



# Device Management

Remotely manage and protect all of your employees' devices. Powerful enough for IT pros and incredibly easy to use.

TABLE OF CONTENTS

[Rippling Device Management makes your company more secure](#) <sup>3</sup>

[Rippling secures your data](#) <sup>6</sup>

[Rippling respects your privacy](#) <sup>8</sup>

[Rippling's security principles for device management](#) <sup>9</sup>

[MDM, DEP, and the Rippling Agent](#) <sup>10</sup>

[How Rippling performs device management services](#) <sup>11</sup>

[Rippling leverages open-source software and third-party tools](#) <sup>17</sup>

## Rippling Device Management makes your company more secure

The IT security landscape is becoming increasingly difficult to navigate. Malware rates are rising. New threats like crypto-ransomware drain \$11 billion annually from businesses.

### Data breaches are becoming more costly

IT administrators need to manage the increased prevalence of remote work and BYOD policies. Securing your employees' devices is your first and strongest line of defense against cybersecurity attacks. Research has shown that the most common causes of data breaches are loss and theft of data on an employee's device. And the most common vector for malware infection is through files downloaded to employee devices.

Even one unmanaged device can expose your network to malware, ransomware, and data loss. Rippling Device Management provides a comprehensive suite of features designed to protect your team's Mac and Windows devices from malware, data loss, and employee negligence. Rippling Device Management is simple to set up and use, and runs a powerful enterprise-grade security agent with the latest technology and security standards.


### Enforce security policies and track compliance

Security policies are the foundation of IT security—but they are only effective when they are continuously enforced. If users are able to override security requirements by creating weak passwords or removing drive encryption, any policies are rendered ineffective, and your organization could be in violation of compliance regulations.

Rippling Device Management allows you to install a simple, lightweight security agent on your devices—automatically for new devices, or through a simple file download for your current devices—that both enforces your company's security policies on an OS (automatically encrypts the drive, requires passwords, patches updates, and more) and gives you instant visibility on adherence into these policies across your company's fleet of devices.

Our lightweight security agent (which you can install automatically on new devices or manually on your current devices) allows you to create and, more importantly, enforce custom security policies across your fleet.

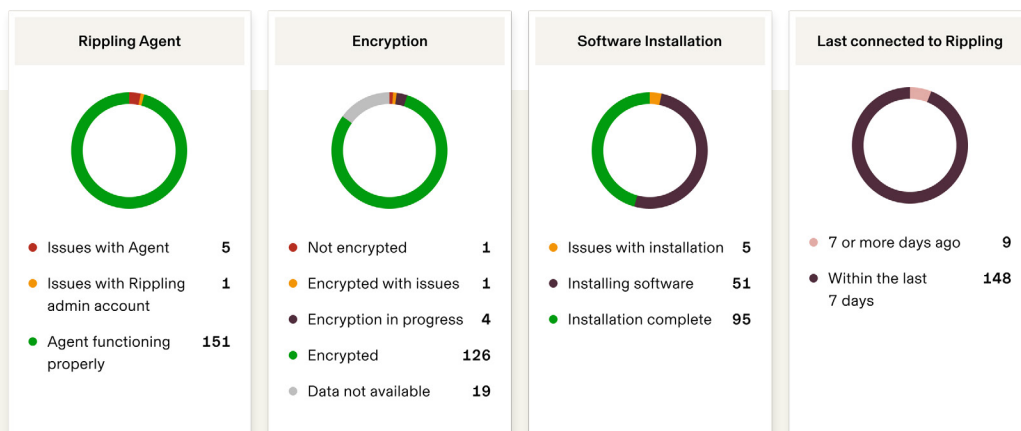


 Create a custom password policy

Should require passwords? <small>Yes, require password.</small>	<input checked="" type="checkbox"/>
Minimum length of the password 8	<input checked="" type="checkbox"/>
Require at least one letter and number? <small>Yes, require at least one letter and number.</small>	<input checked="" type="checkbox"/>
Require special characters? <small>Yes, require special characters</small>	<input checked="" type="checkbox"/>
Should not allow simple passwords? <small>Yes, don't allow simple passwords.</small>	<input checked="" type="checkbox"/>
Force password changes periodically? <small>No, don't force password changes periodically.</small>	<input type="checkbox"/>

## DEVICE MANAGEMENT

Get 24/7 visibility into the health of your entire fleet, from which OS versions all of your devices are on, to what (and how many) active threats exist.



