple with proof of purchase. The unlock PIN should be stored securely, as JumpCloud doesn't save the information anywhere. Windows and Linux devices do not have such a robust locking mechanism. When the command is sent, it just locks the screen. If the user account is still active, the user can unlock the screen with biometrics or a password.

The Restart command works similarly on Linux and macOS devices. When the command is issued, the endpoint will restart immediately without any warnings. A sudden reboot creates a high risk of users losing data as they don't have a chance to save the documents they are working on. Windows devices will show a few popups warning users about the upcoming reboot.

Shut down command works the same way in all computer operating systems. After issuing the command, the endpoint will shut down immediately. All unsaved files are lost if the application

doesn’t have auto-save or recover features. The restart or shutdown commands can be used if the endpoint is slow, stuck, or can’t be locally accessed.

The erase device command works similarly in all macOS Big Sur (version 11) and Linux devices. Once the command has been issued, the endpoint will be entirely erased. The operating system will also be removed and must be manually re-installed after the erasure. Newer macOS systems support Erase All Content and Settings (EACS) on devices with the T2 Security Chip or Apple Silicon CPU. The EACS will delete all user data but keep the operating system that is currently installed. Windows devices have a similar feature called RemoteWipe CSP, but it requires the Windows Recovery Environment (Windows RE). The erase command is very convenient if the endpoint is stolen or if a remote employee has a new laptop and wants to procure the old one from the company. (JumpCloud, n.d.-s.)

3.2.4 API Services

All modern UEMs can be accessed via the Application Programming Interface (API), and JumpCloud is no exception. APIs often require advanced knowledge about the UEM and hands-on skills of the command prompt, such as Terminal application, that can be used with all computer operating systems. API is a powerful tool, and it can be utilized with many tasks that are impossible to accomplish with the admin console, e.g., collecting application versions from all endpoints or adding information to all users using only one command via the PowerShell module. It can also be used with the Human Resource Information System (HRIS) to automate user creation or account suspension. The API key can be generated in the account icon -> My API Key in the admin portal, and it’s only viewable during the creation. For this reason, it should be stored in a secure location, such as a password manager. If a new API key is generated, the old one will be revoked, and the new API key must be updated for all services that are using the key. (JumpCloud, n.d.-g.)

Like all API keys, it’s encouraged to regenerate the keys annually if the key is used with many services. Renewing the key will mitigate the risk if the key has been compromised after a breach or if a stolen endpoint has access to the API key. JumpCloud had a security incident in the summer of 2023 when a North Korean adversary could access JumpCloud systems with developer privileges

by convincing a JumpCloud employee to download malicious software to their laptop. The incident resulted in the force rotation of all JumpCloud's customers' API keys. (Phan, 2023.)

JumpCloud PowerShell Module

PowerShell is installed in Windows by default. For macOS and Linux, it can be downloaded at https://github.com/PowerShell/PowerShell#get-powershell. PowerShell can be launched in macOS or Linux by typing "pwsh" in the Terminal application or by selecting the application from the Start menu in Windows. When the PowerShell is running, JumpCloud's PowerShell module can be installed by typing the following command:

Install-Module JumpCloud -Scope CurrentUser

After installing the module, JumpCloud can be accessed by typing Connect-JCOnline and entering the API key. After the successful login, all commands that can be found from the following link can be used: https://github.com/TheJumpCloud/support/tree/master/PowerShell/JumpCloud%20Module/Docs. One popular reason to use the module is to get the version numbers of installed applications, as this reporting feature is missing in the admin console. Here is an example of a command that finds out the Slack application versions in all enrolled macOS devices, and the second command saves the result to a text file:

$apps = Get-JCSystemApp -name "Slack" -SystemOS "macOS"

$apps | Select -Property Name, SystemID, version, bundleShortVersion | ConvertTo-CSV | Out-File ~/SlackMac.CSV

It's important to understand that the PowerShell module is a powerful tool. If the commands are not carefully reviewed and tested, there can be catastrophic consequences, such as erasing all enrolled endpoints. (JumpCloud, n.d.-i.)

3.2.5 Remote Access

Competition is tough in the mobile device management market, and products are filled with features that are not necessarily required but very welcomed. Remote Access feature is one of them. It's beneficial for IT teams to use only one tool for many tasks. Having a remote access tool integrated into the UEM is cheaper, more accessible, safer, and uses fewer IT team resources compared to having a separate remote access application, such as TeamViewer. Having another application for remote access widens the endpoints' attack surface, and it requires the IT team to ensure that the application stays up-to-date and is appropriately configured to be safe to use. More managed applications also mean more documentation and training.

Remote Access can be turned on from the settings, and it has three different features and use cases. The first is the Remote Assist Service, which lets administrators help users by selecting the "launch remote assist" button from the device's details. After the selection, the administrator must choose if the Remote Assist application is automatically launched or if the user should manually start it. If the application starts automatically, it will ask permission from the user. If the user starts the application, they must type an access code to start the session. Remote Assist has many valuable options and features, as seen in Figure 11, such as:

- Request Control: The administrator can request the endpoint's mouse and keyboard control.
- File Manager: Grants access to the endpoint's file system. Files and folders can be removed, downloaded, uploaded, and renamed.
- Select Display: If the user has multiple displays, this option will help to find the correct one.
- Enable Clipboard Sync: Enables copy-pasting for a maximum of 8MB of image or text data. The sync works two ways: from the administrator's endpoint to the user's endpoint and vice versa.

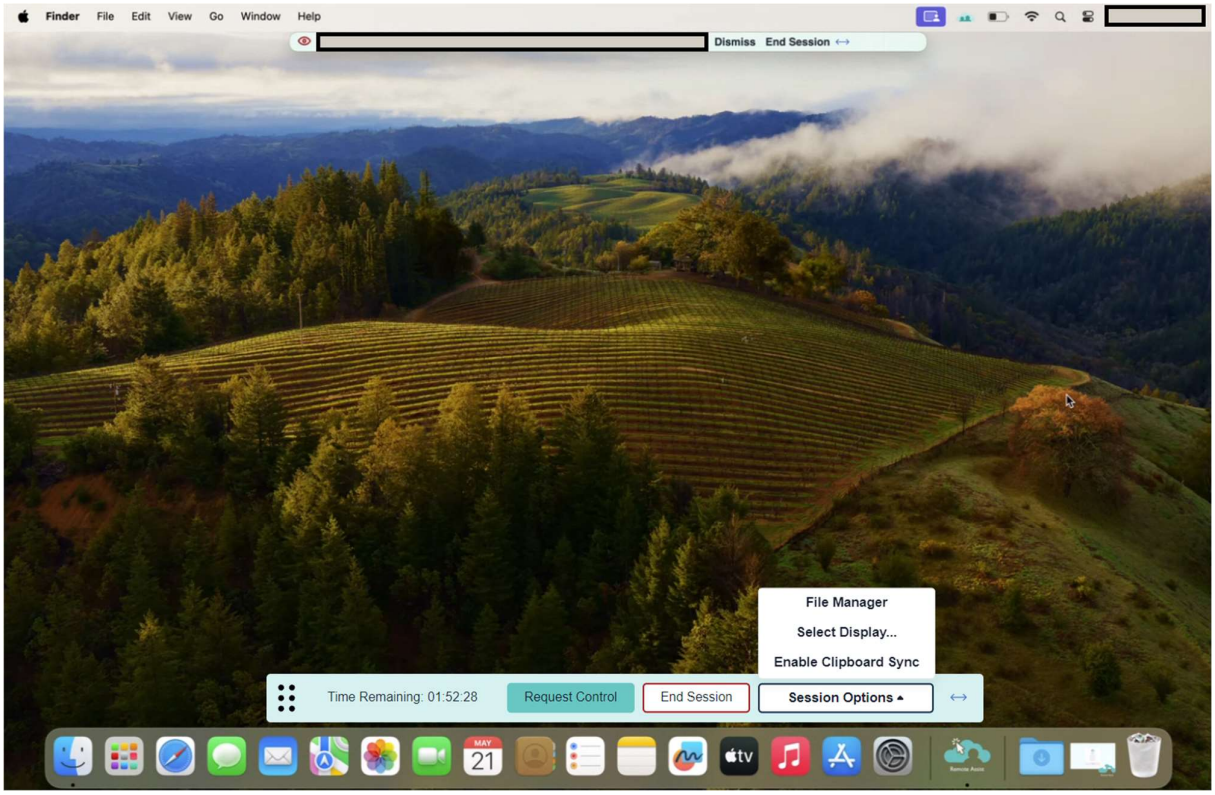

Figure 11 Remote Assist and its options on a macOS device

The Second Remote Access feature is the Silent Assist, which allows administrators to control the endpoint remotely without the user's consent. If this feature is enabled and used, it should be documented and communicated thoroughly to employees. Employees do not like to be spied upon, and nothing will destroy the respect towards IT more than if the cursor starts moving by it-self without any prior communication. However, this can't be used as a perfect spying solution. After the silent assist session has been closed, a permanent window with information about the session will be on top, showing who initiated the session and how long it lasted.

The last Remote Access feature is the Background Tools Service, which allows administrators to establish a terminal connection to the endpoint without the user's consent. If the endpoint's operating system is macOS, the terminal connection uses Bash. PowerShell will be used as a terminal connection if the endpoint is a Windows PC. This feature is a powerful tool for fixing various issues in the endpoints. Background Tools Service also provides a File Manager feature similar to Remote Access's. It's essential to remember that great responsibility comes with great power. There are catastrophic consequences if an adversary can take a silent terminal connection to the endpoint

and infect it with malware. Hence, using strong passwords and MFA in JumpCloud's administrator console is crucial. Also, it is not recommended to enable this feature if it is not used, which is also a good rule of thumb for other features. (JumpCloud, n.d.-j.)

3.2.6 Multi-Factor Authentication

In JumpCloud, Multi-Factor Authentication (MFA) can be used in several ways. The most common purpose for utilizing MFA is to enable it for the user portal and admin console. Currently, the admin console allows only Time-based one-time passwords (TOTP) as an MFA method, which means admins must use a TOTP application on their mobile phones, such as Google Authenticator or Microsoft Authenticator. JumpCloud Go is not supported in the admin console. Admins can enable the identity provider (IdP) log in as an alternative login option. Using the IdP option makes the login process more convenient and faster if the IdP is configured to use passkeys, which means that a fingerprint or facial recognition can be used as an MFA method.

The user portal has more MFA methods than the admin console. Suppose JumpCloud's Global Policy Settings are configured to require MFA in the user portal, and all MFA methods are enabled in the admin console. In that case, the user needs to add at least one of the following MFA methods when they login to the user portal for the first time:

- JumpCloud Protect: A mobile phone TOTP application that supports push notifications and biometrics
- Authenticator App: The user can use any TOTP application that is available in the Google Play Store or App Store
- Security Keys: The physical key is one of the most secure MFA methods, as the user needs to possess the key after typing the Email and password
- Device Authenticators: Mac's Touch ID or Windows' facial recognition or fingerprint are supported

If the company doesn't use security keys, JumpCloud Protect, as seen in Figure 12, is highly recommended for Linux users for convenience, as biometrics are not supported in the operating system. Users can enable multiple MFA methods and select the preferred option during each login. (JumpCloud, n.d.-k.)

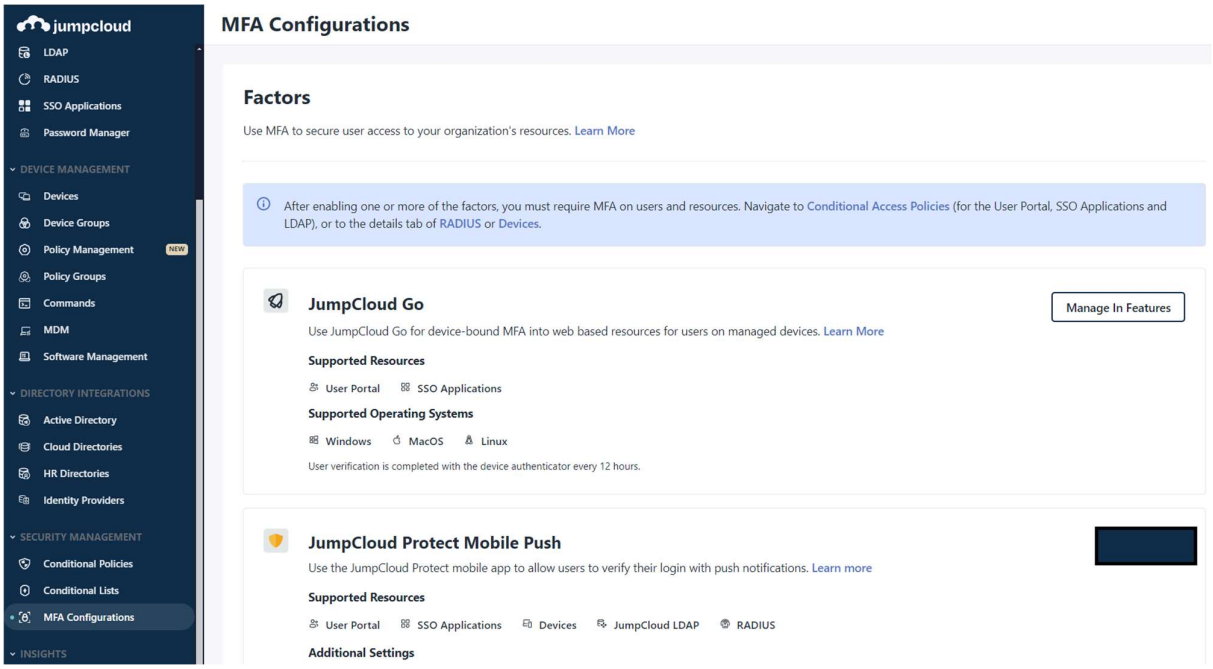

Figure 12 Multi-Factor Authentication Settings

One of the features that separates JumpCloud from competitors is the Device MFA. The Device MFA requires the user to verify the authentication with MFA during each login to the operating system. Device MFA won't affect the screen savers, FileVault login screen, and lock screen, so users need to use the TOTP token only when they have rebooted the endpoint or logged out from the operating system. Device MFA is supported in all computer operating systems: Linux, macOS, and Windows. In the admin console, MFA can be enabled for multiple devices simultaneously from the device list view or one by one from the device's details. Only the TOTP method is supported, so enabling the Device MFA makes the login experience less convenient for users, as the biometrics, security keys, or JumpCloud Protect push notifications can't be utilized. (JumpCloud, n.d.-l.)

3.2.7 Cloud & HR Directories

JumpCloud can be integrated with the most popular cloud directories, Google Workspace, Microsoft 365, and Active Directory. In addition, JumpCloud can be integrated with a Cloud-based LDAP. Using cloud directories allows user accounts to be imported and exported, and passwords

can be synchronized, reducing manual tasks and improving user experience. If the passwords are synced, JumpCloud becomes the password authority. If the user changes the password on their enrolled computer, it will also be changed in the cloud directory. If companies use Active Directory or Microsoft 365 as a cloud directory, they are likely using JumpCloud's biggest competitor, Microsoft Intune, as their mobile device management solution. For this reason, Google Workspace was selected as an example of the integration.

The integration for Google Workspace can be enabled from JumpCloud's administrator console's left pane by selecting Cloud Directory -> plus icon -> Google Workspace. When prompted, a unique name must be entered for the integration that cannot contain invalid characters if it is longer than 255 characters or contains only white spaces. After the name has been entered, select the authorize sync button. Next, Google Workspace Super Admin credentials must be entered into the Sign-in with Google window, allowing the users' provisioning. Once the synchronization has been completed, the users can be imported to JumpCloud all at once or individually. Optionally, group management can be enabled from the integration's Details tab, which allows administrators to manage Google's distribution groups from JumpCloud. It's worth noting that the group management works only one way (JumpCloud -> Google), and changes made in Google are not visible in JumpCloud. Each group's email attribute must be added if group management is enabled. Failing to do so might suspend all users assigned to the groups. Users will be added to the groups automatically in the Google Workspace. (JumpCloud, n.d.-ao.)

