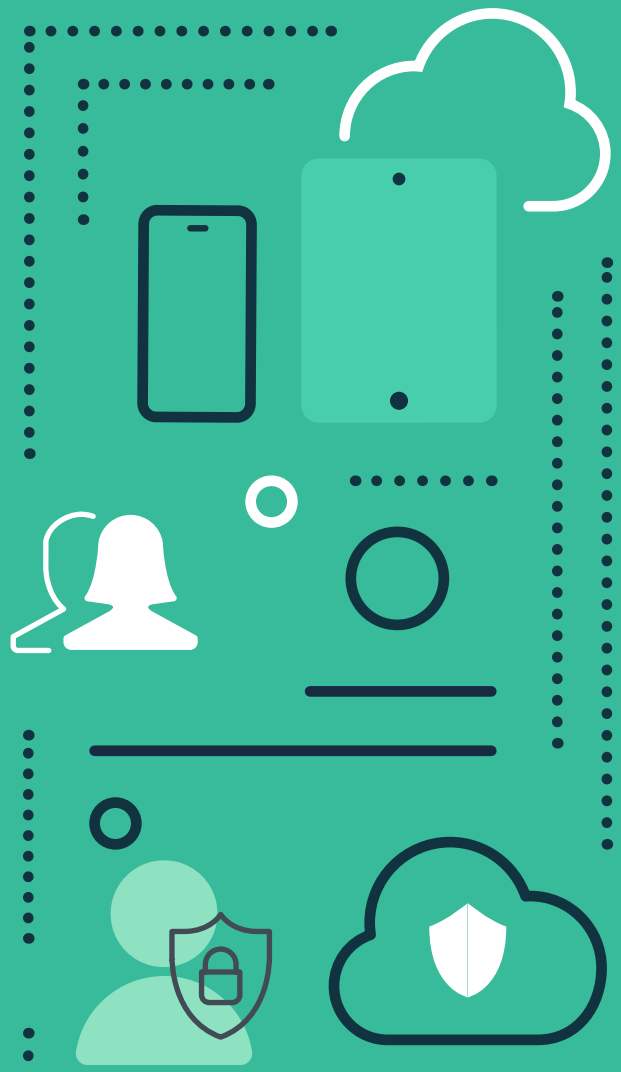

jamf

Administración de la identidad

para principiantes

CADA TRABAJADOR TIENE SU PROPIA IDENTIDAD

Tradicionalmente, los empleados iban a un edificio de oficinas, tenían una computadora de sobremesa en el escritorio y el hardware nunca salía de esa ubicación. Multiplique eso por el número de empleados en cualquier organización para obtener una idea general de los dispositivos y accesos que IT tenía que administrar. El entorno de trabajo de hoy en día es muy distinto. El trabajador moderno se basa en dispositivos móviles, cambia con facilidad de la laptop a la tableta o al teléfono durante el día y necesita acceso a su información y datos en cualquier lugar a donde quiera que vaya.

La huella digital de los trabajadores se ha expandido y acrecentado, tanto en términos de tiempo dedicado a los dispositivos como al volumen puro de datos a los que los empleados quieren acceder. Una de las tácticas clave que las empresas utilizan para proteger esa información es la de salvaguardar quién tiene acceso a archivos, software y datos específicos, software y datos, y cómo acceden a ellos. Esto se duplica como un método simple para mejorar la experiencia del usuario final, dándole lo que necesite cuando lo necesite, nada más y nada menos.

Es un aspecto de la IT que se está normalizando, pero a medida que el mundo de la tecnología avanza y las necesidades de los empleados cambian con ella, es importante que las empresas establezcan sus flujos de trabajo de manera que ambos sean tanto modernos como adaptables. Uno de ellos es la administración de la identidad, y es de alta prioridad.

EN ESTA GUÍA, HABLAREMOS DE LO SIGUIENTE:

- Conceptos básicos de la administración de la identidad
- Flujos de trabajo para la administración moderna de la identidad y el acceso
- Por qué la nube es crítica para el éxito actual
- Cómo se combina todo con Jamf

CONCEPTOS BÁSICOS DE LA ADMINISTRACIÓN DE LA IDENTIDAD

La administración de la identidad, también conocida como administración de identidad y el acceso (IAM), es la disciplina general para verificar la identidad de un usuario y su nivel de acceso a un sistema en particular. **Para lograrlo, los usuarios deben ser autenticados y autorizados.**

La **autenticación** está generalmente relacionada con el acto de "iniciar sesión" y es la parte en la que su identificación es autenticada o establecida como genuina. Lo más común es que esto se produzca en la forma de un nombre de usuario y contraseña.

Sin embargo, en la administración de identidades, la autenticación no significa que tenga acceso real a nada, sino que simplemente se refiere a la capacidad que un usuario tiene para verificarse. Para el acceso a datos, software y archivos, se requiere autorización. La **autorización** está correlacionada con los recursos, software, datos, etc., a los que se le da acceso para autenticarse.

