eBook

jumpcloud

Security for Startups

Growing, Scaling, and Winning Securely

In general, startups are lean, fast, data-driven, and forward-thinking. This makes them prime users of cutting-edge tools, big data, and cloud-based technology. However, security is critical in these fast-paced, high-stakes environments. Regardless of workload, startups can't afford to let security fall to the wayside.

Further, as the business standard moves from on-prem to the cloud and from the office to a work-from-anywhere model, startups need to pay special attention to their remote and hybrid-remote security.

That's a lot for a startup to manage. But with the right security, tools, and practices in place, startups can fuel faster, more effective growth and position themselves for smooth scaling.

This e-book will cover the essentials for security with recommendations tailored specifically for startups. This includes solutions to the challenges most startups face today, remote and hybrid-remote security factors, employee and device management, and cloud infrastructure and application management. We've also included a **synthesized checklist** to act as a quick reference guide to jumpstarting your security.

Startup Security Challenges

Startups have to execute and work fast to create product and market fit without the resources of a fully fledged enterprise. What's more, they're working with the added challenges of tight budgets, a small workforce, and a lack of established processes or highly specialized roles.

On top of these challenges, most startups today have to secure remote environments, *and* many have to secure both remote and in-office environments. As such, we've outlined common challenges startups face, both remotely and in the office, and recommended solutions for each.

Remote Environment Challenges

Network and Resource Access

Remote employees need to be able to connect to all the resources they need to get their work done, but doing so from their home or public networks can be risky. Traditionally, the VPN has been the go-to method for getting employees access to the company's private network and resources. However, as companies shift toward cloud hosting, the VPN becomes less relevant and other cloud-based solutions that encrypt resource access directly have gained in popularity. The JumpCloud Directory Platform, for example, uses LDAP, RADIUS, SCIM, SAML, WebAuthn, and other protocols to provide employees with secure remote access to all the resources they need.

Home and Public Networks

Even with a VPN or other encryption method in place, the user's home network still matters. For example, when working in a cafe, you would need to use its public Wi-Fi for a few moments to connect to the corporate VPN, and that initial activity goes unencrypted and is vulnerable to attack.

Startups should create policies around remote Wi-Fi use — home networks should be protected with a strong password; public, unprotected Wi-Fi should be avoided. Some tools offer conditional access, which can deny access to corporate resources if a user attempts to access them over an unsecured network.

Onboarding and Offboarding

Startups' rapid growth and frequent changes entail a frequent onboarding and offboarding. Both can take several hours per employee, which can be particularly inconvenient when onboarding an entire team or coordinating a quick offboarding.

Single sign-on (SSO) significantly helps with these challenges by applying one set of secure credentials to all the applications an employee needs by automating individual resource provisioning. Additionally, using a directory solution that allows you to create user groups can help you automate provisioning based on department, administrative level, and other criteria. These factors significantly reduce onboarding time.

With these solutions, offboarding becomes just as quick — in a cloud-based directory, all you need to do is delete the user to immediately revoke access to all resources.

Lack of Supervision

Leaders often worry employees won't follow security policies at home. The solution to this challenge is two-fold: first, startups should establish, teach, and enforce security best practices, cultivating a company culture that prioritizes security. Second, companies must invest in the tools that make cloud-based remote security possible and user-friendly. Cloud-based directory platforms combine several of these security tools, including the directory, multi-factor authentication (MFA), secure SSO, and more, into a fairly frictionless user experience.

Cloud-Based Asset Management

With remote environments, some companies worry about keeping track of cloud-hosted assets, especially when users aren't being supervised when accessing and saving them. For items like files, develop and enforce clear naming conventions and storage policies — cloud-based companies shouldn't allow users to store items on their desktop, for instance. For applications, user and device data, and other asset tracking, look for a cloud directory platform that can track and connect cloud-based assets.

Startup Security Challenges

Office Environment Challenges

Personnel Awareness

Awareness of an employee's surroundings is critical. While a startup's office may be small or may be a shared space, knowing who should be in the office is important. Hackers will often try the old technique of masquerading as an employee or a visitor, so if a stranger is in the office, employees should know to ask them if they are in the office to meet someone. Be sure to include personnel awareness in your security awareness training.

