paylocity
HR | Finance | IT

Paylocity for IT

Solutions for Employee Hardware and Identity & Access Management

Contents

Stop chasing ghosts in your machine

Managing employee technology is a constant balance between speed and security. Your team is under pressure to onboard new hires fast while also ensuring every digital and physical asset is tracked, secured, and accounted for.

A disconnect between HR and IT often means you're relying on manual updates, emails, and tickets to manage access and equipment — a process filled with delays and potential security holes.

This gap creates significant risks. A slow or disjointed onboarding process keeps new talent from being productive, while disorganized offboarding can leave a former employee's access active, creating a vulnerability. You're also likely paying for "ghost licenses" for software that sits unused by employees who have changed roles or left the company, a quiet drain on your budget.

There's a more streamlined way to operate. By leveraging IT asset and access management through Paylocity's HCM platform, you create a single source of truth: the employee record. When HR makes a change — whether it's a new hire, a promotion, or a termination — your IT systems are updated automatically. This isn't just about efficiency. It's about building a more secure and resource-conscious framework.

Integration eliminates the manual handoffs that slow you down and create risk. Provisioning becomes automatic, and deprovisioning is instant and comprehensive. You gain full visibility over your assets, stop wasting money on unused licenses, and strengthen your security posture. This guide will show you how unifying your IT and HR platforms can transform your operations, freeing your team to focus on strategic work instead of administrative tasks.

"Paylocity makes it easy for everyone to access the tools they need. It's simple for employees and gives leadership peace of mind with security."

Jessica Aguirre, VP of HR

TOTAL WAREHOUSE

Paylocity hardware and software solutions

Paylocity serves as the central source of truth for employee data, unlocking employee addresses, contact details, titles, role history, department details, and cost centers. With Paylocity for IT, this mission-critical data is passed securely to IT, allowing automated hardware assignments, access provisioning, and role-based updates that free up hours of HR and IT time for each update. Requests that once took days to complete now happen within minutes, keeping systems secure and giving teams more time to focus on meaningful work.

Keep employees in sync

Syncing your IT and HR directories automatically doesn't just save time — it helps prevent security issues. Active employees get access to the systems they need right away when they onboard, and that access is removed as soon as they're terminated in Paylocity. Once an employee's last day is recorded in Paylocity, their access to all systems is revoked at the same time. System administrators can also trigger a manual sync if needed.

Eliminate vulnerable passwords

Paylocity's Access Management provides built-in SSO and MFA support, so employees can securely and efficiently log in to their systems using the OneLogin security app — no need to manage separate passwords for each platform. SSO streamlines access, enhances security, and minimizes data breach risks by eliminating weak, reused, or shared passwords. Additionally, administrators gain full visibility into employee activity logs, enabling them to measure engagement, troubleshoot issues, and ensure compliance.

Additional MFA, SSO, and AI security

Switching to MFA and SSO logins not only improves the login experience but also strengthens account security. Users authenticate with biometrics, like Apple FaceID, for every system login. OneLogin enhances protection with SmartFactor Authentication, powered by Vigilance AI, which analyzes factors like location, time, device, network reputation, and user behavior to determine if a login is legitimate or potentially malicious.

Eliminate ghost licenses

Ghost licenses are unused software seats tied to employees who no longer need access. Revoking these licenses frees up seats for current staff and prevents wasted IT spending on inactive accounts.

Immediate, automated offboarding

When access needs to be removed immediately, Access Management administrators can perform a manual sync for one or more employees. This instantly disables access to corporate email and all software platforms at once, providing a faster and more secure alternative to revoking access system by system.