Autenticación = quién es usted
Autorización = lo que usted puede hacer

CONCEPTOS BÁSICOS DE LA ADMINISTRACIÓN DE LA IDENTIDAD

Para dar vida a este concepto de autenticación y autorización, las empresas creaban un directorio que era, en esencia, un catálogo de los registros tecnológicos de sus empleados. Por ejemplo: nombre, tipo de dispositivo, nombre del puesto, departamento, nombres de usuario, contraseñas y el software y archivos necesarios para acceder. Esto sentó las bases de la administración de las identidades. A veces esto se conoce como IT heredada.

Hace 15 años, la administración de la identidad era algo constante. Usted contaba con el Protocolo ligero de acceso a directorios (LDAP) para catalogar la identificación y la información de sus usuarios; Kerberos, para la autenticación de usuarios, y para combinarlos tenía Active Directory (AD), que en el fondo era la dimensión de la administración de identidad. Sin embargo, en la última década este proceso ha evolucionado.

Los modelos de IT heredados utilizan los servicios de directorio como la "fuente de la verdad", pero a medida que las necesidades de seguridad y de desarrollo van evolucionando, las empresas deben adoptar un nuevo enfoque para administrar la identidad, integrado en su estrategia empresarial. Con un modelo de identidad integral, las empresas pueden unificar la administración de la identidad en todo su hardware y software para desbloquear las funcionalidades y los flujos de trabajo avanzados y, en última instancia, transformar su forma de trabajar.

CONCEPTOS BÁSICOS DE LA ADMINISTRACIÓN DE LA IDENTIDAD

La administración de la identidad va más allá de la autenticación y autorización de usuarios. También dicta cómo acceden los usuarios a los recursos de la organización.

Para los empleados remotos y móviles, la versión de IT heredada para acceder a los recursos es a través de redes privadas virtuales (VPN). Cuando se utiliza una VPN, se concede el acceso de forma global y proporciona a los usuarios acceso a toda la red de recursos, lo que supone un importante riesgo para la seguridad. Si los actores maliciosos obtuvieran acceso total a la red a través de la VPN, podrían desplazarse lateralmente para acceder a cualquier contenido dentro de esa red.

Históricamente, las VPN no son sencillas ni para usuarios ni para móviles. En el mundo laboral moderno, los usuarios necesitan poder acceder desde cualquier lugar y en cualquier momento.

ADMINISTRACIÓN MODERNA DE LA IDENTIDAD Y EL ACCESO

La transición a un modelo de IT heredado a moderno no trata solo de la tecnología, sino sobre todo de cómo poner esta tecnología al servicio de la productividad del usuario final y de la transformación de la empresa.

LA PILA DE LA IDENTIDAD

Servicios de directorio

Es un registro centralizado de información de los empleados, como su nombre y departamento. Se utiliza a menudo para la integración con plataformas de administración, como Jamf Pro, para poner dispositivos personalizados a disposición de los usuarios.

Heredados: Active Directory en las instalaciones

Modernos: directorio en la nube.

SSO en la nube

A partir de información de servicios de directorio, el inicio de sesión único (SSO) en la nube garantiza que los usuarios finales introduzcan unas credenciales seguras para acceder a los recursos de la empresa.

Heredados: los usuarios deben autenticarse cada vez que acceden a aplicaciones o recursos en la nube.

Modernos: los usuarios pueden acceder a aplicaciones en la nube como Microsoft Outlook y Slack con menos solicitudes de autenticación**.**

Jamf Connect

Combinado con servicios de directorio y SSO en la nube, Jamf Connect unifica la administración de la identidad en todas las aplicaciones de la empresa y los dispositivos Mac de los usuarios sin poner en peligro la seguridad. Los usuarios finales utilizan una única identidad en la nube para acceder de forma rápida y sencilla a los recursos que necesitan para trabajar.

Moderno:

- Aprovisionamiento agilizado y autenticación desde la caja para que los empleados a distancia tengan todo lo que necesitan.
- Sincronización automática de identidades del usuario y credenciales del dispositivo.
- Garantiza que IT cuente con todas las capacidades de administración de la identidad.
- Acceso seguro a recursos y aplicaciones empresariales con VPN de última generación

Servicios de directorio

Servicios de directorio + SSO en la nube

Servicios de directorio+ SSO en la nube + Jamf Connect

ADMINISTRACIÓN MODERNA DE LA IDENTIDAD

Cuando usted mira la pila de identidad moderna, hoy en día, está compuesta de tres elementos:

1. **Servicios de directorio y de inicio de sesión único basado en la nube de un proveedor de identidad en la nube (IdP en la nube), normalmente Azure u Okta**
2. **Jamf para la administración de dispositivos móviles**
3. **Jamf Connect para unificar su IdP en la nube, hardware y software, con acceso seguro a las aplicaciones empresariales**

Todos los componentes trabajan juntos para mejorar la experiencia del usuario final para los trabajadores móviles y aumentar el nivel general de seguridad que rodea a toda la implementación.

