

Guide

# **Implementation Guide** Users & Devices

### **Get to Know JumpCloud**

JumpCloud is a comprehensive and flexible cloud directory platform. From one pane of glass, manage user identities and resource access, secure macOS, Windows, and Linux devices, and get a full view of your environment.



As you implement JumpCloud into your organization it is important to understand the best practices related to getting your existing users onboarded, enrolling devices while taking over existing user accounts, integrating with existing IT tools, and enabling user access to all their resources. Implementing resources in piecemeal fashion without a cohesive plan could result in wasted time and a poor user experience. For example, users who come from a preexisting directory (e.g., Active Directory/Azure AD) or an MDM will have a different implementation pathway than organizations implementing a directory platform solution for the first time. Be sure to take advantage of the following resources to streamline your implementation.

#### Sign up for an account in JumpCloud University!

Check out this easy-to-follow infographic for the steps to register for a free account.

JCU gives you access to many resources including interactive courses, short tutorial videos, hands-on practice with guided simulations, and help from our experts. Plus, your progress is saved and tracked as you go.

This quick 30-minute course is a great introduction to JumpCloud and is designed to help familiarize you with JumpCloud University.



What is JumpCloud?

#### **Become certified through JCU!**

Why get certified:

- Feel more confident in your ability to use the JumpCloud platform.
- Be the go-to JumpCloud admin for your IT org.
- Showcase your skills by displaying your certification badge on your professional profiles.

### Phase 2: Users

### **Adding Users From an Existing Cloud Directory**

#### 1. Obtain Cloud Directory Admin Credentials

You will need administrator access to your current cloud directory to begin importing users.

JumpCloud integrates with a variety of popular directory services to synchronize user accounts. These integrations let JumpCloud act as an authoritative directory with a single set of credentials that can be used across all directory services. When you integrate with a directory service, you can securely import existing user accounts as well as persistently replicate data across directories. You're in control of which users get replicated.

#### 2. Navigate to the Cloud Directories Menu



#### 3. Create a new directory, and provide a display name

- 1. Select Cloud Directories under Directory Integrations.
- 2. Select the (+) and choose your company's cloud directory to import from the following:
  - Import from Google Workspace
  - Import from M365/ Azure AD
  - Real-time import from Okta
  - Import JumpCloud LDAP into Okta
- 3. Enter the directory name in the Directory Name field. Then select authorize sync.

+			1 directory
Туре	Name 🔺	Token Status	
<b>.</b>	JumpCloud M365 M365/Azure AD	O Token expired	>
		Set Up a New M365/Azure AD Directory ×	
		You can import and sync users from multiple M365/Azure AD directories. Create a custom name to help you identify this directory in the Directories list, then click Authorize Sync to give JumpCloud control to provision, deprovision, and sync user accounts.	
		Directory Name ex: Jump Cloud The Directory Name field is required	
		Don't authorize the same M365/Azure AD directory more than once. Learn More	
		cancel authorize sync	

4. Utilize the cloud directories admin credentials already obtained to sync with JumpCloud.

Check out these Knowledge Base articles for more details:

Importing Office 365 Users
 Importing G-Suite Users
 Configure Okta Real-time User and Password Import

#### **Importing Users from CSV**

#### **Considerations:**

- Each user you import must be a unique user with a unique email address.
- CSV file headings are case sensitive and will fail if they don't match JumpCloud's expected case. To see the case JumpCloud is expecting, you can download the CSV template and update the headings of the file you want to import accordingly.
- Users without passwords are imported into JumpCloud in an inactive state.
- Users created with or without a password are not sent an activation email on CSV import.
- You can also import users from a CSV file using JumpCloud's PowerShell Module.

Importing Users into JumpCloud from CSV Using the PowerShell Module

**Note:** Keep in mind that the functionality between the two CSV import methods differs.

#### Importing Users from the JumpCloud Admin Portal vs. PowerShell Module

Keep the following differences in mind as you decide whether to import users from CSV into the Admin Portal or the PowerShell Module:

- Users imported from CSV into the Admin Portal can't automatically be connected to user groups. You can create group associations using the PowerShell Module.
- Users imported from CSV into the Admin Portal can't automatically be connected to systems. You can create system associations using the PowerShell Module.
- Users imported from CSV into the Admin Portal can only be created with the following attributes:
  - 1. First Name
  - 2. Last Name
  - 3. Username
  - 4. Email
  - 5. Password
- You can import users from CSV with more than the previously mentioned attributes using the PowerShell Module.

#### To add users via CSV in the Admin Portal:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to USER MANAGEMENT > Users.
- 3. Select (+), then select Import from CSV user entry.



4. You will need to download the CSV template first. Please select Download CSV Template.



5. Once you've downloaded the CSV template, fill it out using the template form and save the CSV with all of your users.

Below are the contents and format of the CSV:

firstname,lastname,username,email,password

You must adhere to the CSV format with these five attributes.

**Note:** If you put passwords in the CSV, this will add the users in an activated state with the password you entered in the CSV. Users will not be automatically emailed an activation or welcome email from JumpCloud.

