jamf

WHITE PAPER

Single Sign-On and Authentication for Beginners

Trusted access in an unsecure world

Security protection at every level of an organization is paramount to success. From network to device to user, all facets must be protected at all times. If not, the results could be catastrophic as data breaches can bring corporations to a halt and completely shatter customer trust.

As more employees work remote and outside of standard working hours — yet still require the same access to resources as their onsite counterparts — keeping all devices and users protected from malicious malware and threats isn't something that "just" happens. It takes planning and the right workflows and resources to achieve.

So, how can organizations combat threats without hindering user productivity? By leveraging single sign-on (SSO) and device/user authentication security measures.

IN THIS WHITE PAPER, WE:

- Define single sign-on and authentication
- Identify the role of cloud identity providers in SSO and authentication workflows
- Provide insight to put security best practices in place

WHAT IS SINGLE SIGN-ON?

SSO is the means by which one set of login credentials is used to access multiple applications. According to **TechTarget**, SSO is a federated identity management arrangement that leverages the OAuth framework so all of a user's account information can be used across third-party services without exposing sensitive password information.

OAuth acts as the intermediary on behalf of the user and provides an access token that authorizes specific account information to be shared. When a user attempts to access an application from the service provider, the service provider sends a request to the identity provider for authentication. The service provider then verifies the authentication and allows the user to successfully log in or denies if the user cannot be verified.

Types of SSO configurations:

- Security Assertion Markup Language (SAML) facilitates the exchange of user authentication and authorization across secure domains. This process involves communications between the user, an identity provider that maintains the user directory and the service provider.
- Kerberos-based SSO issues a ticket-granting ticket (TGT) once the user credentials are provided. The TGT fetches service tickets for applications the user wishes to access without asking the user to re-enter their credentials each time.
- Smart card SSO asks a user to use a card with their sign-in credentials. After first use, the user will not have to enter their username or password again, as the smart card stores these credentials.

SSO empowers users to remember fewer passwords and usernames, thus eliminating many help tickets to resolve forgotten credentials. It also streamlines the process of logging into applications.

WHAT IS AUTHENTICATION?

According to **The Next Web**, authentication is the process of identifying and verifying the identity of a system or person in a secure manner. For example, you leverage a username and password to log in to a device. The process of authentication verifies that you are who you say you are prior to granting access.

Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) are examples of authentication services for on-premises identity and account management. However, these services are quickly becoming antiquated in today's modern environments where more users are accessing resources in the cloud.

AD and LDAP limitations:

- Remote users must be on the local area network (LAN) or use a virtual private network (VPN) to access internal resources. This provides a sub-optimal experience.
- If using an AD plugin, users can only change their passwords when AD is reachable. This causes both confusion and costly help desk tickets when a user forgets their password.
- It's extremely difficult to implement multifactor authentication to increase security protocols with AD or LDAP.
- With more organizations moving from Windows PCs to Mac, leveraging AD as their primary identity provider reduces management capabilities for Mac. This requires the use of third-party add-ons, which adds complexity to user management and higher costs.
- IT admins can't deploy commands and scripts in the form of policy documents that apply their settings to the computers and users within their control.

These limitations have led to the need for cloud identity providers.

WHAT IS CLOUD IDENTITY?

Cloud identity allows IT to centrally and remotely manage users, groups, passwords and access to corporate applications and cloud resources. Cloud identity providers such as Microsoft, Google, Okta, IBM, OneLogin and Ping leverage SAML and OAuth to offer all employees — remote and onsite — secure access to the cloud resources they need to be productive.

With the available power of cloud identity, Microsoft is encouraging organizations to transition from on-premises Active Directory to cloud-based Microsoft Azure Active Directory.

Microsoft Azure is cloud services that allow business to build, manage and deploy applications on a massive, global network. Microsoft Azure is used by **95 percent of Fortune 500** companies, but as previously stated, they aren't the only provider available.

CLOUD IDENTITY INTEGRATION

With many cloud identity providers to choose from, organizations will want to leverage a solution that integrates with most, if not all of them. Jamf Connect allows for simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multifactor authentication.

A user can simply unbox their Mac, turn it on and access every system-approved application after signing on with a single set of cloud identity credentials.

Benefits include:

- **Account creation:** Create local Mac accounts based on Okta, Microsoft Azure, Google Cloud, IBM Cloud, PingFederate and OneLogin identities, resulting in an improved log in experience for users and organized fleet of Mac for IT to manage.
- **Secure enrollment:** Leverage modern authentication to track and monitor what devices are being accessed, from where and by whom, ensuring the right user is on the device before deploying anything sensitive.
- **Eliminate shared admin accounts:** Create multiple IT admin accounts leveraging permissions from the cloud identity provider, without requiring the use of shared service accounts.
- **Enforce password policies:** Admins can enforce password policies via the identity provider, maintain consistency and security across all users.
- **Password synchronization:** Keep the Mac username and password in sync with Azure, Okta and PingFederate credentials, leveraging a single identity for everything needed to be productive.

THE ROLE OF MOBILE DEVICE MANAGEMENT (MDM)

As organizations shift from AD and bring on more Mac devices to adhere to the growing demand, organizations must get workflows in place to keep corporate information secure, while providing an ideal user experience.

Cloud identity providers integrated with Jamf Connect allow IT to remotely manage user passwords and access to corporate applications. Using an automated MDM enrollment, the process is simple and secure:

1. A user is invited to enroll in the automated MDM enrollment.
2. During the enrollment, Jamf Connect is downloaded and installed from the MDM server.
3. Users are taken directly to the Jamf Connect login window, as opposed to creating their own username and password.

The user has the same username and password for everything, creating an incredible experience while also establishing account security.

Make your environment more secure today

SSO, authentication and cloud identity providers are the future of identity and security management. Protect your environment and eliminate needless help tickets. Win-win.

Contact us today to get started or take Jamf Connect for a trial run and put these workflows to the test first.

Request Trial

Or contact your preferred authorized reseller of Apple devices to start your Jamf Connect trial.

jamf

www.jamf.com