Control and Monitor Physical Access

Many offices have some sort of physical access control, either through a key, fob, or card access system. Consider investing in a digital solution with regular logging of who enters and exits to track unsolicited visitors, as in the in-person social engineering tactics described above. Video cameras are also advisable to monitor your equipment and materials — some cameras are intelligent and network-connected so they can alert you to after-hours activity and save footage in the cloud.

Internet Connection Security

The internet connection in your office needs to be secure. There should be, at a minimum, a next-generation firewall at the connection that blocks malicious traffic. Investing in more security like content filtering or intrusion detection technology is a great improvement, but a strong firewall is a must.

Wi-Fi Security

Wi-Fi security should not just be an SSID and passphrase. That level of security is simply too easy to compromise.

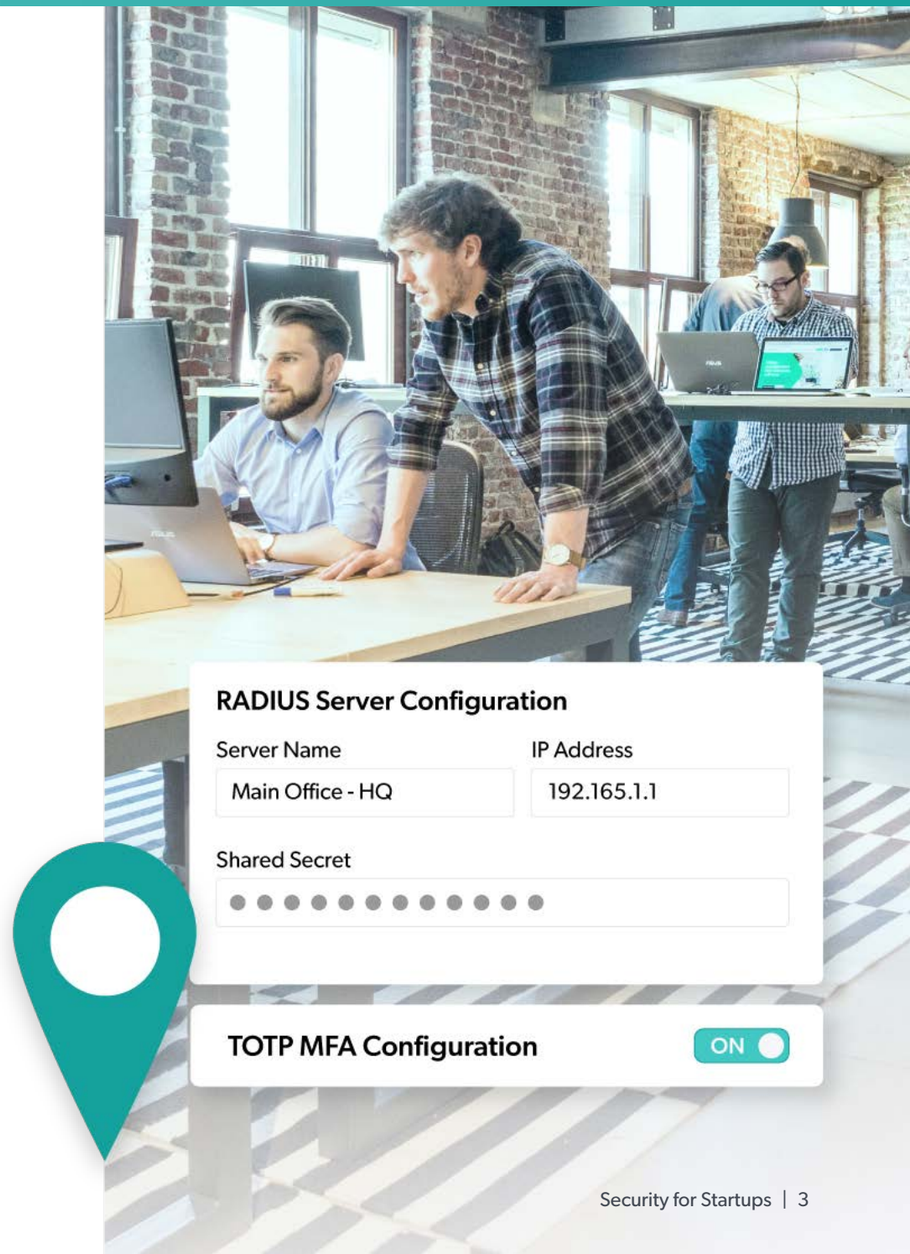
Each user should have unique access to the Wi-Fi network through an authentication system like RADIUS, which authenticates each user individually. RADIUS eliminates the problems that shared network credentials pose (like writing the Wi-Fi password on the office whiteboard).

