jamf

# Identitäts-verwaltung

für Einsteiger

# Jeder Mitarbeiter hat eine eigene Identität

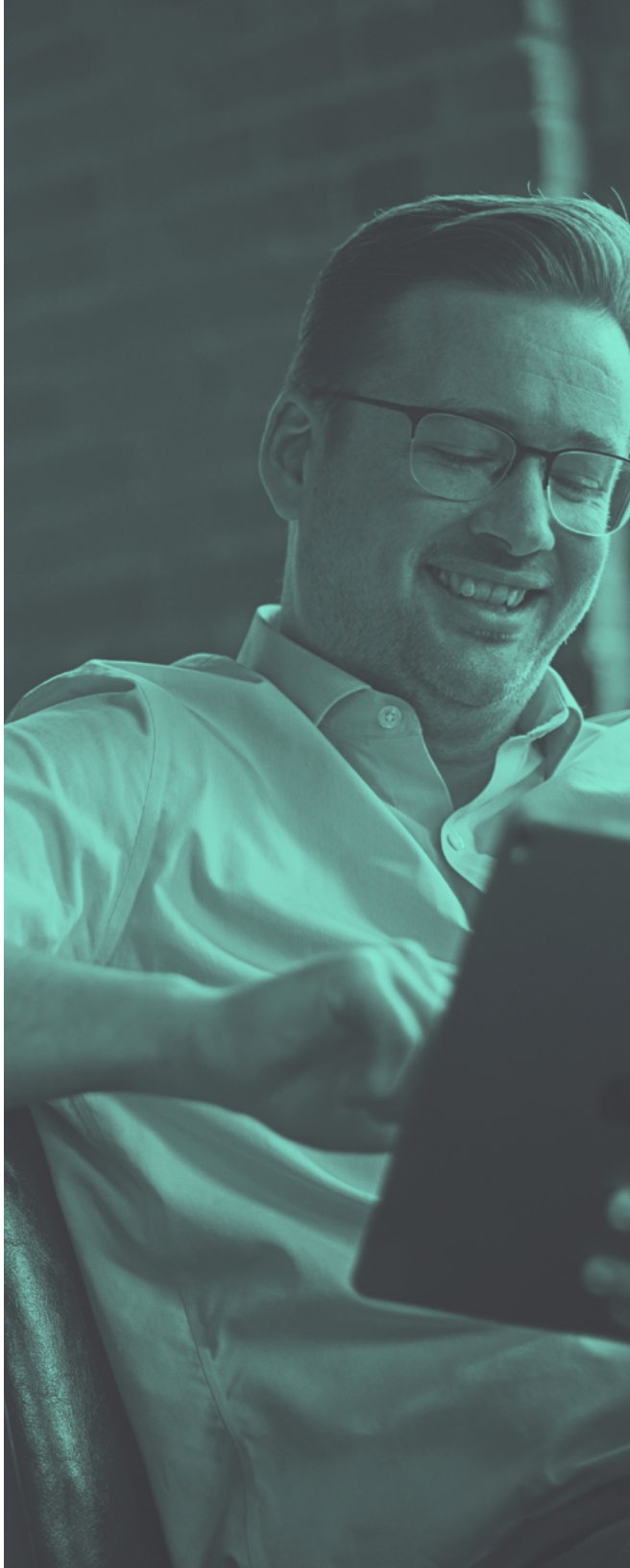
Früher gingen die Mitarbeiter:innen in ein Bürogebäude, hatten einen Desktop-Computer an ihrem Schreibtisch und die Hardware verließ diesen Standort nie. Multipliziert mit der Anzahl der Mitarbeiter:innen einer Organisation ergibt sich ein Überblick über die Geräte und Zugriffe, die die IT-Abteilung verwalten muss. Die heutige Arbeitsumgebung sieht jedoch ganz anders aus. Der moderne Arbeitnehmer ist mobil, wechselt im Laufe des Tages nahtlos von Laptop zu Tablet zu Telefon und braucht überall Zugang zu seinen Informationen und Daten.