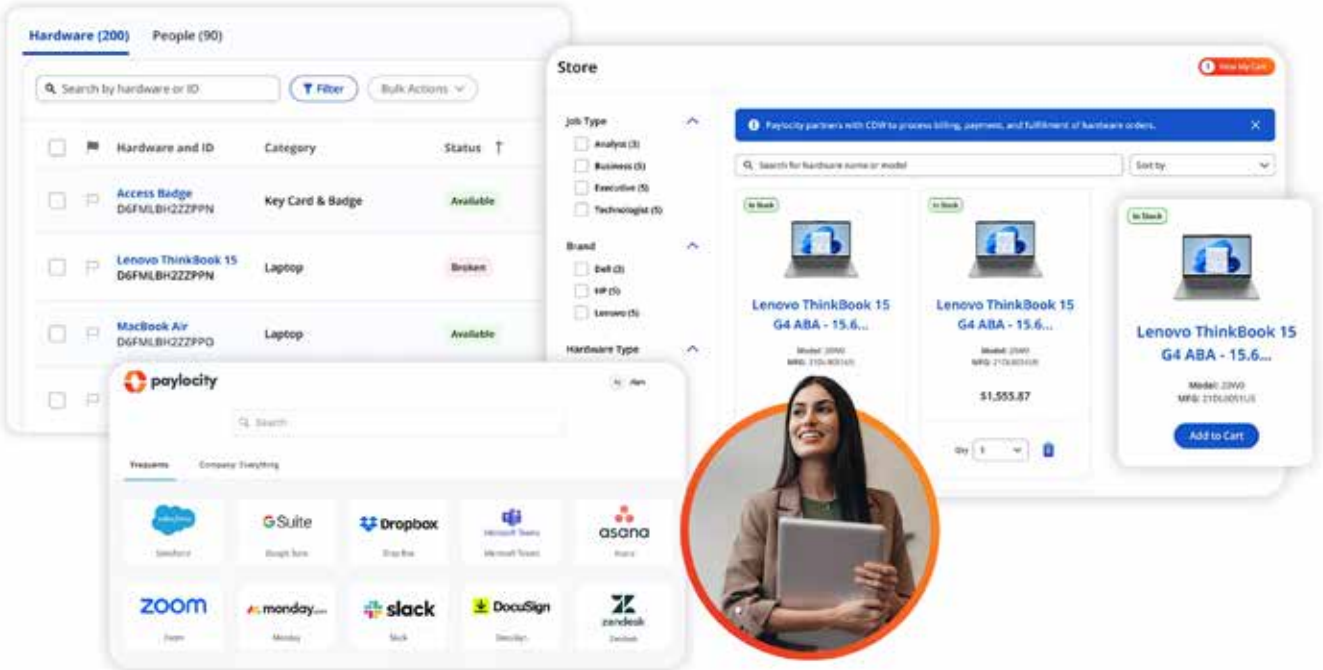
Logging and compliance tools

Paylocity's Asset Management provides centralized logging of employee account activity, giving IT teams clear visibility into engagement, potential issues, and compliance reporting. It also tracks company hardware throughout its lifecycle, linking devices like computers, phones, software licenses, and accessories to employee records. Features like return requests ensure secure hardware returns during warranty swaps or offboarding.

Security and privacy beyond IT

Our commitment to security goes beyond IT tools, with layered defenses built into every level of our platform's application and infrastructure to ensure data security and integrity. Our in-house security team, certified by ISC2 and ISACA, includes infosec champions embedded within product teams.

For a detailed look at our policies, visit trust.paylocity.com.



Paylocity hardware and software solutions

Our IT solutions help teams manage company hardware and software needs, powered by dynamic data stored in Paylocity. Customers can choose tools tailored to their specific goals, seamlessly integrating with existing platforms and security systems to boost productivity and strengthen security.

Asset Management

Organize, automate, and restock employee hardware assets based on HR data throughout key employee lifecycle events like onboarding, device upgrades, and offboarding. For IT teams, Asset Management can automate hardware purchasing, employee device assignment, and hardware retrieval, all from a centralized IT dashboard linked directly to the employee record.

Asset Management goes beyond IT hardware and software licenses, allowing organizations to track specialized tools, fleet vehicles, and other company property employees use for their jobs. Custom categories can be tailored to manage advanced IT equipment or any other company-owned assets.

How does it impact employees?

New hires can select IT-approved devices during pre-boarding for a seamless start. IT can configure selections of computers, phones, and peripherals based on department or role, while also making optional accessories available, like monitors, keyboards, and mice.

Once the new employee makes their selection, IT can choose to have CDW fulfill the shipment with support for Microsoft Intune configuration to the employee's address on file with Paylocity, or IT can have the employee pick up their devices on site.