Ideally, RADIUS should integrate with the user directory to streamline user data and maintain one central repository system.

For an additional layer of protection, create a separate guest VLAN with restricted access to ensure security while providing a positive user experience.

On-Prem Infrastructure

Just as you would only assign administrative privileges to a select few people, you should keep the server room just as tightly restricted and monitored. If your organization still has on-prem servers, keep them locked up, only grant access to people who need it, and keep track of those who have access.



Securing Cloud Infrastructure and Applications

With cloud infrastructure and web applications becoming the new business standard, the cost of starting a business is far less expensive than it has ever been. However, just because starting a company has become more accessible doesn't mean it carries less risk. With the power of cloud computing, storage, and services, comes the responsibility of security.

Securing Your Cloud Infrastructure

Configure Security Groups

An important first step in protecting your cloud infrastructure is appropriately enabling the firewall and network. AWS calls this function Security Groups, but just about every IaaS provider has an equivalent functionality. Make sure that you lock down inbound and outbound access to the most restrictive policy that works for your application and organization.

In addition, make sure that every server that you spin up is behind the firewall and appropriately networked. It's easy to forget a server, leaving it unprotected on the public internet. Ideally, you'll also have VPN access to the cloud infrastructure with restrictions such as certificate-based access or even IP/geolocation requirements to continue to level up security.

Patch

Trust us — even the most recent operating system images can need patches. Make sure that all of your servers and applications are up to date. Out-of-date servers (especially internet-connected ones) are highly susceptible to attack; they can be targeted by automated techniques that scan for (and exploit) known vulnerabilities, or fall to a zero-day exploit previously unknown to the manufacturer or public. Some cloud providers offer patching services, and we recommend supplementing with SaaS-based patching services like those from JumpCloud, which offers patching for virtual servers, VMs, and third-party solutions.

Tightly Control User Access

Cloud infrastructure security depends heavily on precise and tightly controlled user access. A central user management system like JumpCloud can solve this problem by managing who can access your Windows, Linux, or Mac systems (although Macs are less likely to be cloud servers). Users can be required to use complex passwords, SSH keys, or MFA to gain entry to the server infrastructure.

No matter how you manage credentialed access, the principles of *least privilege* should always apply. This can be challenging in a startup environment, where a small set of engineers, developers, or contractors may share accounts or be given full sudo (or admin) to maintain speed. However, the extra time spent determining *who* should have access to *what* and at *what level* could mean the difference between a security incident and a full-blown breach.

With AWS SSO and AWS IAM solutions often being leveraged for access to various cloud infrastructure components, take care to assign users the right roles and permissions. Further, integrating a cloud directory with AWS SSO or AWS IAM is critical to having full control over user access to IT resources, and detailed logging of all user access is also a must in today's compliance-heavy environments.

Encrypt Data at Rest

If possible, it's best to secure data at rest with encryption. Different providers offer different levels and types of encryption, and the highest security encryption isn't always enabled by default. Check your provider's encryption policies and offerings; if they don't meet your organization's needs, there is a wide variety of tools and systems that can help you encrypt your data stored in the cloud.