6. When you've finished compiling the CSV, you can then select Upload CSV for Import and upload the CSV you just made.



7. Once you've selected your CSV from your local file folder where it's stored, select Upload.



8. The next screen shows all of the users you just added to the CSV.

Impo	Import from CSV										
	First Name	Last Name 🔺	Email	Username							
	Bob	Fay	bob.fay@csjumpcloud.com	bob.fay							
Currently i 19 use	in JumpCloud TS			<u>cancel</u>	import						

- 9. Select all of the users by selecting the top left checkbox button.
- 10. You will see all of the users with a checked checkbox now. Optionally, you can now change any of the attributes in this list if you need to, such as email address or username.

Impo	ort from CSV				×
	First Name	Last Name 🔺	Email	Username	
	Bob	Fay	bob.fay@csjumpcloud.com	bob.fay	

11. Next, select the Import button in the bottom right to fully import the users into JumpCloud.

Impo	rt from CSV				×
	First Name	Last Name 🔺	Email	Username	
	Bob	Fay	bob.fay@csjumpcloud.com	bob.fay	
0					
19 user	JumpCloud S			cancel	import

- 12. This pane will go through the entire user list and add them into JumpCloud. For larger batches over 100 users, this could take several minutes.
- 13. Once completed, as indicated by a green checkmark next to the user entry, you can download the confirmation CSV by selecting the download CSV button in the bottom right, or you can close the window by hitting the close button in the bottom right.

Import from CS	v					×
Add user attributes a resources Add user attributes, assign add to a user group Go to Users	and assign n a device or directory, or	Add users to user groups Assign user groups to give users the correct acces to the resources they need Go to User Groups	S	Add users to device groups Assign device groups to give users the right le access to multiple devices Go to Device Groups		
FIRST NAME	LAST NAME	EMAIL	USER	NAME	IMPORT RESULTS	
🕗 Bob	Fay	bob.fay@csjumpcloud.com	bob.fa	ау	Success: User Imported	
					close download CSV	

#### Navigate to Users Menu in JumpCloud Admin Portal

1. For User Management, navigate to Users in JumpCloud Admin Portal.

n jumpcloud	Home			\$ Alerts	D Resources	@ Support CB
<b>Ø</b> Discover						
• 🙆 Home						
✓ USER MANAGEMENT	Welcome,			Manage Home		
Q Users						
x¶n. User Groups		_				
✓ USER AUTHENTICATION	23 15	7	9	51		
	Users User Groups	Managed Devi	ces Managed Software	Device Policies		
(* RADIUS						
SSO						
* DEVICE MANAGEMENT	0 🥝 4	0	0 S	0 🥝		
C Devices	User Lockouts Expired Pass	words	Expirations	New Users (Past 7 Days)		
Device Groups						
Policy Management NEW		6		16		
Policy Groups	Device Notifications	6	User Notifications	10		
🖬 Commands	Devices inactive greater than 7 days	6	Users with admin sudo access	2		
Ć MDM			Users with admin sudo passwordles	s access 1		
Software Management			Users with no password on file	12		
✓ DIRECTORY INTEGRATIONS			Users with samba access	1		
🗟 Active Directory						
Cloud Directories						
📾 HR Directories	Recent OS Releases (Past 14 Days)	10				
	MacOS	3				
Settings						
Account	Windows	7				
<ul> <li>Collapse Menu</li> </ul>	Ubuntu	0				

#### 2. Select the newly imported users to access their information.

**Note:** You can select more than one user at a time.

m jumpcloud	Use	ers 🛈				ပံ Alerts 🖸 Resources 👁 Su	upport CB
C Discover	All	23 Staged	11 Active 9 Suspende	:d 3			
USER MANAGEMENT	+	Q Search			filter by - 23 users	change state + more actions +	delete
VUSER AUTHENTICATION		User State	Name •	Email	Password Status	columns +	t export <del>v</del>
C RADIUS					•		-
DEVICE MANAGEMENT     Co Devices							<u>.</u>
<ul> <li>∂ Device Groups</li> <li>⊘ Policy Management NUW</li> </ul>							
<ul> <li>Policy Groups</li> <li>Commands</li> <li>Units</li> </ul>		Staged	Aduma, John john.adumu	john.aduma@demo.jumpcloud.com	Password pending	NOT ENROLLED	>
රු MDM ඬ Software Management							
DIRECTORY INTEGRATIONS     Active Directory     Cloud Directories							
HR Directories     SECURITY MANAGEMENT							
<ul> <li>Conditional Policies</li> <li>Conditional Lists</li> </ul>							
(8) MFA Configurations							
Setungs     Account     Collapse Menu							

