

onelogin

EBOOK

Securing the Cloud for the Modern Enterprise



Executive Summary

In this ebook, we dive into how identity management streamlines access to the cloud while protecting corporate data.

The location of many resources is changing to the cloud, yet companies still need central management of those resources. Trying to maintain security and order in a chaotic free-for-all use of cloud apps and bring-your-own-device culture is like a black hole sucking in IT's time—time they could be dedicating to other projects.

OneLogin's cloud identity management platform spans the entire application portfolio with secure single sign-on (SSO), multi-factor authentication (MFA), user provisioning, integration with common directory infrastructures such as Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and various cloud directories, and more.

We recommend the following:

- IT departments leverage OneLogin for all their identity management needs
- IT departments educate users about security and safe sharing
- App owners enable Security Assertion Markup Language (SAML) to provide better security and user experience

Contents

Introduction	4
Chapter 1 Identity Management	6
Chapter 2 App Provisioning	19
Chapter 3 User Provisioning	28
Chapter 4 Trusted Gatekeeper	35
Chapter 5 360° View of Cloud Security	40
Conclusion	45

Introduction

“ With great power there must also come—great responsibility! ”

-AMAZING FANTASY, August 1962

The Cloud: Power and Vulnerability

The cloud is amazing and powerful. And with its great power of convenient access, increased collaboration, and connectivity comes the great responsibility to protect all the data stored within.

However, new strengths come with new vulnerabilities, like over-sharing and unnecessary connections between cloud apps and other systems, providing attackers easy ways to steal data.

IT Security Nightmare

While the use of cloud applications has empowered employees, contractors, partners, and so forth, it has caused increased identity-related costs, not to mention the headaches and lost sleep for IT departments:

Shadow IT (unsanctioned apps)

- Our own survey of 200 IT leaders showed that 71 percent admit to using unsanctioned apps like Dropbox and Google Apps to get work done.
- Another survey (by Cisco), revealed that the large majority of IT professionals believe unauthorized programs resulted in as many as 50 percent of companies' data loss incidents.

Poor Password Hygiene

- Employees still store passwords on sticky notes or in spreadsheets, create weak passwords, and share credentials.
 - 44 percent of the 200 IT leaders said employees manage passwords on sticky notes and spreadsheets.
 - An estimated 18 percent of employees share their passwords with co-workers.

Poor visibility

- It's difficult to see who has access to what, who signed in when.
- IT has to operate in a bring-your-own-device, anytime, anywhere culture.
- Poor visibility hinders IT from enforcing security policies, like multi-factor authentication (MFA).

Increased manual maintenance

- Provisioning and deprovisioning users manually from cloud applications not only takes up your valuable time, but also introduces risk of human error.

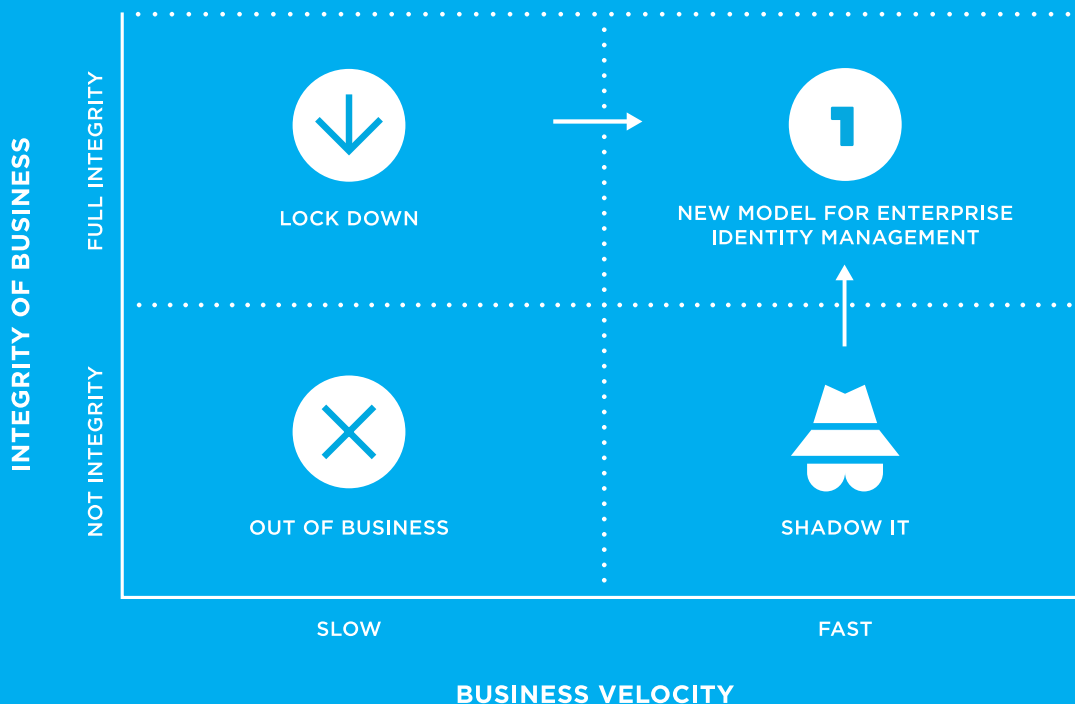
Some industries take a firewall approach and lock people out, but in a high-tech environment, you can't afford to do that. So, how can you enable your workforce without giving up business integrity?

Secure corporate data (and get more sleep) with an identity management solution.

“ Data security in the cloud is a priority for every company, ”
regardless of size and industry.

-THOMAS PEDERSEN, CEO and Co-founder of OneLogin

FIGURE 1. The Problem: Forced Choice Between Speed and Integrity



1. Identity Management

Identity and Access Management (IAM)

noun

1. The security discipline that enables the right individuals to access the right resources at the right times for the right reasons.¹

Identity-as-a-Service (IDaaS) is a safe, long-term solution for reducing IT costs, increasing security, meeting compliance requirements, and being in a position to tackle the next new business initiative.

Note: If you do not have AD, you might not need it. Skip to the last section of this chapter ([p16](#)).

In this chapter we'll focus on the following:

- Benefits of directory integration
- How to integrate Active Directory with OneLogin
- Questions to ask about real-time AD sync
- How a cloud directory can bring order out of chaos

Benefits of Directory Integration

Although employees are increasingly using cloud apps to do their jobs, Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) still play a critical role in how a company manages directory-based identity-related services. That's why OneLogin securely connects your AD or LDAP infrastructure to OneLogin and your cloud applications.

With directory integration, users can sign into applications with their existing network credentials, not to mention the following benefits for IT.

Eliminate passwords

Once a user has logged into OneLogin, the combination of SAML-based single sign-on (SSO) and OneLogin's AD integration eliminates additional passwords for all the applications that support SAML (Security Assertion Markup Language) by using the XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. Fewer passwords mean improved user experience, reduced IT workload and increased security.

Enforce AD password updates

When a user with an expired password tries to sign into OneLogin, they are prompted to enter the existing password and select a new password that complies with password requirements as defined by the user's security policy in OneLogin. Security policies define password minimum length, whether the password must contain digits or special characters, how often the password expires and how long to prevent reuse of old passwords. Once the user enters a valid new password, OneLogin updates the user's password in AD and the user is signed into OneLogin. It is possible to disable this password update feature in OneLogin.

Unify multiple directories

For organizations that have their user base spread over multiple directories, OneLogin can combine and present them as one, unified directory to other applications for federation via SAML. OneLogin allows for the integration of any number of AD and LDAP directories. Most applications are only able to integrate with one directory per customer, but the combination of OneLogin's directory integration capabilities and SAML overcomes this limitation.

Avoid point-to-point application integration

Some applications can delegate authentication to a directory via LDAP; however, as the number of applications increases, the cost of maintaining the integrations increases, and your firewall ends up looking like Swiss cheese.