¿Qué es un proveedor de identidad?
Un proveedor de identidad (IdP) es un servicio que almacena y administra identidades digitales. Las empresas utilizan estos servicios para permitir a sus empleados o usuarios conectarse con los recursos que necesiten. Ofrecen una manera de administrar el acceso, agregar o eliminar privilegios, a la vez que la seguridad siga siendo sólida.

¿Qué es el inicio de sesión único (SSO)?
El SSO es un proceso de autenticación que permite a los usuarios autenticarse de manera segura en múltiples aplicaciones y sitios web mediante un solo juego de credenciales.

ADMINISTRACIÓN MODERNA DE LA IDENTIDAD Y EL ACCESO

Con los trabajadores en una sola ubicación, creando una huella digital más pequeña al aprovechar solo la tecnología disponible, las prácticas básicas de administración de la identidad eran suficientes. El problema es que la tecnología ha cambiado, los empleados utilizan cada día más dispositivos para acceder a muchos más datos y software, los riesgos de seguridad han aumentado y esos empleados han pasado de ser estáticos a dinámicos.

Como con muchos aspectos de la tecnología y la infraestructura de IT, el juego tuvo que cambiar cuando los empleados se adaptaron cada vez más a los dispositivos móviles. La administración de la identidad no fue distinta. Para utilizar AD y LDAP, un usuario vincula su dispositivo a un AD local. Pero como se mencionó, los empleados ya no se encontraban en las instalaciones constantemente, lo que ocasionó problemas:

- Los usuarios solo pueden cambiar sus contraseñas en las instalaciones cuando el AD es accesible. Esto provoca tanto confusión como costosos tíckets de solicitud de soporte cuando un usuario olvida su contraseña o necesita cambiarla por completo.
- Debido a que AD está diseñado para Windows, la ventaja de AD como proveedor de identidad principal reduce las capacidades de administración para Mac. Esto obliga a utilizar complementos de terceros, lo que suma complejidad a la administración de usuarios y aumenta los costos.
- Los usuarios remotos tienen que estar en la red de área local (LAN) o usar una red privada virtual (VPN) para acceder a los recursos internos. Esto arruina la experiencia del usuario y provoca frustraciones.

Estas razones, además de otras, hacen que la adopción de IdP en la nube sea un elemento crucial de la administración moderna de identidades y accesos.

POR QUÉ LA NUBE ES CRÍTICA PARA EL ÉXITO ACTUAL

La identidad en la nube permite al equipo de IT administrar usuarios, grupos y contraseñas de forma centralizada y remota, así como acceder a aplicaciones de las organizaciones y recursos en la nube. Los IdP en la nube como Microsoft, Google y Okta ofrecen a todos los empleados —tanto remotos como in situ— un acceso seguro a los recursos que necesitan para ser productivos.

Identidad heredada	Identidad moderna
• Active Directory	• Azure
• Directorio Abierto	• Okta
• LDAP	• Google Suite

Asociarse con un proveedor de identidad en la nube permite a las organizaciones ir más allá de las paredes de su oficina a donde están sus usuarios y proporcionar una experiencia de usuario sin problemas, a la vez que mantiene sus datos y dispositivos seguros.

POR QUÉ LA NUBE ES CRÍTICA PARA EL ÉXITO ACTUAL

Su IdP —Okta, Azure, G Suite, etc.— actuará como su servicio de directorio (es decir, su "libreta telefónica" para los empleados). Esto incluye toda su información personal, en qué departamento están, el nombre de su puesto de trabajo y, lo que es más importante, qué aplicaciones / recursos se les asigna. Cuando un usuario inicia sesión en la IdP de la nube y valida su identidad, entonces tiene acceso a todo lo que se le permite dentro del directorio de nube. **¡Autenticación y autorización en acción!**

Esta IdP en la nube también le permitirá aprovechar el poder de inicio de sesión único (SSO) para aumentar los niveles de seguridad de los dispositivos móviles de su organización y mejorar la experiencia de usuario de una sola vez. En lugar de exigir a los usuarios que se autentiquen e inicien sesión en cada una de las plataformas, aplicaciones y servicios de la organización, el SSO les permite que lo hagan una sola vez, de manera segura, y para tener acceso a todo lo que necesiten.

POR QUÉ LA NUBE ES CRÍTICA PARA EL ÉXITO ACTUAL

Para llevar esta seguridad un paso más lejos, las empresas pueden optar por la autenticación de varios factores (MFA). Al agregar MFA a la mezcla, se agrega un sencillo paso adicional que requiere que su usuario final confirme su identidad más allá de un nombre de usuario y contraseña vulnerables, y obtener así acceso a los recursos que necesite.