Der digitale Fußabdruck von Arbeitnehmern hat sich vergrößert und verschlimmert, sowohl in Bezug auf die Zeit, die sie mit Geräten verbringen, als auch in Bezug auf das reine Datenvolumen, auf das sie zugreifen möchten. Eine der wichtigsten Maßnahmen, die Unternehmen zum Schutz dieser Informationen ergreifen, besteht darin, zu kontrollieren, wer Zugriff auf bestimmte Dateien, Software und Daten hat. Dies ist eine einfache Methode, um die Erfahrung der Endbenutzer zu verbessern, indem man ihnen das gibt, was sie brauchen, wenn sie es brauchen, nicht mehr und nicht weniger.

Es ist ein Aspekt der IT, der immer alltäglicher wird, aber da die technologische Welt voranschreitet und die Bedürfnisse der Mitarbeiter sich mit ihr verändern, ist es wichtig, dass Unternehmen ihre Arbeitsabläufe so gestalten, dass sie sowohl modern als auch zukunftssicher sind. Eine davon ist die Identitätsverwaltung, und sie hat höchste Priorität.

## In diesem E-Book lernen Sie:

- Grundlagen der Identitätsverwaltung
- Workflows für die moderne Identitätsverwaltung
- Warum die Cloud für den Erfolg von heute entscheidend ist
- Wie das alles mit Jamf zusammenkommt



# Grundlagen der Identitäts-verwaltung

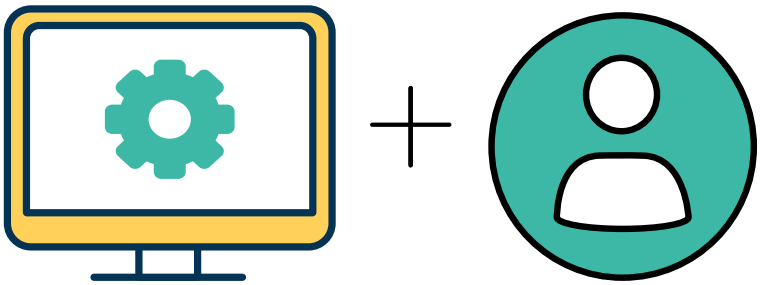
Identitätsverwaltung — auch Identitäts- und Zugriffsmanagement (IAM) genannt — ist die übergreifende Disziplin zur Überprüfung der Identität eines Benutzers und seiner Zugriffsrechte auf ein bestimmtes System. **Dazu müssen die Benutzer authentifiziert und autorisiert werden.**

Die **Authentifizierung** ist im Allgemeinen mit dem Akt des „Einloggens“ verbunden und ist der Teil, in dem Ihre Identifikation authentifiziert oder als echt festgestellt wird. In den meisten Fällen handelt es sich dabei um einen Benutzernamen und ein Passwort.

Im Identitätsmanagement bedeutet Authentifizierung jedoch nicht, dass Sie tatsächlich Zugang zu etwas haben, sondern es bezieht sich einfach auf die Fähigkeit eines Benutzers, sich zu verifizieren. Für den Zugriff auf Daten-, Software und Dateien benötigen Sie eine Autorisierung. Die **Autorisierung** bezieht sich auf die Ressourcen, Software, Daten usw., zu denen Sie Zugang erhalten, um sich zu authentifizieren.

## Authentifizierung = wer Sie sind

## Autorisierung = was Sie tun können



# Grundlagen der Identitäts-verwaltung

Um dieses Konzept der Authentifizierung und Autorisierung mit Leben zu erfüllen, erstellten die Unternehmen ein Verzeichnis, das im Wesentlichen ein Katalog der technischen Daten ihrer Mitarbeiter war. Zum Beispiel: Name, Gerätetyp, Berufsbezeichnung, Abteilung, Benutzernamen, Kennwörter und die Software und Dateien, auf die sie zugreifen mussten. Damit wurde die Grundlage für die Verwaltung von Identitäten geschaffen. Dies wird manchmal auch als Legacy IT bezeichnet.