### Encrypt your hard drives—automatically

Encryption is a critical requirement for device security. The deeper it's integrated with your device's operating system, the better it protects data from attackers. Rippling uses tools that integrate natively with macOS (FileVault) and Windows (BitLocker) to encrypt your workstations. Encryption keys are securely managed on Rippling's hardened, highly available infrastructure (see our Rippling Security Program whitepaper), and encryption keys can be centrally managed, so you can revoke, reset, and access data after staff leaves. In addition, keys can be rotated for better security.

### Enforce strong password policies

With Rippling Device Management, you can enforce custom password policies specifying minimum length, required character types, complexity, and frequency of password rotation. Preset password policies make it easy for you to be compliant with Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and other regulatory standards with just one click.

### Enforce OS updates

To protect against security breaches, your devices must remain up to date and patched regularly with the latest security releases. Patch management is critical to stopping newer threats from affecting vulnerable devices. Rippling provides an automated way to track

and enforce OS updates. As a default setting, you can have all updates auto-installed within a certain number of days after the updates are released. You can also choose to override this setting for specific updates when necessary.

### Remotely track and manage your fleet

[ MAC & WINDOWS ]

Rippling Device Management gives you a clear overview of every device in your organization—who each device is registered to, the current status of that device, the device details (settings, operating system version, serial number, profiles, patch updates), and more. If an employee loses their device or suddenly leaves the company, you can remotely track, lock, wipe, and reassign their device.

### Diagnose your fleet and get real-time alerts

[ MAC & WINDOWS ]

With Rippling Health Check, you get full visibility into the inner workings of your devices, with a complete audit log of events showing you exactly who did what, when, where, and how. Rippling can also proactively flag devices and send alerts, so you don't have to review devices manually one by one.

## Secure your endpoints and detect threats in real time

Endpoint security protects your workstations from vulnerabilities and malicious threats. It is becoming increasingly important as hackers have started using vulnerable endpoints as entry points to download malware and move laterally across the network targeting high-value assets.

To help protect your devices, Rippling integrates with SentinelOne, a leader in endpoint security with innovative and robust threat management. SentinelOne empowers SOC & IT Operations Teams with a more efficient way to protect information assets against today's sophisticated threats.

Learn more about SentinelOne threat detection and Rippling's integration:  
[rippling.com/app-shop/app/sentinelone](https://rippling.com/app-shop/app/sentinelone)

## Automate employee offboarding across HR and IT

Rippling is the only master data management (MDM) solution that integrates directly with your core HR and employee onboarding/offboarding system (requires Rippling Core Platform). When an HR manager or another team member offboards an employee through Rippling, they can instantly (and remotely) disable the employee's computer on a specific day and time—either before or immediately after their departure—to ensure your organization's data is protected.

Rippling's SentinelOne integration allows you to detect and protect your employees' devices in real time. You can quarantine threats or mark them as benign in one click.

**Devices**

Overview Devices People Orders Store Software Threats Advanced Updates Settings

Employee	Device	Threat Name	Detected On	Threat Level	Threat Status
Courtney Henry Web Designer	DHKML2T...	backupdbs.exe	11/18/2021	Malicious	Not Mitigated
Jacob Jones Marketing Coordinator	DYZQN6M...	backupdbs.exe	11/18/2021	Malicious	Not Mitigated
Cameron Williamson Nursing Assistant	D0SAE0Y...	backupdbs.exe	11/18/2021	Malicious	Not Mitigated
Devon Lane Web Designer	D85YBKK...	libarchive.2.dylab	11/18/2021	Malicious	Marked as benign
Brooklyn Simmons President of Sales	DLNGH16...	libarchive.2.d...			

**Mark as unsafe**  
Mark a threat as safe and therefore not requiring any mitigation

**Quarantine**  
Encrypt and move the threat and its executables (also kills the threat)

# Rippling secures your data

Security and privacy of your data is our highest priority, and our comprehensive approach reflects this.