Use OneLogin's integration capabilities with Active Directory Federation Services

OneLogin can co-exist and seamlessly integrate with your Active Directory Federation Services (AD-FS). Through OneLogin's catalog of thousands of pre-integrated applications, you can use AD-FS to sign users into OneLogin and directly into SAML-enabled applications. Rather than investing time and energy in learning how to integrate applications into AD-FS, you can simply leverage OneLogin's integration capabilities. [For more information about how OneLogin can integrate with AD-FS, please refer to the Trusted IdPs whitepaper.](#)

Automate app provisioning and deprovisioning

Because OneLogin's Active Directory Connector subscribes to AD change notifications, IT no longer has to provision and deprovision users manually. Provisioning and deprovisioning happens automatically in real-time.

Configure OneLogin to push user provisioning updates to AD

If you are managing users in OneLogin or Workday, you can configure OneLogin to automatically push user updates to AD. For example, if Workday is the system of record for users, any new user in Workday is automatically created in OneLogin and in AD (see Figure 2).

You can even use Workday provisioning groups to define the user's organizational unit and permission groups. [For more information on how OneLogin integrates with Workday, read the OneLogin for Workday whitepaper.](#)

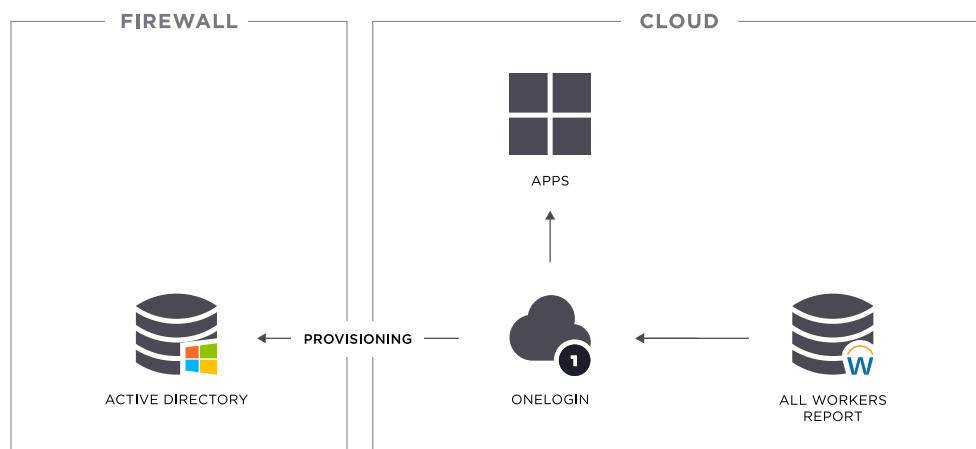


FIGURE 2. WORKDAY PROVISIONING INTO ONELOGIN

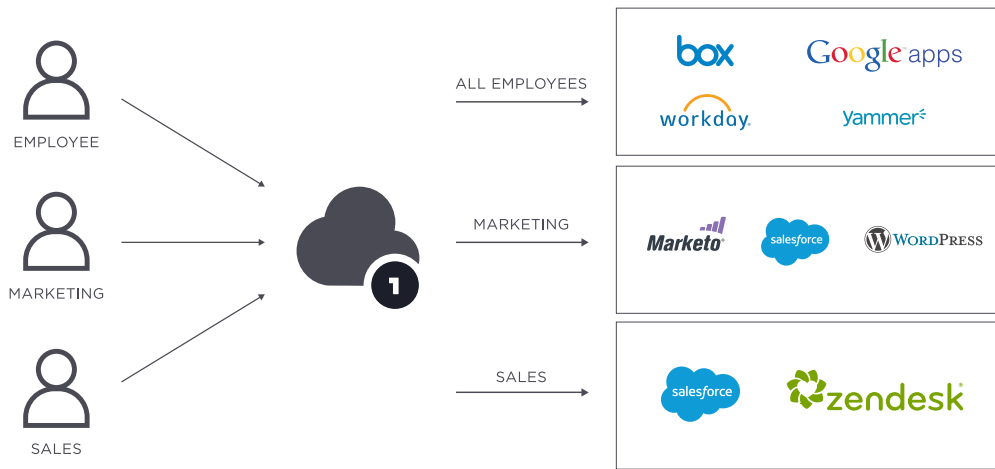


Figure 3. Role Assignments in OneLogin

Create rule-based mappings

OneLogin automatically imports user AD security group memberships, which can be used to automate the assignment of applications to users. This is done via powerful rule-based mappings that make it possible to express rules such as the following:

For all users where OU contains “Sales” and OU does not contain “USA,” assign the roles Employee and European Sales.

Roles are the mechanism within OneLogin that assigns applications to users. A user can have multiple roles, and one application can belong to multiple roles (see Figure 3). For example, even though both the marketing and sales roles contain Salesforce, assigning both roles to a user will only give the user one Salesforce login.

Enforce MFA with centralized access control

Instead of signing into applications directly, users must authenticate via the identity provider, subject to multiple authentication factors.

Increase AD security through delegated authentication

The outbound, persistent connection from the AD Connector enables OneLogin to validate user credentials against AD, without having to store any AD passwords in OneLogin. When a user tries to sign into OneLogin by entering

the username and password, OneLogin sends a delegated authentication request to the AD Connector, which in turn validates the user's credentials against AD. Delegated authentication ensures that your AD passwords are not stored anywhere outside the firewall.

Gain visibility with a centralized audit trail

All sign-in activity is recorded in a centralized audit trail, which simplifies compliance and enables cross-application analysis.

Manage remote access

OneLogin supports key remote management capabilities including AD Connector auto update as well as remote log retrieval.

OneLogin's turnkey solutions seamlessly connect your AD infrastructure to OneLogin and your cloud applications without compromising security or productivity—and IT departments can install OneLogin quickly and easily. Read the next section to find out more about how OneLogin integrates with AD.

How to Integrate Active Directory with OneLogin

Installation

Installation only takes a minute.

Integrating internal directories with cloud applications can be an expensive and cumbersome process that frustrates IT administrators and causes maintenance headaches for the entire organization. OneLogin's AD integration sets a new standard for ease-of-use with its no-touch installation process, which can be completed in as little as one minute.

The AD Connector runs as a Windows service.

The AD Connector is installed by downloading a Windows executable that deploys the Connector as a Windows service. Because the AD Connector runs as a Windows service, you don't have to worry about manually restarting it after a Windows reboot. OneLogin issues a unique 40-character security token for each directory connected with OneLogin, which must be entered during the connector installation process. OneLogin uses it to identify each directory.

No firewall changes are required.

The AD Connector does not require any firewall changes to communicate with OneLogin, as all communication is performed over two separate, outbound SSL connections (see Figure 4).

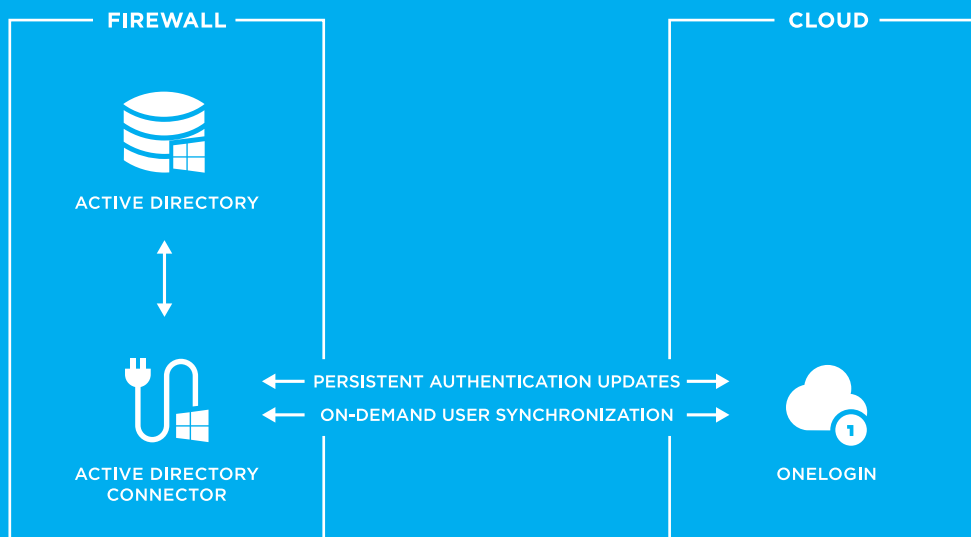


Figure 4. OUTBOUND SSL CONNECTIONS TO ONELOGIN

The AD Connector has a 100% up time.