3. Select the Directories tab for this user, and bind to the cloud directory.

iumpcloud	Us	ers 🛈						ධ Alerts 🖸 Resources 🔇	) Support CB
ර Discover බ Home	All	23 Stage							×
<ul> <li>✓ USER MANAGEMENT</li> <li>● Q Users</li> <li>♠ User Groups</li> </ul>	e	Q Sear	(2)	Det Joh	tails U: n Aduma h	ser Groups Devices Directories as the selected directories enabled:			3 directories
- USER AUTHENTICATION		User State	$\bigcirc$		Туре	Name 🔺	Token Status	Access Configurations	a directories
C RADIUS		Active	John Aduma		1	DC=DEMOJUMPCLOUD;DC=COM Active Directory Domain			
SSO     DEVICE MANAGEMENT		Active	Implementation Engineer Implementation		1	JumpCloud LDAP			
C Devices		Active	Current State Change -		<b>(</b>	JumpCloud M365 M365(Azure AD	O Token expired		
Policy Management     Netw     Policy Groups     Commande		Staged	Staged						
رغ MDM Diftware Management		Suspended	Password Pending     TOTP MFA Inactive						
DIRECTORY INTEGRATIONS     Active Directory     Claud Directories		Staged	<ul> <li>JumpCloud Protect Inactive</li> <li>WebAuthn Inactive</li> </ul>						
HR Directories		Suspended							
SECURITY MANAGEMENT     Conditional Policies     Conditional Lists		Active							
(e) MFA Configurations		Active							
Settings     Account     Collanse Manu		Staged						-	67000 U.S.O.T
Collapse Menu								cancel	save user

#### Bind a User to the JumpCloud Directory

Please follow the instructions in these Knowledge Base icon articles:

- Binding JumpCloud Users to Microsoft 365
- Binding JumpCloud Users and Groups to Google Workspace

#### After the User Is Bound

- 1. The user will receive a Get Started email that requires them to set a JumpCloud password, and in turn update their cloud directory password.
- 2. The user will become active within JumpCloud.

#### **Create User Groups to Align with Org Layout**

JumpCloud saves you time by letting you create groups of users, devices, and policies. Performing groupbased assignments on resources can save you time.

**User groups** grant users access to resources, and connect the resources you want users to be able to access (applications, LDAP resources, networks, and more).

#### Complete the following steps to create a user group:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to USER MANAGEMENT > User Groups.
- 3. Select (+). The Details tab appears by default.

Us	er Groups <sup>①</sup>	Alerts II Resources O Support
4	- Q SI	×
	Type 1	Details Users Device Groups Applications RADIUS Directories
0		Group Configuration
	• · K Y	Engineering
	• Engineering &	Description
	•	
0	•	Enable users as Administrator/Sudo on all devices associated through device groups     O     Create Linux group for this user group
0	•	Enable Samba Authentication
	•	Custom Attributes Create and store custom attributes for users in this user group. Attribute field names must be unique. Conflicting attributes set at the user level will override attributes set at the group level. These attributes can
	•	be used on SSO Applications. Learn more about how to use group inherited attributes.
	•	add new custom attribute •
0	•	
	O I	
0	•	Cancel Save

- 4. For the Name field, enter a description or purpose for the group name.
- 5. For the Description field, enter the purpose of the group.
- 6. (Optional) Under Custom Attributes, select add new custom attribute and choose an attribute.

**Custom User Attributes** 

#### Adding Users to the Group

#### Complete the following steps to add users to the group:

- 1. On the New User Group panel, select the Users tab.
- 2. Select users from the list.
- 3. Select Save.

JumpCloud	Us	er Gro	ups	6 (i)					¢	Ш	?	RK 🗸
✓ USER MANAGEMENT	Ŧ	٩	N	ew U	ser Gr	oup						
A Users		Туре										
• AR User Groups	_	0	De	etails	Users	Device Groups	Applications	RADIUS	Directori	es		
✓ USER AUTHENTICATION	U	69	The	e followi	ng users	are members of this	user group:					
Co LDAP		•	Q	Search					99 users	s show bound users (0)		
C RADIUS		-		ocuren					bb users		in bound	45615 (6)
SSO (SAML)		-		Status	Name 🔺		Email					_
✓ DEVICE MANAGEMENT		-		•	<u>Mark</u> mshortride	ge	mshortridge@d	emojumpcloud.	com			
C Devices		Ŧ	_		Mirna		mzungn@domc	iumpolaud com				
🔂 Device Groups	_	•	U	-	mzupan		mzupan@demo	gumpcioua.com				

Additionally, JumpCloud has a tutorial, course, and module on User & Device Groups.

#### **Enroll Users in MFA**

Use multi-factor authentication (MFA) with JumpCloud to secure user access to your organization's resources. Admins can use Verification Code (TOTP) MFA, Duo Security MFA, WebAuthn MFA, and Push MFA to strengthen security in their organization.

JumpCloud MFA Guide

#### **Requiring Multi-Factor Authentication on an Individual User Account**

To require MFA on an individual user account:

- 1. Go to User Management > Users.
- 2. Select a user to view their details. See Getting Started: Users.
- 3. In the User Security Settings and Permissions section, select Require Multi-Factor Authentication for User Portal.