HR Directories

Two significant challenges in the corporate world are the lack of internal communication and manual processes. Forgetting to tell critical stakeholders about fired employees and leaving their accounts active can have catastrophic consequences. Even if HR and IT departments work together well, humans can make mistakes, which might tense up the office atmosphere or cause a bad user experience for the person leaving the company. JumpCloud has recognized these problems and has created pre-build Human Resources Information System (HRIS) connectors for the most common HR applications, such as BambooHR, Personio, Namely, Bob, and Workday. Without integrating a mobile device management tool and HR system, HR must keep the IT department in the loop when suspending the laptop, IdP, and SaaS applications accounts.

The pre-built HRIS connectors, as seen in Figure 13, are very easy to enable in a few steps. Firstly, the API key needs to be created in the upper right corner of the JumpCloud's console. Next, the JumpCloud application needs to be installed in the HR application. Lastly, the API key must be added to the HR application after selecting what kind of data will be sent to JumpCloud. It's essential for all relevant parties involved in the onboarding and offboarding processes that all necessary personal information for daily tasks can be completed efficiently, such as shipping a new laptop to an employee's home address. The address fields can be synchronized from the HR system to JumpCloud, so IT knows where to order the computer, removing a need to ask for the address every time from HR or the employee. At the same time, too much visibility can cause confidentiality issues, such as accidentally syncing salary information to JumpCloud, so great caution must be taken when configuring the tools.

After everything has been configured correctly and the user account gets deactivated in the HR system, the following critical offboarding tasks will occur: First, the computer's user account will automatically get disabled. Secondly, if JumpCloud has been integrated with an identity provider like Google Workspace, that account will also be suspended. Lastly, the user will lose access to all their SSO applications in JumpCloud. The HR department can do all of these by themselves without asking for help from IT (Lee, 2022). Automated offboarding processes and tools are a fantastic data loss protection mechanism, as almost 90% of employees can access sensitive company material after their last work day. The studies also show that an automated onboarding process increases the new employee retention rate and initial employee efficiency by more than 15%. (JumpCloud, n.d.-ap.)

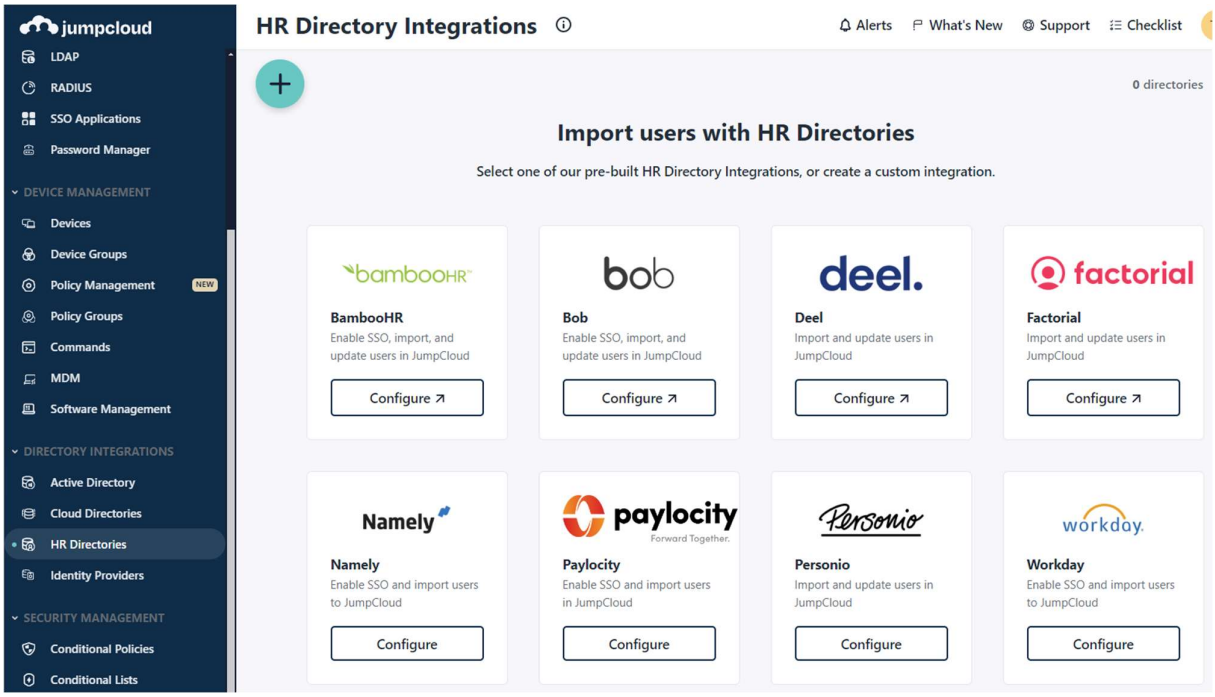

Figure 13 Pre-built HRIS integrations

3.2.8 Commands

JumpCloud supports sending commands to devices, excluding mobile phones (iOS & Android). Commands can be created from scratch or using command templates, as seen in Figure 14. Templates include useful scripts for gathering information from the devices, such as listing all available macOS updates or all Linux users. Additionally, command templates include installation scripts for usual security applications, such as CrowdStrike Falcon and Sentinel One. It is also possible to deploy Slack and Microsoft VS Code to Linux devices using command templates, as JumpCloud currently lacks other mechanisms to install applications remotely to Linux devices.

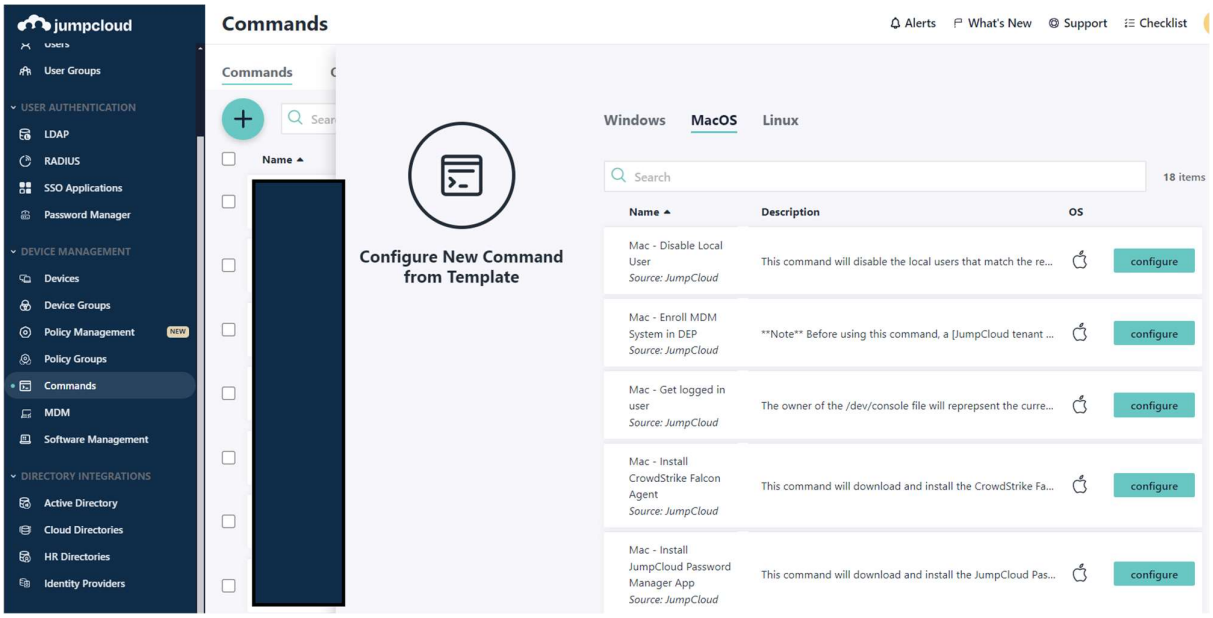

Figure 14 Command templates for macOS, sorted by name

When creating a command, the following information is needed before assigning the script for device groups or individual devices:

- Name: It's preferred to use a descriptive name, which should at least include the operating system and what is the script's purpose
- Run As: Selecting a user for running the script in Linux and Mac devices is required. Usually, the root user is selected, as it has the most permissions.
- Type: Linux, Windows, or Mac needs to be selected. Only one can be chosen for each command.
- Command: The actual command or a script. You can use a Command-line shell or a PowerShell for Windows.
- Launch Event: The script can be run manually, as scheduled, as repeating, on the trigger (webhook), every JumpCloud login, and the next JumpCloud login.
- Timeout After: The default value is 120 seconds, which can be changed in this field. The timeout limits the command's execution before the agent automatically stops it.

- Time to Live (TTL) Settings: If the default value (3 Days) is chosen, JumpCloud tries to run the command for three days before exiting the queue. Setting the setting to 10 days is preferred, as users might have a one-week holiday, and the endpoints will be offline for an extended period.
- Files: This is the only optional information for commands. A maximum of 1MB of files can be uploaded to devices to run the command successfully. The default file destination for Mac and Linux commands is /tmp/, and for Windows, C:\Windows\Temp. The endpoint will download the file before the command is executed.

After creating the command, it can be launched manually in the Commands tab. If the endpoint is offline, the command will remain in the Queued tab for the specified Time to Live duration. The results tab will show all ran commands and their Exit Code. The command log, start time, and completion time are accessible from the view button (JumpCloud, n.d.-m). The command result codes for Linux and Mac are shown in Figure 15, and Windows in Figure 16.

Linux/Mac Result Codes

Result Code	Description
0	The operation completed successfully
1	Catch-all for general errors
2	Misuse of shell built-ins (according to Bash documentation)
124	Function timeout
126	Command invoked cannot execute
127	Command not found
128	Invalid argument to exit
128+n	Fatal error signal "n"
255*	Exit status out of range

Figure 15 Command result codes for Linux and Mac devices

Windows Result Codes

Result Code	Description
0	The operation completed successfully
1	Incorrect function
2	The system cannot find the file specified
124	Function timeout
126	The specified module could not be found
127	The specified procedure could not be found
128	There are no child processes to wait for

Figure 16 Command result codes for Windows devices

3.2.9 JumpCloud Go

The world is slowly going passwordless. People nowadays log in to their laptops with their fingerprints and to their phones with facial recognition. These authentication methods are called biometrics. Some vendors consider them more secure than regular passwords and use biometrics as a multi-factor authentication method. Typically, the user must enter an email address and a password to the user portal and verify the authentication with a multi-factor authentication method. JumpCloud Go replaces the password with the biometrics. JumpCloud Go works similarly to other passwordless solutions, such as Google Workspace's passkeys.

Passwordless solutions have multiple benefits. They are safer and faster to use, so users will have less downtime when they don't need to remember and type their passwords. It also saves the administrator's time when there are fewer password-related support tickets. JumpCloud Go needs an enrolled device, so the authentication is protected by the hardware and JumpCloud login service, which mitigates the adversaries' point of entry.

JumpCloud Go is supported on all computer operating systems and can be enabled in the admin console's Settings -> Features. It works with Google Chrome and Chromium-based browsers. Firefox is also supported, but only on macOS & Windows. JumpCloud Go browser extension is required for all operating systems and browsers. Users can install the extension themselves, or the

JumpCloud administrator can deploy it automatically to all endpoints. The most usual way to deploy the browser extension is using Google's Chrome Browser Cloud Management (CBCM). If the company is not using Google Workspace and the Chrome browsers are not managed, the "Chrome Browser Force-Installed Extension Policy" policy can be used in JumpCloud.

There are a couple of hardware requirements for using JumpCloud Go. Windows devices require a Trusted Platform Module (TPM) 2.0 and an infrared camera or a fingerprint sensor. A Touch ID sensor and a Secure Enclave are needed for Mac devices. Linux devices require a GNOME-based distribution and the TPM chip (JumpCloud, n.d.-n). Linux differs from other operating systems because it does not require biometrics, which is controversial. After all, if the device is stolen and credentials are compromised, the adversary can access the company's resources if JumpCloud Go is used as an MFA method.

When JumpCloud Go is enabled in the admin console and the Chrome extension is installed, users must log in to the user portal with their credentials by selecting the "Log in with JumpCloud Go" button, as seen in Figure 17. After the successful login, the JumpCloud Go is enabled if the user has enabled the Device Authenticator in the security -> Multi-factor Authentication pane. The default User Verification Frequency is 12 hours, which means that the user portal session will expire after 12 hours, and after that, the user needs to re-login, but this time without a password. The frequency setting can't be modified. (JumpCloud, n.d.-o.)

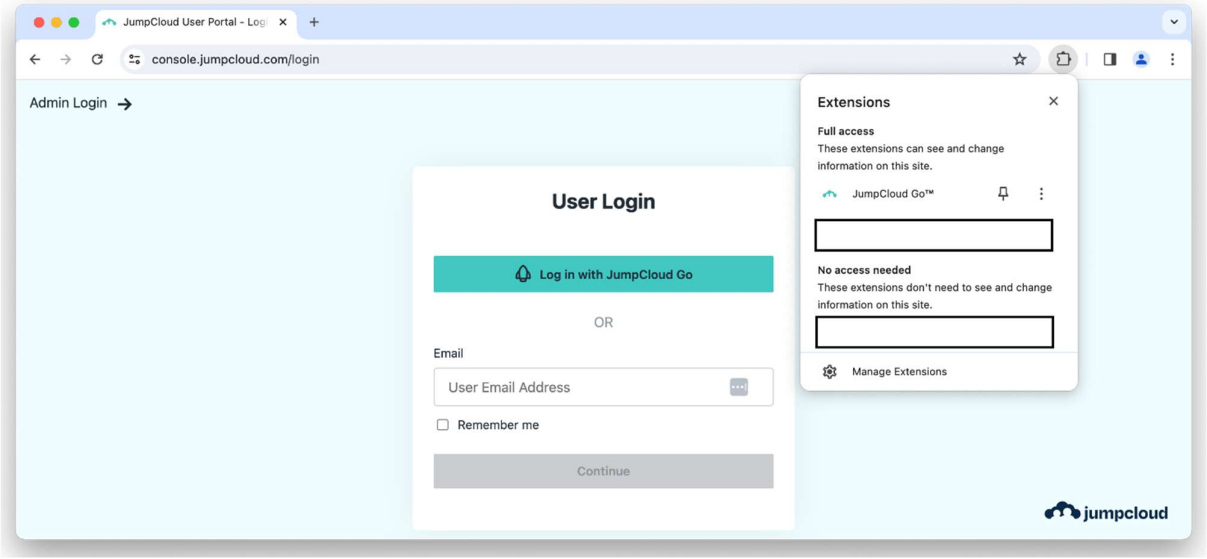

Figure 17 JumpCloud Go and its Chrome extension on a macOS device

3.2.10 LDAP & RADIUS

JumpCloud supports Cloud LDAP, enabling users to access legacy, open-source, and on-premises apps. The service can be configured in the administrator console without managing any on-prem LDAP infrastructure. The Cloud LDAP service has many compliance, performance, and security benefits: it improves IT teams' productivity, reduces hardware costs, is always backed up, takes advantage of the latest hardware, and keeps everything up-to-date and secure (Lake, 2021). Configuring Cloud LDAP is outside this thesis's scope, and more information can be found at https://jumpcloud.com/support/use-cloud-ldap.

Remote Authentication Dial-In User Service (RADIUS), the industry standard for Wi-Fi authentication, is one of JumpCloud's features. All JumpCloud users can connect to the office network without knowing the password for the Wi-Fi, and it supports all computer and mobile phone operating systems. RADIUS has two significant security-related benefits compared to wireless networks, which are only password-protected. The biggest reason for using RADIUS is to eliminate the Wi-Fi network security protocols WEP, WPA-Personal, and WPA2-Personal, which are considered legacy and insecure nowadays. Many corporations still use shared passwords and WPA2-Personal networks. The WPA2-Personal protocol was cracked in 2017 (Vanhoef, 2017), and it's possible for anyone who has a basic knowledge of Linux operating systems to get hold of any weak or predictable

WPA2-Personal password. One method for cracking WPA2-Personal passwords is to utilize applications such as Airmon-ng, Hxcdump, and Hashcat on a Kali Linux with a Wi-Fi dongle supporting packet injection and monitor mode (Null Byte, 2018). Human factors and physical security are the other reasons for using RADIUS and getting rid of WPA2-Personal networks. Even if the WPA2-Personal would be unhackable, there are multiple sources of how the password can leak, such as a computer note, a conversation between employees, or an office whiteboard.