## Comprehensive device management

Rippling Device Management is a set of tools that, bundled along with the capabilities of MDM/Data Execution Protection (DEP), provides IT administrators with an easy way to comprehensively monitor a fleet of devices under IT control. Device endpoint management has been available for some time now, but has been usually disconnected from a company's HR module, thus causing duplication of work and out-of-sync information.

By combining an organization's HR module and device management, Rippling is able to automate an entire set of functions, which would otherwise be duplicated. Take, for example, configuring a set of applications based on departments. If an employee changes departments, Rippling is able to automatically install the new set of applications without any intervention or knowledge transfer between the HR department and the IT department.

Furthermore, an organization has the full set of HR attributes when making IT decisions, which allows for greater freedom and finer control when it comes to configuring computers.

## Security is at the heart of what Rippling does

- All data is transferred using 256-bit TLS 1.2+ encryption, which is the latest cryptographically secure algorithm used by banks and governments.
- Bank-grade Advanced Encryption Standard (AES) encryption protects your data at rest
- We follow industry best practices for defense in depth: data is encrypted with multiple keys, keys are rotated regularly, and sensitive data uses end-to-end encryption



## **A strong team enables strong security**

- We keep our team up to date on the latest security practices with regular security and privacy awareness training
- New features go through extensive testing and peer review with a rigorous Systems Development Life Cycle (SDLC)
- Administrator access requires a strong password with two-factor authentication, and separation of duties is built into sensitive tasks.
- Security teams work around the clock to protect your data and respond to threats.

## **Tested and trusted**

- Rippling works with independent third parties as well as external researchers who regularly assess our site for vulnerabilities.
- All data is hosted and processed in an SSAE 16 SOC 2 compliant data center, with 24/7 physical security.
- Rippling proactively identifies and fixes issues by inviting hackers to investigate and report issues in exchange for monetary compensation with a bug bounty program.

## **Rippling makes your whole organization more secure**

- Easily enable two-factor authentication for all of your services. Use Rippling's device management for sophisticated endpoint protection.
- Quickly remove access for ex-employees.
- Download audit logs of Rippling app access.

## Rippling respects your privacy

Rippling's Device Management software collects information about a workstation in order to enforce security policies and OS patch updates. The data collected is limited to non-sensitive information.

### What information is collected?

- Basic information about local user accounts (FileVault status, timestamp of last password change, etc.)
- Installed configuration profiles
- Package receipts
- Available software updates
- FileVault 2 status, BitLocker status, enabled users, and individual recovery keys

### What information is not collected?

- Application usage information
- Keychain passwords
- Personal information such as the contents or names of personal files or any browsing history
- Employee passwords
- Organization data and files will remain confidential. No personal data is scanned, indexed, or transmitted from a device by Rippling Device Management Software. SentinelOne, however, will scan potential malware in order to flag any potential vulnerabilities

### Can Rippling remotely log into our employees devices? No.

Rippling Device Management does not have the ability to remotely log into the computer by itself. As an IT administrator, if you do wish to have that ability, you can upload custom software that Rippling will install on all computers.

### Can Rippling see or store employee passwords? No.

Rippling sometimes requires the employee's password to perform specific actions on the computer. In those cases, we explicitly ask the employee for their computer password. We don't store this password anywhere on the system nor transmit it to our servers. We use the password as needed and forget it.



# Rippling's security principles for device management

Rippling Device Management is a suite of software tools that—in combination with other security policies—give you a complete management system for Apple macOS and Windows workstations. These tools help administrators proactively maintain the entire lifecycle of registered devices, including deployment, distributed settings, security threat management, and inventory analysis.

## Simpler and more secure

As more systems are added to handle security, complexity adds to your administrative overhead. More complexity means added points of failure, possible vulnerabilities, and potential bugs. In software security, security takes the shape of added software layers. A system with native-level security controls is much easier to manage and is inherently more secure. Since Rippling's security framework works at the operating system layer, updates are painless and complexity is minimized.