After onboarding, employees can request hardware replacements for lost, damaged, or aged hardware from Paylocity and track the status of their device replacements.

Commonly tracked assets include:

- Employee computers
- Keyboards, mice, and monitors
- Docking stations, printers, and peripherals
- Company-issued phones
- Keycards or badges
- Specialty tools
- Software licenses
- Fleet vehicles or heavy equipment

Access Management

Deploy a complete identity and access management (IAM) solution that syncs employee data from Paylocity to IT directories like Google Workspace or Microsoft Entra ID. Automated provisioning updates permissions throughout employee lifecycle milestones — like onboarding, role changes, and offboarding — saving up to 95% of the time typically spent on manual IT tickets or emails.

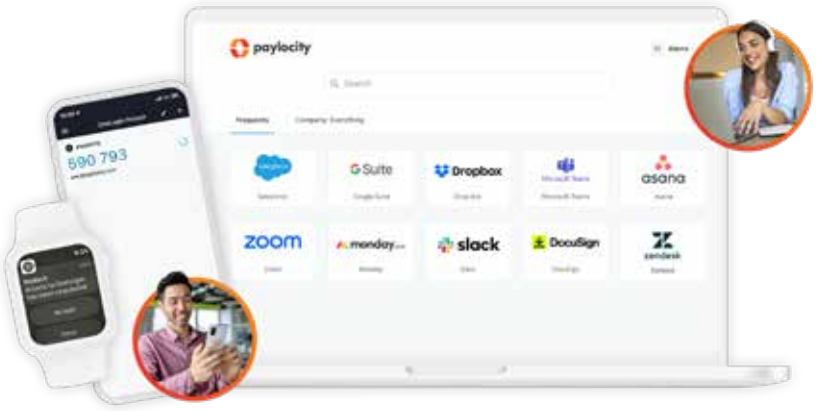
Access Management is powered by our partnership with OneLogin, a leader in employee identity management. It includes the OneLogin smartphone application and licensing for a fully integrated security experience within Paylocity. IT administrators can use Access Management to configure and monitor activity, while employee end users can use Access Management to see all productivity titles configured for SSO logins.

How does it impact employees?

Employees can access their provisioned software by selecting the Access Management section of Paylocity.

Selecting a software tile opens a new tab to log in using the OneLogin smartphone or smartwatch app, which uses location data and biometrics for industry-leading MFA and SSO safeguards. Clicking the SSO login option sends a push notification to the employee's OneLogin smartphone app confirming they requested the login attempt. The user can tap the notification, using biometrics to unlock their device, and confirming the attempt by tapping "Accept."

Once authenticated, the application will refresh, bringing the employee to their logged-in homepage for the software platform. This method is much faster and more secure than relying on individual employee-set passwords. For employees, it means faster logins without the need to manually enter multiple passwords. IT administrators benefit from enhanced security by eliminating password vulnerabilities and gaining the ability to quickly launch, modify, or revoke access across multiple software platforms.



Compatible software platforms include:

Microsoft 365 Copilot

Google Workspace

salesforce

zendesk

zoom

Dropbox

docusign

slack

servicenow

... and 7,000+ other titles

SCIM API

The Paylocity SCIM API allows IT to completely configure data syncing between Paylocity and the identity provider for granular control and maximum customization and is compatible with a variety of modern IdP providers. The SCIM API supports smart filtering, advanced employee selection, and non-employee users.