JumpCloud's RADIUS-as-a-service (RaaS) supports three different RADIUS configurations. The first configuration option is password-based authentication, the default authentication method requiring less configuration. The second configuration option is Passwordless-based authentication, which requires more configuration and uses EAP-TLS to connect devices to the network. These first two can be seen in Figure 18. The last authentication method is the Delegated authentication with Entra ID, which uses EAP-TTLS/PAP for the connection and Entra ID as the identity provider. With Entra ID, JumpCloud works only as an authentication server.

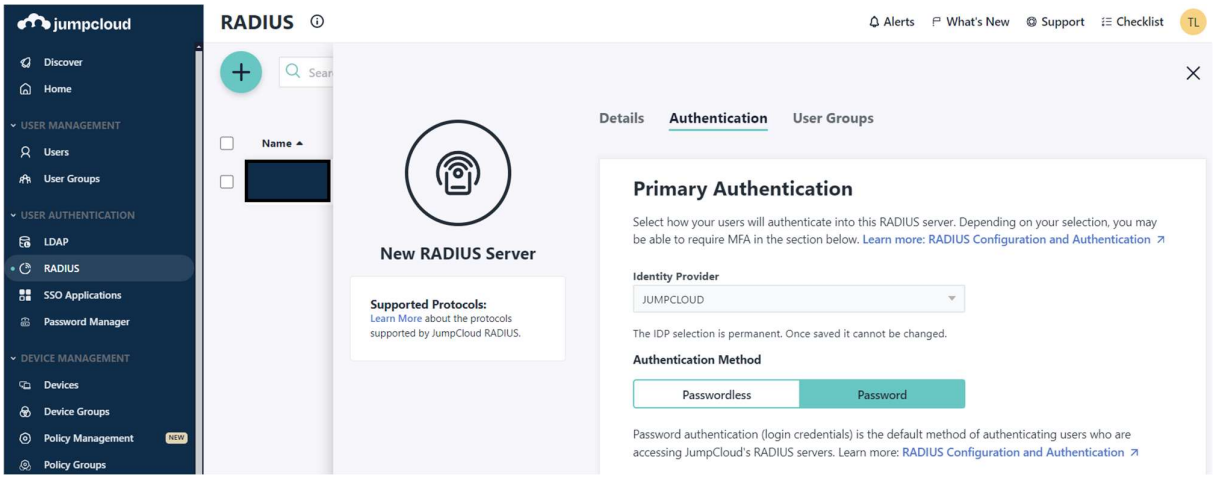

Figure 18 Passwordless and password-based RADIUS configurations

Detailed instructions on how to configure and implement RADIUS are outside of the scope of this thesis. JumpCloud has created detailed instructions on configuring the different RADIUS configurations at https://jumpcloud.com/support/get-started-radius. The RADIUS implementation also requires that the networking equipment be configured correctly. On the same website, vendor-specific documentation can be found on configuring Fortigate, Ubiquiti, Cisco, and Ruckus devices to

work with JumpCloud's RADIUS service alongside the generic configuration that works with other vendors.

3.2.11 Software Management

As mentioned in the Commands chapter, JumpCloud currently lacks software management options for Linux devices, and the application deployment must be done with commands. Installing applications remotely with commands has downsides, as it requires manual work, applications might not stay up to date, or they might get removed from the endpoint for various reasons. JumpCloud currently supports Windows, macOS, iOS, and Android software management.

In early 2024, JumpCloud announced a new feature called Private Repository. Being unable to store and deploy applications has been a downside of JumpCloud's application deployment feature. Before this change, if a company wanted to install a custom application that was not publicly available, they would need to store the application somewhere and run a script for the device that downloads and installs it. Today, the application can easily be stored and installed on devices or device groups via JumpCloud's admin console. However, there are some technical limitations and considerations. Only MSI file formats are supported for Windows, so the installers with the EXE file formats can't be used. Lacking EXE support might be an issue for some applications as the file format is widely used in application installers. For macOS, only PKG file formats are supported. Command Line Options can be added to the MSI installer, but customization for PKG installers is not supported.

Another limitation of using the private repository to store custom applications is the storage. The maximum size of individual applications can be 5 GB, and the total storage for all applications is 10 GB. It's also important to remember that users can only download applications from the private repository for a maximum of 10 GB each month. (JumpCloud, n.d.-ad.)

Windows

Windows software management has two different options for installing applications from public repositories. The first is the Chocolatey package manager, the only option until early 2024. All the

applications deployed with Chocolatey can be found at https://community.chocolatey.org/packages. When adding a new application for Windows, you need to fill in the following information to the New Managed Software:

- Software Name: Using the application's actual name is recommended.
- Package ID: This information can be found on Chocolatey's web page. Usually, it's all lowercase, and it doesn't include any spaces, e.g., Google Chrome = googlechrome, and Adobe Reader = adobereader
- Custom Package (optional): Deploying applications from proxy or custom package repositories is possible, and it is outside this thesis's scope.
- Keep software package up to date: JumpCloud agent will check periodically if a new application version is available and install it automatically. Selecting this reveals a new setting, allowing end users to delay updates for up to one week.
- Uninstall this software: Selecting this will uninstall the application if JumpCloud has installed it.

It's important to understand that if JumpCloud installs an application and the application is removed from the console, it will not uninstall it from the endpoints. When the application is added to the Software Management, information about the deployment is available in each application's Status tab. The tab will show the application's status, version, and details. (JumpCloud, n.d.-p.) The application's different states are shown below in Figure 19.

Status	Description
INSTALL SUCCESS	App was successfully installed or updated.
INSTALL PENDING	App is queued for installation
INSTALL FAILED	App was not successfully installed.
UNINSTALL SUCCESS	App was successfully removed.
UNINSTALL PENDING	App is queued for removal.
UNINSTALL FAILED	App was not successfully removed.
UPDATE PENDING	App is queued for updates.
UPDATE FAILED	App was not successfully updated.

Figure 19 Application status for Windows devices

The second option to deploy applications from public repositories to Windows devices is the Microsoft Store, an equivalent official application marketplace to Apple's App Store. Microsoft Store offers verified applications that stay up to date. The applications are also sandboxed, meaning they don't have visibility to other files on the device. The application is added by adding the application's name and Package ID (PID) to the Software Management -> Windows -> Microsoft Store, as seen in Figure 20. The PID can be seen in the URL when selecting an application in the Microsoft Store. Two optional settings can be enabled before scoping the application for a device or to a device group. The first setting is "Prevent auto-update." Selecting this will keep the application on the same version number and should be only used rarely and after a careful evaluation, as vulnerabilities are often found in unpatched applications. The second setting is "Prevent users from uninstalling." This option is beneficial and should be enabled in all applications installed on all Windows devices. It ensures that users are not installing work-related applications from unverified sources and keeps the mandatory applications installed, even though users would have administrator rights to the device.

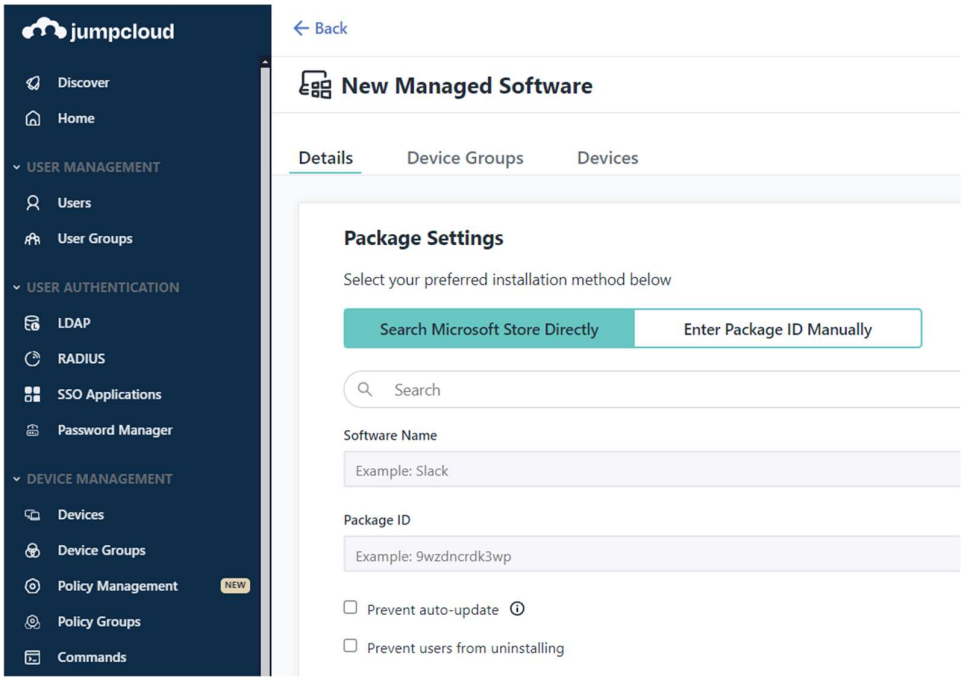

Figure 20 Microsoft Store application settings

Only some Microsoft Store applications can be installed via JumpCloud. If the application's Package ID does not start with the number 9, it lacks a Package Family Name and thus can't be deployed. JumpCloud considers all other applications as legacy applications. According to the tests conducted for this thesis, half of the application's PID starts with some other character than 9, such as Zoom's or Adobe Acrobat Reader DC's. Vendors need to update their applications to include the Package Family Name to be used with JumpCloud. (JumpCloud, n.d.-ae.)

iOS & macOS

Software Management for iOS and macOS uses Apple's Volume Purchasing Plan (VPP) for application deployment from the Mac App Store, which requires an Apple Business Manager (ABM) account and a purchased application. Apple's naming convention might be misleading because free applications like Slack or Microsoft Outlook must be "bought" in the ABM. When the procurement has been completed in the ABM, it will appear in the JumpCloud's console. After that, a managed configuration for the application in XML format can be added, and devices or device groups can be selected for the deployment.

If the application installation fails, the retry button can be found in the Status tab. Selecting the retry button will re-install the application. The status of each installation can also be seen from the Status tab. The different installation statuses can be seen below in Figure 21.

- **Install Pending** – The app is queued for installation.
- **Command Sent** – The install command was received by the device.
- **License Failed** – There are not enough available licenses.
- **Command Failed** – The installation command was sent but the installation might have been interrupted due to communication issues.
- **Uninstall Pending** – This device has not responded to the request to remove the device and reclaim the license. The task will be completed at next check-in.
- **Uninstall Success** – The device has been removed and the license reclaimed.

Figure 21 Application status for Apple devices

Figure 22 below shows the Apple Business Manager and its Apps and Books pane. Using the search word jumpcloud, the relevant applications can be found from the App Store. By selecting the application and entering the quantity, it can be assigned to the correct MDM server by selecting Get.

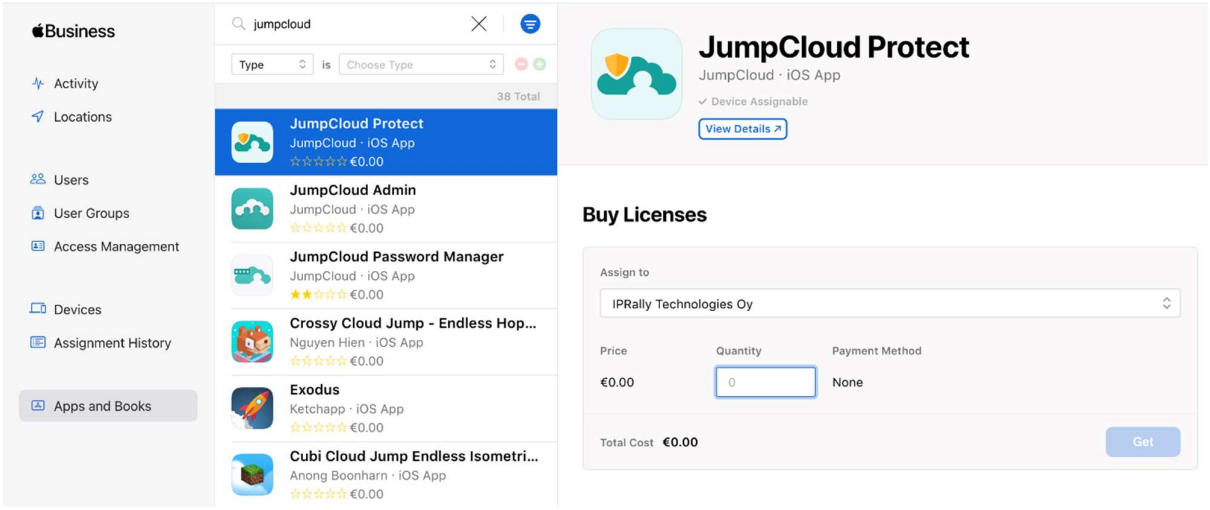

Figure 22 Apple business manager and JumpCloud Protect application for iOS

An alternative method to deploy applications to macOS devices is JumpCloud's Custom App Packages feature, which only requires two pieces of information: Software Description and Software

Package URL. Once these have been filled out, a Validate button must be selected. If the URL is correct, the application's name and version will appear at the bottom of the screen. There are downsides to this deployment style. The application has a maximum size of 500MB; if the vendor updates it, it won't be deployed to new devices anymore. The latter can be solved by entering a new URL and/or selecting the Validate button again to update the Software Version to the newest version. (JumpCloud, n.d.-q.)

As the Mac App Store lacks many applications, and the Custom App feature can't automatically keep the applications up to date, many open-source solutions have been created to fill these gaps. One of the widely used solutions is called Installomator. This application can be pushed remotely to devices with the Custom App feature. When Installomator is successfully deployed to the end-point, an application can be installed or updated using the Commands feature with a one-liner script, shown below. If the command's launch event is selected as "Every JumpCloud Login" for the example script, it will install or update Zoom every time the user logs in to the endpoint.

/usr/local/Installomator/Installomator.sh zoom NOTIFY=silent

Android

Android application deployment is done via the Google Play Store, as seen in Figure 23. When selecting the Software Management -> Google -> Add New button, three options are offered: Search Play Store can be used to deploy all public applications, and Private apps can be used to upload publicly unavailable applications. The last option is Web apps, which create a website shortcut to the Android device that looks like an application. When the public or internal application is added to the console, it can be selected to modify additional settings. These are the settings that affect the applications' installation and user experience:

- Install Mode
    - Available (default): The application will be available to download in the work profile's Play Store.
    - Force Install: Automatic deployment, the user can't remove the application.
    - Block: User can't install the application

- Update Mode
    - Default (default): The application will be updated automatically.
    - High Priority: The application will be updated as soon as possible.
    - Postpone: Update will occur automatically after 90 days
- Runtime Permissions
    - Allow: The application will get all necessary permissions granted automatically.
    - Prompt (default): This selection will allow users to grant or deny permissions.
    - Deny: Denies the permissions automatically.

There are various enrolment methods for both iOS and Android devices. It's important to understand that if the device is not automatically enrolled and the user enrolls it, there is no visibility of the installed applications or their versions. (JumpCloud, n.d.-r.)