The connection for authentication and password updates is a persistent connection that the AD Connector keeps up at all times. If, for some reason, the connection fails, the AD Connector re-establishes it immediately. The AD Connector for user synchronization communicates with OneLogin's REST API and is only established when there are pending user updates.

The AD Connector also supports high-availability mode, in which there are multiple domain controllers per domain (see Figure 5).

You can install multiple instances of AD Connectors per controller, all of which will be connected to OneLogin simultaneously. One AD Connector is designated as the primary AD Connector. If OneLogin is unable to reach the primary AD Connector, one of the secondary AD Connectors is promoted to primary automatically.

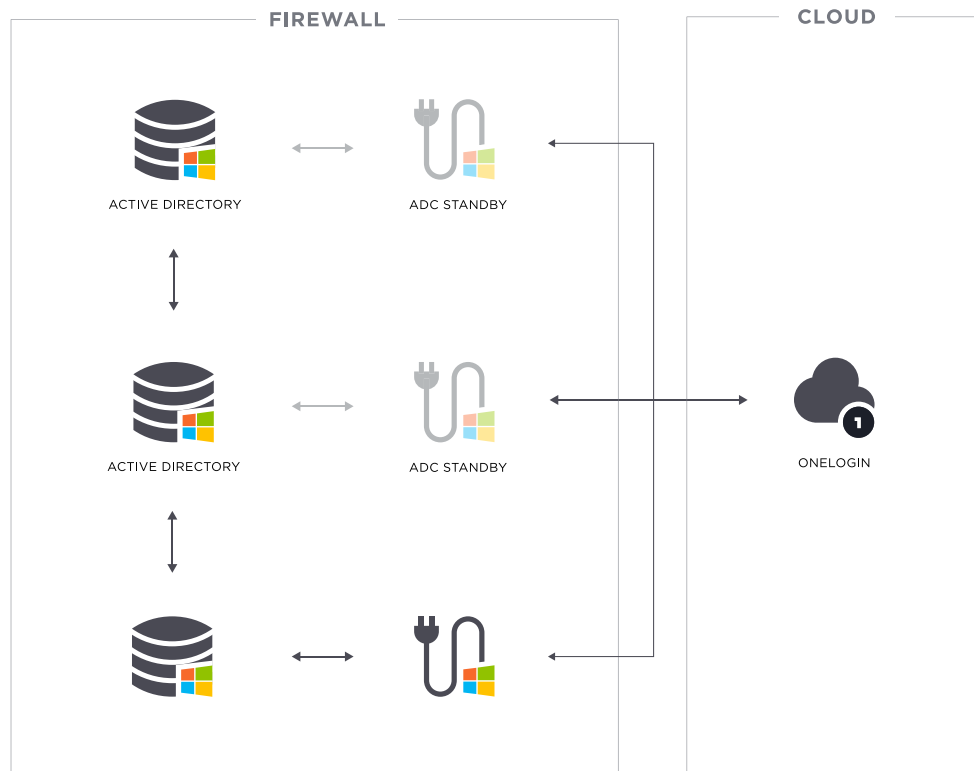


Figure 5. ACTIVE DIRECTORY FAIL-OVER

When Real-Time Isn't Real-Time: Exploring AD Sync Across IAM Software

As you explore different IAM platforms, you'll want to be sure "real-time" is exactly what it means—milliseconds, not days.

Ask these four questions to find out if "real-time" is truly real-time:

1. When you add a user to AD, how much time passes before the user can login and access apps?

Most IAM platforms will say anywhere from seconds to 1 hour to 1 day.

With OneLogin, users can start working immediately.

Since the OneLogin AD Connector subscribes to change notifications instead of scanning the full directory, updates appear in milliseconds. So new users don't have to wait until the next periodic sync before they can sign into OneLogin and start using their applications. You'll never have to say, "Just wait a couple hours ...". Consider this when assessing your needs for fast time to productivity.

2. Do roles and attributes sync with user information?

More specifically, do users come over into the cloud directory with roles and attributes correctly matched to allow them to be automatically provisioned into the correct application roles or are manual steps required to further "set up" the user?

IT can configure OneLogin for full AD attribute mapping.

As a minimum, OneLogin synchronizes email address, SAM Account, distinguishedName and memberOf, i.e. security group memberships. You can also configure OneLogin to synchronize additional fields and map them to custom fields. Note that OneLogin does not synchronize passwords from AD, unless the administrator explicitly enables this feature.

IT can easily switch app access when an employee changes departments.

For applications that are being provisioned by OneLogin, the real-time aspect is twice as useful. For example, when a user is created in AD and mapped to the Sales security group, OneLogin provisions a user in the target application within seconds.

Consider this when evaluating hidden costs of manual maintenance of your directory.

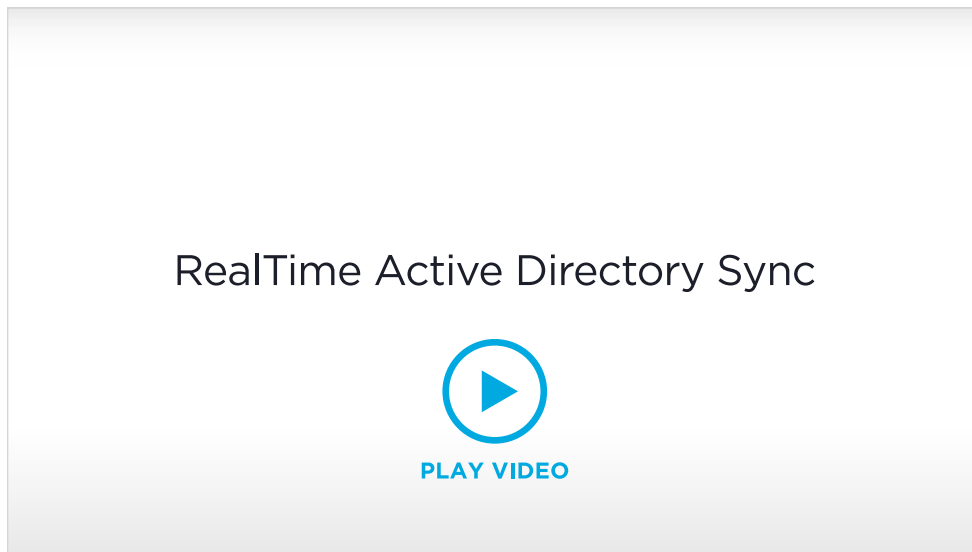
3. When you remove a user from AD, how much time passes before the user no longer has access to applications?

With OneLogin's AD Connector, deprovisioning when someone leaves the company happens in milliseconds.

You don't have to remove them from both OneLogin and AD either. Removal from AD will cause removal from OneLogin thanks to our bi-directional synchronization and authentication across AD domains, trees and forests. The real-time user sync provides an instant kill switch that effectively locks users out of OneLogin, which reduces prevents unauthorized access and data loss.

Consider this when evaluating with your Security Officer your needs for security compliance.

[Watch this 2-minute video on provisioning and deprovisioning a user with OneLogin's real-time AD sync:](#)



4. Would a user remain logged in to an app even after he or she is deprovisioned from the directory?

Most sessions expire within several minutes of inactivity, so the user will be unable to log back into the application.

But what if a user is currently in applications that tend to remain open for days or even indefinitely on mobile before expiring the session, like Google Drive or Slack, will they get locked out?

Here's just one story we've heard:

“ My last day at work was last week Friday. The IT department removed access fast. I forgot to wrap up one last thing, tried to sign in the following morning, but couldn't. ”

The odd part is I still can access files in Google Drive, maybe because I never closed Chrome? ... it's going on day 9.

You wouldn't want to rely on an application's settings of session expiration for deprovisioning.