Vor 15 Jahren war die Identitätsverwaltung noch einigermaßen einheitlich. Sie hatten Lightweight Directory Access Protocol (LDAP) für die Katalogisierung der Identifikation und der Details Ihrer Benutzer:innen, Kerberos für die Benutzerauthentifizierung, und wenn man beides zusammenfügte, erhielt man Active Directory (AD), das im Kern das Ausmaß des Identitätsmanagements darstellte. In den letzten zehn Jahren hat sich dieses Verfahren weiterentwickelt und ist in den letzten fünf Jahren noch stärker in Schwung gekommen.

Die herkömmliche IT verlässt sich auf Verzeichnisdienste als „Quelle der Wahrheit", aber da sich die Sicherheits- und Bereitstellungsanforderungen weiterentwickeln, müssen Unternehmen einen neuen Ansatz für die Identität als Teil ihrer Unternehmensstrategie wählen. Mit einem vollständigen Identitätsstack können Unternehmen die Identität über Hardware und Software hinweg vereinheitlichen, um Funktionen und erweiterte Arbeitsabläufe freizuschalten und letztendlich das Geschäft zu transformieren.

# Moderne Identitäts-verwaltung

**Bei der Umstellung von der alten auf die moderne IT geht es nicht nur um die Technologie, sondern auch darum, wie die Technologie eingesetzt wird, um die Produktivität der Endbenutzer zu steigern und das Unternehmen zu verändern.**

## Der Identitätsstapel

### Verzeichnisdienste

Dient als zentraler Datensatz für Mitarbeiter:innen, z. B. Name und Abteilung. Sie werden oft bei der Integration von Apple-Geräteverwaltungs-Plattformen wie Jamf genutzt, um Endbenutzern maßgeschneiderte Geräte bereitzustellen.

Altlasten: Active Directory vor Ort

Modern: Cloud-Directory.

### Cloud SSO

Cloud-SSO baut auf Informationen aus Verzeichnisdiensten auf und stellt sicher, dass Endbenutzer sichere Anmeldeinformationen eingeben, um auf Unternehmensressourcen zuzugreifen.

Altlasten: Benutzer müssen sich jedes Mal authentifizieren, wenn sie auf Cloud-basierte Apps oder Ressourcen zugreifen.

Modern: Benutzer genießen Zugriff auf Cloud-basierte Apps wie Microsoft Outlook und Slack bei weniger Authentifizierungs-Aufforderungen

### Jamf Connect

Mit Verzeichnisdiensten und Cloud SSO vereinheitlicht Jamf Connect die Identität über alle Unternehmensanwendungen und den Mac des Benutzers hinweg, ohne das Vertrauen zu beeinträchtigen. Endbenutzer nutzen eine einzige Cloud-Identität, um einfach und schnell Zugang zu den Ressourcen zu erhalten, die sie für ihre Produktivität benötigen.

Modern:

- Optimieren Sie die Bereitstellung und Authentifizierung für die vollständige Unterstützung von Mitarbeitern an entfernten Standorten.
- Automatische Synchronisierung von Benutzeridentitäten und Geräteanmeldeinformationen.
- Sicherstellen, dass die IT-Abteilung über umfassende Identitätsmanagement-Funktionen verfügt.