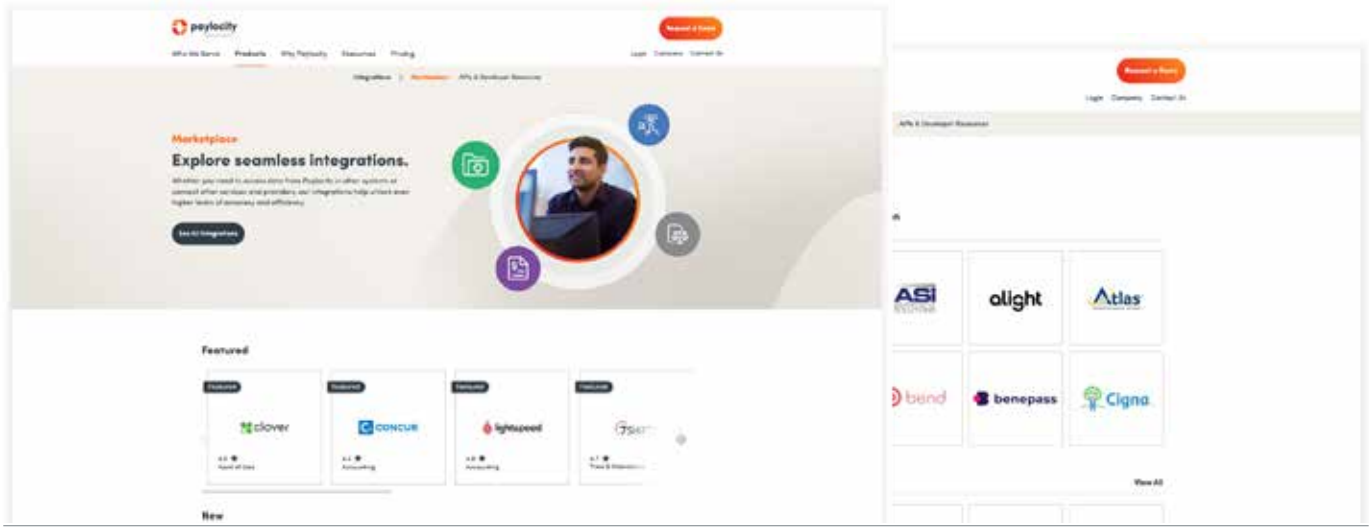
This developer API is ideal for companies that have developer resources and specific requirements to keep employee data synced from Paylocity without disrupting IT policies already preconfigured in the organization's identity platform.

Prebuilt integrations

Paylocity supports Google Workspace and Microsoft Entra ID for teams requiring a standard way to sync Paylocity data to an identity platform without advanced employee filters, non-employee support, or SSO and MFA tools that may already be configured by their IT directory.

Built for your success

Our technical solutions team is here to walk you through our solutions, understand your goals and requirements, and put together a proposal that's genuinely aligned with what your organization needs.



Supported Identity & Access Management Platforms

Microsoft Entra ID

Paylocity supports syncing to Microsoft Entra ID across Access Management, the SCIM API, and our prebuilt integration. Customers leveraging Access Management can choose whether to manage and configure employee security tools like MFA/SSO access via the Paylocity/OneLogin security app or keep this within Microsoft Entra ID.

Paylocity's Access Management solution integrates directly with your existing Microsoft ecosystem — whether it's fully cloud-based, on-premises, or hybrid. Through our partnership with OneLogin, the platform connects to the Active Directory (AD), streamlining authentication, provisioning, and lifecycle management without duplicating sensitive credentials.

At the core of this integration is the AD Connector, a lightweight Windows service installed on your domain controller. It establishes a secure outbound TLS connection to OneLogin's cloud service, enabling real-time authentication and user synchronization behind your firewall — so passwords never leave your environment.

The connector supports multiple AD instances for redundancy and scalability across forests and domains, automatically managing failover if one becomes unavailable. Admins can update connectors and access logs directly from the OneLogin interface for simplified maintenance and troubleshooting.

Tested to handle directories with millions of users, this integration ensures Paylocity Access Management scales with enterprise-grade performance while preserving your existing Microsoft identity infrastructure.

Google Workspace

Paylocity is also compatible with Google Workspace for customers interested in Access Management, the SCIM API, and our prebuilt Google integration. Google Workspace customers choosing our Access Management product can choose to rely on the Paylocity/OneLogin security app for MFA/SSO login support or keep this configured within Google Workspace.

Okta Identity

IT teams relying on Okta Identity can sync Paylocity data using our SCIM API. This method keeps Okta Identity updated with any employee changes made within Paylocity while preserving security policies and login tools configured within Okta.

One Identity

Our partnership with One Identity powers the Paylocity Access Management solution, making it seamless to integrate Paylocity and One Identity for new and existing customers via Access Management. One Identity is also a compatible IdP for use with the Paylocity SCIM API.

Other IdP providers

While these identity solutions cover a majority of the market, additional identity providers may be supported via our SCIM API. Our team can assist in exploring compatibility with additional providers.