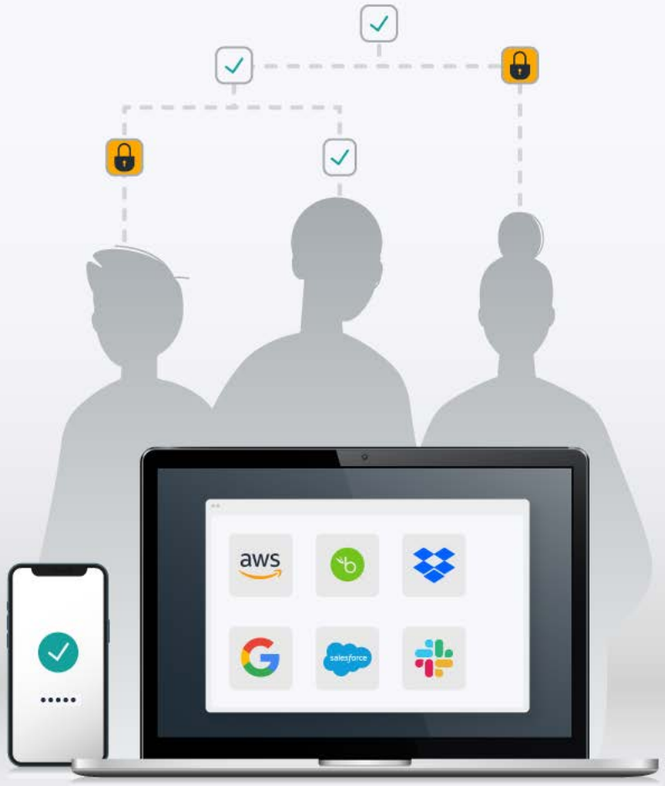
Establish Secure Communication

In addition to at-rest encryption, you'll need to protect your data in transit. For example, if your servers communicate with each other from behind different firewalls, there should be secure communication between all involved components. This may be accomplished through VPNs or other mechanisms for encrypting data in transit.

Choose Your Vendors Wisely

Cloud infrastructure providers and SaaS vendors only go so far with their security measures; customers should do their due diligence to check their vendors' security measures and either customize or supplement them to meet their organization's security standards. Virtually every cloud infrastructure provider and SaaS platform conducts business under a shared security model — some aspects are covered by the provider and many others are the customer's responsibility. Every startup should understand how their cloud provider approaches security and execute on the security that remains the startup's responsibility. Read more about doing your due diligence in our **blog on commonly overlooked vendor vulnerabilities**.

Securing Cloud Infrastructure and Applications



Securing Your Applications

User Access

Controlling user access to applications and effective user lifecycle management are some of the most important aspects of security in a growing startup. The modern organization now stores its critical data in several different locations: for example, a startup might store its source code in GitHub, customer data in Salesforce, and financials in Xero. In an environment where the crown jewels are stored in disparate locations, organizations need to be extremely restrictive and diligent about who they grant application access to.

Connecting user access to your core directory service can make the user lifecycle management process much simpler and more secure. Look for a directory service that can attribute roles to each user and intelligently provision application access and security policies based on that user data. Context also matters, and innovative organizations are leveraging conditional access techniques to ensure that access to critical web applications is verified and secure based on identity, device, network, and least privilege access.

Shared Access

Shared access is a common issue in startups. Often, this occurs in an attempt to save on licensing costs or as the result of shadow IT; to move quickly and efficiently, employees at startups sometimes leverage solutions without involving IT (or they may not have a designated IT department to regulate application use). However, the cost or time-saving benefits don't outweigh the risk of sharing credentials.

Aside from the obvious problems with sharing passwords, it also makes tracking who has access to the credentials nearly impossible. Organizations should never cut corners by skimping on licensing or allowing users to share accounts with one another — especially when it comes to access to cloud infrastructure or web applications.

Multi-Factor Authentication

Despite a widespread understanding of the importance of password best practices, many users still do not follow them. This, coupled with hackers' increasing sophistication in password cracking, drives a need for a more sophisticated login solution than a password alone.

MFA alleviates the problems with passwords; whenever possible, MFA should be turned on. This exponentially increases security by requiring access to both credentials and a user's proprietary device at the same time.