## Windows and Mac, together at last

Most, if not all, device management solutions are built just for Mac or just for Windows. This is a huge problem for IT administrators, because if you have even just one employee on a Windows machine (looking at you, finance guy!), your entire device management infrastructure is rendered useless, and you have to build an entirely new one just to support that one person or device. Rippling allows you to manage your Windows and Mac devices in a single, unified system.

## 24/7 real-time enforcement

Securing a device once and neglecting it leaves the device vulnerable to future zero-day malware from user activity (intentional or unintentional). Rippling continuously (at short periodic intervals) monitors and enforces security policies across your fleet. By continuously monitoring devices, Rippling ensures your devices are always up to date. Our passwords are always available regardless of your location or device. All you need is access to the internet.

## Low resource utilization and minimal touchpoints

What good is security if it grinds your devices to a halt? Rippling's background agent requires very few resources and bandwidth utilization, so network administrators and users do not see performance degradation from agent software.

## Automatic setup for new devices, easy setup for old devices

For devices ordered through Rippling—either leased or purchased through your own Apple Business Manager account—Rippling Device Management comes pre-configured through Apple DEP or a pre-setup process by Rippling. For devices that are already deployed to users, you can easily start managing them by having the workstation user or an administrator install Rippling Management Software.

# MDM, DEP, and the Rippling Agent

Rippling manages your organization's workstations with the latest methods, including MDM, DEP, and our own agent built on Chef. Before we explain everything Rippling Device Management does, it's important to understand what MDM, DEP, and our Rippling Agent are, and what they do. Each one plays a role in controlling different functions of device management.

## MDM

The MDM protocol is built on top of HTTPS, Transport Layer Security (TLS), and push notifications. It allows IT administrators to control, secure, and enforce policies on smartphones, tablets, computers, and other endpoints.

Apple's built-in support for handling MDM commands is a valuable asset in managing devices. MDM commands are pushed to the devices through Apple's push notification service (APNs2).

Rippling uses MDM commands to automatically install Rippling Device Management software, send various commands (including configuration profile installation), and collect device information.

## DEP

Rippling uses Apple DEP, which automatically enrolls devices to a specific MDM server during the initial device setup process. The use of Apple DEP requires an Apple Business Manager account.

When you purchase a computer through your Apple Business Manager account with DEP, the computer's read-only memory (ROM) is permanently linked to your DEP account. When the computer is first turned on, it connects to Apple's servers, and its DEP registration causes Apple to redirect communication to

Rippling's MDM servers, allowing Rippling to automatically install the management software remotely—no manual setup required.

DEP also helps protect your computer in case of theft. Even if the thief wipes and reinstalls the OS, a computer with DEP registration will ping Apple and Rippling upon reboot.

## Rippling Agent

Rippling installs a small, lightweight agent on your workstations that periodically gathers information and ensures policies are enforced. The agent itself is built on top of Chef, an open-source tool that is widely supported and used for deployment and management of server fleets.

The agent is launched through LaunchDaemons (Mac) and Task Scheduler (Windows) to ensure Rippling is continuously monitoring a workstation.

One of the key features of the Rippling Agent is the ability to wipe the computer and reassign it to another employee remotely. Wiping the computer removes all the user accounts, including the data for each of those accounts. Reassigning a computer creates a new user account with a temporary password, which the user is forced to change when they log in for the first time.

# How Rippling performs device management services

Now we'll cover all the things the Rippling Agent does for you and how it does them.

## Encrypt your Apple hard drives [ MAC ]

- Encryption on macOS workstations is managed with FileVault 2. FileVault is a full-disk encryption application that uses XTS-AES-128 encryption to help prevent unauthorized access to the information on a startup disk. FileVault has a command line tool (`fdsetup`) which helps programmatically manage it
- When the Rippling Agent first runs, it uses the following code to check the current status of FileVault

```
sudo fdsetup status
```

- If the workstation is already encrypted, Rippling will retrieve the recovery key so we can back it up securely. If Rippling can't obtain the recovery key from the workstation, we change the recovery key instead

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Password</key>
    <string>
      <alice_password>
    </string>
  </dict>
</plist>
```