Some directories and apps, or vendors, don't support session expiration (due to deprovisioning) at all. Second, some of those who do, aren't doing it in realtime and it could take hours for the user to be locked out of apps.

If the application supports real-time account deprovisioning, such as Salesforce, Office365, and Box, that user will be logged out instantaneously to protect corporate data. We are the only identity provider that subscribes to AD change notifications, so users can be logged out of an active session instantly, enhancing application security and compliance.

In addition to the above questions, be sure to ask if AD sync is a feature that's easy to enable and is included in the price point you're looking at.

How a Cloud Directory Can Bring Order out of Chaos

Although 90 percent of our clients use our AD real-time sync, **if you aren't already using AD, you might not need it.** Sometimes the cloud directory can provide the benefits of business integrity you are looking for without having to add on-premise complexity.

And if you do have AD and your company is using cloud apps, it should also be using a cloud directory.

Benefits of a Cloud Directory

Using a cloud directory can bring order to the chaos without creating the undue complexity that comes with AD. A cloud directory is simple, fast, secure, and at the same time, provides flexibility and increased collaboration.



“In an era where business runs on Red Bull, Active Directory is old and bloated.”

THOMAS PEDERSEN
CEO and Co-founder of OneLogin

Simplicity

A cloud directory introduces simplicity for both IT and end users. The IT department can once again manage all the resources employees use: hacking away at unessential duplicate accounts and preventing security risks. IT can use a cloud directory to automate app provisioning and deprovisioning, and easily map user roles to application role reducing a complex process into several clicks (See [p28](#)). Also, they wouldn't have to spend resources having and maintaining on-site servers needed for AD either. That's a lot of wins for IT.

The end user wins too; a cloud directory brings the simplicity of single sign-on (SSO) for all employees. For example, OneLogin's portal gives users one-click access to all their web apps in the cloud and behind the firewall.

Speed

Centralized management via AD means one more hoop to jump through, delay, and downtimes for scheduled maintenance. Yet with a cloud directory, IT can maintain centralized management without causing any delay. Changes and

updates to cloud app access can happen within seconds for any location and any device. And with the cloud directory backed by servers in multiple locations, there is no downtime.

SSO and automated provisioning also increase the speed at which employees can start using the resources they need to do their jobs.



“OneLogin’s simple approach to SAML is giving us confidence to think about shifting from Active Directory altogether, something we just wouldn’t have done before.”

COLLIN HACHWI
IT Infrastructure Manager at DISYS

Security

Usually security and complexity go hand-in-hand. So how does a cloud directory offer simplicity without sacrificing security?

Eliminating passwords

By eliminating passwords whenever possible through technology like SAML, phishing attacks and other password vulnerabilities are reduced. OneLogin also elegantly handles web applications that don’t support federation, using a technique known as password vaulting. Although not an actual physical vault, the mechanism by which vaulted passwords are stored has been extra hardened to protect them against unauthorized access.

Focusing on identity

Eliminating passwords allows OneLogin to focus on identity. Additionally, MFA and other security policies increases the likelihood that the person logging into an application is the person they say they are. You can be confident the connection between the user’s identity—that we’ve rigorously verified—and app access is accurate.

Providing audit reports

Through auditing, OneLogin knows when a user has accessed an app, which provides a higher level of security for shared applications.



“You’re going to need to be able to access all of your work—your data and your applications—no matter what device you’re on or where you’re at. OneLogin allows that to happen seamlessly.”

GARY GRAEFF
IT Group Manager at Steelcase

Flexibility

Because IT can log and view access audits and enforce MFA and other security policies, employees have the flexibility to use cloud applications that might otherwise create too high of a security risk as well as use those applications from their phones, tablets, laptops at home, the local coffee shop, library, hotel, etc.

Security policies can be created to allow a user on-premise to launch an application without any passwords, but for off-site access to the same application they will be required to use two-factor authentication.

Collaboration

Using a cloud directory is a lot like driving on the freeway and SSO is the on-ramp for employees accessing the apps they need to be productive. When employees can work without being on different roads where red lights of invalid passwords and app sign-ups slow them down—in addition to the flexibility of accessing apps from various devices in various locations—increased collaboration happens and the speed of business gains velocity.

No more black holes eating up IT’s time and no more red lights slowing down productivity.

If you are using AD, you’ve already read how easy OneLogin is (five minutes easy) to integrate. If you aren’t using AD, don’t sweat it, a cloud directory may be all you need.

2. App Provisioning

“Historically, the hardest part about implementing an identity and access management system was integration. OneLogin is changing all that with the most complete set of pre-integrated cloud applications, open source SAML toolkits, third-party SAML plug-ins, and supported directories and VPNs.

-THOMAS PEDERSEN, CEO and Co-founder of OneLogin

Once an IDaaS solution is in place, then you can begin to integrate applications. OneLogin comes with thousands of pre-integrated applications, and makes it easy to build custom integrations.




































In this chapter we'll focus on the following:

- Thousands of apps we support
- How to add an app to OneLogin
- Categories of authentication
- Why your app should be SAML-enabled ([For App Owners](#))

Thousands of Apps We Support

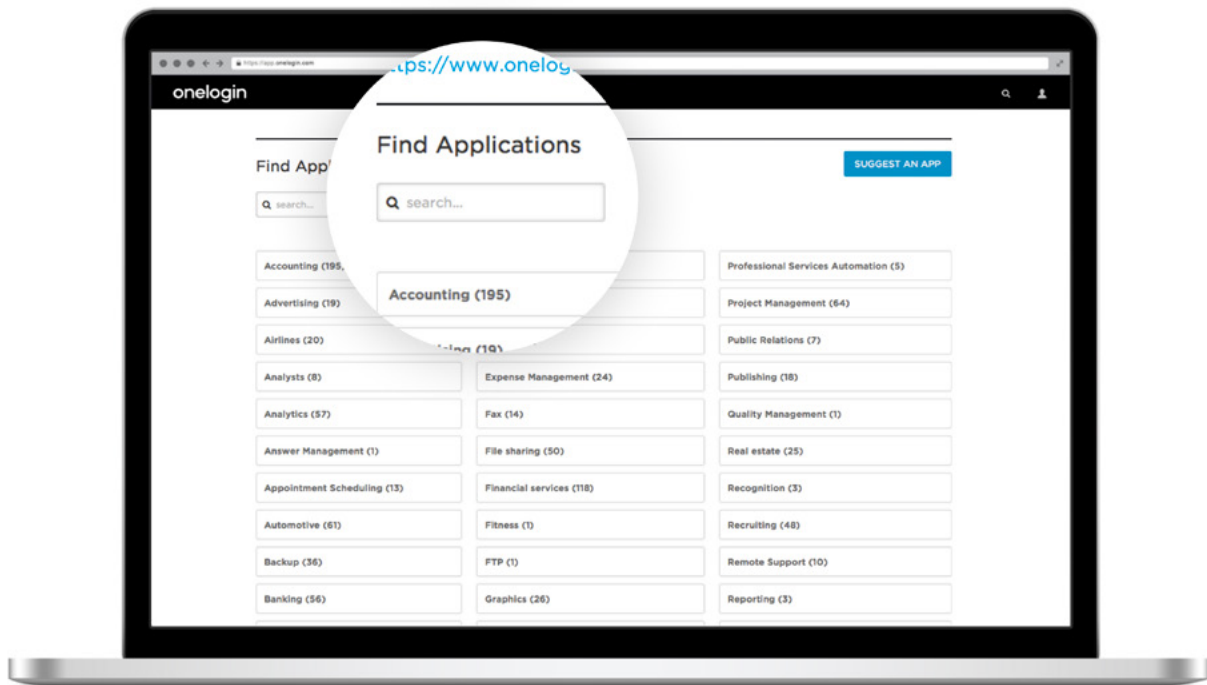
We have a catalog of more than 4,000 pre-integrated applications—making it easy to enable single sign-on (SSO) and user provisioning for your enterprise applications. OneLogin proactively maintains the integrations and adds new ones on a daily basis.

Here are the top 35 most popular apps we support.