Al llevar esto a la práctica, y unificar su proveedor de identidad en la nube con sus dispositivos, es cuando entra en juego Jamf Connect.

¿Qué es la autenticación de varios factores?

La autenticación de varios factores (MFA) es un proceso de autenticación que requiere que el usuario proporcione dos o más factores de verificación para obtener acceso a un recurso. Este podría ser un PIN en el teléfono de un usuario, FaceID, verificación de huellas dactilares o algunas otras opciones.

JAMF CONNECT LO UNE TODO DE MANERA FLUIDA

Active Directory se creó para Windows, lo que significaba que los usuarios de Apple no tenían ninguna opción excepto la vinculación a AD antes de que Jamf Connect lo cambiara todo. Cada vez más organizaciones optan por prescindir de AD e incorporan los dispositivos Mac a sus flotas en respuesta a la creciente demanda. Y eso implica también introducir flujos de trabajo que velen por la seguridad de la información y, a la vez, ofrezcan una excelente experiencia a los usuarios.

Los proveedores de identidad en la nube integrados con Jamf Connect permiten al equipo de IT administrar contraseñas de los usuarios y acceder a las aplicaciones de la empresa en forma remota. Utilizando la inscripción de MDM automática, el proceso es sencillo y seguro:

1. **Un usuario recibe una invitación para apuntarse a la inscripción de MDM automatizada.**
2. **Durante la inscripción, se descarga Jamf Connect y se instala desde el servidor de MDM.**
3. **Los usuarios son dirigidos directamente a la ventana de inicio de sesión de Jamf Connect e introducirán sus credenciales de identidad en la nube, en lugar de crear su propio nombre de usuario y contraseña.**

JAMF CONNECT LO REÚNE TODO DE MANERA FLUIDA

El usuario tiene el mismo nombre de usuario y contraseña para todo, lo que es garantía de una experiencia excepcional y también de un gran nivel de seguridad de la cuenta.

Estas son las principales ventajas:

Creación de cuentas: cree cuentas locales de Mac basadas en identidades Okta, Microsoft Azure, Google Cloud, IBM Cloud, PingFederate y OneLogin, lo que conducirá a experiencias mejoradas en los inicios de sesión para los usuarios y una flota de Mac organizada que IT podrá administrar.

Inscripción segura: aproveche la autenticación moderna para supervisar el acceso a cada dispositivo, desde dónde se produce la conexión y por quién, para asegurar que el usuario correcto esté en el dispositivo antes de utilizar contenidos sensibles.

Elimine las cuentas de administrador compartidas: cree diversas cuentas para el administrador de IT para reforzar los permisos del proveedor de la identidad en la nube, sin la necesidad de usar cuentas de servicios compartidos.

Fortalezca las políticas de contraseñas: los administradores pueden aplicar políticas de contraseñas a través del proveedor de identidad y garantizar la coherencia y la seguridad de todos los usuarios.

Sincronización de contraseñas: mantenga sincronizados el nombre de usuario y la contraseña del dispositivo Mac con las credenciales de identidad en la nube, fortaleciendo una sola identidad para acceder a todo lo que necesite para ser productivo.*

*La sincronización de contraseñas no está disponible para Google Cloud en este momento

JAMF CONNECT LO REÚNE TODO DE MANERA FLUIDA

Administración moderna de la identidad y el acceso y solución Zero Trust Network Access (acceso a red de confianza cero, ZTNA) todo en uno.

Cuando las organizaciones implementan ZTNA, sus usuarios se autentican y autorizan, y los dispositivos se verifican cada vez que un usuario accede a datos o recursos. La aplicación de privilegios mínimos y las comprobaciones de la postura de los dispositivos en tiempo real permiten el acceso a cada aplicación solo a usuarios específicos y autorizados en dispositivos de confianza.

ZTNA permite la autenticación de usuarios mediante SSO a través de su IdP preferido basado en la nube. La integración con los IdP existentes basados en la nube permite una rápida implementación y administración de las políticas. La única manera de que se establezca una conexión es que el usuario tenga los permisos adecuados para la aplicación especificada.

Obtenga más información sobre ZTNA con nuestro libro electrónico.

LA ADMINISTRACIÓN DE IDENTIDADES Y ACCESOS YA ESTÁ AQUÍ.

Con más demanda de trabajadores a distancia, una fuerza laboral adaptada a dispositivos móviles y un acceso a materiales de trabajo en todo momento, se ha convertido en una necesidad. Jamf Connect reúne toda su infraestructura en una experiencia imperceptible tanto para los usuarios como para IT.

Solicitar prueba

O póngase en contacto con su distribuidor preferido de Apple, para empezar.