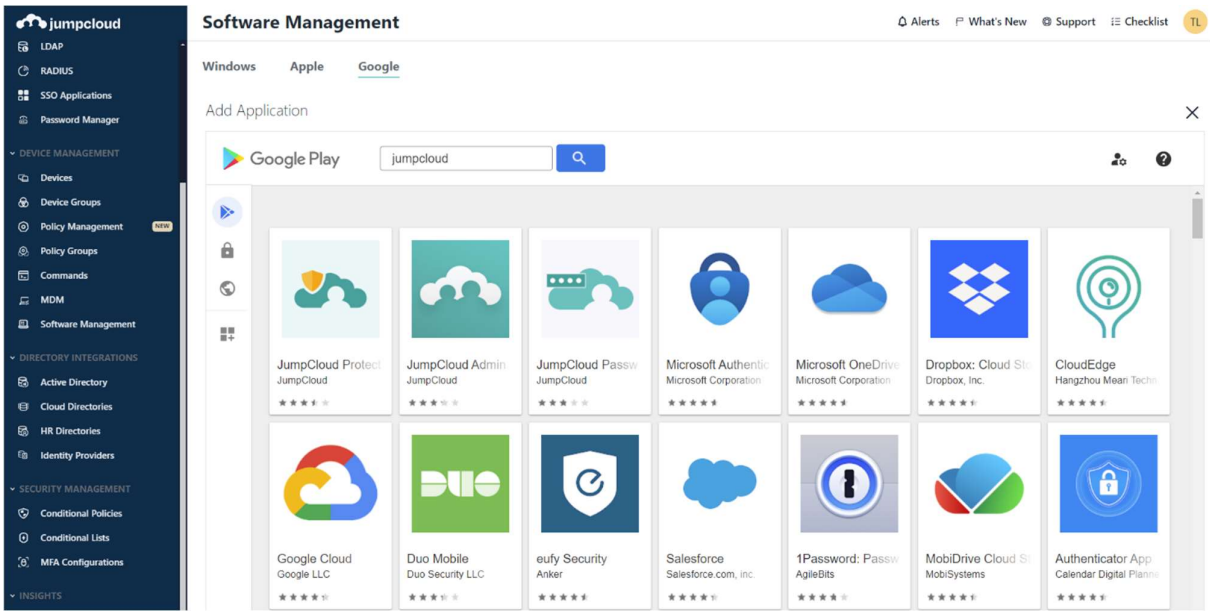

Figure 23 Google Play store

3.2.12 Insights

For auditing and troubleshooting purposes, a UEM must include a feature to view the details of different events, device details, applications' status, etc. JumpCloud's solutions for showing de-

tailed information are System Insights, Directory Insights, and Reports. System Insights are accessed from the device's details tab. Data is displayed only for one device at a time, as JumpCloud does not provide an overview or report for all device details in one view. This missing feature is a considerable deficiency and might drive potential customers away, as it is hard to memorize the details of hundreds of devices. However, there is a workaround, and the data can be accessed with an API.

System Insights are turned off by default for privacy reasons, as it collect extensive amounts of data from the endpoints, as seen in Figure 24. It can be turned on from the Settings -> Features. Auto-enabling the System Insights for new endpoints can be done from the same page. System Insights must be manually turned on for each device if endpoints were enrolled to JumpCloud before the auto-enable feature was turned on. System Insights is only available for 64-bit operating systems and doesn't support mobile devices. The data is refreshed every 60 minutes, so some often-changing data might already be outdated. Some organizations might need to store the data history for compliance purposes, which can be accomplished by migrating the data to another system, such as Azure Blob or AWS S3 Bucket. The data can also be exported, but only in CSV text format. The complete list of collected information can be found at this link: https://jumpcloud.com/support/system-insights. A few of the most popular System Insights data items for JumpCloud admins are:

- Uptime: A high uptime usually degrades the endpoint's performance. If the operating system is restarted every 10-14 days, the security software, application updates, and MDM commands operate more smoothly. For this reason, many IT admins deploy restart notification tools to keep the endpoints secure and healthy (GitHub, n.d-b).
- CPU, Memory, Model: The operating system and application requirements are getting more demanding yearly. If the endpoint's details are missing from the asset management database, they can be found in System Insights. These pieces of information play an important role when determining which endpoint gets replaced next to a new one.
- Storage Available: Running out of disk space while using the endpoint can lead to data loss. New operating systems and application updates might require lots of free space. Also, applications can malfunction and slowly consume the available storage space. For these rea-

sons, it's crucial to know how much disk space devices have so admins can plan the operating system upgrades or automate a notification so users know when to remove unnecessary files from the endpoints.

- Network: Knowing the details of the endpoint's hostname, public and private IP addresses, and MAC address are essential details regarding network security. The IP addresses can be used to determine which network the endpoint is connected to, or the office network can be configured so that only selected MAC addresses can connect to the network. (JumpCloud, n.d.-t.)

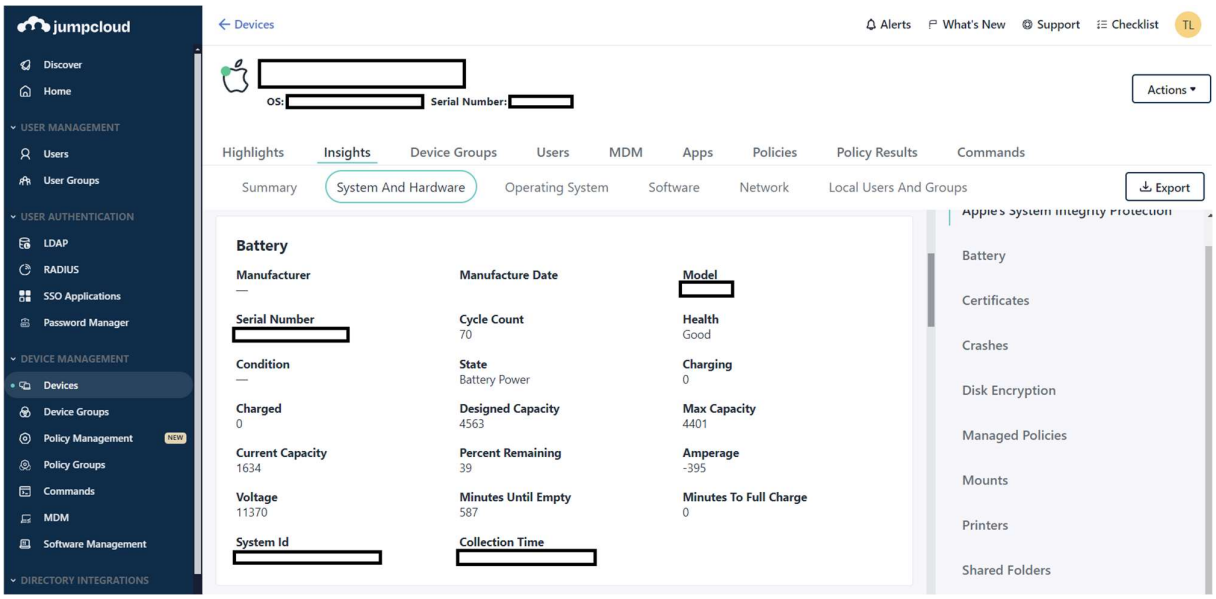

Figure 24 System Insights and battery information of a macOS device

Directory Insights and Reports

System Insights is an excellent tool for knowing the details of the endpoint. However, it doesn't show what people are doing with them, which is why Directory Insights exists. It is a tool for viewing different kinds of activities that people are doing with the endpoints, user portal, and admin console. This information is stored in JumpCloud for 90 days. If a company wants to see logs for an extended period for compliance reasons, the logs can be viewed and exported via JumpCloud API. An alternative solution is to use an AWS Serverless Application to store the logs.

Directory Insights consists of two different features: Views and Search. Quick Views can be selected when selecting the Views dropdown menu, as seen in Figure 25. These nine pre-built Views help administrators find the most common information, such as login attempts, user creations and deletions, and admin activity. The predefined Views are easily accessible and intuitive, especially for administrators and auditors without an extensive background in JumpCloud. If the information can't be found by using the Quick Views, new Views can be saved. To save a new View, an administrator can select from the following information: Service, Event Type, User, Device, and Time Range. When the criteria have been chosen for the new View, the following information is shown by default: Timestamp (when), Event Type (what), Result, Initiated By (who), Success (true/false), GeoIP (location), Repeat Count (how many times). The event columns can be modified to show more or less information on the screen. The Search feature can be used to enter text, but it can't be saved as a View. A few of the most popular Directory Insights event types for JumpCloud admins are:

- Admin login attempt: One of the most critical information about a management solution with administrator access to all endpoints is knowing who uses it. If an adversary can access JumpCloud and infect endpoints with malware, directory events can show which administrator account was used.
- SSO auth: Keeping track of the company's software licenses is an excellent way to save money. As previously mentioned, JumpCloud only stores Directory Insights logs for 90 days. By default, this event data can only be utilized to create a report for those not using a selected SSO application within the last three months.
- Login Attempt: Password issues are still a thing in 2024. Even though passwordless solutions are widely used nowadays, passwords are unfortunately still needed. The information will be shown here when the user enters a wrong password multiple times - or if there is a hacking attempt – and the account gets locked. (JumpCloud, n.d.-v.)

The complete list of event types can be found at this link: https://docs.jumpcloud.com/api/insights/directory/1.0/index.html#section/Event-Types.

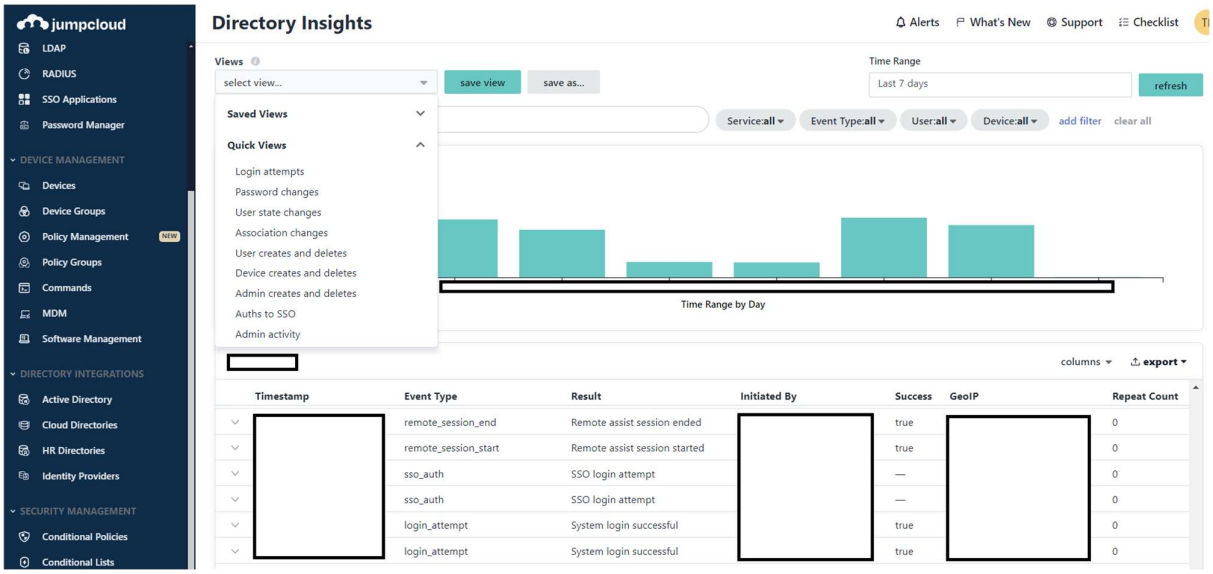

Figure 25 Quick views in Directory Insights

The reports feature can be found in the left pane and has features similar to those of Directory Insights. It can be easily used to create reports, such as User-to-devices and user-to-SSO applications. The data can be exported in JSON or CVS text format, similar to Directory Insights. As mentioned above, the JumpCloud admin console can't be unfortunately used to create customized and detailed device reports. Reports include only two Device Reports: Browser Patch Management Policy and OS Patch Management Policy, which gives a clear text-based overview of all devices' current policies. (JumpCloud, n.d.-u.)

3.3 Other Features

3.3.1 Support

Product support is an essential feature of every mobile device management tool. There are different reasons why IT administrators need to contact support: they can make mistakes or have questions about some of the features. Sometimes, the product has bugs, and some features might not work as they should. If an admin suspects some feature might be working abnormally, the first step is to check JumpCloud's Service Status, which can be found at https://status.jumpcloud.com/. If all service status systems are green and operational and the issue persists, it's suggested that support be contacted.

There are two different methods to contact support. Platform Prime licenses include premium support, which means that the support is available via Email, phone, or chat 24x7x365. Chat is the most convenient method for getting help or reporting issues, as support is immediately available, and screenshots can be easily added to the chat. Other licenses include only email support, which SLA is from 4 hours to the next business day, depending on the severity of the issue. Email support tickets can be created from the upper right corner of the console, and the live chat can be accessed from the lower left corner.

Feature requests are an essential part of making the product better. JumpCloud admins worldwide have a very diverse background and great ideas for improving the product. For this reason, feature requests can be submitted straight from the support menu in the upper right corner of the admin console. The feature request must include a short description of the idea, current problem, category, and importance.

All the feature requests and support tickets can be easily found in the Case Portal, accessed from the screen's upper right corner. A centralized portal in the console is incredibly convenient for teams with multiple administrators to see each request's status. The cases can be exported in JSON or CSV format or filtered with the following statuses: New, Reviewing, In Progress, Closed, Future Consideration, and Not Being Considered.

The last category of the Support pane is the Knowledge Base. Selecting the link will open JumpCloud's Help Center in the browser, which is accessible to everyone on the Internet, and has support articles for end users and administrators. The main feature of the Help Center is the search function, which can be used to find an answer to any topic with a support article. If a user does not know what search words to use, they can select one of the categories, such as Insights, Authentication, or Automation Tools. The Troubleshooting Knowledge Base (KB) can be found at the bottom of the page. It's crucial to let end users know about this page, as it contains essential information and removes the need for administrators to create internal documentation about the same topics for them, such as: "Troubleshoot: JumpCloud Protect" or "Troubleshoot macOS Hardware or Firmware Issues." For administrators, the KB is the best source to start troubleshooting an issue if something is not working as it should, e.g., "Troubleshoot: RADIUS Server Authentication" or "Troubleshoot: Google Workspace Integration." (JumpCloud, n.d.-ai.)

3.3.2 Training and certifications

All major mobile device management vendors have training materials for their products. The material has not been created for end users but for administrators who use JumpCloud to manage devices within their companies, consultants who provide professional services, or vendors who are JumpCloud's official resellers. All the training material can be found at https://university.jumpcloud.com, and it has been divided into different learning paths. All learning paths, such as Device Management, Security and Compliance, and Identity Management, include courses. The courses are divided into introduction, lessons, and the course wrap-up. The lessons include videos, flip cards, and quizzes.

Once the student has completed enough courses, especially the ones included in the Certification learning paths, they can register for the certification exam if they feel confident about their know-how. JumpCloud offers two different certifications. Core certification validates a solid foundational knowledge of JumpCloud and its configuration, implementation, and daily operations. The advanced certification is meant to validate strong expertise in complex deployments and implementations and those who have already implemented JumpCloud and use it for daily management. The exams cost $99 for the core certification and 199$ for the advanced certification. JumpCloud offers three attempts to pass either of the exams, and there must be at least 24 hours between the attempts. The exams have 45 questions and 60 minutes to complete them. The core certification expires after one year, and the advanced certification expires after two years. The renewal course will cost $49, becoming available in 2024 and 2025. (JumpCloud, n.d.-ab.)

3.3.3 Professional services

Some companies choose to have fewer employees in their IT departments and use outsourcing to help with their device and identity management challenges. JumpCloud offers professional services within three different categories. The first category is Implementation Services, which is meant to design and create the JumpCloud instance for customers and integrate it into the current IT environments. The Implementation team provides recommended strategies and expert guidance for various components, configurations, and capabilities. In other words, JumpCloud's employees with deep technical expertise will implement JumpCloud for the company.

The second category is Customer Success Management (CSM), which provides services continuously and not on a project basis like the implementation services. The team will streamline and simplify the IT administrator's tasks and ensure that all functionalities and features are used correctly and that the maximum advantage is utilized. They will also help with the end-user adaptation and facilitate the meetings with the internal stakeholders. The CSM team will also perform health checks, analyze the customer's needs, escalate support tickets, provide feedback to JumpCloud's developers, and manage the feature requests. In other words, the team will assist the customer in utilizing the JumpCloud to its full potential.