• USER MANAGEMENT		$\bigcirc$	Highlights Details User Groups Devices Directories
• A Users	Q Sear	$\left( \begin{array}{c} \\ \\ \\ \\ \end{array} \right)$	Creation data: ID10 Distinguished Name
<b>ሐዋ</b> ሉ User Groups			2019-07-05T16:39:43.905Z uid=super.admin,ou=Users,o=5b0edf4aa82efb07403515d3,dc=jumpcloud,dc= com
✓ USER AUTHENTICATION	User State	$\smile$	• These fields are set to read-only for your users and they must contact you to make changes. Go to the
🗟 LDAP		Super Admin	settings tab to turn this off.
🖑 RADIUS	Active	super.admin@demojumpcloud.com	
sso sso			
✓ DEVICE MANAGEMENT	Active	Current State Change -	✓ User Security Settings and Permissions
🗅 Devices		Active	
🔂 Device Groups	Active		<ul> <li>Employment Information</li> </ul>
Policy Management NEW		Security Status	
Policy Groups	Staged	<ul> <li>Password Active -</li> </ul>	✓ Personal Employee Information
Commands	otagou	password never expires	
Ć MDM		<ul> <li>TOTP MFA enrollment expired -</li> </ul>	
Software Management	Suspended	Jume Olaud Broteat Inactive	Custom Attributes

- 4. Specify the number of days the user has to enroll in TOTP MFA before they are required to have MFA at login. You can specify a number of days between 1 and 365. The default value is 7 days. The enrollment period applies only to TOTP MFA and not to other MFA factors.
- 5. Select save user. After you save, users are notified in an email and are prompted to set up TOTP MFA the next time they log in to their User Portal.
- 6. During enrollment, the user's details indicate how much time remains on their enrollment period.
- 7. After the enrollment period expires, the user is locked out of the User Portal.

## **Phase 3: Devices**

#### **Identify Initial Devices to Test Deployment Methods**

You can connect Mac, Windows, and Linux devices to JumpCloud by installing the JumpCloud agent. Check JumpCloud Agent Compatibility, System Requirements, and Impacts before you install an agent. After the agent is installed and connected to a device, you can:

- Remotely and securely manage the device and its user accounts and policies.
- Enable MFA.
- Create, modify, and disable local user accounts.
- Manage SSHD configuration (Linux).
- Enforce MFA on Windows, Mac, and Linux SSH.
- Execute <u>commands</u>.

#### **Adding Windows and Linux Devices**

To add a new device:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to DEVICE MANAGEMENT > Devices.
- 3. Select the Devices tab.
- 4. Select (+). The New Device panel that appears contains various device tabs. Each tab includes information about downloading and installing the JumpCloud agent for that device's OS. You can also read the following about installing agents from the <u>command line</u>, <u>template or system image</u>, or the <u>JumpCloud API</u>.
- 5. (Optional) You can add the JumpCloud agent to your <u>allow list</u> with your antivirus vendor.
- 6. After installation completes, the agent checks in with JumpCloud and is active in the Admin Portal. You can view details about the device on the Device panel.

Watch this video about installing the agent remotely:



This Knowledge Base article shows you how to install the agent from the User Portal:

Installing the JumpCloud Agent from Your User Portal

#### Adding Apple Devices Using MDM

Configure JumpCloud as a Mobile Device Management (MDM) server by establishing a secure connection between Apple and JumpCloud using certificate-based authentication. You can use a push certificate to establish a secure connection between JumpCloud and Apple Push Notification service (APNs). MDM lets you securely and remotely configure your organization's devices, including updating software and device settings and monitoring compliance with your organization's policies.

In order to get the most out of JumpCloud with your Apple devices, you must enroll your devices in JumpCloud's MDM. If you do not enroll your macOS devices in MDM, you will not be able to use the following JumpCloud features:

Policy Management

Note: As a prerequisite, you will need an Apple ID and password.

- Software Management
- Remote lock, Restart, Shutdown & Erase Security Commands
- Zero-Touch Enrollment
- OS Patch Management

#### Configuring Your JumpCloud MDM Server

You must download a Certificate Signing Request (CSR) from the JumpCloud Admin Portal. The unique CSR contains your organization's MDM configuration within JumpCloud. Next, you log in to the Apple Push Certificate Portal and upload the CSR file. Apple validates JumpCloud's information and issues a push certificate with the public key included in the CSR. After you download the push certificate, you upload it to JumpCloud to create a secure connection. You need to renew the certificate yearly.

#### To configure MDM:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to DEVICE MANAGEMENT > MDM.
- 3. On the MDM homepage, select Configure MDM.
- 4. Under Download Your CSR, select download and save the file.

