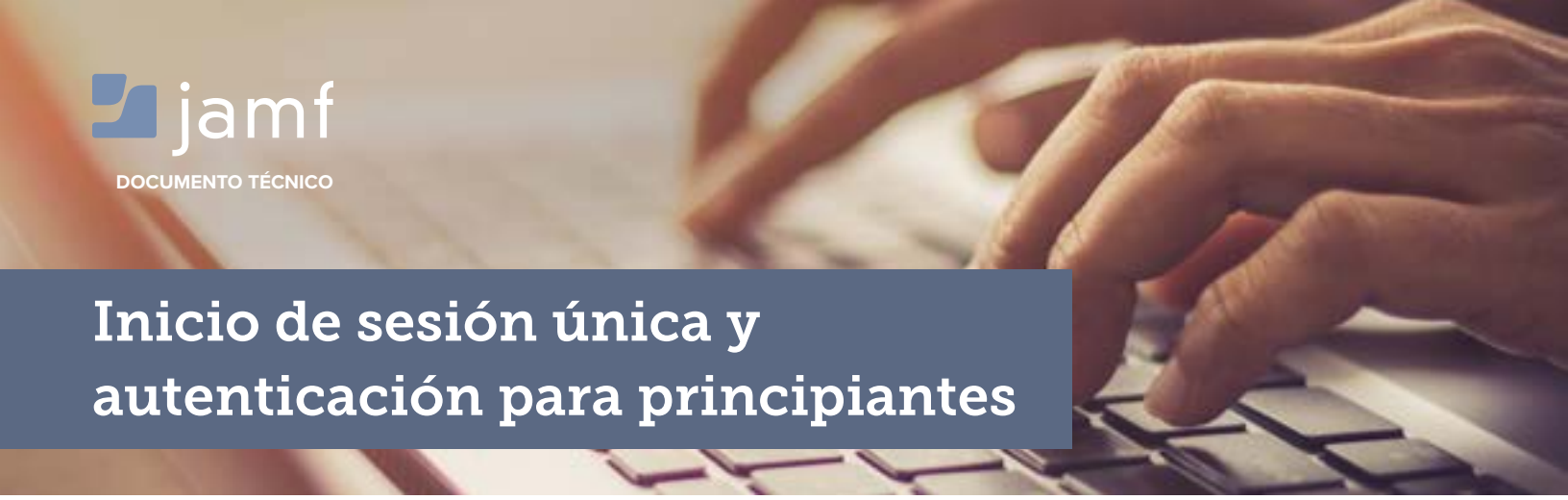

jamf

DOCUMENTO TÉCNICO

Inicio de sesión única y autenticación para principiantes

Acceso sin riesgos en un mundo inseguro

La protección de la seguridad en todos los niveles de una organización es clave para su éxito. Hay que proteger todos los frentes en todo momento: desde la red y los dispositivos hasta los usuarios. De lo contrario, las consecuencias pueden ser catastróficas: un robo de datos puede poner en jaque una gran empresa y destruir por completo la confianza de sus clientes.

En un momento en que cada vez más empleados trabajan a distancia y fuera del horario habitual (aunque necesitan acceder a los mismos recursos que sus homólogos de la oficina), no se puede confiar al azar la protección de todos los dispositivos y usuarios frente a malware malicioso y otras amenazas. Hace falta planificación y también contar con los procesos y los recursos adecuados.

¿Cuál es la solución para poner cerco a estas amenazas sin perjudicar la productividad de los usuarios? Introducir el inicio de sesión única (SSO) y medidas de autenticación de dispositivo/usuario.

EN ESTE DOCUMENTO TÉCNICO, NOS PROPONEMOS:

- Definir qué es el inicio de sesión única y la autenticación
- Identificar el papel de los proveedores de identidad en la nube en el SSO y los procesos de autenticación
- Ofrecer argumentos para implantar buenas prácticas en materia de seguridad

¿QUÉ ES EL INICIO DE SESIÓN ÚNICA?