 Office 365	 Salesforce	 Box	 Google Apps	 Slack
 Concur	 Zendesk	 Dropbox	 LinkedIn	 Workday
 Evernote	 Desk.com	 New Relic	 Hootsuite	 Asana
 GoToMeeting	 Join.me	 LivePerson	 Yammer	 LinkedIn
 GitHub	 Quickbooks	 MailChimp	 SurveyMonkey	 Netsuite
 Clarizen	 Egnyte	 DocuSign	 Oracle RightNow	 Google Analytics
 PagerDuty	 EMC Syncplicity	 Asure	 BambooHR	 Findly

How to Add an App to OneLogin

You can search for apps in the OneLogin App Catalog via the **App > Add Apps** menu. Just start typing and OneLogin will show matches below the search box. Once you have found the app you're looking for, simply select it and proceed with configuring the app for your users ([see p33](#)).



If you are using an application that we don't yet support, use our built-in suggestion feature to add it to our list.

If the app you were looking for doesn't already exist in the catalog, a suggestion box will appear. If this is a commercially available business application, OneLogin's support staff will add it to the catalog and notify you when it's ready.

OneLogin's App catalog supports any web application even if it's placed behind your firewall.

Do it yourself and build custom connectors.

We make it really easy to add additional apps into your OneLogin app portal, either via SAML or our connector wizard.

Use our connector wizard to create custom connectors for custom in-house applications.

Custom connectors can be used to provide SSO to in-house applications that are specific to your organization. All you need is a basic understanding of HTML and regular expressions and you could configure a connector in a few minutes.

Several of a connector's fields are regular expressions, which can be a little tricky to understand for beginners. Rubular is an excellent interactive regex tester that we use.

Visit our [Help Center](#) to get more details on how to build a custom connector.

Categories of Authentication

OneLogin can integrate applications in several different ways.

The ideal authentication approach depends on a number of different factors, such as the application's current SSO capabilities, whether it has a mobile or desktop client and whether it's a commercial application or one that your organization has built internally.

Here are the different categories of authentication:

- Security Assertion Markup Language (SAML)
- WS-Federation
- Federated authentication
- NAPPS
- RADIUS
- Proprietary API
- Form-based authentication

SAML

Security Assertion Markup Language (SAML) is the preferred way of handling SSO to web-based applications. It's standards-based, fast, secure, and does not rely on user passwords.

Enabling SAML only takes a few hours. OneLogin provides free, open-source SAML toolkits for Java, .NET, Ruby and PHP which both vendors and enterprises can use to add enterprise-strength SSO to their applications.

WS-Federation

WS-Federation is an identity federation specification for SSO, which is mostly used by Microsoft solutions, such as SharePoint and Office 365.

Federated Authentication

An alternative to SAML is OneLogin's Federated Authentication API, which provides an even quicker way of integrating in-house applications.

RADIUS

Clients that support the RADIUS protocol, such as IPsec VPN clients and WiFi Access Points, can authenticate against OneLogin's RADIUS interface.

Proprietary API

Some applications have their own, proprietary SSO API and OneLogin can in some cases integrate with those.

NAPPS

NAPPS, or Native Applications, is an emerging authentication standard focused on providing SSO for native mobile applications, either supplementing or replacing the traditional web browser channel often serviced by SAML. NAPPS provides SSO through a “token agent” which will enable native mobile applications to authenticate users more easily.

Form-based Authentication

Most web applications do not support SAML and in most of these cases, OneLogin stores the user’s password securely in the cloud and automates the sign-in process via the application’s login page. This sometimes requires the use of OneLogin’s browser extension, but not always.

Why Your Cloud App Should Be SAML-Enabled

If you've built an app that's not SAML-enabled, here are just a few reasons why you should.

1. Your customers are demanding it. You WILL lose business if you don't support SSO.

For many companies, SSO and MFA have gone from being “nice extras” to “must-haves.” If you haven't already lost business because your application doesn't support these features, chances are good that you soon will. In many regulated industries, such as healthcare and legal, identity management and SSO are mandated. Other industries that place a high value on efficiency and business integrity, simply won't use a product that doesn't support SAML. Doug Meier, the director of security and compliance at Oakland-based Pandora says, “Identity management SSO is so crucial to Pandora that if a prospective cloud app vendor doesn't have a SAML-connector for its SSO system—which happens about 30 percent of the time—the company will walk away.”



“Identity management SSO is so crucial to Pandora that if a prospective cloud app vendor doesn't have a SAML-connector for its SSO system—which happens about 30 percent of the time—the company will walk away.”

DOUG MEIER

Director of Security and Compliance at Pandora

Other companies may not require SAML, but without a doubt, they sure would love to have the features SAML provides. Thousands of customers have made SAML one of the top feature requests for HipChat. Commenters are begging for SSO because the ease would increase app usage by employees. Others reveal they have given up the app after 3 years of an unmet request and have already turned to a competitor.

2. Implementing SSO and MFA on your own is time consuming.

Getting it wrong can be disastrous: similar to any other crucial technology decision, choosing a solution that turns out to be difficult to maintain or doesn't hold up over time can be a major setback in time and money. So, your focus should be on finding a solution that is hassle-free and long-lasting. Managing

federation with a slew of different providers or rolling your own MFA adds a significant amount of technical debt.

For early to mid-stage startups, simply rolling out SAML enables organizations using an identity management system, such as OneLogin, to layer MFA before authentication happens via SAML, effectively increasing the security of your application, with no work on your part. Add a line like this to your FAQs: “We support multi-factor authentication through our cloud IAM partners,” and call it a day.

3. SAML is hassle-free and an established protocol.

SAML is easy because it doesn't take a lot of time and money to implement—not nearly as much as you probably think it does. SAML is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider (like OneLogin) and a cloud application (like you). It's true that SAML used to be a huge and complex investment to enable. However, now you can enable SAML in as little as 2 hours. [Learn how to enable SAML here.](#)

And SAML is safe because it is an industry standard that has been around since 2002, and is used by thousands of applications and all the leading IAM vendors. It isn't going to disappear any time soon or be replaced by some new flavor of the day that comes along.

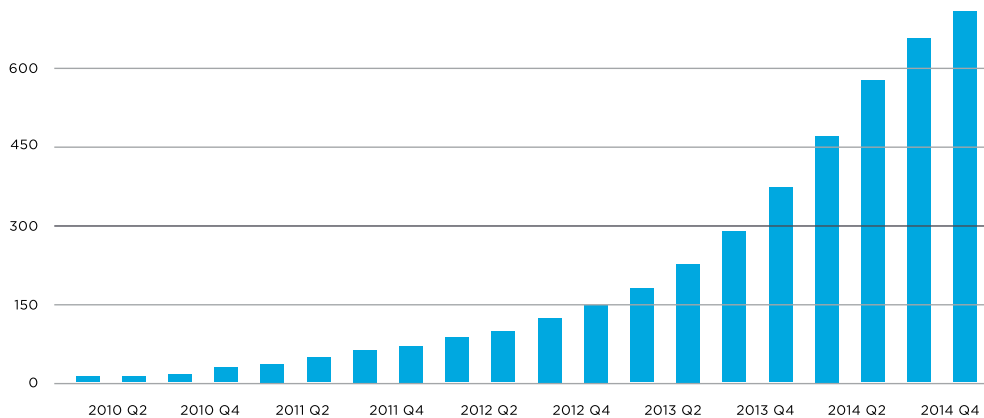


FIGURE 6. GROWTH OF SAML-ENABLED APPS IN ONELOGIN'S CATALOG

4. Add value (that you can charge for).

Application developers have embraced SAML to increase the value of their apps through all the benefits SAML provides: SSO, better usability, speed, and phishing prevention.

In talking to cloud app customers, this single feature is often what moved them up the pricing tier of an application and they don't really mind the extra cost, because the feature has become an imperative.

5. Improve your application's security profile.

By using SAML to authenticate an identity instead of passing a username and password, it can decrease your vulnerability to several attacks:

- Completely eliminates phishing attacks. The user doesn't even have a password that they could enter and they won't ever see a login screen.
- Users often reuse passwords between sites. If another site is compromised and the passwords leaked, they won't be able to be used on your application.
- Password resets can be used to compromise an application if a user's email account has been hacked. With SSO there is no password to reset (and no users sending frustrated emails that they can't login).