Configuring access

Role-based access and control

As the source of truth for both HR and IT directories, Paylocity can map many attributes on the employee record to inform systems access. Attributes like role, department, and location can be used to configure automated rules to provision software. As employees change roles, Paylocity shares updates with the IT directory to make the appropriate updates. During offboarding, systems and software access can be quickly revoked to safeguard data.

Flexible entitlement mappings

With Access Management, automated user provisioning also includes licensing and entitlements for various software platforms. These license and entitlement definitions are automatically assigned and provisioned to the user for the application based on OneLogin's identity provisioning system.

Similarly, employee offboarding also includes automated deprovisioning with Access Management, ensuring software spend is not wasted on "ghost licenses" linked to inactive employee accounts.

Support for non-employee users

Many teams may depend on non-employee users for third-party providers across Finance, IT, or other contracted roles. Both Access Management and the SCIM API support defining access permissions for these non-employee role types to ensure workflows are not disrupted for hybrid workforces.

Advanced search and filtering

Access Management, the SCIM API, and our prebuilt integrations support 2-level employee filtering to drill down into specific groups of employee users based on position code and cost center combinations.

Access Management and SCIM API also support smart filtering with attributes like position code and cost center. Additional options, such as employee work location and pay groups, provide more granular control for syncing specific employee groups to the IT directory and setting rules for software provisioning.

Both products also support smart filtering that enables inclusion of users based on cost center assignments, employment details, position, supervisor assignments, and work location fields for granular control over group assignments and overall inclusion into the identity platform.

3 steps to staying in sync:

Records updated: Paylocity employee records get created when employees join the company and are updated as role changes occur.

Syncing to the IT directory: Paylocity securely shares these updated records with the IT identity platform automatically.

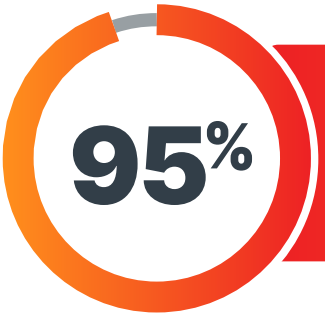
Identity platform grants access: With new data, the identity platform grants access to key systems based on preconfigured profiles.

These steps create a single source of truth that's always updated between HR and IT. For employees, this means faster access with no disruption and safer logins.

Automated provisioning

Beyond syncing HR data with the IT directory, Paylocity's IAM solutions can also be used to automatically provision corporate email and calendar accounts, and to create software access to workplace productivity platforms like Slack, Zendesk, Salesforce, Zoom, Docusign, and thousands more.

IT and HR teams can define preset rules to provision software access to employees based on title, department, and location.



Customers using Access Management or the SCIM API for automated account provisioning have seen a 95% reduction in time to create the accounts needed for new hires.

Automated deprovisioning

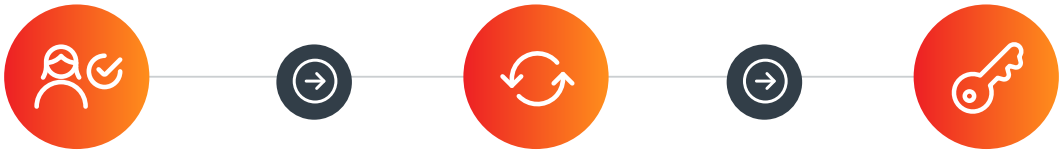
With each employee's active status synced from Paylocity, revoking access is just as simple as granting it. Using Access Management or the SCIM API will ensure employees retain needed access until the end of their last day in the role.

Once this milestone occurs, access to all systems configured using the IT directory will be revoked simultaneously. This systemic approach ensures systems and platforms are secured from former employee access and drives better compliance to safeguard company and client data.

Forcing a manual sync

For circumstances where there is an immediate need to grant or revoke access for one or more employees, administrators can trigger a manual sync. This forced sync ensures access is updated instantly, instead of waiting for the next scheduled sync set by the identity platform.

Fully integrated into your Paylocity experience



Paylocity Employee Record Created	Employee Synced to Active Directory	Access Granted to Key Software and Systems
Provision software access based on secure Paylocity employee data	Configure access and run reports directly from Paylocity	Eliminate vulnerabilities from weak or reused employee passwords

Keeping data secure

The technology powering Access Management and our SCIM API follow modern industry standards to secure data.