El SSO es el sistema que permite acceder a varias aplicaciones utilizando unas únicas credenciales para iniciar sesión. Según **TechTarget**, el SSO es un sistema federado de gestión de la identidad que recurre al entorno OAuth para que toda la información de la cuenta de un usuario pueda utilizarse en servicios de terceros sin exponer información delicada sobre las contraseñas.

OAuth actúa como intermediario en nombre del usuario y proporciona un token de acceso que autoriza que se comparta determinada información de la cuenta. Cuando un usuario intenta acceder a una aplicación desde el proveedor del servicio, dicho proveedor envía una solicitud de autenticación al proveedor de la identidad. A continuación, el proveedor del servicio verifica la autenticación y permite que el usuario inicie sesión o bien rechaza la conexión si no se ha podido verificar el usuario.

Tipos de configuraciones de SSO:

- SAML (lenguaje de marcado de aserción de seguridad) facilita el intercambio de autenticaciones y autorizaciones del usuario en distintos dominios seguros. Este proceso implica comunicaciones entre el usuario, un proveedor de identidad encargado de mantener el directorio del usuario y el proveedor del servicio.

- El SSO basado en Kerberos genera un ticket de acceso (TGT) una vez que se facilitan las credenciales del usuario. El TGT obtiene tickets de servicio para las aplicaciones a las que el usuario desea acceder sin necesidad de pedirle que vuelva a introducir las credenciales cada vez.

- El SSO con tarjeta inteligente pide al usuario que utilice una tarjeta con sus credenciales de inicio de sesión. Una vez que el usuario haya introducido su nombre de usuario o contraseña, no tendrá que volver a escribir sus credenciales, porque estarán guardadas en la tarjeta inteligente.

Con el SSO, los usuarios tienen que recordar menos contraseñas y nombres de usuario, lo que también permite reducir muchos tickets de asistencia por credenciales olvidadas. Además, agiliza el proceso de inicio de sesión en las aplicaciones.

¿QUÉ ES LA AUTENTICACIÓN?

Según **The Next Web**, la autenticación es el proceso de identificar y verificar la identidad de un sistema o persona de forma segura. Uno de los sistemas es utilizar un nombre de usuario y una contraseña para iniciar sesión en un dispositivo. El proceso de autenticación verifica que el usuario es quien dice ser antes de darle acceso.

Active Directory (AD) y Lightweight Directory Access Protocol (LDAP) son ejemplos de autenticación para la gestión de la identidad y de cuentas en local. Sin embargo, estos servicios se están quedando rápidamente anticuados en los modernos entornos actuales, en los que cada vez más usuarios acceden a los recursos a través de la nube.

Limitaciones de AD y LDAP:

- 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. Estos requisitos perjudican la experiencia.

- Si utilizan un plugin de AD, los usuarios solo pueden cambiar sus contraseñas cuando existe una conexión con AD. Este requisito provoca confusión y genera también costosos tickets de asistencia cuando un usuario olvida su contraseña.

- Es extremadamente difícil implementar la autenticación multifactor para incrementar los protocolos de seguridad con AD o LDAP.

- En un momento en el que cada vez más organizaciones se pasan de los PC con Windows al Mac, la utilización de AD como principal proveedor de identidad reduce las opciones de gestión para el Mac. Esto obliga a utilizar complementos de terceros, lo que suma complejidad a la gestión de usuarios y aumenta los costes.

- Los administradores de IT no pueden implantar comandos y scripts en forma de documentos de políticas que aplican sus ajustes a los ordenadores y usuarios bajo su control.

Estas limitaciones han generado la necesidad de recurrir a proveedores de identidad en la nube.

¿QUÉ ES LA IDENTIDAD EN LA NUBE?