m jumpcloud	MDM	Pricing	↓ Alerts	III Resources	③ Support	NH
Contract Home	Set Up Apple MDM Certificate					
✓ USER MANAGEMENT	Set up Apple MDM to unlock additional services across your organization such as remote lock or erase. You can't enroll devices until you upload your MDM push certificate.					
A Users	Before you get started with MDM, here's what you'll need:					
APA. User Groups	Role-based apple ID (i.e. itadmin@example.com)     A					
<ul> <li>USER AUTHENTICATION</li> </ul>	ABM Account >					
🔂 LDAP	Apple Push Notifications Service Certificate (APNS Cert.) >					
C RADIUS	A Mac device, or a virtual machine					
sso sso	If you don't have access to these resources, or don't need the capabilities offered by Apple MDM, use our proprietary protocol to manage your mac devices in the JumpCloud console.					
✓ DEVICE MANAGEMENT						
Q Devices	Described Very CSD					
Device Groups	Use the Certificate Sonina Request (CSR) to establish trust between Apole and your organization using JumpCloud's MDM credentials. You need this for the next step in Apole's Push Certificate	e Portal.				
Policy Management	demonstrat					
Policy Groups						
Commands						
• Ć MDM	Sign in to Apple					
Software Management	uns jour company a represe discussana o agri ni company and create a new continuero na your organizations.					
<ul> <li>DIRECTORY INTEGRATIONS</li> </ul>						
Active Directory	3 Upload MDM Push Certificate					
Cloud Directories	To finish setting up your connection, upload MDM_JumpCloud IncCertificate.pem. You downloaded this file from Apple and can find it in your Downloads folder if you saved it to the default is	ocation.				
B HR Directories	P					
· SECURITY MANAGEMENT						
S Conditional Policies	Browse or drag your file here					
Conditional Lists	S					

- 5. Under Sign in to Apple, select sign in to Apple or log in to the <u>Apple Push Certificate Portal</u>.
- 6. Select Create A Certificate.



#### Enroll Devices into MDM using Mac MDM policy

After you configure JumpCloud's MDM server, you can enroll your macOS, iOS, and iPadOS devices in MDM. MDM lets you securely and remotely configure your organization's devices and update software and device settings.

There are a variety of ways to enroll company-owned and personal devices.

Enrollment Methods	Company-Owned macOS	Company-Owned iOS, iPadOS	Personal iOS, iPadOS
Automated Device Enrollment with Supervision	~	~	×
Device Enrollment	~	~	×
User Enrollment	×	×	(iOS and iPadOS only)

You can enroll Apple devices in MDM with these enrollment methods:

- Apple's automated device enrollment Remotely enroll company-owned macOS Apple devices • in MDM so that you can securely configure and deploy devices. The device must be added to your Apple Business Manager (ABM) or Apple School Manager (ASM) account. Supervision can provide additional control over a device.
- Device enrollment If a company-owned iOS device was not added to ABM or ASM, you can't • use Apple's Automated Device Enrollment. Instead, you can go to the JumpCloud Admin Portal and scan the QR code or you can download the enrollment profile to enroll the device in MDM. Device enrollment is supported for devices that run iOS 13 and later.
- User approval You can enroll personal iOS and iPadOS devices in MDM so that users can access ٠ company resources. These devices must run iOS 13 and later, and are owned by the user and enrolled by the user.

This Knowledge Base article covers these MDM enrollment methods:

Choosing an MDM Enrollment Method

For more information on MDM, check out this short course:

Intro to MDM

#### **Assign Users to Their Respective Devices**

View the article(s) relevant to the devices you are trying to connect to JumpCloud.



Connecting Users to Windows Devices

Connecting Users to macOS Devices

n jumpcloud	Device Groups <sup>①</sup>	↓ Alerts 🖽 Resources 💿 Support 🛛 PK
ゆ Discover 合 Home	Q Sear	×
USER MANAGEMENT	Type G	Details Devices User Groups Policies Policy Groups
USER AUTHENTICATION		Group Configuration
C Devices		Name
• 🔂 Device Groups	New Device Group	
<ul> <li>Policy Management NEW</li> <li>Policy Groups</li> </ul>		Description
Commands		
C MDM	G	
Software Management		
	6	
Cloud Directories		
B HR Directories	G	
Settings		
Collapse Menu	n en fi	cancel save

#### **Create Device Groups**

Complete the following steps to create a device group:

- 1. Log in to the <u>JumpCloud Admin Portal</u>.
- 2. Go to DEVICE MANAGEMENT > Device Groups.
- 3. Select (+) to add a new device group.
- 4. Enter the device group Name.
- 5. (Optional) Enter a short Description of the group's purpose.
- 6. Select save.

#### Adding Devices to the Device Group

Complete the following steps to add devices to the device group:

n jumpcloud	Device Groups <sup>①</sup>		
۞ Discover ⓒ Home	+ Q Sear		×
USER MANAGEMENT	C Type G	Details Devices User Groups Policies F	Policy Groups
USER AUTHENTICATION		The following devices are members of this device group:	
DEVICE MANAGEMENT     Devices		Q Search	96 devices Show bound devices (0)
• 🔂 Device Groups	New Device Group	Status Device Name	OS
Policy Management     NEW		Abbie's Windows 10 VM	Windows 10 Pro
Ø Policy Groups			
Commands		BLAIRSWARTZ5AF9	Windows 11 Home
Software Management		BabeRuthWin10P-Cruz	Windows 10 Pro
DIRECTORY INTEGRATIONS		CHASEDOELLIB20E	Windows 11 Pro
SECURITY MANAGEMENT			
INSIGHTS	e e	DAVIDWORTHIC352	Windows 11 Home
Settings		DESKTOP-GNLJAVN device	Windows 10 Pro
<ul> <li>Collapse Menu</li> </ul>	n fi		<u>cancel</u> save

#### **Configure and Test Commands (if applicable)**

You can run JumpCloud commands to execute scripts on fleets of machines through JumpCloud's system agent. You can deploy files, schedule maintenance activity, or install software on endpoints in PowerShell, Bash, Shell, and more. Commands can run across one or more devices in parallel and retrieve command results (including stdout, stderr, and exit codes).