Many systems and applications have the option to enable MFA; for those that don't, single sign-on solutions can apply MFA to all of a user's applications with one secure login.

Eliminate Old Accounts

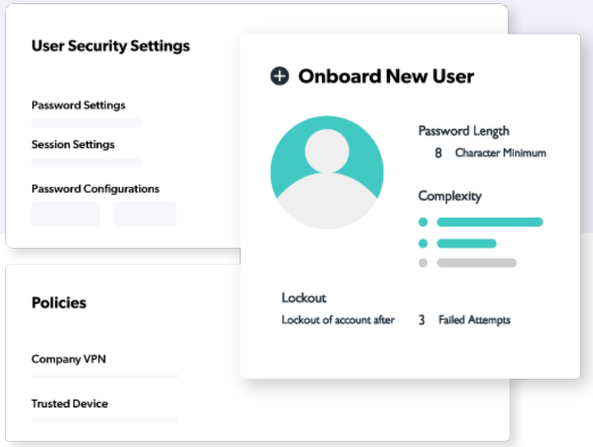
Retaining unused and unattended accounts is one of the top ways organizations are compromised; in fact, **48% of people** retain access to at least some of their former organization's IT resources. This presents both security and compliance risks.

Cloud directory platforms drastically reduce the risk of leaving accounts open unattended through fast, integrated offboarding: when one IdP manages all of a user's applications, you can deprovision them all at once. Reporting and analytics solutions can also highlight old accounts that are on systems that need to be removed.

Securing Employees and Devices

As security experts know, the most critical component in the security chain is the user. No matter how great the systems in place or the processes, a mistake by an individual can render all of those safeguards useless.

In this section, we'll cover the common challenges startups face when securing users and their devices — especially in the increasingly common remote or hybrid workplace — and solutions to help you continue growing quickly and successfully.



Securing Employees

User Management

You should be able to account for every user in your organization and store critical data about them, like permissions and assigned resources, at any time, and from anywhere. Here are some of the attributes you should be able to see and manage:

- Assigned device(s)
- Role in the organization/group membership
- Access to IT resources
- Permission levels
- Provisioned resources
- Password security settings
- Account lockouts

Most companies use directories to accomplish this. Some startups wait to start using a directory if they're only managing a few users; however, opting to go without a directory service and tracking this data manually hinders startups when it's time for exponential growth.

While most directories allow for user and user data tracking, cloud directory platforms give cloud-first startups a step-up by offering SSO to all cloud-based applications, automated provisioning and deprovisioning, system management/MDM capabilities, RADIUS integration, compliance reporting, and several other time-saving features, all with no on-prem equipment.

Strong Passwords

While you may set up password complexity requirements for your systems and applications, getting your users comfortable with creating strong passwords is critical.

Some tools, like JumpCloud, enable you to establish and enforce minimum password complexity requirements. Password managers are another highly effective way to ensure employees create strong and unique passwords without compromising their effectiveness by writing them down.

Separating Business and Personal Accounts

When employees mix their business and personal account passwords, compromise to a personal account puts the business at risk. Encourage your employees to create unique passwords for each of their accounts, preferably with a password manager, as detailed above. Their security training may even encourage them to add MFA to their personal accounts as well.

Securing Employees and Devices

Securing Devices

Device Responsibility

While all work devices should have strong controls and be encrypted, this should not be the only method of defense. Employees must understand that they are responsible for keeping physical control over the devices they use for work, whether personal or corporate-issued. Adding this layer of diligent control and protection by the employee further secures corporate data.

Device Encryption

The latest operating systems offer full-disk encryption to help protect the data located on endpoints. Because it is highly likely that corporate data can be found on endpoints despite using cloud services, device encryption is an important step to take in protecting valuable corporate data.

Disk encryption is relatively simple to enable, and it is also user-friendly. The password to the device can toggle the disk encryption on or off, which underscores the importance of a complex password. A centralized approach will ensure that recovery keys are safely stored as well as reporting on what users/machines have disk encryption enabled and those that don't.