Verzeichnisdienste

Verzeichnisdienste + Cloud SSO

Verzeichnisdienste + Cloud SSO + Jamf Connect

# Moderne Identitäts-verwaltung

## Der moderne Identitätsstapel besteht heute aus drei Komponenten:

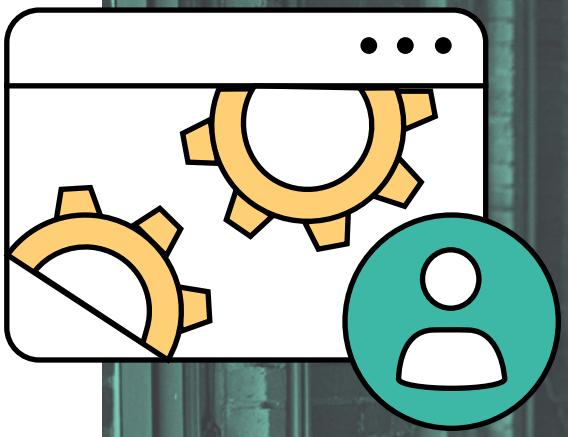
1. Verzeichnisdienste und Cloud-basiertes Single-Sign-On von einem Cloud Identity Provider (Cloud IdP), in der Regel Azurblau oder Okta
2. Jamf für die Verwaltung mobiler Geräte
3. Jamf Connect zur Vereinheitlichung Ihres Cloud-IdP, Ihrer Hardware und Software

Die Komponenten arbeiten alle zusammen, um die Endbenutzererfahrung für mobile Mitarbeiter zu verbessern und das allgemeine Sicherheitsniveau für Ihre gesamte Bereitstellung zu erhöhen.



**Was ist ein Identity Provider?**
Ein Identity Provider (IdP) ist ein Service, der digitale Identitäten speichert und verwaltet. Unternehmen nutzen diese Services, um ihren Mitarbeitern oder Benutzern die Verbindung zu den von ihnen benötigten Ressourcen zu ermöglichen. Sie ermöglichen die Verwaltung des Zugriffs, das Hinzufügen oder Entfernen von Privilegien, während die Sicherheit weiterhin gewährleistet ist.

# Moderne Identitäts-verwaltung



Da sich alle Mitarbeiter an einem Standort befanden und nur die verfügbare Technologie nutzten, um einen kleineren digitalen Fußabdruck zu hinterlassen, waren die grundlegenden Identitätsmanagementverfahren ausreichend. Das Problem ist, dass sich die Technologie verändert hat, dass Ihre Mitarbeiter täglich mehr Geräte benutzen, um auf viel mehr Daten und Software zuzugreifen, dass die Sicherheitsrisiken gestiegen sind und dass Ihre Mitarbeiter nicht mehr statisch, sondern dynamisch sind.

Wie bei vielen Aspekten der Technologie und der IT-Infrastruktur musste sich das Spiel ändern, als die Mitarbeiter mobil wurden. Bei der Identitätsverwaltung war das nicht anders. Um Active Directory und LDAP zu verwenden, bindet ein Benutzer sein Gerät an ein lokales Active Directory. Aber wie bereits erwähnt, waren die Mitarbeiter nicht mehr durchgängig vor Ort, was zu Problemen führte:

- Benutzer können ihre Passwörter nur vor Ort ändern, wenn AD erreichbar ist. Dies führt zu Verwirrung und kostspieligen Helpdesk-Tickets, wenn ein Benutzer sein Passwort vergisst oder es ganz ändern muss.
- Da AD für Windows entwickelt wurde, werden durch die Nutzung von AD als primärem Identity Provider die Verwaltungsfunktionen für Macs eingeschränkt. Dies erfordert den Einsatz von Add-ons Dritter, was die Verwaltung der Benutzer komplexer macht und höhere Kosten verursacht.
- Benutzer aus der Ferne müssen sich im lokalen Netzwerk (LAN) befinden oder ein virtuelles privates Netzwerk (VPN) verwenden, um auf interne Ressourcen zuzugreifen. Das ruiniert die Benutzererfahrung und steigert die Frustration.

Diese und andere Gründe führen zur Einführung von Cloud Identity Anbietern, einem Kernstück der modernen Identitätsverwaltung.