Commands let you quickly and easily automate tasks across multiple servers, launch those tasks based on a number of different types of events, and get full auditing of all command results. From the commands list, you can quickly run or delete a command using the Run Now or Delete buttons.

<b>m</b> jumpcloud	Co	mmands						Pricing © Alerts (2) Resources	) Support
G Home	collass diamin.freed								
USER MANAGEMENT	Depk	by files, schedule maintenance activity, or install software on endpoints	in PowerShell, bash, shell, and more. Learn How.						
USER AUTHENTICATION		nstall CrowdStrike Falcon Agent	Change Hostname	List Users		Set Background		Run as User	
DEVICE MANAGEMENT     Devices	¢	to command will download and install the CrowdStrike Falcon Agent to in dow de if it is not already installed.	Lets you change the hostname.	Returns a list of user profiles.		Define the background of your end users devices.		Target a command to run as the signed in user of a system.	<b>→</b>
Device Groups     Policy Management      SEE		unique faire windows	Configure for: Mac Windows	Configure for: Mac Windows Linux		Configure for: Mac		Configure for Windows	
Policy Groups									
Commands	-								
d MDM	(+	Q Search						filter by + 7 commands nun now	delete
Software Management		Name *			Command		os		
DIRECTORY INTEGRATIONS     SECURITY MANAGEMENT		List Users Laurch Manually			avk -P^{(j)})° '{if (\$3 ≈ 1000 66	6 53 (* 65534) print 51)* /etc/passwd	۵	Run Now Delete	->
<ul> <li>INSIGHTS</li> </ul>		Est 46 bit programs     Level Minute			dir citaropram films			Run Now Delete	>
		Bist filesystems Launch Manualy			ef -4h		۵	Run Now Delete	>
		list logs Launch Manualy			ls -al /var/log/			Run Now Delete	>
		repeating command     Launch every day at 0100 (Server Time)			cp /users/user1/data /tmp/datace	ngy/cngy\$	۵	Run Now Delete	>
		scheduled command Launch on Thursday Jun 16th 2022, at 12:51 (Server Time)			echo "this is a test"		۵	Run Now Delete	>
		S triggered command Launch when test is received			cs/dir			Run Now Delete	>
Settings									
Account									
<ul> <li>Collapse Menu</li> </ul>									

#### Create a New Command

To create a new command:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to DEVICE MANAGEMENT > Commands.
- 3. In the Commands panel, select (+). The New Command panel appears.

iumpcloud	Commands		Q Alerts D Resources	③ Support	СВ
Discover     Discover     Home	Commands Recommended C	Details Device Groups Devices Command Runners			×
Q Users	Deploy files, schedule	Details			
USER AUTHENTICATION	This command will de CrowdSarike Falcon A already installed.	Name Run As Select user		¥.	
DEVICE MANAGEMENT     CL Devices     AD Device Groups	Configure fact: Made 1	Windows Mac Command #/b1n/bash		🗇 Сору	
Policy Management      NEW     Policy Groups     Commands	Name      Chocola				
MDM     Software Management     JIRECTORY INTEGRATIONS	Chocolatey - Launch Merically	Launch Event			
Active Directory     Cloud Directories     HR Directories	Chocola Launch evy	Run Manually v			
SECURITY MANAGEMENT     Conditional Policies     Conditional Lists     MFA Configurations	Chocolatey - Launch Manually	Options Timeout Atter 120 seconds			
Settings	Linux - t Launch eve	Time to Live (TTL) Settings Commands expire from the queue after 3 days by default. To change the expiration period, make a selection or enter a custom duration			
Collapse Menu	Linux - Disat Launch Manually			cancel sa	ve

- 4. On the Details tab, enter a name for the new command. This is the name shown in the sortable list view of commands.
- 5. Select users that you would like the command to Run As.
- 6. Select your operating device type: Linux, Windows, or Mac.
  - Linux only: Select the Run As user account to use to run the command.
  - Windows only: Commands will be run as the LocalSystem account and optionally can be run as Powershell.
- 7. Type or paste in a script. The script can be in any language that your servers can execute.
- 8. Select the Launch Event.
- 9. Enter a Timeout After value (in seconds). This determines how long the command can continue running before the agent will terminate it.
- 10. (Optional) Select Upload File to attach a file to the command (see below for details).
- 11. Select the Device Groups tab to set the specific device groups on which this command will execute.
- 12. Select the Devices tab to set the specific devices on which this command will execute.
- 13. (Optional) Select the Command Runners tab to select a user as a Command Runner with access to run the command. By default, admins can run commands on all devices.
- 14. Select save.

For more information on commands, check out this tutorial:



#### **Enable MFA for Devices**

JumpCloud gives organizations the power to layer multi-factor authentication (MFA) on top of nearly any resource you need to secure: Windows, Mac, Linux, applications, networks, infrastructure, and more.