La identidad en la nube permite al equipo de IT gestionar de forma centralizada y en remoto usuarios, grupos y contraseñas, así como acceder a aplicaciones de las organizaciones y recursos en la nube. Los proveedores de identidad en la nube como Microsoft, Google, Okta,

IBM, OneLogin y Ping utilizan SAML y OAuth para ofrecer a todos los empleados —tanto a los que se conectan en local como en remoto— acceso seguro a los recursos en la nube que necesitan para ser productivos.

Con todo el potencial de la identidad en la nube, Microsoft invita a las organizaciones a iniciar la transición del servicio local Active Directory al servicio en la nube Microsoft Azure Active Directory.

Microsoft Azure es un servicio en la nube que permite a las empresas crear, gestionar e implantar aplicaciones en una red a gran escala y global. Microsoft Azure es utilizado por el **95 % de las compañías de la lista Fortune 500**, pero como apuntábamos antes no es el único proveedor que existe.

INTEGRACIÓN DE LA IDENTIDAD DE LA NUBE

Con tantos proveedores de identidad en la nube por elegir, las organizaciones necesitan una solución que se integre con la mayoría y, a ser posible, con todos. Jamf Connect es garantía de una distribución sencilla de perfiles de datos de usuarios desde un servicio de identidad en la nube en un flujo de trabajo de Apple y ofrece, además, autenticación multifactor.

Un usuario puede sacar su Mac de la caja, encenderlo y acceder a todas las aplicaciones aprobadas del sistema tras iniciar sesión con unas únicas credenciales de identidad en la nube.

Estas son las principales ventajas:

- **Creación de cuentas:** Cree cuentas locales de Mac basadas en identidades de Okta, Microsoft Azure, Google Cloud, IBM Cloud, PingFederate y OneLogin. Los usuarios podrán iniciar sesión más fácilmente y el equipo de IT tendrá una flota de Mac perfectamente organizada.

- **Inscripción segura:** Aproveche la autenticación moderna para supervisar el acceso a cada dispositivo, desde dónde se produce la conexión y cuál es el usuario que se conecta. Así tendrá la certeza de que el dispositivo es utilizado por el usuario correcto antes de una implantación de contenidos sensibles.

- **Eliminación de cuentas de administración compartidas:** Cree varias cuentas para administradores de IT con permisos del proveedor de la identidad en la nube, sin necesidad de usar cuentas de servicios compartidos.

- **Imposición de políticas de contraseñas:** Los administradores pueden imponer políticas de contraseñas a través del proveedor de identidad y garantizar la coherencia y la seguridad de todos los usuarios.

- **Sincronización de contraseñas:** Sincronice el nombre de usuario y la contraseña del Mac con las credenciales de Azure, Okta y PingFederate. Y podrá acceder a todo lo que necesite con una única identidad, toda una garantía de productividad.

EL PAPEL DE LA GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)

Cada vez más organizaciones optan por prescindir de AD e incorporan los Mac a sus flotas en respuesta a la creciente demanda. Y eso implica también introducir procesos 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 gestionar las contraseñas de los usuarios y acceder a las aplicaciones de la empresa en remoto. 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 automática.

2. Durante la inscripción, se descarga Jamf Connect y se instala desde el servidor de MDM.

3. A los usuarios les aparece directamente la ventana de inicio de sesión de Jamf Connect. No tienen que crear su propio nombre de usuario o contraseña.

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.

No espere más para reforzar la seguridad de su entorno

El SSO, la autenticación y los proveedores de identidad en la nube son el futuro de la gestión de la identidad y la seguridad. Proteja su entorno y acabe con las interminables listas de tickets de asistencia innecesarios. Una apuesta doblemente ganadora.

Póngase en contacto con nosotros para empezar hoy mismo o solicite una prueba de Jamf Connect y descubra cómo funcionan estos procesos.

Hablar ahora

Solicitar prueba

O hable con su distribuidor autorizado de dispositivos Apple para iniciar su prueba de Jamf Connect.

jamf

www.jamf.com