The last category is the Solutions Architecture, which provides personalized health checks, analytics, custom scripting, and best practices by a dedicated technical expert. Exclusive access to these services will be tailored to meet customers' requirements, increasing overall project success and ensuring effective solutions. The solution architects are highly skilled with AD, Okta, and Powershell, among other technologies, and the project's milestones, phases, and tasks are transparent to the customer. By leveraging the service, the work can be outsourced to experts who cooperate with other teams at JumpCloud. (JumpCloud, n.d.-aj.)

3.3.4 Community

Mobile device management companies usually have an active online community for sharing feedback, asking questions, and providing peer support. Usually, IT administrators face similar challenges, suffer from the same bugs, and get identical requests from the companies where they work. For this reason, JumpCloud has created two different forums where customers can connect. The first forum is the JumpCloud Community, found at https://community.jumpcloud.com/. This traditional website, with over 1200 members and 2500 posts, is full of essential knowledge about leveraging the Powershell module, scripting, integrations, operating systems, and other important JumpCloud features by the customers, for the customers. JumpCloud employees also use this platform to post recordings of the IT Hour and make announcements about the new features. As this is a forum, all posts are thorough, well-written, and created to educate JumpCloud administrators so they can learn about features that might need in-depth knowledge or a long history of the product. The community can be browsed without an account. The community does not provide any Single Sign-on mechanisms. Hence, the registration process is manual and requires the user to

create a username, password, and a valid email address that needs to be verified after the registration. Registered community users can create posts, give the post author kudos (thumbs up), receive email notifications, and reply to the posts.

The second forum is the JumpCloud lounge, a modern approach to providing a chat-based solution for everyone involved with JumpCloud. The Lounge utilizes Slack, a top-rated messaging app in the corporate world, so the community can be added to the same Slack application that JumpCloud administrators use for their internal communication. With over 3800 members and 60 channels, the Lounge is a very convenient method to get peer support in minutes. The conversation is more fast-paced, and the posts are shorter than in the JumpCloud Community. The most popular channels in the Lounge are #welcome and #house-rules, mainly because the users are added to these channels automatically. The second most popular channels are #macos, #mdm, and #sso, which get new posts or questions almost daily.

JumpCloud employees are also active in the Lounge, making sure all questions are answered if no one else replies to the message. The Lounge is also used to post JumpCloud Community posts, job advertisements, and direct messages to other members. The only downside about the Lounge is that the messages disappear after 90 days, unlike the JumpCloud Community, as the Lounge uses Slack's Free Plan. The JumpCloud Lounge can be found at https://jumpcloudlounge.slack.com/, and it can be accessed through Email, Google SSO, or by utilizing Sign in with Apple. JumpCloud suggests signing in using the same Email used at work.

3.3.5 Blog, webinars, and release notes

JumpCloud Blog is an incredible information resource for current JumpCloud customers and anyone interested in the blog's topics. The blog has a search field and a dropdown menu for Categories and Topics. All these three things can be used together when searching for a blog post. The Categories consist of Devices, Directory Services, Integrations, IT Admins, Mental Health, Security, and User Access. The Topics include Best Practices, How-To, JumpCloud, MSP, News, Remote Work, and Unification. Some of the blog posts are targeted at IT administrators, and they are purely technical and work as a step-by-step tutorial on how to do something, e.g., "How to Upgrade from Ubuntu 22.04 LTS to Ubuntu 24.04 LTS" by David Worthington on April 25, 2024.

Some other blog posts have two different functions: they are technical, and at the same time, they work as marketing material. These kinds of blog posts are targeted at decision-makers, especially those evaluating mobile device management tools and comparing them with each other. A good example is the blog post “Miradore vs. Hexnode: Comparing Mobile Device Management Tools” by Kelsey Kinzer on February 19, 2024. Usually, the topics mention two different MDM tools, but the article eventually compares JumpCloud to these tools. (JumpCloud, n.d.-ak.)

JumpCloud webinars can be divided into two categories. The recorded and official webinars can be accessed at https://jumpcloud.com/resources/type/webinars by filling out a short form. From the same page, people can also register for upcoming webinars, such as “Authentication in 2024: Using Passwords and Passwordless Methods”. Of all the recorded webinars, quarterly recurring JumpCloud's Partner and Product Roadmap is the most popular topic. Watching these videos is beneficial as administrators can learn about upcoming features and plan the change well before the feature becomes available. (JumpCloud, n.d.-am.)

The second webinar category is less official. JumpCloud hosts an IT Hour every Friday at 18:30 (EET). The IT Hour is self-explanatory: JumpCloud employees talk about IT for approximately one hour. JumpCloud’s Becky Scott hosts the relaxed webinars, and the show usually has two to three visitors, e.g., Sehrat Can and Mustafa Akin, the cofounders of Resmo, on the 100th IT Hour episode on 26.4.2024. The IT Hour focuses on the life of IT administrators, and the conversations usually consist of the weekly IT news and curated JumpCloud community topics. The IT Hour is also a great way to learn about new features, such as JumpCloud Go (19.4.2024), Microsoft Store integration (12.4.2024), and Temporary Elevated Device Privileges (5.4.2024). All IT Hour episodes can be watched from the JumpCloud community or YouTube. Last but not least, there are giveaways from time to time. (JumpCloud, n.d.-al.)

Another vital website for JumpCloud administrators to visit recurringly is the Release Note and Bug Fixes, which can be accessed at https://jumpcloud.com/support/category/release-notes-and-bug-fixes. From these sources, administrators can see what new features have been implemented for the product and agent and what bugs have been fixed. Keeping up with the changes and fixes helps administrators utilize JumpCloud better and communicate the information to the end users. Here is an example of a Bug Fix and two release notes:

- Bug Fix Report for March 22 to 28: “Fixed an issue with autofill in the Password Manager Browser Extension”
- JumpCloud Agent Release Notes for April 16, 2024: “Resolved an issue with the Windows Agent installer failing in some rare circumstances after a previous uninstall”
- Release Notes April 18, 2024: “macOS users will now be prompted to grant the required permissions to run JumpCloud Remote Assist (Screen Recording, Accessibility and Full Disk Access) every time you log in to the system until you grant all the required permissions.” (JumpCloud, n.d.-an.)

4 Single Sign-on

Single Sign-On (SSO) is a user authentication process that allows an employee to access multiple applications using one set of login credentials, usually a combination of a username and password. Users can log in once and gain access to all supported applications without being prompted to log in with different credentials and remembering separate usernames and passwords for each service.

SSO is widely used in larger companies to streamline accessing multiple IT systems, enhance security, and improve user experience by reducing the time a user needs to log in and enter the credentials. It also simplifies the management of user accounts and permissions for IT administrators. According to JumpCloud (n.d.-at), 50% of all support requests are related to passwords, employees reuse the same password on 16 different applications on average, and 68% of the employees switch between 10 apps hourly.

4.1 Just-in-Time & System for Cross-domain Identity Management

Every IT person working in a small or medium-sized business is very familiar with the onboarding and offboarding tasks, which are usually manual and time-consuming. A typical cloud-native company uses dozens of SaaS applications. Usually, IT will ensure that access to applications is revoked for employees leaving the company. Going through each application for every leaver takes precious time away from exciting development projects that help the company succeed. Also, mistakes can happen while scrolling through tens or hundreds of user accounts in each application. To reduce the IT administrator's manual tasks and make sure that SSO applications do not have any extra user accounts, JumpCloud offers two mechanisms for user account management in other applications: Just-in-Time (JIT) and System for Cross-domain Identity Management (SCIM).

JIT protocol extends the SAML protocol by transferring user attributes from JumpCloud to the supported SSO applications. This technology makes the account creation possible the first time the user logs in to the SSO application. JIT support allows the administrator to simplify the onboarding process and enable the automatic account creation to multiple applications using only one view in the JumpCloud console. The only downside with JIT is that it only helps with the onboarding and

account creation. SCIM, however, can create and delete accounts from the integrated SSO applications. SCIM utilizes the REST API and HTTP verbs to standardize the identities between JumpCloud and the application. SCIM can be used to update user attributes through the ongoing sync, but its primary purpose is to delete unnecessary user accounts from all SSO applications that support the feature. While the automatic account removal might sound tempting, it's essential to verify from the product owner that the user accounts can be removed on the employee's last working day, as they might contain valuable information to the company, such as sales data. Sometimes, the user accounts are suspended and not removed for a month or even longer, depending on the application and what kind of data is saved to the account.

JumpCloud's SSO application catalog at https://jumpcloud.com/integrations can be sorted with JIT and SCIM, which can be seen in Figure 26. Currently, 200 applications support JIT, which is 22% of all the pre-configured SSO applications in the catalog. SCIM is supported by 120 applications, which make up 13% of all applications. Even though the applications are supporting JIT or SCIM, it doesn't necessarily mean that they will work out of the box. SCIM is generally considered an enterprise-grade feature and is targeted towards big corporations, even though they might have security requirements similar to those of smaller companies. Applications rarely support SCIM at the cheapest license levels. Some vendors, such as Linear and TeamViewer, do not even show the pricing on their website to enable SCIM for their application, and they ask to contact the sales department for customized pricing.

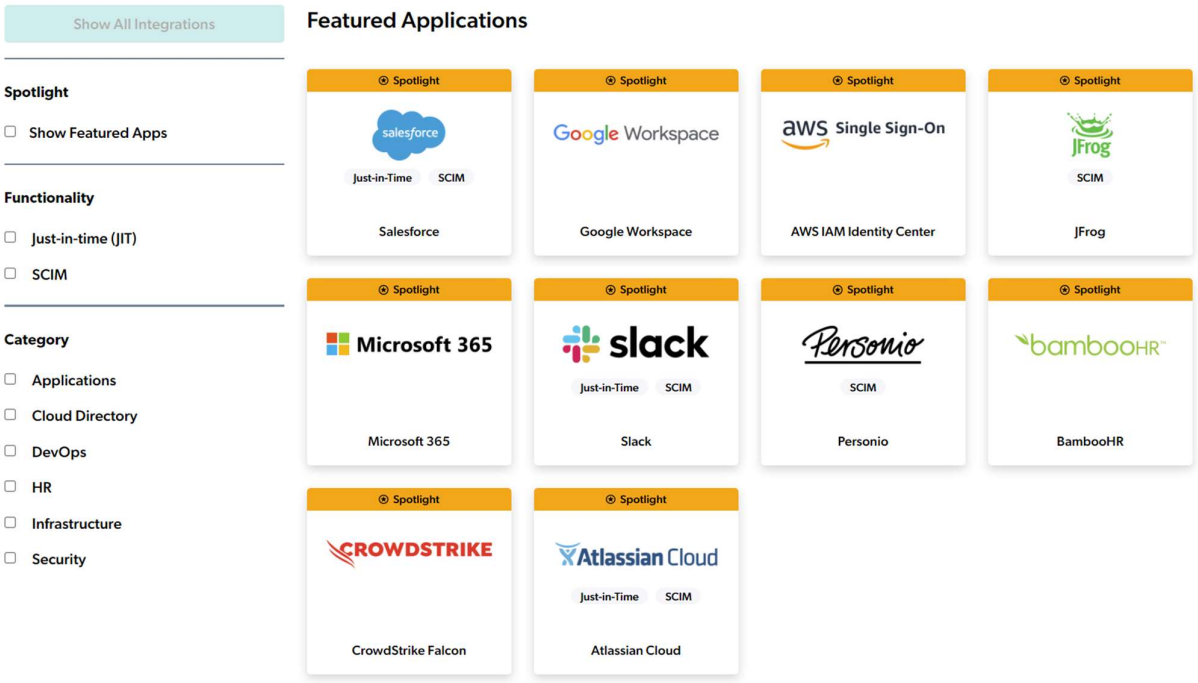

Figure 26 Integration catalog's featured applications

SCIM should be one of the SaaS applications' core security features to help with manual tasks and remove stale accounts. It should not be considered a luxury feature only for wealthy companies. For this reason, an SSO Wall Of Shame website has been created at https://sso.tax/ to show everyone how many hundreds or thousands of percent more the licenses will cost if a customer would like to manage the application's user accounts within their identity provider and not in the application itself. (Niedringhaus, 2020.)

4.2 SSO in JumpCloud

JumpCloud offers an extensive SSO integration catalog that can be browsed at https://jumpcloud.com/integrations or within the administrator console in the left pane (SSO Applications). Over 900 pre-configured applications can be chosen, and the list is constantly growing as JumpCloud adds more applications based on feedback and requests. The website provides a better search functionality, as the applications can be sorted with functionality (JIT/SCIM) and with categories (Applications, Cloud Directory, DevOps, HR, Infrastructure, Security). JumpCloud also shows the featured applications by default on the page, as these are vital tools in the enterprise, and

there is a high possibility that these applications are one of the requirements when selecting an identity provider for creating Single Sign-on integrations.

On average, employees use dozens of SaaS applications, and there are multiple ways to access these. Someone can access the application using their browsing history or might have all websites saved as a bookmark in their browser. JumpCloud offers a user portal at https://console.jumpcloud.com/ that can be accessed 24/7 and shows all SSO applications and their icons. The user portal is a great way to show which applications employees can access. If the SSO integration has not been created, an administrator can add a bookmark to the user portal, redirecting to the correct URL when clicked. If an employee accesses the SSO application on the application's website, the login is called SP-Initiated (Service Provider). If the application is accessed from the user portal, the login is called IdP-Initiated (Identity Provider).

Administrators can create SSO integrations in two ways: by using the pre-configured applications from the catalog or by creating a custom application. The pre-configured applications can be selected from the administrator console by choosing the SSO Applications in the left pane. After the application has been selected, the following information can be modified or added to the application on the General Info page: Display Label, User Portal Image, Description, and whether the application is visible in the user portal. After the application is saved, it will appear in the Configured Applications list. Next, the application must be configured correctly in the JumpCloud console and the application's website. Different applications might have significant differences in how to enable SSO. I have selected TeamTailor as an example application. Here are the steps on how to configure TeamTailor and JumpCloud so that users can access the application only with their JumpCloud credentials:

1. Check JumpCloud's and TeamTailor's documentation about the SSO integration, cross-reference the steps, and make sure they match.
2. In JumpCloud, select the TeamTailor application in SSO Applications (Figure 27), check the name and picture, add a description, and select Save Application.
3. Contact TeamTailor support and ask them to activate the company's account SSO.
4. Once the support has enabled the SSO activation, login to TeamTailor with an account with Company Admin permissions and select Settings -> General -> Security.

5. In TeamTailor, copy the Entity ID and Assertion Consumption Service (ACS) URL
6. In JumpCloud, select TeamTailor from the Configured Applications and select the SSO tab.
7. In JumpCloud, paste the Entity ID to the SP Entity ID field
8. In JumpCloud, paste the Assertion Consumption Service (ACS) URL to the ACS URL field
9. In JumpCloud, copy the IDP URL
10. In JumpCloud, export the JumpCloud Metadata by selecting the Export Metadata button.
    a. Alternatively, you can copy the Metadata URL
11. In JumpCloud, select the User Groups tab and scope the application to a test user group.
12. In TeamTailor, paste the IDP URL to the Single Sign-on URL field
13. In TeamTailor, upload the JumpCloud Metadata file by selecting the Browse button under the Upload IdP metadata file
    a. Alternatively, you can paste the Metadata URL to the IdP Metadata XML URL field
14. Save the changes in JumpCloud and TeamTailor
15. Test the SP-Initiated login by selecting Log in using SSO at https://app.teamtailor.com and entering JumpCloud credentials. After a successful login, log out.
16. Test the IdP-initiated login at https://console.jumpcloud.com with JumpCloud credentials by selecting the TeamTailor application.
17. In TeamTailor, select the Enforce SSO and select Save changes
18. Test the default login method by entering the email and password used during step 4 and selecting Sign in. The login should fail.
19. In JumpCloud, select the User Groups tab and scope the application to all groups that should have access to TeamTailor. (Lundmarck, 2024.)