```
sudo fdsetup changerecovery -personal
-inputplist < input.plist
```

- If the computer is not encrypted, Rippling will start the encryption process

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Username</key>
    <string>alice</string>
    <key>Password</key>
    <string>
      <alice_password>
    </string>
  </dict>
</plist>
```

```
sudo fdsetup enable -inputlist
< input.plist
```

- Rippling securely transmits and stores the recovery key on our secured servers for easy access. In addition, we encrypt the recovery key when at rest and restrict who has access to it. Only hardware administrators granted permission via Rippling are shown the recovery key
- As indicated in the code above, Rippling requires the workstation password in order to work with FileVault. When adding user accounts to FileVault, we will prompt the user to enter their password (and confirm their password matches the required complexity). For security reasons, we do not store the password for any duration longer than what is needed to run these commands. If the password is needed in the future, we will prompt the user again

## Encrypt your PC hard drives [ WINDOWS ]

- Windows manages encryption using BitLocker. BitLocker is generally available only on Windows 10 and later versions, so Rippling is unable to manage encryption on computers with versions earlier than Windows 10. We clearly identify these workstations and bring them to an administrator's attention so they can either upgrade or manually manage encryption on them
- If the device is not encrypted, we use BitLocker to encrypt

```
`Enable-BitLocker -MountPoint $volume
-EncryptionMethod Aes256 -Pin $SecureString
-TPMAndPinProtector`
```

the volume by using the following command:

- BitLocker offers multiple options (recovery key, numbered pin, password) when it comes to securing workstations with encryption. We use the recovery key option by default, as it provides the most flexibility. If a device is already encrypted but not using a recovery key, we set

```
Add-BitLockerKeyProtector -MountPoint $volume
-RecoveryPasswordProtector
```

a recovery key by using the following command. If it already has a recovery key, Windows does allow us to retrieve it, so we do so for safe storage:

## Enforce strong password policies

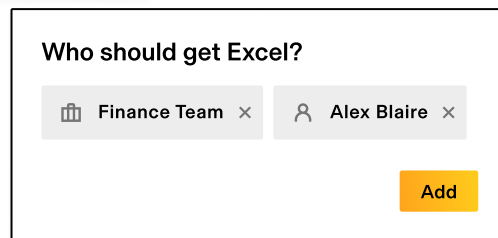
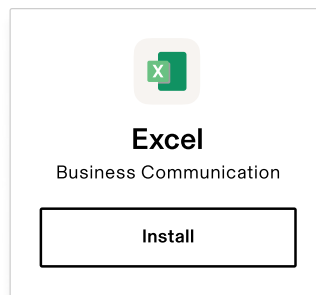
[ MAC & WINDOWS ]

- Password policies on macOS computers are enforced using Configuration profiles. Windows uses registry keys. The following is a snippet from a profile used to

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD
PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadEnabled</key>
      <true/>
      ...
      <key>allowSimple</key>
      <false/>
      <key>forcePIN</key>
      <true/>
      <key>maxFailedAttempts</key>
      <integer>6</integer>
      <key>maxGracePeriod</key>
      <integer>0</integer>
      <key>minLength</key>
      <integer>9</integer>
      <key>minutesUntilFailedLoginReset
      </key>
      <integer>30</integer>
    </dict>
  </array>
  <key>PayloadDisplayName</key>
  <string>Password</string>
  <key>PayloadOrganization</key>
  <string>Rippling</string>
  <key>PayloadRemovalDisallowed</key>
  <true/>
  <key>PayloadType</key>
  <string>Configuration</string>
  ...
</dict>
</plist>
```

enforce the password policy on macOS: Setting a policy is sometimes not enough to fully manage password requirements on a workstation. Rippling uses `pwpolicy` and `LocalUser` commands on macOS and Windows

Rippling automatically installs the right software for each employee's role or department—on any computer, Mac or PC, no matter where you bought it.



workstations, respectively, to further enhance password enforcement

- As an example, operating systems and password policies can force a user to change their temporary password. When a new user account is created, a temporary password is used and relayed to the end user. Rippling uses command line tools to mark the password for one-time use. This Rippling policy forces the user to pick a new policy-compliant password when they first log into the workstation
- Since we have a fully managed administrator account on the computer, on the rare occasion an employee forgets their password, we are able to reset it
- On Mac computers, we use the `pwpolicy` command to reset the password for that specific account and force the employee to change the password the next time they log in:
- On Windows computers, we use Chef's built-in cookbooks to change the password for that specific user account