# Warum die Cloud für den Erfolg von heute entscheidend ist

Mit Cloud Identity kann die IT-Abteilung Benutzer, Gruppen, Passwörter und den Zugang zu Unternehmensanwendungen und Cloud-Ressourcen zentral und aus der Ferne verwalten. Cloud Identity Anbieter wie Microsoft, Google, Okta, IBM, OneLogin und Ping bieten allen Mitarbeitern — aus der Ferne und vor Ort — sicheren Zugriff auf die Cloud-Ressourcen, die sie für eine produktive Arbeit benötigen.

| Identität des Erbes | Moderne Identität |
| --- | --- |
| Active Directory | Azure |
| Open Directory | Okta |
| LDAP | Google Suite |

Da die Arbeiter:innen durch die globale Pandemie aus ihrer gewohnten Arbeitssituation gerissen wurden oder da erwartet wurde, dass mehr Arbeitnehmer unterwegs sein würden, um an der globalen Wirtschaft teilzunehmen, mussten sie von überall her Zugang zu ihren Arbeitsmaterialien haben. Zu Hause, auf Flughäfen, in Hotels, an temporären Arbeitsplätzen, in den Büros von Geschäftspartnern; die Grenzen, in denen Arbeit erledigt wird, existieren nicht mehr. Die Partnerschaft mit einem Cloud-Identitätsanbieter ermöglicht es Unternehmen, über die Grenzen ihres Büros hinaus dorthin zu gehen, wo sich ihre Benutzer aufhalten, und ihnen eine nahtlose Benutzererfahrung zu bieten, während ihre Daten und Geräte sicher sind.

# Warum die Cloud für den Erfolg von heute entscheidend ist

Ihr IdP — Okta, Azurblau, G Suite usw. — wird als Ihr Directory Service fungieren (d.h. das „Telefonbuch“ für Mitarbeiter). Das heißt, alle persönlichen Daten, die Abteilung, in der sie arbeiten, ihre Berufsbezeichnung und vor allem, welche Apps/Ressourcen auf sie zugeschnitten sind. Wenn sich ein Benutzer beim Cloud-IdP anmeldet und seine Identität validiert, hat er Zugriff auf alles, was im Cloud-Verzeichnis für ihn vorgesehen ist. Authentifizierung und Autorisierung in Aktion!

Mit diesem Cloud-IdP können Sie auch die Vorteile von Single Sign-On (SSO) nutzen, um die Sicherheit Ihrer mobilen Geräte zu erhöhen und die Benutzerfreundlichkeit auf einen Schlag zu verbessern. Anstatt dass Ihre Benutzer sich selbst authentifizieren und bei jeder einzelnen Plattform, Anwendung und jedem Dienst anmelden müssen, den Sie anbieten, können sie dies mit SSO einmalig und sicher tun und erhalten dann Zugang zu allem, was sie benötigen.

**Was ist Single-Sign-On (SSO)?**
Single Sign-On (SSO) ist ein Authentifizierungsverfahren, das es Benutzern ermöglicht, sich mit einem einzigen Satz von Anmeldedaten sicher bei mehreren Anwendungen und Websites zu authentifizieren.

## Warum die Cloud für den Erfolg von heute entscheidend ist

Um diese Sicherheit einen Schritt weiterzubringen, können Unternehmen die Multi-Faktor-Authentifizierung (MFA) nutzen. Durch Hinzufügen von MFA fügen Sie einen einfachen zusätzlichen Schritt hinzu, bei dem Ihr Endbenutzer seine Identität über einen anfälligen Benutzernamen und ein Kennwort hinaus bestätigen muss, und erhalten dennoch Zugriff auf die benötigten Ressourcen.

Um dies zum Leben zu erwecken und Ihren Cloud-Identitätsanbieter mit Ihren Geräten zu vereinen, kommt Jamf Connect ins Spiel.

**Was ist die Multi-Faktor-Authentifizierung (MFA)?**
Multi-Faktor-Authentifizierung (MFA) ist ein Authentifizierungsverfahren, bei dem der Benutzer zwei oder mehr Verifizierungsfaktoren angeben muss, um Zugang zu einer Ressource zu erhalten. Das könnte eine PIN auf dem Smartphone des Benutzers sein, Face-ID, Fingerabdruckverifizierung oder einige anderen Optionen.