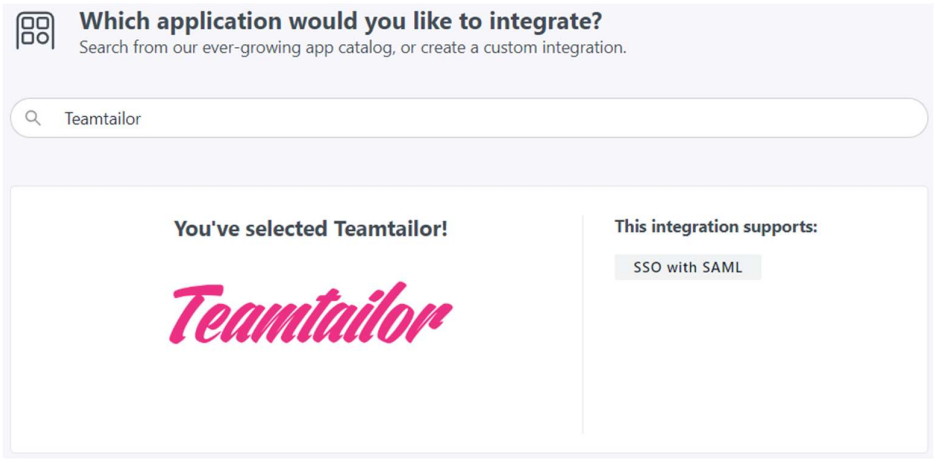

Figure 27 Step 2/19 of creating an SSO integration with the TeamTailor application

The steps for adding and configuring other applications using SSO through SAML 2.0 are similar to TeamTailor. The second method for creating an SSO integration is to add a Custom Application. Administrators can create the integration with SAML 2.0 Connector, also known as Custom SAML App, or with OIDC. The integration can also be made for importing users from an application into JumpCloud or exporting users from JumpCloud into an application. If the user accounts are exported into an application, JumpCloud becomes the authority of the user accounts. Lastly, bookmarks can be created with the custom application, as seen in Figure 28.

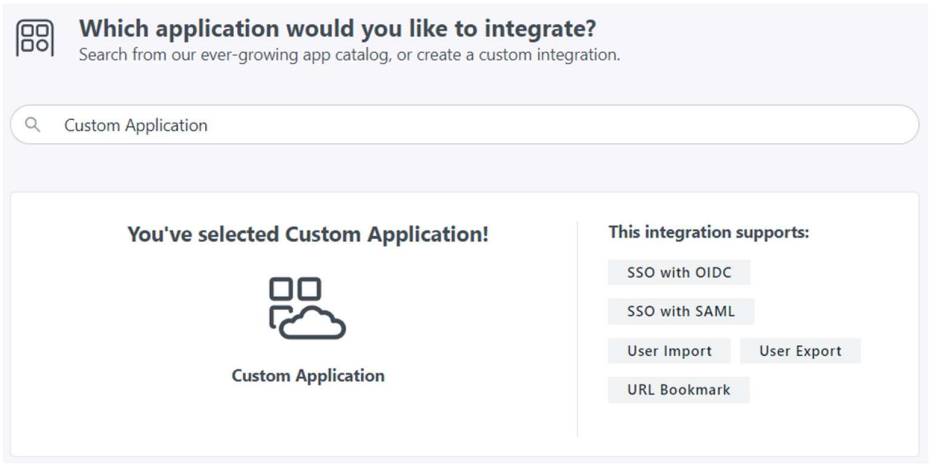

Figure 28 SSO Application's Custom Application

Creating custom applications requires in-depth knowledge of the Service Provider's SAML 2.0 connector requirements and SAML compatibility. Custom application SSO integrations are not in the scope of this thesis, as applications are often configured very differently. The support article about how to create custom integrations can be found at: https://jumpcloud.com/support/sso-using-custom-saml-application-connectors.

4.3 SSO cost-benefit analysis

For this analysis, let's assume that a hypothetical 50-employee company has been using Google Workspace as the Identity Provider (IdP) and uses the Sign in with Google login mechanism for signing into all supported SaaS applications. The company would like to implement JumpCloud's Zero Trust solution, meaning the application's login flow needs to go through JumpCloud for additional verification. There are two different solutions for creating this, both of which have advantages and disadvantages.

The first solution is to create the SSO integration directly from JumpCloud to the application, where the service provider (SP) initiated login is redirected to JumpCloud and then back to the SP if the authentication is allowed by the Zero Trust policies. Theoretically, this solution is the best method to build scalable solutions, keep the IT team as small as possible, mitigate risks, and reduce manual tasks, but only if the application supports SCIM. The only issue with this method is the applications' licensing costs. Usually, the cheapest licensing level supports only the Google Sign-in mechanism but not SCIM and custom SSO integrations, such as JumpCloud's. The middle-tier licensing level might support custom SSO but not SCIM, which can be bought with the most expensive licensing level. Here are the annual price differences between the cheapest license level and the one that supports SCIM for a 50-employee SaaS company:

- Slack: $8,75 vs. $15 / month. Price difference for 50 users: $3750
- GitHub: $4 vs. $21 / month. Price difference for 25 users: $5100
- Bitwarden: $4 vs. $6 / month. Price difference for 50 users: $1200
- Docker: $5 vs. $24 / month. Price difference for 25 users: $5700
- Sentry: $26 vs. $80 / month. Price difference for 5 users: $3240
- Evernote: $14,17 vs. $ 20,83 / month. Price difference for 25 users: $1998

- Zoom: $13,32 vs. $18,32 / month. Price difference for 20 users: $1200
- Atlassian Guard: Annual price for 50 users: $2000

As Chapter 2.2, Research Ethics and Methods mentions, this application list is purely fictional and does not reflect IPRally Technologies' used applications and user amounts. The answer to the research question can be easily calculated using the list: upgrading only a handful of applications would have an annual extra cost of over $24,000. Everyone understands that upgrading the licenses only for the SCIM feature is not worth the price, as removing the user accounts during offboarding tasks can be done in minutes in small and medium-sized companies. However, the case is not that black and white, as all companies have different application requirements. Let's assume that a company requires a 99% guaranteed uptime and a four-hour support response time for the Slack application. In that case, the more expensive licenses are justified, and the SCIM feature is a free-of-charge giveaway included in the licenses, which the IT administrators will be pleased to implement to help their offboarding tasks.

The second solution – without the SCIM feature – can also be used with JumpCloud's Zero Trust features, which will protect all applications using the Sign in with Google login mechanism, which most SaaS applications support. The method can be created with JumpCloud's Google Workspace (GWS) SSO integration.

With GWS SSO, IT administrators can redirect all GWS or applications' Sign-in with Google login attempts to JumpCloud and then back to the service provider if the authentication is allowed by the company's Zero Trust policies. This SP -> GWS -> JC -> GWS -> SP login has more redirects and is slightly slower than the first solution's SSO's SP -> JC -> SP login flow, which has fewer steps. GWS SSO is a cost-effective way to protect most of the company's applications, but only if they are accessed through Google Sign-In. However, the GWS SSO doesn't support SCIM, so the onboarding and offboarding account-related tasks must be done manually, which expands the company's attack surface with former employees' accounts that are not needed anymore. Figure 29 shows the different login flows to clarify JumpCloud's SSO features:

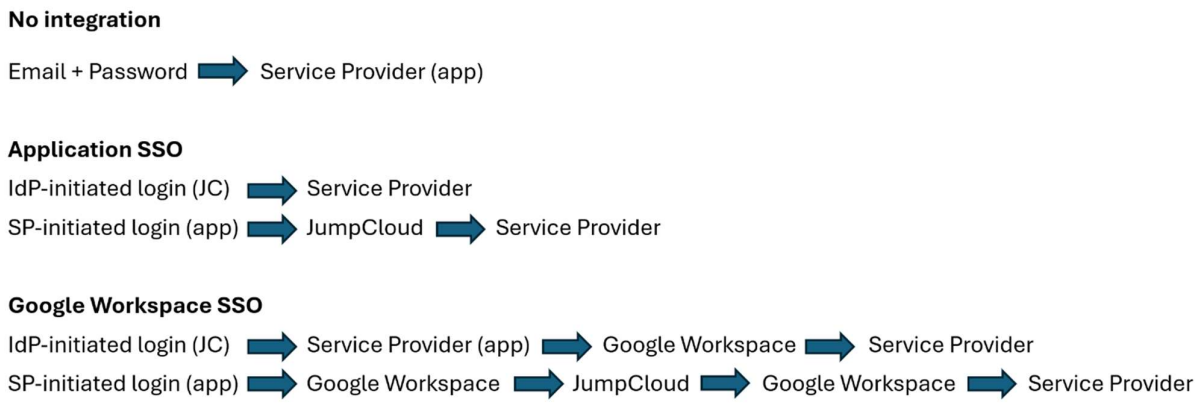

Figure 29 Application login flows without SSO, with Application SSO, and with GWS SSO.

Ultimately, it all comes down to the amount of IT budget and risk acceptance level, which are different in every company. It's suggested that the first method be used – if the budget allows - as the SCIM will mitigate the risks regarding unused accounts. If the SaaS application has a dynamic licensing model so that the user account amount reflects the monthly invoice, the first method might save some money for the company as all licenses are fully utilized all the time, and the company is not overpaying for any application. The human error risk of forgetting to delete the accounts during de-provisioning tasks must be accepted if the company is unwilling to spend money for automated user account deletion by utilizing SCIM.

It's essential to remember that if a person leaves a company and has a user account in a SaaS application that is only registered with an email address and a password and without an MFA, there is a very high risk of the account being exploited if the credentials get compromised. Hence, if the application supports it, enabling the Sign in with Google feature is essential, as the session will expire when the user account is suspended during offboarding tasks after the employee's last working day. Note: resetting the user's password and sign-in cookies before suspending the account is recommended, as some applications do not honor the change, and suspended users can keep using the account with the old password if they have a session open in some device, even though the account is suspended in the GWS.

The instructions on creating the Google Workspace SSO in JumpCloud and configuring it in the GWS console can be found at: https://jumpcloud.com/support/sso-with-google-workspace. Most

applications' SSO can only be made with an all-or-nothing principle, meaning that the SSO is enabled for everyone or no one. However, Google has created a way to exclude some users from the Organization-wide Third-Party SSO Profile or add some users to the Individual Third-Party SSO Profile. Both ways can be used for testing and slowly rolling out the changes. It's worth noting that the Organization-wide Third-Party SSO Profile bypasses Google's two-step verification (2SV) requirement, but the Individual Third-Party SSO Profile does not. If the latter is used, new users will be locked out from Google after the grace period if they don't manually add a 2SV at https://myaccount.google.com/security.

On the last day of writing this thesis, JumpCloud has not yet released the Mobile Device Trust feature, which has left the companies in an awkward position that would like to utilize some of JumpCloud's Zero Trust features, which will be addressed more thoroughly in the next chapter. It's safe to assume that most employees in SMEs use mobile phones to access company resources through the sign-in with Google login mechanism. In this case, the company can decide not to use the Device Trust policy and mobile phones will be granted access. Alternatively, the company can enable the Device Trust policy, which means that all mobile phones (Android, iOS), even enrolled ones, will be blocked from accessing the selected resources. The problem with the first is that it will leave the door open to all devices worldwide, making the company more vulnerable.

The JumpCloud's Platform Vision, Roadmap, and Review webinar on 30.5.2024 will address the Mobile Device Trust, and most probably, the feature will be released for all customers in the third quarter of 2024. After that, JumpCloud customers can adequately protect the resources accessed with all computer and mobile operating systems. (JumpCloud, n.d.-au.)

5 Zero Trust

Zero Trust is widely noted as a paradigm shift in cyber security, a fundamental change. John Kindervag founded the term in 2009, and it's derived from the Russian proverb "trust but verify," which most people heard for the first time when Ronald Reagan jokingly used the expression to Mikhail Gorbachev during the nuclear disarmament negotiations with the Soviet Union back in the 1980s, as both parties did not trust each other (Atwell, n.d-a). I will explain the concept of Zero Trust, why it is mandatory in today's world, and what risks can be mitigated using practical examples everyone understands and can relate to. Let's use Antti, who works in IT, as an example.

Antti goes to the company's office daily. He uses a managed company-owned Windows laptop for work-related tasks that do not have an enterprise endpoint security solution installed. Access to the company resources is solely based on the physical location, meaning the office network, and a username + password combination. Antti has super admin credentials for all applications and systems. Sometimes, when Antti is not feeling well, or if there is a blizzard outside, he works from home, using his personal desktop computer in the living room, which his family members use from time to time with their administrator credentials. As the office's private network protects the company's resources, he uses a VPN application on his computer to connect to the office. The company does not provide any other working tools besides the Windows laptop. However, Antti is a keen Apple fan and wants to work with other devices, so he is accessing company resources with his unmanaged personal devices: an iPad, a MacBook, and an iPhone, which are all old and outdated. Antti doesn't want to use multi-factor authentication as he doesn't like getting time-based one-time passwords to his phone via SMS or mobile applications.

By evaluating the current situation that poses multiple threats to the company, understanding all the risks, and adopting the Zero Trust initiative, the following three most important tenets can be achieved:

1. User identity: Multi-factor authentication must be enforced on all systems so the company can verify user's identities. Network monitoring plays a critical role in this tenet, as suspicious activity, such as login attempts from another side of the world, can be detected and blocked automatically.

2. Device posture: Adversaries can steal Antti's tablet or a mobile phone or infect his personal computers with malware. The solution is that all devices used for work must comply with the company's security policies by enrolling them in a mobile device management system that includes device trust policies.
3. Principle of least access: Employees should only have access to the resources they need for their jobs. A role-based access control can accomplish this. Continuous adaptive trust should be utilized to decide what employees can access at any given time based on the risk score. (Kolide, 2023.)

By using a UEM like JumpCloud, almost all of these tenets can be achieved by enforcing MFA, managing all operating systems with various built-in security policies, keeping the operating system and core applications up to date, protecting the identity by allowing the logins only from a managed device, and giving access to only applications that are relevant to the employee. The continuous adaptive trust or a dynamic risk score that evaluates the device posture and identity's reliability can be calculated with an XDR product, such as CrowdStrike.

5.1 Zero Trust in JumpCloud

JumpCloud's Zero Trust settings can be found in the administrator console's left pane by selecting Conditional Policies. The page has two sections: Default Access Policies and Zero Trust Policies. If the custom Zero Trust Policies are not created, the Default Access Policies will be used. In the Default Access Policies, enabling the Global Certificate Distribution is mandatory if the Device Trust policy is enabled.

The Global Certificate Distribution will install a JumpCloud certificate, also known as a device certificate, to the endpoint. If the certificate is missing from the endpoint, JumpCloud's authentication mechanism does not know if the endpoint is managed or not. Not all web browsers are supported officially by JumpCloud. Suppose the unsupported browsers are not blocked with an EDR solution. In that case, all end users should be notified that some browsers will show a popup that requires the user to confirm the JumpCloud certificate selection when accessing JumpCloud. If the users do not understand the message, they might cancel the selection, which will result in the user being unable to access the application.

Some macOS applications do not open a browser window when authenticating the user. Alternatively, the applications ask the user to enter their credentials to an in-app website within the application. These applications need to be configured as trusted; otherwise, the user will get repetitive keychain password prompts, making the application unusable. By default, JumpCloud has configured these applications as trusted: Keeper Password Manager, Microsoft applications (Excel, OneDrive, OneNote, Outlook, PowerPoint, Teams, Word), and Zscaler. Other applications can be added to this list easily by clicking the plus icon in the Conditional Access Policies and adding the exact name of the application. If the application is not in the system's or user's application folder, the application's location must be added to the Additional Search Location (optional) field. At the bottom of the page, global policy authentication settings can be modified for three different resources. The user portal can be modified with the following options:

- Allow authentication: Allows authentication to the user portal
- Allow authentication & require MFA: Allows authentication to the user portal, which requires multi-factor authentication.
- Deny access: Denies authentication to the user portal
- Require MFA based on user setting: Allows authentication to the user portal, which requires multi-factor authentication if the MFA has been enabled in the user's details

The SSO Applications and JumpCloud LDAP can be modified to allow authentication, with or without MFA, or deny access.