Multi-Factor Authentication

In addition to using MFA for systems and applications, employees should enable MFA on their devices. A complex password adds to the security of the endpoint, but adding MFA access to the endpoint raises it to another level. Conditional access can reduce the friction of this step when a user signs on using other known criteria, like on an approved network.

Antivirus/Anti-Malware

Antivirus (AV) software should be installed on every device. There's a reason that this security protocol has been an IT staple for many years. While AV software does not catch every issue, it does dramatically decrease the chances of an endpoint being compromised. Again, layered security is always better than a uni-dimensional approach, and antivirus/anti-malware is an effective frictionless layer.

Lead with Documentation and Training

To cultivate a security-oriented company culture, startups need to create a security program that specifies their security standards and policies. They must also issue mandatory training to ensure employees understand these policies.

The security program doesn't need to be a complex or long document; in fact, a clear, concise program for your employees is likely to work much better than a long list of items that they need to do or be aware of. The right security program gets your employees thinking about how they protect their personal data, accounts, and access because they understand the significance.

Security Plan Checklist

The following checklist synthesizes the information above into an actionable guide to developing a comprehensive and strategic security plan. This checklist is not all-encompassing; individual processes, equipment, goals, and other factors will influence each company's security needs. However, it does provide a solid foundation for building an effective startup security plan.

Note: Because MFA is a critical component of **Zero Trust security**, it is included MFA as a recommendation for multiple sections in this checklist. One factor should never be enough for authentication to access IT resources.

Users

- ☐ Controlled user access to IT resources, including:
  - Devices and equipment
  - Applications
  - Files
  - Networks
  - Data and databases
  - Reporting and analytics
- ☐ Central directory that extends to cloud and on-prem resources
- ☐ Secure user authentication and authorization that supports MFA
- ☐ Automated resource provisioning and de-provisioning based on user groups and policies
- ☐ Customizable security policies that can be implemented remotely
- ☐ Policy-driven user groups.
- ☐ Secure SSO to IT resources
- ☐ Audit logging, insights and reporting

Devices

- ☐ Disk encryption enabled on all machines.
- ☐ Devices assigned to policy-governed device groups
- ☐ Devices assigned to users
  - Installing a PKI certificate on the device for authentication is ideal
- ☐ MFA login required for all devices
  - Conditional access may bypass this if the device can be verified via PKI certificate
- ☐ An MDM tool that can manage all devices in your environment
  - This should include user-owned devices and different operating systems
- ☐ Screen lock after inactivity (one minute is ideal)
- ☐ Regular updates and patching
  - Use a patch management tool to track patching and avoid creating vulnerabilities by missing an update
- ☐ Visibility and tracking for all network-connected devices
  - MDM solution should alert to items like lockouts, computers with disks that aren't encrypted, and devices without MFA enabled
- ☐ A BYOD policy

Network

- ☐ Means for secure remote connections
  - Network and resource access from unprotected WiFi should be prohibited
- ☐ RADIUS to avoid shared credentials for network access and VPNs
- ☐ MFA
  - Conditional access policies may increase or relax MFA based on the conditions of the login attempt
- ☐ VLANs for network segmentation
  - **Dynamic VLAN assignment** is ideal — it allows you to automatically assign users to their appropriate VLAN based on their directory-issued permissions using RADIUS
- ☐ A next-generation firewall
  - Ideally, it should include application-level inspection and intrusion prevention

Security Plan Checklist

The following checklist synthesizes the information above into an actionable guide to developing a comprehensive and strategic security plan. This checklist is not all-encompassing; individual processes, equipment, goals, and other factors will influence each company's security needs. However, it does provide a solid foundation for building an effective startup security plan.

Note: Because MFA is a critical component of **Zero Trust security**, it is included MFA as a recommendation for multiple sections in this checklist. One factor should never be enough for authentication to access IT resources.