# Jamf Connect bringt alles nahtlos zusammen

Active Directory wurde für Windows entwickelt, was bedeutete, dass Apple Benutzer keine andere Möglichkeit als die Anbindung an AD hatten, bevor Jamf Connect dies änderte. Da Unternehmen sich von AD abwenden und mehr Mac-Geräte einsetzen, um der wachsenden Nachfrage gerecht zu werden, müssen sie Arbeitsabläufe einrichten, um die Unternehmensdaten zu schützen und gleichzeitig eine ideale Benutzererfahrung zu bieten.

Mit Jamf Connect integrierte Cloud-Identitätsanbieter ermöglichen der IT-Abteilung die Fernverwaltung von Benutzerpasswörtern und den Zugriff auf Unternehmensanwendungen. Mit einer automatisierten MDM-Registrierung ist der Prozess einfach und sicher:

1. Ein Benutzer wird eingeladen, sich für die automatische MDM-Registrierung anzumelden.
2. Während der Registrierung wird Jamf Connect vom MDM Server heruntergeladen und installiert.
3. Benutzer werden direkt zum Jamf Connect Login-Fenster weitergeleitet und geben ihre Cloud Identity Anmeldedaten ein, anstatt ihren eigenen Benutzernamen und ihr eigenes Passwort zu erstellen.

# Jamf Connect bringt alles nahtlos zusammen

## Der Benutzer hat für alles denselben Benutzernamen und dasselbe Passwort, was ein unglaubliches Erlebnis schafft und gleichzeitig die Sicherheit des Kontos gewährleistet.

Zu den Vorteilen gehören:

- Erstellung von Konten: Erstellen Sie lokale Mac-Konten auf der Grundlage von Okta-, Microsoft Azure-, Google Cloud-, IBM Cloud-, PingFederate- und OneLogin-Identitäten, was zu einem verbesserten Anmeldeerlebnis für die Benutzer und einer organisierten Mac-Flotte für die IT-Abteilung führt.
- Sicheres Enrollment: Nutzen Sie die moderne Authentifizierung, um zu überwachen, auf welche Geräte von wo und von wem aus zugegriffen wird, und stellen Sie sicher, dass sich der richtige Benutzer auf dem Gerät befindet, bevor Sie sensible Daten bereitstellen.
- Eliminieren Sie gemeinsam genutzte Administratorkonten: Erstellen Sie mehrere IT-Administratorkonten, indem Sie die Berechtigungen des Cloud-Identitätsanbieters nutzen, ohne dass die Verwendung gemeinsamer Servicekonten erforderlich ist.
- Durchsetzung von Kennwortrichtlinien: Admins können über den Identitätsanbieter Kennwortrichtlinien durchsetzen und die Konsistenz und Sicherheit für alle Benutzer aufrechterhalten.
- Passwort-Synchronisierung: Halten Sie den Mac-Benutzernamen und das Kennwort mit den Azure-, Okta- und PingFederate-Anmeldeinformationen synchronisiert und nutzen Sie eine einzige Identität für alles, was Sie für Ihre Produktivität benötigen.*

*Die Synchronisierung von Passwörtern ist für Google Cloud derzeit nicht verfügbar.

# Jetzt gibt es die Identitätsverwaltung und die Akzeptanz wird immer größer.

Die steigende Nachfrage nach Remote-Belegschaften, mobilen Mitarbeitern und dem ständigen Zugang zu Arbeitsmaterialien macht dies zu einer Notwendigkeit. Jamf Connect führt Ihre gesamte Infrastruktur in einem nahtlosen Erlebnis für Benutzer und IT zusammen.

**Fordern Sie eine kostenlose Testversion an** oder wenden Sie sich an Ihren bevorzugten Apple Hardware-Händler, um loszulegen.