6. Drive application adoption.

If your application is easy to use and automatically provisioned for employees, the likelihood that they will use it increases significantly. For many applications, the hassle of trying to remember the password or ask a coworker to "add you to the account" slows adoption.

3. User Provisioning

“ With OneLogin, we can quickly provision new users, control on-premises vs off-premises access, and streamline employee on-boarding and off-boarding. ”

-MARK RIDLEY, Director of Technology at reed.co.uk

As you add applications to the platform, you'll want to configure access based on role, department, location, and other attributes. This upfront effort decreases the risk for human error and frees you up to work on other projects.

In this chapter we'll focus on the following:

- How the type of app impacts user provisioning
- Why you should automate provisioning and deprovisioning
- How to set up role mapping

How the Type of App Impacts User Provisioning

Influenced by the authentication method, apps tend to fall into 3 different types, or “tiers.” Each tier affects how a user is provisioned, some more seamless than others. Despite the type of app, IT can use group assignments to show the right people the right apps on their OneLogin dashboard.

Tier 1: The best apps support both SSO and automated user provisioning.

These apps are often the top 5 to 10 apps someone needs access to right away. Authentication is seamless, helping a user onboard faster, and automated user provisioning saves IT time.

Tier 2: Some apps support SSO, but do not support automated provisioning.

In this situation, once IT has manually set up the user account, the user will have direct access when they click on the app from their OneLogin dashboard.

Tier 3: Some apps support neither, so OneLogin provides password vaulting.

In this scenario, the user can see the app icons and upon clicking, create login credentials that OneLogin will securely store and they'll never have to see again.

Why You Should Automate Cloud App Provisioning and Deprovisioning

When an employee quits or is let go at 5 p.m. on a Friday, how often will access to key data and applications, like Box or the corporate Twitter account remain accessible until sometime Monday morning?

Here are 7 reasons to use a cloud-based IAM solution for provisioning and deprovisioning

1. Give new employees access to important apps really fast

How fast is fast? When you add a new employee to your directory, such as Active Directory, LDAP, Google Apps, or even Workday, OneLogin synchronizes users in real-time, and automatically provisions new accounts in the applications your organization uses, such as Office 365, Box, Google Apps, Salesforce, Slack, Concur and AWS. This frees up valuable IT resources.

A new employee doesn't have to futz with creating logins, storing passwords, resetting temporary passwords, or jumping through other hoops. The first time they sit (or stand) at their desk, a single login provides them a portal to all assigned applications that are accessible in a single click.

2. Make it easy for IT to provision app access based on user needs, reducing Shadow IT

Since employees generally need access to different apps based on attributes like role, department, and location, OneLogin makes things easy for you to map applications to roles and other directory attributes. For example, everyone gets access to Slack, Box and Office 365, but only developers are provisioned in AWS and only Sales and Marketing get Salesforce accounts. You can even set up role-based app access for contractors, partners, and customers.

3. Make sure users have the correct level of app permissions

Users are frequently provisioned with the wrong level of access control when provisioned manually. OneLogin provides a flexible configuration for establishing role-based controls by syncing custom user attributes from external directories and pushing them to applications that support them, such as Google Apps. This ultimately removes one more step for IT staff and increases security.



4. Protect sensitive data and applications by cutting off former employees' access to apps in seconds

When an employee leaves, deactivating their account in AD or OneLogin can automatically log the person out of all connected applications, which not only protects data but also helps prevent paying for unused licenses. Even if an application doesn't support automatic deprovisioning, as long as the application uses SAML-based authentication (over 1,000 applications in our library do), users whose OneLogin accounts have been deprovisioned will be unable to authenticate into the application. Therefore, once OneLogin is disabled, former employees are effectively cut off.

5. Allow any application to take advantage of automated user provisioning and management through open standards and toolkits

If your application doesn't support SCIM for user provisioning or SAML authentication, our developer portal and integration team can help you quickly integrate support into your applications. OneLogin's toolkits have been used by hundreds of software vendors, including Dropbox, New Relic and Zendesk to make their applications accessible through these leading standards.

6. Empower end users; increase operational velocity

Empowering users to use cloud applications is key to increasing operational velocity and creating a competitive edge in a fast-paced environment. However, the loss of business integrity is an unacceptable consequence of the bring-your-own-app/Shadow IT reality. OneLogin is a win-win-win for security, IT administration overhead, and end user productivity.

7. Save time and money

IT can maximize departmental and organizational efficiency by using the strong, centralized management of applications that OneLogin provides—eliminating passwords and the need to manage app permissions one-by-one, or change user permissions. An independent Forrester Total Economic Impact Study has shown the payback period for one of our customer's OneLogin implementation and licensing costs to be a single month.

Forrester Total Economic Impact™ of OneLogin

Summary of benefits

Through customer interviews, Forrester concluded that OneLogin had the following financial impact:

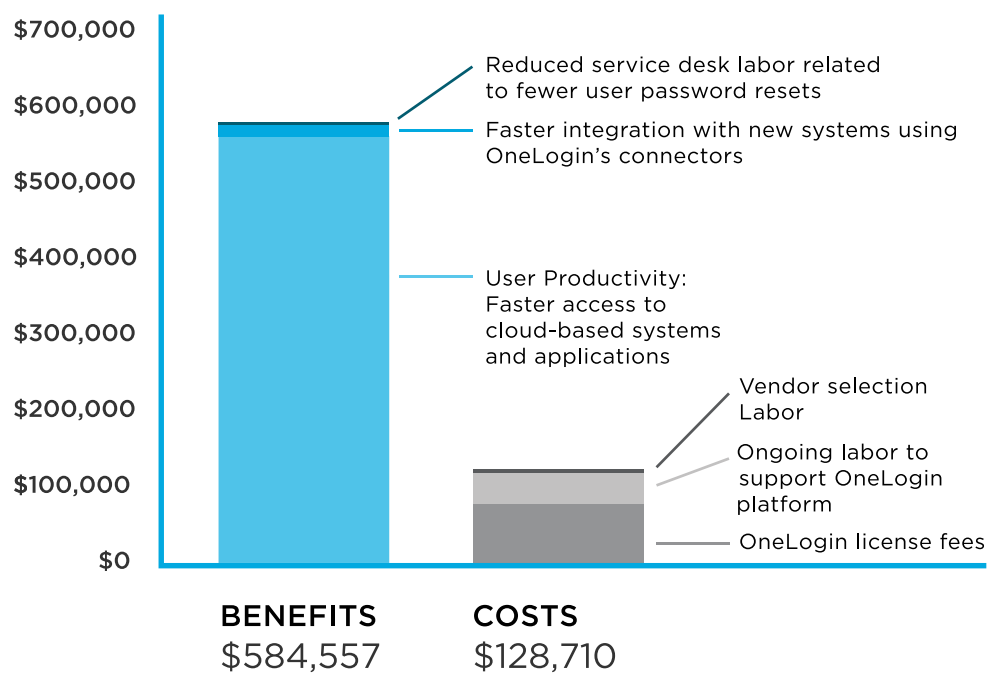
ROI
356%

Payback
1 month

NPV
\$456K

Net Present Value And Risk Adjusted

THREE YEAR ANALYSIS

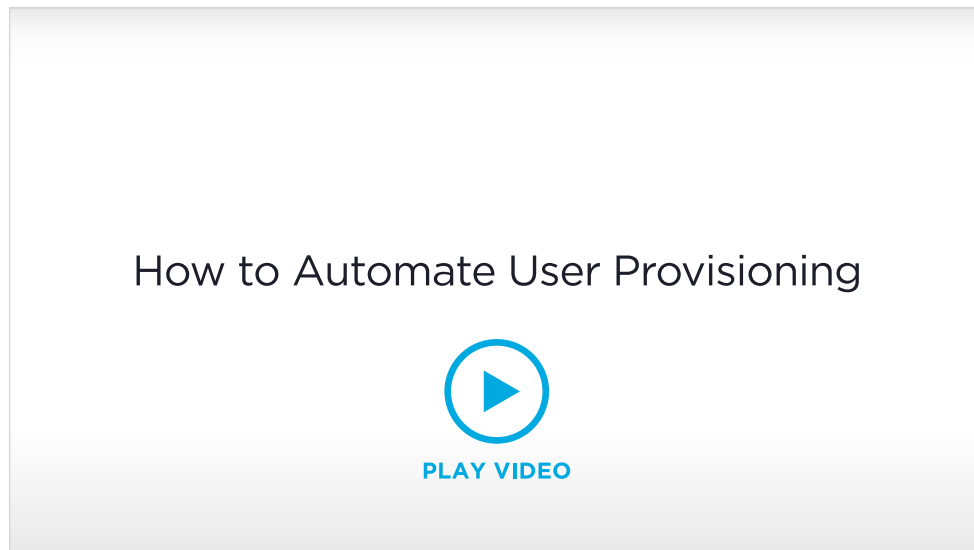


How to Set Up Role Mapping

As mentioned earlier, you can configure apps and users to give appropriate access to users that match a specific role, such as department or contractor. Role determines not only which applications users have access to but also the permissions level to which they have access within an application. You can even have overlapping roles, i.e. a user can have two roles with the same app. OneLogin will automatically figure out when to grant or revoke the app.

You'll configure both SAML and form-based applications for your users as you add apps. This will allow you to configure them for SSO and for mapping to users via roles and groups. You'll also find the configuration options for user provisioning, if the application supports it.

[Watch this webinar on how to automate user provisioning:](#)



Roles vs. Groups

Roles are used to grant apps to users, and groups are used to delegate administration of users. Groups are especially helpful in large organizations.

- Groups are typically departments, like sales, marketing, customer service, or engineering.
- Roles are collections of apps, like PR tools, social media, development, CRM.

Managing Roles

You can create and manage roles under **User > Roles**. A role consists of a name and the apps made available to users of that role. For example, if the Sales role has SugarCRM and WebEx, any user of with the role Sales will have logins for SugarCRM and WebEx. You can view and configure these logins when you edit a user.

Managing Groups

You can create and manage groups under **Users > Groups**. A group consists of a name and the user who is responsible for managing the group. For example, an engineering department manager could be responsible for managing all users in Engineering.

Punch List for User Provisioning

Not all apps will support provisioning through a solution such as Onelogin, but you can organize and manage access for users across all their apps through their OneLogin profile.

4. Trusted Gatekeeper

“If you want to do enterprise security and enterprise cloud architecture well, you’ve got to have some type of reliable identity management system or authentication portal. It’s really hard to scale and secure things and management the environment without something like that.”

-DOUG MEIER, Director of Security and Compliance at Pandora

You need better visibility and insight into app usage. But how do you get it? With OneLogin, not only do you get the benefits of user and app provisioning, deprovisioning, and organization of a cloud directory, but also the benefit a “gatekeeper.”

In this chapter we’ll focus on the following:

- Best multi-factor authentication practices
- Audit reporting & capabilities
- OneLogin compliance initiatives

If OneLogin were a gatekeeper in person, it'd look like a Secret Service agent with a sixth degree black belt—no-nonsense and rigorous about checking IDs.

However, the gatekeeper checks IDs in a way that is conscientious. He'll double check if something seems abnormal or if a person is trying to access sensitive information, and will not allow a person to access protected information without accurate identity verification. Then, in addition to making sure the right person has access, he remembers and reports on all activity.

Best Multi-Factor Authentication Practices

Ask for MFA when it matters most

With OneLogin, you can enforce MFA for increased security—and only when you decide it matters. Here are a few common situations that demand MFA:

Require MFA appropriate to user behavior

For example, Office 365 may be always accessible without MFA, while Box requires a second factor when a user is not on the corporate network.

Require MFA appropriate to the sensitivity of data

For example, opening an application with highly sensitive data such as Workday HR always prompts for MFA.

OneLogin will help you set up the conditional rules.

Companies often adopt MFA without the means to adapt it across the organization and turn to OneLogin to apply complex conditional rules to protect their data.



Provide an easy, yet secure, way for users to authenticate

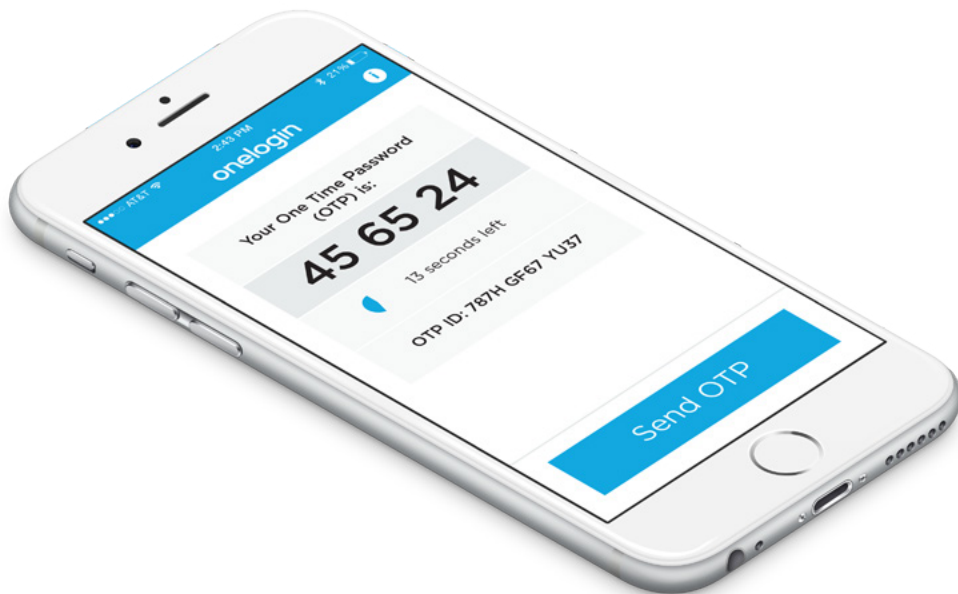
Back to the gatekeeper analogy, it's fairly easy for the person trying to get through to show their ID, and if necessary hand it over, to the gatekeeper.

Similarly, users should be able to access apps with as little friction as possible.

OneLogin OTP Mobile App

OneLogin OTP was purpose-built for use with OneLogin and provides a seamless, integrated user experience. Instead of manually entering the time-based code, the user simply presses a button and gets signed in automatically. OneLogin OTP is available on Android, iOS, Windows Phone and Blackberry devices.

In addition to OneLogin's own free one-time password app, OneLogin comes pre-integrated with Duo Security, RSA SecurID and many others.



Audit Reporting and Capabilities

Apps come and go. How can you figure out which ones are being used and which ones aren't? Who's using what? Which ones can you deactivate?

Some apps show a user's last login, but most don't. And what about apps that multiple people are using under the same credentials. How do you know who, for instance, turned off advertising when they weren't supposed to?

Gain visibility with a centralized audit trail

A key benefit of identity and access management is the centralized recording of all user management and login activity. OneLogin's audit trail records all user changes and activity, which can be used for powerful app analytics or retroactive forensics.

Analyze app usage

OneLogin's audit reports help you see what apps are being used, by what teams and how frequently. For compliance purposes, you have to be able to know who had access to what at what time. By analyzing reports, you can also accomplish the following:

Evaluate an app's cost to benefit ratio

Since reporting will help you see which applications are being used and how frequently, you'll have more accurate means to weigh the cost of an application against the value it provides the organization.

Reduce attack risks or encourage app usage

If you see that no one is using an app, either shut it down or tell people if they are supposed to be using it. Shutting down inactive applications reduces the risk of malware threats and saves you from paying for an unused app.

Plan for training and education

By gaining insight into how many people are using a particular app, let's say Salesforce, management can more easily make decisions about hiring a Salesforce specialist to help train the team or sending the most active users to a Salesforce conference.