Resources and Data

- ☐ Data encrypted in transit
  - This means opting for secure protocols like HTTPS, SSL, TLS, SSH, and others when transmitting data from one location to another
  - Develop standards for acceptable protocols for different data transmission types
- ☐ Data encrypted at rest
  - Enforce full disk encryption
  - For data stored in the cloud, check the encryption policies of the company or application storing the data
- ☐ Passwords stored with cryptographic hashes
  - Salt the hashes
- ☐ MFA where possible
- ☐ Account or password sharing prohibited
- ☐ Don't re-use login information
  - Use a password manager to help users create strong, unique passwords without having to remember them all
  - Use SSO to allow users to sign into everything with one secure set of credentials. It also simplifies and secures onboarding and off-boarding as well as logging of all access
- ☐ Keep track of vendors
  - Only work with those who demonstrate security and compliance practices that meet your company's standards
  - Update software, applications, and equipment regularly

Security Best Practices

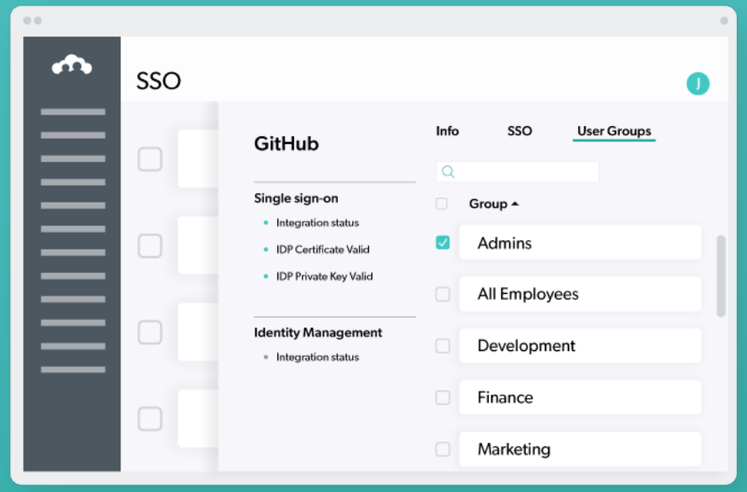
- ☐ Assign users the lowest privilege necessary
- ☐ Create role redundancy so that privileged access doesn't rely on one sole person in case of an emergency
- ☐ Make sure personally identifiable information (PII) is only accessible by privileged users
- ☐ **Disable guest accounts** if you don't need them (most startups don't)
- ☐ Make sure all users and their information and activity are tracked and visible
  - Ideally, your IAM program should be able to flag issues like lockouts, suspicious login attempts, expired passwords, and other data that needs an admin's attention
- ☐ Follow password security best practices
  - Include a minimum length (we recommend 12-16 characters at least)
  - Create complexity requirements, if required
  - Require password rotation periodically (try once every 90 days)
  - Don't allow name or username to be used in the password
  - Encourage password uniqueness — ideally with a password manager
  - Prohibit password sharing
  - *For a full list of recommended policies, **read our in-depth blog on password security best practices***

Training

At a minimum, your security training should include:

- ☐ Personal data security best practices
- ☐ Password best practices
- ☐ Device best practices
- ☐ Using MFA and other security initiatives
- ☐ Recognizing and reporting phishing or other suspected security vulnerabilities

jumpcloud



- LDAP, RADIUS, SSO, MFA, and more
- 10 users and 10 devices free forever
- 24/7 live premium chat for first 10 days

Looking Ahead: The Future of the Directory

While some see startups' size and early lifecycle stage as a disadvantage, they present the opportunity for startups to build themselves and their security practices exactly how they want. Chipping away at a mountain of legacy equipment is difficult, from the configurations themselves to advocating for change from the top. Startups get to skip these steps and move straight to optimization and growth in a modern business model.

For cloud-based startups building their security practice and preparing to scale, don't fall into the trap of doing something because that's how it's been done in the past. Instead of investing in an on-prem directory service like Active Directory, consider maintaining your cloud momentum with a cloud-based directory platform that can accomplish more with fewer solutions (and expenses). The JumpCloud Directory Platform combines LDAP, RADIUS, SSO, MFA, and other critical features in one cloud-based platform. It's free to try with up to 10 users and 10 devices, and it comes with 24/7 live premium chat for the first 10 days to help you optimize it to your environment.

Try JumpCloud Free →