If you'd like to use the JumpCloud Protect<sup>™</sup> Push MFA mobile app for your MFA needs, see Logging into your Device with JumpCloud Protect Push MFA.

#### Check out this Knowledge Base article for more details on how to enable TOTP MFA:



You can also view this tutorial:



#### Configure Device Configurations/Policies for Mac, Windows, & Linux

You can save time by creating JumpCloud policies to remotely apply a set of rules to one managed device, a group of devices, or your entire fleet. Applying policies lets you customize these types of managed devices and make them more secure:

- Windows
- MacOS
- iOS and iPadOS
- Linux

You can also create a policy group, adding multiple policies to it, and apply the policy group to multiple devices or device groups. For example, you create a policy group that uses JumpCloud's Lock Screen policy to automatically turn on the screen saver if a device is inactive for a specific amount of time. The policy group could also contain a policy to control Apple App Store purchases to allow only updates to existing apps. A policy group is especially useful in implementing security or compliance-related issues on managed devices.

Every policy contains these sections:

- **Policy name** You can customize this or keep the default. Your policy names must be unique. (All references to policies in this documentation use the default name.)
- **Policy description** Provides more information on the policy's function and lists the specific OS versions this policy supports.
- **Policy behavior** Describes the device behavior when the policy is applied.
- **Policy activation** Lists any additional steps you must take after creating the policy and saving it. After you complete these additional steps, the policy takes effect.
- **Settings** These options vary depending on the policy and allow you to further define the behavior you want to enforce on a device.

After you apply and save a policy, the system agent checks in with JumpCloud. The agent on an individual device continuously compares the local policy with the policies you set in JumpCloud. If a user modifies the device policy, JumpCloud automatically modifies the device's policy to comply with the JumpCloud policy. This process ensures that JumpCloud policies and local devices are kept in sync.

Check out this tutorial to learn more about configuring policies:

Configuring Policies

#### **Configure Full-Disk Encryption for Mac and Windows**

#### Mac

You can use this policy to remotely enforce FileVault on macOS devices and easily view Recovery Keys. FileVault full-disk encryption (FileVault 2) helps prevent unauthorized access to the information on your user's startup disks. FileVault 2 uses XTS-AES-128 encryption with a 256-bit key.

After you enforce a FileVault policy, your users need a secure token to enable it. The advent of Apple File Systems (APFS) in macOS 10.13 changed the way Apple manages FileVault encryption keys. To secure and provide access to encryption keys required for FileVault decryption, Apple introduced Secure Tokens. Ensure your users have Secure Tokens by following the instructions in <u>Installing and Using the Service Account for macOS</u>.

#### **Administrator Experience**

When you create a FileVault policy, you can enable and configure the following settings:

- Show the FileVault Recovery Key to the user when enabled: When this option is selected, the user sees the Recovery Key and can store it in a safe place.
- **Do not prompt the user to enable FileVault at logout**: There are two possible prompt locations for the user to enable FileVault, at login and at logout. With this option selected, the user is only prompted to enable FileVault when they log in.
- Number of times the user can bypass enabling FileVault: You can let the user postpone enabling FileVault for the number of times you enter in this field. When the value you enter has been exceeded the user is forced to enable FileVault before they can login to their device.

To create a FileVault 2 policy:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to DEVICE MANAGEMENT > Policy Management.
- 3. Select (+).
- 4. In the New Policy panel, select the Mac tab.
- 5. Next to the FileVault 2 policy, select configure.

n jumpcloud	Policy Management 3		ပို Alerts ထိ Resourc	es 💿 Support 🔀
<ul> <li>Ø Discover</li> <li>A Home</li> </ul>	All 🖄 OS P:			×
✓ USER MANAGEMENT	Recommended P	Windows Mac iOS Linux	Recommended	
A Users	Protect and configure			40 14
AR Osci Citops	Block macOS Bi	Search	1	tter by + 43 items
LDAP	Prevents the macOS application and mac	Name Disable iCloud Private Relay	Description	and and
🕐 RADIUS	New Policy	Enterprise Settings, Security	This policy disables icloud Private Relay for macOS.	configure
sso :	Configure for:Mac O	Disable Removable Storage Access Security, Compliance	This policy prevents mounting of removable storage devices.	configure
Device MARAGEMENT     C     Devices     Device Groups		Disable Siri Enterprise Settings, Compilance	This policy will disable all access to the Siri assistant.	configure
O Policy Management      New     Policy Groups	Type N	Disable Unlocking with Biometrics Security, Compliance	This policy prevents users from unlocking their macOS devices using Touch ID.	configure
සි Commands රෑ MDM		Disable Unlock with Apple Watch Security, Device Access	This policy prevents users from unlocking their macOS devices with an Apple Watch.	configure
Software Management     DIRECTORY INTEGRATIONS		Encrypted DNS over HTTPS Enterprise Settings, Security	This policy enables you to encrypt Domain Name System (DNS) over HTTPS, so that you can use encrypted DNS services on your macOS devices.	configure
Active Directory     Cloud Directories		Encrypted DNS over TLS Enterprise Settings, Security	This policy enables you to encrypt Domain Name System (DNS) over Transport Layer Security (TLS) services, so that you can use encrypted DNS services on your macDS devices.	configure
<ul> <li>SECURITY MANAGEMENT</li> </ul>	C C C	FileVault 2	This policy allows you to enable and enforce FileVault.	configure
Conditional Policies	0 A C	Security, Compliance		
Conditional Lists     (6) MFA Configurations		Gatekeeper Control Security, Compliance	This policy controls the ability of the machine to install and run software by leveraging Gatekeeper in macOS.	configure
• інсілите	- · ·	iCloud Access Security, Compliance	Users on managed machines will only be able to access the features of iCloud allowed by an administrator.	configure
<ul> <li>Settings</li> <li>Account</li> </ul>	c c	Install Certificate	This policy lots you install a certificate on a macOS device, so that the certificate is trusted.	configure
<ul> <li>Collapse Menu</li> </ul>				close