OneLogin Compliance Initiatives

If you're in a regulated industry, you most likely need to comply with SOC and/or HIPAA. OneLogin is committed to establishing and maintaining a robust control environment that meets and exceeds the security, availability, confidentiality, and privacy commitments made to our customers. We maintain several security, risk, and compliance initiatives as part of this commitment.

SOC 2 Type 2

Companies that use cloud service providers use SOC 2 reports to assess and address the risks associated with third party technology services. These reports are issued by independent third party auditors covering the principles of Security, Availability, Confidentiality, and Privacy. Audits of OneLogin are performed semiannually.

HIPAA

OneLogin does not store electronic protected health information (ePHI), but has mapped its control framework to HIPAA security requirements to validate we are able to comply with HIPAA should the need arise. This control framework is tested as part of the SOC 2 Type 2 reports.

5. 360° View of Cloud Security

“ Cloud-focused IAM providers are under increasing pressure to deliver a unified and secure way to ensure compliance across all of an enterprise’s technology investments, both cloud and on-premise. OneLogin’s melding of cloud with legacy and on-premise solutions can help provide greater security and compliance for the many firms that are pursuing a hybrid cloud strategy.

–GARRETT BEKKER, Seniro Security Analyst at 451 Research

IAM is just one piece to the cloud security puzzle. OneLogin partnered with CloudLock to put together more pieces of the puzzle.

In this chapter we’ll focus on the following:

- How IDaaS combined with CASB provides comprehensive security
- Best practices of cloud security
- Cloud security assessment

How IDaaS Combined with CASB Provides Comprehensive Cloud Security

Is My Data Safe?

The question, “Is my data safe?” is one that every app, every company, and every user needs to answer.

To answer that question with an unequivocal “Yes!” we’ve combined our award-winning IAM platform with cloud access security brokers (CASB), such as CloudLock®, an industry-leading cloud cybersecurity platform.

OneLogin + CloudLock

OneLogin and CloudLock together allow you to better manage every single identity that touches corporate data, and protect against threats and cloud malware in real-time.



“Bridging our unique API approach with OneLogin’s single sign-on and identity management platform empowers our joint customers to gain control over suspicious activity and the growing volume of cloud malware.”

GIL ZIMMERMAN
CEO and co-founder at CloudLock

Analyze behavior to protect against account compromises

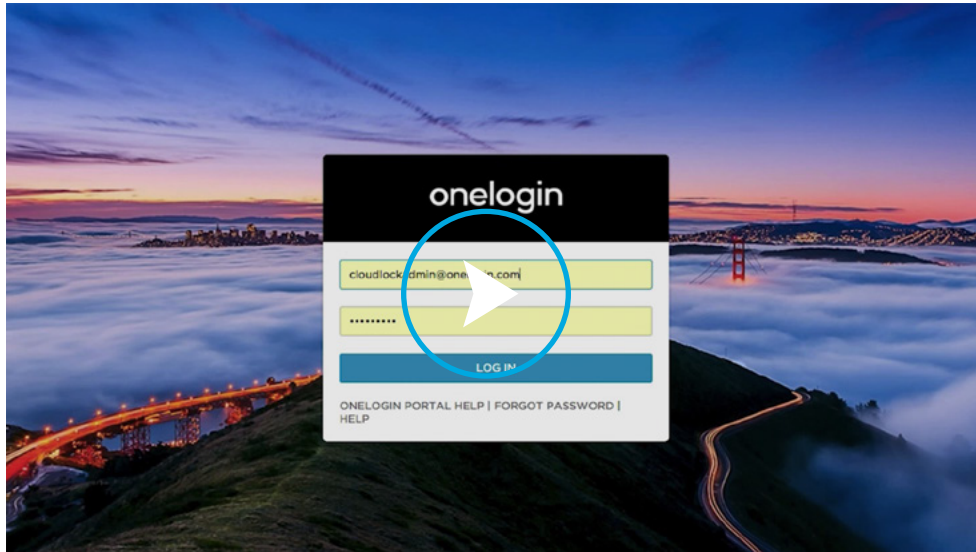
CloudLock, the cloud-native CASB, protects against account compromises through cross-platform User and Entity Behavior Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environments by flagging unusual use of apps based on advanced machine learning.

For example, behavior based on location can indicate a security risk when only the United States is on the whitelist for countries and a user tries to log into applications in London.

Or when only a time machine could cover the distance between the physical locations of consecutive access requests. If, for example, a user logs into an app in San Francisco, and 30 minutes later tries to log into the app in Boston,

CloudLock will flag the second attempt. This will trigger OneLogin to require more authentication in real-time, thus adding another layer of security to the business data.

[See how OneLogin integrates with CloudLock to protect your data:](#)



Keep Users Happy

As a bonus, the enhanced security has minimized impact on the end user. OneLogin provides a robust security solution, but does not hinder users' abilities to complete their daily tasks. Employees can access all of their apps conveniently, but should suspicious activity be noted on their account, admins can easily enhance their security requirements as necessary.

The more convenient the process is for the user, the more likely they'll be to follow security policies, and the less likely they'll turn to unsanctioned apps.

[Read more about the integration of CloudLock and OneLogin.](#)



Best Practices of Cloud Security

In addition to implementing IAM software and a CASB solution, one of the best ways to make the cloud secure is to educate end users.

Educate users on safe sharing

- Share some DOs and DON'Ts without being big brother. Hard, fast policies often cause users to ignore them.
- Remember that employees generally want to do the right thing and that they are generally intelligent about technology.

Kick off a phishing awareness campaign

- Give users examples of when they should (and shouldn't) open links in an email.
- Remind them to look twice at email signatures.
- Ask them to avoid saving files directly to the company's cloud storage solution.
- Build an accessible library of common phishing attacks within your organization.

Cloud Security Assessment

Answer these four questions to assess your organization's cloud security:

1. Have you categorized your apps based on the sensitivity of the data they contain?

Yes = good; No = risky

Not categorizing your apps based on the sensitivity of data they contain often leads to hard, fast network policies, which leads to Shadow IT.

2. Did you automate the categorization of your apps?

Yes = good; No = risky

Automating the categorization of your apps helps prevent manual error.

3. Do you regularly educate your users on best security practices and company security policies?

Yes = good; No = risky

Educating users on security practices and policies will help them understand why the practices and policies are vitally important, and they'll be more likely to follow them.

4. Do you restrict access immediately for any security policy violation?

No = good; Yes = risky

Step-up authentication, based on the seriousness of the violation (e.g. suspicious user behavior, sensitive data), is less likely to drive people to unsanctioned apps than immediate restriction for all violations. You'll also want to make sure you have a solution that enforces policies in real-time to effectively protect your data.

Conclusion

OneLogin can be your solution to the security nightmare brought on by the explosion of cloud applications.

With thousands of pre-integrated applications, powerful role mapping, and policy-enforcing capabilities, OneLogin helps you secure the cloud without impacting end users.

Request a Demo of OneLogin

Get a live demo of the OneLogin solution from one of our OneLogin Product Experts. Participate. Ask your specific questions and get real-time answers during Q&A.

[REQUEST A DEMO](#)

(855) 426-7227

Resources

OneLogin Help Center

Explore our [Help Center](#) for more information on topics from app management and building custom connectors to installing an Active Directory Connector.

OneLogin Developers Portal

Visit our [Developers Portal](#) to see the 5 steps to securing your app for enterprise usage. The first step is implementing SAML.

Open-Source SAML Toolkits

OneLogin has [open-source SAML toolkits](#) for five different web development platforms: Java, ASP/.NET, PHP, Python and Ruby.

Intelligent Cloud Cybersecurity with IDaaS & CASB

Learn more about the securing power of the combined solution of [IDaaS and CASB](#), such as OneLogin and CloudLock.

Total Cost of Ownership Overview AD-FS vs OneLogin

Explore the [costs of federating Active Directory](#) to Azure AD using AD-FS, and learn how the OneLogin solution can minimize complexity and costs.

Forrester Total Economic Impact Study

Read more details about the calculations of [financial impact](#) for one of our customers who found cost savings and business benefits by using OneLogin's IDaaS/SSO solution.