5.2 Zero Trust Policies

At the bottom of the Conditional Access Policies, custom Zero Trust policies can be created for the following resources: User Portal, SSO Applications, and JumpCloud LDAP. The teamTailor application was used as an example for creating the SSO integration in Chapter 4.2, and it will also be used for this thesis's real-life Zero Trust tests. Figure 30 illustrates the policies developed for this thesis, which do not reflect the current status of IPRally Technology's security posture.

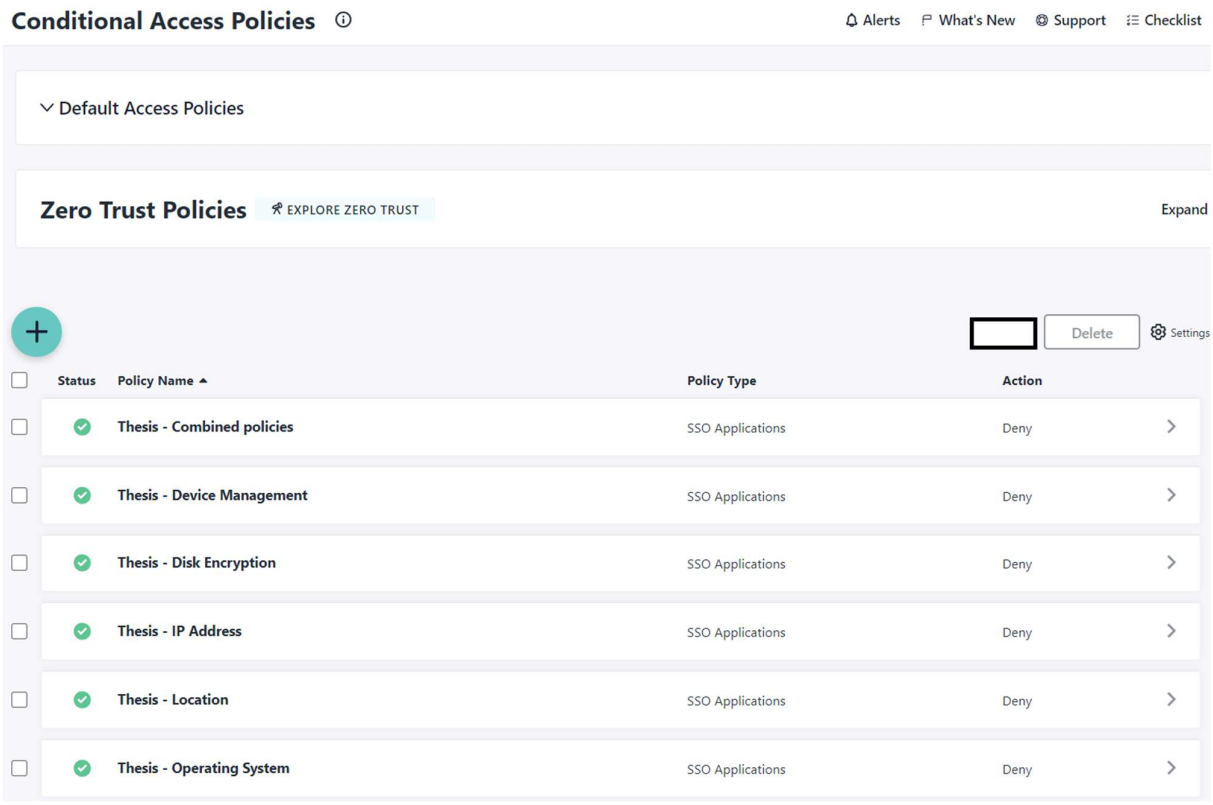

Figure 30 Zero Trust policies

The first step is to click the green plus icon under the Zero Trust Policies and select the SSO Applications. Policy Name and Description can be added in the General Info section, as seen in Figure 31, but only the first one is mandatory. In the Assignments section, all or only selected applications can be chosen. In this case, TeamTailor was selected after clicking the Search field.

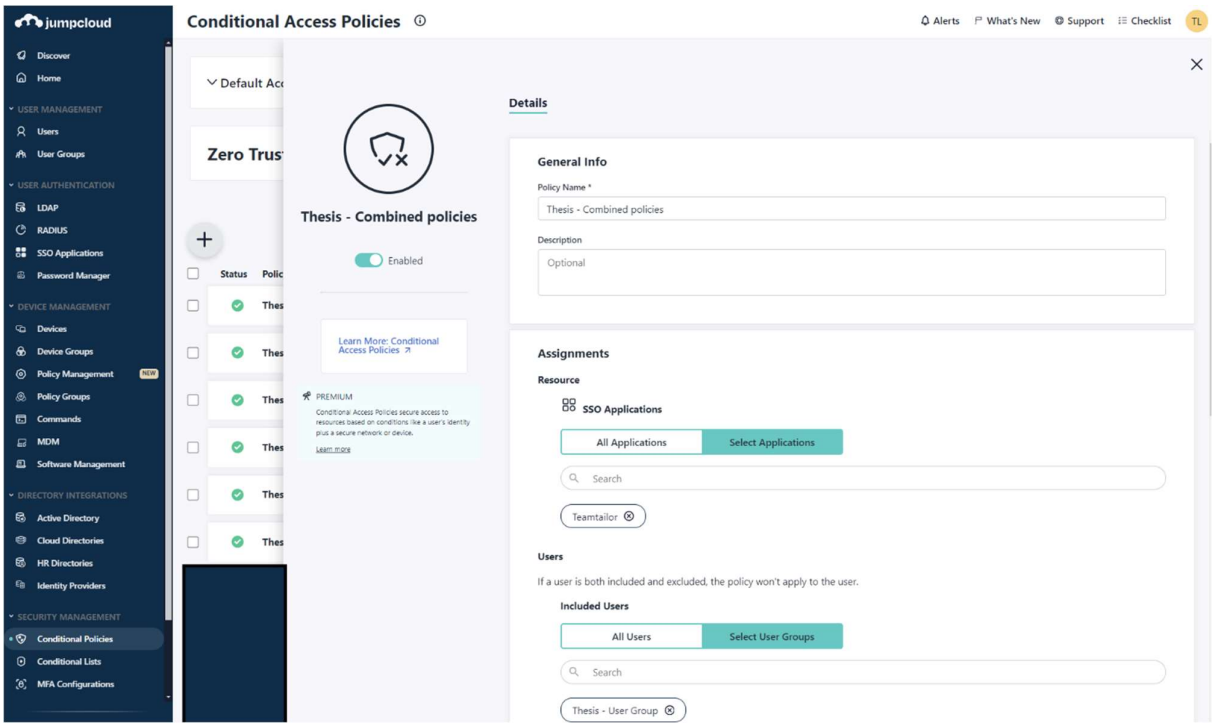

Figure 31 Zero Trust policy's name and assignment

After selecting TeamTailor, user groups can be added to the included or excluded user groups list. Adding user groups to this exclusion list means they are exempt from this Zero Trust policy, and the actions do not apply to them. Exceptions should only be given if there is a business reason and should be reviewed periodically.

Next, five different conditions can be applied to the policy: Device management, Disk Encryption, IP Address, Location, and Operating System. These have been added to “Thesis – Combined policies” for illustrative purposes. However, it’s recommended that all conditions be added to their policies for troubleshooting purposes and more granular control. When the conditions have been selected, the last step is to choose Access and Authentication from the Action section. Both of these are self-explanatory. Access to the selected resource is allowed or denied if the conditions are met. Authentication has two selections: Password and Password + MFA. The latter requires an MFA verification, which is good to have enabled if the user portal can be accessed without an MFA. (JumpCloud, n.d.-aq.)

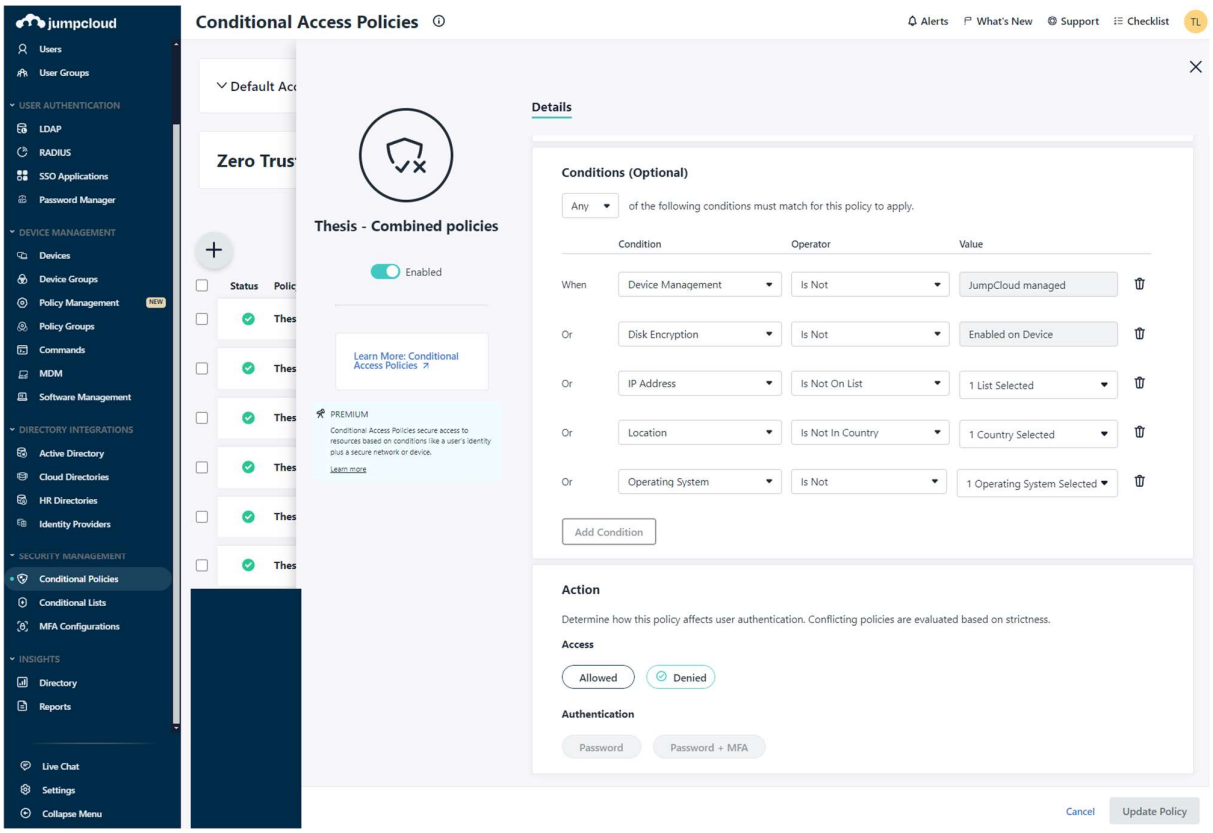

Figure 32 Zero Trust Policy's Combined Conditions and Actions

If any policies fail, the Single Sign-on login attempt will show a similar error message in the user console, shown in Figure 33. The lack of details is due to the nature of the Zero Trust, as JumpCloud does not know if the login attempt was initiated by the company's employee or an adversary. If the error message says that the Location condition does not apply, a malicious actor could change their location easily with a VPN solution.

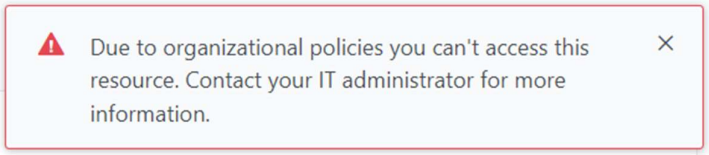

Figure 33 Zero Trust error message after an unsuccessful SSO login from a user perspective

Similarly to the user error message, Directory Insights will also show a generic message for all errors, as shown below in Figure 34. As the Result column shows, the user was only attempting to log in, and it was not an actual authentication for the application, as the Summary wrongly shows.

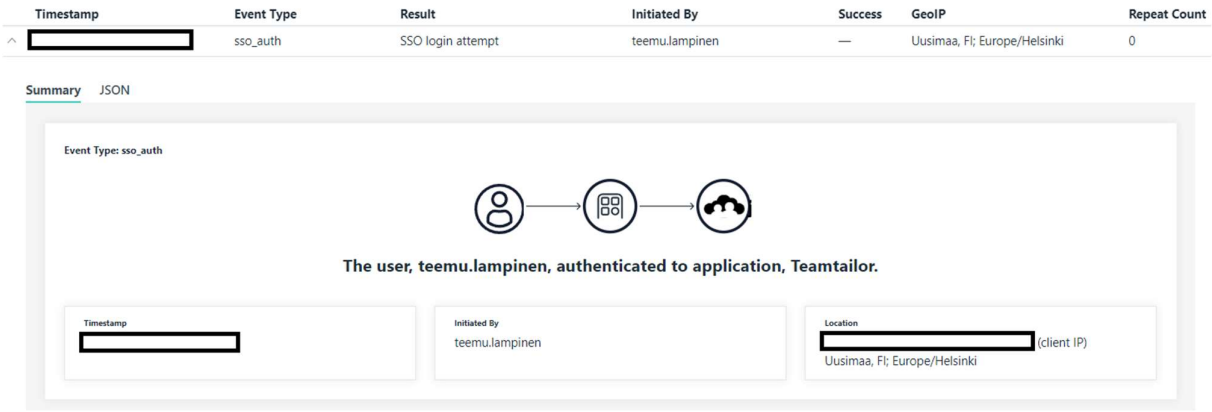

Figure 34 Zero Trust logs of an unsuccessful SSO login from an admin perspective

If an administrator wants to know which Zero Trust policy blocked the access, more details can be found by selecting the JSON text next to Summary. The logs show additional information about the login attempt missing from the summary, such as which policy blocked the access, user name, IP address, operating system's and browser's versions, and whether MFA was used. For this thesis, a login attempt to Teamtailor was made from an unknown IP address from New Zealand using a personal VPN solution and an unmanaged Windows device with disabled disk encryption, hoping to see an error message. As seen in Figure 35, access was blocked as all the conditions failed, as the device was not a managed and encrypted macOS device using the company-provided VPN solution.

```
"auth_context": {
  "auth_methods": {},
  "policies_applied": [
    {
      "metadata": {
        "resource_type": "APPLICATION",
        "action": "DENY",
        "conditions": [
          "IP_ADDRESS",
          "MANAGED_DEVICE",
          "GEOLOCATION",
          "ENCRYPTED_DEVICE",
          "OS_FAMILY"
        ],
        "targets": [
          "USER_GROUP_INCLUSION"
        ]
      },
      "name": "Thesis - Combined policies",
```


Figure 35 Directory Insight logs in JSON format

Device management

The device management policy, also known as device trust, is the most valuable condition, ensuring that only devices enrolled in JumpCloud will be granted access. According to Kolide's Shadow IT report (Atwell, n.d-b), nearly half of companies permit employees to access their resources using devices that the company does not manage. Leaving the door open for all devices causes significant risks for the company, as the employees' personally owned devices can be infected with malware, and adversaries don't need access to the company-owned devices for their malicious acts. The Device Management condition ensures that the user's identity is protected and that the SSO applications, in this case, TeamTailor, can only be accessed from a company-provided and managed device and nowhere else. If the login attempt comes from an unmanaged device, the Directory Insight's logs show that the action was denied as the MANAGED_DEVICE condition failed, as shown in Figure 35. As mentioned in Chapter 4.3, mobile phones are not supported, so the administrators must decide if they block mobile devices altogether from accessing the resources or disable the Device Management feature.

Disk Encryption

Disk Encryption condition can also be added, which works with all operating systems. However, users with Zettabyte File System (ZFS) must be excluded from the policy as JumpCloud does not support it (JumpCloud, n.d.-av). The key benefit of the disk encryption check is not to defend against adversaries, as they can easily encrypt their devices, but to ensure that the company-owned devices' data is always protected. If the disk encryption policy fails and the user is denied access to a resource, they will contact IT, and the policy will be fixed or re-applied. If the login attempt comes from an unencrypted device, the Directory Insight's logs show that the action was denied as the ENCRYPTED_DEVICE condition failed, as shown in Figure 35.