- 6. On the New Policy panel, optionally enter a new name for the policy, or keep the default. Policy names must be unique.
- 7. Select or clear the Show the FileVault Recovery Key to the user when enabled option.
- 8. Select or clear the Do not prompt the user to enable FileVault at logout option.
- 9. If you select the Do not prompt the user to enable FileVault at logout option, in Number Of Times The User Can Bypass Enabling FileVault, enter a number greater than zero.
- 10. Select the Device Groups tab. Optionally, select one or more device groups to apply this policy to. For device groups with multiple OS member types, the policy is applied only to the supported OS.
- 11. Select the Devices tab. Optionally, select one or more device groups to apply this policy to.
- 12. Note in the POLICY ACTIVATION that a user will need to log out and log back in for the policy to take effect.
- 13. Select save policy.

After you save the policy and the user logs out and back in, the policy takes effect on active devices in nearreal time, but could take up to a few minutes. The policy is enforced on any inactive devices the next time they become active.

In the Admin Portal, you can check the policy to see if it's successfully applied. If FileVault is already enabled on the device when the policy is applied, the following behavior occurs:

- JumpCloud rotates the Recovery Key on the device.
- Key rotation may be immediate, but may also take up to one hour.
- In order for JumpCloud to rotate the Recovery Key, the JumpCloud Service Account must be present on the device.
- Once the Recovery Key is successfully rotated, JumpCloud records the new Recovery Key in the Admin Portal on the device's details.

At this point, FileVault is now completely enabled on the devices where you applied this policy. You can view the Recovery Key for the device, and users can't disable FileVault.

Here is a tutorial on FileVault management:



#### Windows

BitLocker is an encryption feature built into computers running Windows. It secures your data by scrambling it so it can't be read without using a recovery key. BitLocker differs from most other encryption programs because it uses your Windows login to secure your data; no extra passwords necessary. Once you're logged in, you can access your files normally. After you log out, everything's secured.

JumpCloud's BitLocker policy lets administrators remotely enforce BitLocker Full Disk Encryption on JumpCloud managed devices.

#### **Administrator Experience**

Administrators can create a policy to force BitLocker encryption on managed devices and easily view Recovery Keys.

To create a BitLocker policy:

- 1. Log in to the JumpCloud Admin Portal.
- 2. Go to DEVICE MANAGEMENT > Policies.
- 3. Select (+).
- 4. On the New Policy panel, select Windows.
- 5. Find the BitLocker Full Disk Encryption policy, then select policy.
- 6. (Optional) Select Encrypt All Non-Removable Drives to encrypt all fixed drives on the devices the policy will be enforced on.
- 7. Apply the policy to a Group of Devices in the Device Groups list, or to an individual device in the Devices list.
- 8. Select save policy.

After an administrator saves the policy, JumpCloud enables BitLocker on the devices where this policy is applied.

- When the device's volume is completely encrypted, you can view a Recovery Key that can be used to unlock all encrypted drives on that device.
- The drive isn't fully encrypted until the policy result shows that it was applied successfully in the Administrator Portal.
- Removing this policy doesn't disable BitLocker or remove key protectors.

The administrator must wait for the following actions to happen before viewing Recovery Keys:

- 1. A user sees a prompt requesting that they restart their device to enable BitLocker.
- 2. On the Administrator Portal the Policy Status is updated to BitLocker Not Protected Encryption has been enabled. Device drive encryption will begin on the next boot.
- 3. The user restarts their device.
- 4. BitLocker begins encrypting the user's volume.

After the drive is completely encrypted, Administrators can view the Recovery Key:

- 1. In the Administrator Portal, go to DEVICE MANAGEMENT > Policy Management.
- 2. Select the BitLocker Full Disk Encryption policy and select the Devices tab to display a list of encrypted devices.
- 3. From the displayed list, locate your desired device, and select "View Key" to display the system's Recovery Key. Users who are not administrators on the device can't disable BitLocker.

Here is a tutorial on BitLocker Policy:

**BitLocker Policy** 

For more information on these topics, please refer to the following courses:



Adding Windows and Linux Devices



Adding Apple Devices using MDM

Enabling MFA