Paylocity IT security roles

To administer IT functions within Paylocity, a new pre-built security role grants access to configure and change directory syncing without access to HR-specific modules or employee information like salary, performance reviews, employee contact information, and more. This approach allows IT to make required updates without granting full access to HR-specific tools and information.

OAuth 2.0 and RESTful standards

Paylocity uses OAuth 2.0 for token-based authentication. Data shared via API follow a RESTful approach, using standard web methods (GET, POST, PUT, DELETE) for secure data interaction.

Data encryption

Paylocity uses a combination of RSA and AES cryptography and will provide the Paylocity Public Key when sending API credentials. The Paylocity Public Key has the following properties:

- 2048 bit key size
- PKCS1 key format
- PEM encoding

Syncable data

The following data can sync to Paylocity and the IT directory via Access Management or the Paylocity SCIM API:

- Company ID
- Employee ID
- Preferred First Name
- First Name
- Last Name
- Username
- Personal Email Address
- Work Email Address
- Work Location
- Supervisor ID

Paylocity Trust Center

For detailed information on Paylocity privacy standards, information security teams, compliance programs, and overall governance, visit: trust.paylocity.com

Access Management customers can also view OneLogin security governance details at onelogin.com/compliance/

The value of full lifecycle support

Paylocity for IT provides the right information at the right time to ensure employees get the software and hardware they need at every stage of their journey. Our IT solutions keep you in lockstep with your team's needs as they evolve.

New hire onboarding

Making a great first impression can make or break the employee experience for your new hires. Paylocity makes it easy to get hires set up with the technology they need to make an early impact in their roles.

- Allow new hires to select computers and accessories during onboarding to build their excitement.
- Ship devices directly to the employee or to a central office.
- Create corporate email and calendar accounts automatically.
- Automate software access to thousands of productivity platforms like Salesforce, Zendesk, Slack, and many more.
- Set access based on role, department, location, and more.

Throughout role changes

As employees grow within the organization, Paylocity for IT keeps everything up-to-date with the right access they need to continue their success. Updates are synced from Paylocity to IT in real-time to keep everyone on the same page.

- Proactively update access to software and systems based on role changes as they happen in Paylocity.
- Proactively flag device needs like warranty replacements, lost equipment, and required repairs.
- Reduce security vulnerabilities with industry-leading SSO/MFA security tools that let employees go password-free.
- Track device history and access events through comprehensive reporting and audit logs.
- Eliminate manual emails and support tickets for any team changes, freeing up hours of productivity for HR and IT.

Streamlined offboarding

When it's time for an employee to move on, Paylocity for IT makes it simple to revoke system access, request device returns, and secure company data. Disable access based on the termination date or manual trigger for complete control over access.

- Revoke access based on termination date set in Paylocity, or force an update manually if data access is at risk.
- Automated emails instruct employees on returning their devices securely and efficiently.
- Secure SSO logins remove the vulnerabilities of manually revoking employee access system by system.
- Prevent "ghost licenses" to ensure only active employees are using software seats.
- Robust audit trails, event logging, and dashboards keep IT informed and audit-ready.

Get started

To learn how Paylocity for IT can bring your IT and HR teams together, contact your rep or email: ITsales@paylocity.com

"I can count on one hand the number of requests for password resets we've had over the last year."

TOTAL WAREHOUSE

Harnessing Paylocity for IT empowers **Total Warehouse** to automate the tedious, manual work required to get new employees set up with their technology and improves the day-to-day experience for HR, IT, and employees.

Read the complete case study

Headquartered in Schaumburg, IL, Paylocity (NASDAQ: PCTY) is an award-winning provider of HR, Finance, and IT solutions through one unified cloud-based platform. Founded in 1997 and publicly traded since 2014, Paylocity offers an intuitive, easy-to-use product suite that helps businesses automate and streamline HR and payroll processes, attract and retain talent, and build culture and connection with their employees. Known for its unique culture and consistently recognized as one of the best places to work, Paylocity accompanies its clients on the journey to create great workplaces and help all employees achieve their best.