IP Address

The IP Address condition can be added to the Zero Trust policies, meaning that if the network traffic is coming from an address on the list or not in the list, the condition will match. The IP addresses can't be added to the view shown in Figure 32. Before creating the conditional policies, the IP addresses must be added to a list in the Conditional Lists in JumpCloud's left pane. This policy is the 2nd most potent Zero Trust feature, as the VPN solution's or office's IP address can be added to the list, reducing the attack surface and mitigating many networking-related risks. If the login attempt comes from an IP address not added as a value to the selected Conditional List, the Directory Insight's logs show that the action was denied as the IP_ADDRESS condition failed, as shown in Figure 35.

Location

The second last condition is the location. All countries worldwide have a set of public IP addresses that can be found here: https://lite.ip2location.com/ip-address-ranges-by-country. The condition will match if Finland is added to the Condition's value and the network traffic comes from an IP address included in Finland's public IP address pool. It's important to understand that a VPN solution can quickly spoof the IP address. The location condition can be used in two ways. The first method is to allow only countries with employees or VPN gateways. The second is to deny countries that don't have employees or VPN gateways. The problem with the location policy is the working holidays when employees go to a country that is or is not on the list. It's recommended that employees use a VPN solution when accessing company resources from abroad, as people

tend to use unsafe public Wi-Fi networks during their travels. If the login attempt comes from a country added as the value, the Directory Insight's logs show that the action was denied as the GEOLOCATION condition failed, as shown in Figure 35.

Operating System

The last condition is the operating system. A company with only macOS devices could add a rule that Windows, Linux, Android, and iOS operating systems cannot access company resources. Alternatively, they could allow only macOS devices. The key benefit of the operating system rule is that it blocks access from operating systems that employees do not use. Ideally, the operating systems should be narrowed down by chosen SSO applications if all operating systems are used, e.g., all devices can access HR applications, desktop operating systems can access GitHub, and macOS devices can access the asset management system (if the IT team are using only Macs). If the login attempt comes from an operating system added as the value, the Directory Insight's logs show that the action was denied as the OS_FAMILY condition failed, as shown in Figure 35.

Summary

It's highly recommended that Device Management, Location, and operating system conditions be enabled so only enrolled and company-owned devices with correct operating systems can access the resources from selected countries. Disk encryption condition is also recommended so that administrators know immediately if the encryption policy is malfunctioning or has been tampered with. An operating system policy can be added but will only slow down the adversaries. Adding the VPN IP address as one of the conditions is recommended for high-risk applications that contain the most classified data, such as the source code in GitHub. Suppose the office IP address is used as a condition for high-risk applications. In that case, the office network must be well protected using the latest enterprise-grade network security protocol, as the legacy protocols can be easily hacked, as learned in Chapter 3.2.10. However, if the VPN solution is not easy to use and robust, it might cause a bad user experience and negatively impact the respect towards the IT department.

6 Conclusions

Utilizing all of the features together, JumpCloud makes a great Zero Trust product that helps to keep the company's devices and user identities protected. With new advanced features such as temporary elevated privileges, the company can comply with security certificates and apply for them, such as the ISO 27001 or Cyber Essentials. Even though JumpCloud does not currently provide any security framework baselines, making the macOS devices CIS or NIST-compliant is possible using the Jamf Compliance Editor with JumpCloud's command and policies.

I highly recommend JumpCloud for small and medium-sized businesses to manage all systems, such as devices, RADIUS, SSO applications, passwords, remote access, and identities, as having only one tool will reduce the number of applications in use. Using JumpCloud, IT administrators can focus on only one set of documentation, training, certifications, support, release notes, settings, blogs, and community, which gives them more time for other work tasks.

This thesis answered the main research question by listing the Zero Trust key benefits, narrowing the attack surface with multiple policies, and improving the overall security posture with real-life test policies. The second research question was answered with a conclusion that it's not beneficial for an SME to upgrade only a handful of applications' annual licenses with almost $25,000 for the automated de-provisioning feature, and the Google Workspace integration and robust offboarding processes should be used instead.

I learned a lot about JumpCloud during the writing process, and I'm now more prepared to pass the upcoming expert-level certification exam. The Zero Trust mobile device trust feature for Android and iOS is on JumpCloud's roadmap, and unfortunately, it was not released before the deadline of this thesis. For this reason, I could only test the device trust feature with desktop operating systems. The device trust feature can't be utilized for SSO applications accessed with computers and mobile phones. If the device trust feature is enabled, JumpCloud will block access to resources from a mobile phone, even though it's enrolled.

This research would have been expanded by utilizing the quantitative research method to compare different tools with a similar feature set, such as Microsoft Intune. It would also have been

fascinating to audit the enrolled devices against the common security frameworks and create numerical statistics about vanilla operating systems compared to hardened versions. Lastly, the user satisfaction questionnaire's results would have been compared before and after the JumpCloud implementation. These three items combined would make a great thesis topic, and I hope to see someone researching at least one of them.

By obeying the Zero Trust tenets mentioned in Chapter 5, the company's overall security level of devices and identities will be on par with what's widely considered the recommended level as of 2024. The company's security is everyone's job, and everyone should participate in it by reporting unusual activity and marking suspicious emails as phishing attempts. However, the company's IT administrators, such as myself, are more responsible for protecting its resources by keeping the endpoints compliant and ensuring that the company follows Zero Trust's principles. Nothing should be trusted automatically, and all supported conditions should be continuously verified, such as the user's identity, device posture, and access level.

References

Atwell, E. (n.d-a). *The History, Evolution, and Controversies of Zero Trust.* https://www.kolide.com/blog/the-history-evolution-and-controversies-of-zero-trust

Atwell, E. (n.d-b). *Unmanaged Devices Run Rampant in 47% of Companies.* https://www.kolide.com/blog/unmanaged-devices-run-rampant-in-47-of-companies

Apple. (2023). *Sign up for Apple Business Manager.* https://support.apple.com/guide/apple-business-manager/sign-up-axm402206497/web

Apple. (2024). *Service access with Managed Apple IDs.* https://support.apple.com/guide/deployment/service-access-with-managed-apple-ids-depdc4ba8d82/web

Apple. (n.d.). *Manually Adding Devices to Your Organization.* https://it-training.apple.com/tutorials/deployment/dm060

Atera. (2024). *RMM vs. MDM - Which one is best for your IT*. https://www.atera.com/blog/rmm-vs-mdm/

Broadcom. (n.d.). *What is Unified Endpoint Management (UEM)?* https://www.vmware.com/topics/glossary/content/unified-endpoint-management.html

Deepak, H (2024). *Windows LITE-Touch Deployment via Provisioning Package (PPKG).* https://community.jumpcloud.com/t5/jumpcloud-product-news/windows-lite-touch-deployment-via-provisioning-package-ppkg/m-p/3920

Fitzl, C. (2024). *How Malware Can Bypass Transparency Consent and Control (CVE-2023-40424).* https://blog.kandji.io/malware-bypass-tcc

GitHub. (n.d-a). *Baseline*. https://github.com/SecondSonConsulting/Baseline

GitHub. (n.d-b) *Renew*. https://github.com/SecondSonConsulting/Renew

Harding, S. (2024). *Linux market share passes 4% for first time; macOS dominance declines* https://arstechnica.com/gadgets/2024/03/linux-continues-growing-market-share-reaches-4-of-desktops/

IBM. (n.d.). *What is MDM?* https://www.ibm.com/topics/mobile-device-management

JumpCloud. (2021). *JumpCloud Announces $159 Million Series F at a Valuation of $2.56 Billion. https://jumpcloud.com/press/seriesf*

JumpCloud. (n.d.-a). *Policies: Point-and-Click System Management.* https://jumpcloud.com/policy-list

JumpCloud. (n.d.-b). *Policy Group Template Gallery.* https://jumpcloud.com/support/policy-group-template-gallery

JumpCloud. (n.d.-c). *Get Started: Policies.* https://jumpcloud.com/support/get-started-policies

JumpCloud. (n.d.-d). *Get Started: Patch Management.* https://jumpcloud.com/support/get-started-patch-management

JumpCloud. (n.d.-e). *Awards & Recognition.* https://jumpcloud.com/press/awards-and-reviews

JumpCloud. (n.d.-f). *Create a Universal Browser Patch Policy.* https://jumpcloud.com/support/create-a-universal-browser-patch-policy

JumpCloud. (n.d.-g). *JumpCloud APIs.* https://jumpcloud.com/support/jumpcloud-apis

JumpCloud. (n.d.-h) *Understand the JumpCloud Agent.* https://jumpcloud.com/support/understand-the-agent

JumpCloud. (n.d.-i). *Install the JumpCloud PowerShell Module.* https://jumpcloud.com/support/install-the-jumpcloud-powershell-module

JumpCloud. (n.d.-j). *Get Started: Remote Assist.* https://jumpcloud.com/support/get-started-remote-assist

JumpCloud. (n.d.-k). *MFA Guide for Users.* https://jumpcloud.com/support/mfa-for-users

JumpCloud. (n.d.-l). *Enable TOTP MFA for Devices.* https://jumpcloud.com/support/enable-totp-mfa-for-devices

JumpCloud. (n.d.-m). *Get Started: Commands.* https://jumpcloud.com/support/get-started-commands

JumpCloud. (n.d.-n). *Get Started: JumpCloud Go™.* https://jumpcloud.com/support/get-started-jumpcloud-go

JumpCloud. (n.d.-o). *Use JumpCloud Go™.* https://jumpcloud.com/support/use-jumpcloud-go

JumpCloud. (n.d.-p). *Manage Software for Windows Devices with Chocolatey.* https://jumpcloud.com/support/software-management-windows

JumpCloud. (n.d.-q). *Manage Self-Hosted macOS Apps.* https://jumpcloud.com/support/software-management-macos

JumpCloud. (n.d.-r). *Software Management: Android.* https://jumpcloud.com/support/software-management-android

JumpCloud. (n.d.-s). *MDM Commands*. https://jumpcloud.com/support/mdm-commands

JumpCloud. (n.d.-t). *Get Started: System Insights.* https://jumpcloud.com/support/system-insights

JumpCloud. (n.d.-u). *JumpCloud Reports.* https://jumpcloud.com/support/jumpcloud-reports

JumpCloud. (n.d.-v). *Get Started: Directory Insights*. https://jumpcloud.com/support/directory-insights

JumpCloud. (n.d.-w). *Run the MAID Import Script.* https://jumpcloud.com/support/run-the-maid-import-script

JumpCloud. (n.d.-x). *Add Personal Apple Devices to MDM with User Enrollment.* https://jumpcloud.com/support/add-personal-apple-devices-to-mdm-with-user-enrollment

JumpCloud. (n.d.-y). *Users: Enroll Your Personal iOS Device.* https://jumpcloud.com/support/users-enroll-your-personal-ios-device

JumpCloud. (n.d.-z). *Create an iOS Supervised Restrictions Policy.* https://jumpcloud.com/support/create-ios-supervised-restrictions-policy

JumpCloud. (n.d.-aa*). Take Over an Existing User Account with JumpCloud.* https://jumpcloud.com/support/take-over-an-existing-user-account-with-jumpcloud

JumpCloud. (n.d.-ab). *Get JumpCloud Certified.* https://university.jumpcloud.com/pages/get-jumpcloud-certified

JumpCloud. (n.d.-ac). *JumpCloud Agent Compatibility, System Requirements, and Impacts* https://jumpcloud.com/support/agent-compatibility-system-requirements-and-impacts

JumpCloud. (n.d.-ad). *Manage Software with JumpCloud Private Repository.* https://jumpcloud.com/support/manage-software-with-jumpcloud-private-repo

JumpCloud. (n.d.-ae). *Manage Software for Windows with Microsoft Store*. https://jumpcloud.com/support/manage-software-for-windows-devices-with-microsoft-store

JumpCloud. (n.d.-af). *Add and Manage Android Devices.* https://jumpcloud.com/support/add-and-manage-android-devices

JumpCloud. (n.d.-ag). *Install the Linux Agent.* https://jumpcloud.com/support/install-the-linux-agent

JumpCloud. (n.d.-ah). *JumpCloud Agent Windows Installation Walkthrough.* https://jumpcloud.com/support/jumpcloud-agent-windows-installation-walkthrough

JumpCloud. (n.d.-ai). *Contact JumpCloud Support.* https://jumpcloud.com/support/contact-jump-cloud-support

JumpCloud. (n.d.-aj). *Getting Started with JumpCloud Professional Services* https://jump-cloud.com/professional-services

JumpCloud. (n.d.-ak). *JumpCloud Blog.* https://jumpcloud.com/blog

JumpCloud. (n.d.-al). *The IT Hour.* https://community.jumpcloud.com/t5/the-it-hour/bd-p/ITHour-forum-board

JumpCloud. (n.d.-am). *JumpCloud Webinars.* https://jumpcloud.com/resources/type/webinars

JumpCloud. (n.d.-an). *Release Notes and Bug Fixes.* https://jumpcloud.com/support/category/re-lease-notes-and-bug-fixes

JumpCloud. (n.d.-ao). *Get Started: Google Workspace Integration.* https://jumpcloud.com/sup-port/google-workspace-integration-overview

JumpCloud. (n.d.-ap). *Automate Onboarding and Offboarding.* https://jumpcloud.com/solu-tions/automated-onboarding-offboarding

JumpCloud. (n.d.-aq). *Configure a Conditional Access Policy.* https://jumpcloud.com/support/con-figure-a-conditional-access-pol

JumpCloud. (n.d.-ar*). The People Behind the Connections*. https://jumpcloud.com/about-us

JumpCloud. (n.d.-as). *What is the Value of JumpCloud?* https://jumpcloud.com/resources/what-value-of-jumpcloud

JumpCloud. (n.d.-at). *Single Sign-On (SSO).* https://jumpcloud.com/platform/single-sign-on

JumpCloud. (n.d.-au). *JumpCloud's Platform Vision,* Roadmap, and Review. https://jump-cloud.com/resources/jumpclouds-q2-2024-product-roadmap

JumpCloud. (n.d.-av). *Configure Data Encryption for Linux Devices. https://jumpcloud.com/sup-port/configure-data-encryption-for-linux-devices*

Klaassen, J (2024). *[macOS/iOS] How to make use of the Jamf Compliance Editor along with Jump-Cloud and Custom Policies?* https://community.jumpcloud.com/t5/jumpcloud-product-discus-sions/macos-ios-how-to-make-use-of-the-jamf-compliance-editor-along/m-p/4399

Kolide. (2023, Dec 19). *What is Zero Trust Security?* [Video]. YouTube. https://youtu.be/i3Xxhef-bUY8?feature=shared

Lake, K. (2021). *Overview of Cloud LDAP.* https://jumpcloud.com/blog/overview-of-cloud-ldap

Lake, K. & Worthington, D. (2023). *JumpCloud Password Manager.* https://jumpcloud.com/blog/password-manager

Lee, B. (2022). *JumpCloud HRIS — How JumpCloud Makes it Happen.* https://jumpcloud.com/blog/how-jumpclouds-hris-integration-works

Lundmarck, E. (2024). *Using SSO (Single sign-on) with Teamtailor.* https://support.teamtailor.com/en/articles/1272018-using-sso-single-sign-on-with-teamtailor

Niedringhaus, C. (2020). *Difference Between JIT and SCIM Provisioning.* https://jumpcloud.com/blog/jit-scim-provisioning-comparison

Null Byte. (2018). *Cracking WPA2 Passwords Using the New PMKID Hashcat Attack*. https://nullbyte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/

Okta (n.d.). *The State of Zero Trust Security 2023*. https://www.okta.com/state-of-zero-trust/

Phan, B. (2023). *[Security Update] June 20 Incident Details and Remediation.* https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation

Stack Overflow. (n.d.). *2023 Developer Survey – Operating system.* https://survey.stackoverflow.co/2023/#section-most-popular-technologies-operating-system

Vanhoef, M. (2017). *Key Reinstallation Attacks.* https://www.krackattacks.com/