```
pwpolicy -a #{adminUser} -p #{adminPassword}
-u #{username} -setpassword #{password}
```

```
pwpolicy -u #{username} -setpolicy
"newPasswordRequired=1"
```

## Preinstall software [ MAC & WINDOWS ]

- Rippling can be configured to auto-install a set of applications on each computer. The list of applications to be installed can be programmed based on many variables in Rippling, including employee HR attributes, like department or location. Rippling maintains a wide range of software applications that clients can select for installation. However, the applications are not limited to just that list. Organization admins can upload any custom application to be installed, as long as it is in an installable format supported by each platform
- Rippling performs application installations using open-source tools Munki and Chocolatey on macOS and Windows, respectively. Both Munki and Chocolatey validate the signatures on the signed binaries. All the application packages are directly from the companies that produce the product and thus signed by them as well
- For security reasons, Rippling restricts who can upload and manage custom software. Only employees with full hardware administrator privileges, are provided this option. For further details on Munki and/or chocolatey, please refer to the section "Open-source software and third-party tools"

With Rippling, you can push out Apple or Windows updates A) instantly and automatically, B) in the time period you set, or C) as a forced one-off.

Title ▾	Version ▾	Date ▾	Status ▾
Fortemedia - Exte...	10.12.6	05/18/22	● <a href="#">Affects 8 comp.</a>
macOS 11.6.6 - 012...	11.12.6	05/16/22	● Force by
Kumulatives Update	-	05/12/22	● <a href="#">0 comp. updated</a>

## Track and enforce OS updates

[ MAC & WINDOWS ]

- Rippling maintains a list of OS updates that are relevant to specific workstations. For macOS computers, Rippling pulls the list of all available updates daily from the Apple Server with its full descriptions and details. For each device, we pull the list of relevant updates from the device directly every few hours. We match those together to ultimately decide on how to process the updates
- For Windows computers, the list of updates from Windows is far too long to show all computers. To make the list more manageable, we only show a list of apps that are relevant to the computers we manage. Based on administrator settings, Rippling enforces update installation in a timely fashion. To avoid disruption of user productivity, users are sent emails warning them when system updates are required. If users do not voluntarily update their systems within the designated time, Rippling management software will automatically install the updates. Note that updates requiring a restart need to be forced explicitly by the administrator, as they could potentially cause disruption to user workflows
- Rippling performs OS updates using the open-source tool Munki on macOS. On Windows, updates are managed using registry configurations as well

## Remotely track and manage your fleet

[ MAC & WINDOWS ]

- As part of continuously monitoring devices, Rippling gathers a variety of information about a workstation and can quickly flag devices that require administrator attention

## Audit and diagnose your fleet

[ MAC & WINDOWS ]

- Rippling Health Check includes a high-level overview of your Encryption Enforcement, System Threats, OS Versions and Update Statuses, and more



# Detect and respond to threats in real time

[ MAC & WINDOWS ]

- SentinelOne is a leader in endpoint security, converging an endpoint protection platform with endpoint detection and response to provide innovative and robust threat management for your organization
- Rippling has deep integration with SentinelOne APIs, allowing us to manage devices and threats automatically
- We perform a sync with SentinelOne periodically (every few hours) to gather all the detected threats and details
- Based on what was detected, we reach out to the Device administrators with a list of action items for a speedy resolution

Remotely manage and protect all your employees' devices with Rippling Device Management.

The screenshot displays the 'Devices' section of the Rippling interface. It features a sidebar with navigation icons and a top navigation bar. The main content area shows a table of devices assigned to employees. A context menu is open for the 'Lenovo ThinkPad E14' device, listing actions such as 'Assign/Unassign', 'Lock/Unlock', 'Relocate', 'Reset password', and 'Delete'.

Device	Assigned To	Last Connection	Asset tag	Rippling Status	Tracking Status
MacBook Air	Jacob Jones	10 days ago	84723	Installed	Order created
LG 27BL85U-W 27"...	Devon Lane	10 days ago	0987	Installed	Order created
Lenovo ThinkBook...	Courtney Henry	10 days ago	83753	Installed	Order created
Acer TravelMate P6	Savannah Nguyen	4 days ago		Installed	
Lenovo ThinkPad E14	Kathryn Murphy	4 days ago		Installed	

## Configuration profiles [ MAC ]

- In macOS, a configuration profile is an XML file that allows administrators to distribute configuration information. Native support on macOS makes it convenient to configure a large number of devices or to provide numerous custom settings, including:
  - Restrictions on added device features
  - Wi-Fi settings
  - VPN settings
  - Credentials and keys
- Configuration profiles are powerful administrator tools that can be used for a vast array of use cases. With Rippling, administrators can upload a configuration profile that was created using Apple's Profile Manager
- For detailed information about each profile payload and setting option, see Apple's Profile Manager documentation: [support.apple.com/guide/profile-manager/welcome/mac](https://support.apple.com/guide/profile-manager/welcome/mac)
- The full reference can be found at: [developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf](https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf)
- By blocking features on a workstation, an administrator can stop users from bypassing policy enforcement, which leaves a workstation vulnerable to attacks. For example, the XML configuration file shown here blocks the use of touch ID to unlock a workstation

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadDisplayName</key>
      <string>Restrictions</string>
      <key>PayloadIdentifier</key>

      <string>com.rippling.company_name.
restrictions</string>
      <key>PayloadOrganization</key>
      <string></string>
      <key>PayloadType</key>
      <string>com.apple.applicationaccess
      <string>
      <key>PayloadUUID</key>

      <string>713E0735-97AF-4B05-A1EC-F20F5C5512CF
</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
      <key>allowFingerprintForUnlock</key>
      <false/>
    </dict>
  </array>
  <key>PayloadDisplayName</key>
  <string>Company Restrictions</string>
  <key>PayloadIdentifier</key>
  <string>com.rippling.company_name.
restrictions</string>
  <key>PayloadOrganization</key>
  <string>Company Name</string>
  <key>PayloadScope</key>
  <string>User</string>
  <key>PayloadType</key>
  <string>Configuration</string>
  <key>PayloadUUID</key>
  <string>11F9ED9C-0F57-4205-BAFE-
DD5219191B26</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
</dict>
</plist>
```

## Rippling leverages open-source software and third-party tools

For reference, Rippling Device Management uses the following open-source software and third-party tools:

**Chef** is a systems integration framework built to bring the benefits of configuration management to enterprise infrastructure. Rippling uses Chef as the base for management software to apply specific configurations to each managed workstation. [github.com/chef/chef](https://github.com/chef/chef)

**Munki**, also known as Managed Software Center, is an open-source tool that automates application installations and software updates (including ones from Apple) on macOS workstations. It also has a customizable application (Managed Software Center) with an Apple App Store-like UI to manage the application/update installations. Rippling uses Munki to install applications and OS updates on macOS computers. [github.com/munki/munki/wiki](https://github.com/munki/munki/wiki)

**Chocolatey** is a package manager for Windows. It was designed to be a decentralized framework for quickly installing applications and tools needed on enterprise workstations. Rippling uses Chocolatey to automate and manage application installations on Windows workstations. [chocolatey.org/](https://chocolatey.org/)

**MicroMDM** is a Mobile Device Management server for Apple devices currently focused on managing macOS devices. Rippling uses MicroMDM as the MDM server for registered macOS devices within an organization. [github.com/micromdm/micromdm](https://github.com/micromdm/micromdm)



LEARN MORE

[sales@rippling.com](mailto:sales@rippling.com)

[rippling.com/hardware](https://rippling.com/hardware)

Rippling helps businesses manage every employee system—their payroll, benefits, computers, apps, and more—all in a single, modern platform.

By connecting every system in a company to one employee system of record, businesses can automate all the manual work they normally have to do to make employee changes. Take onboarding, for example. With Rippling, you can set up a new employees' payroll, health insurance, laptop, and apps like Gmail and Slack—all in just 90 seconds.