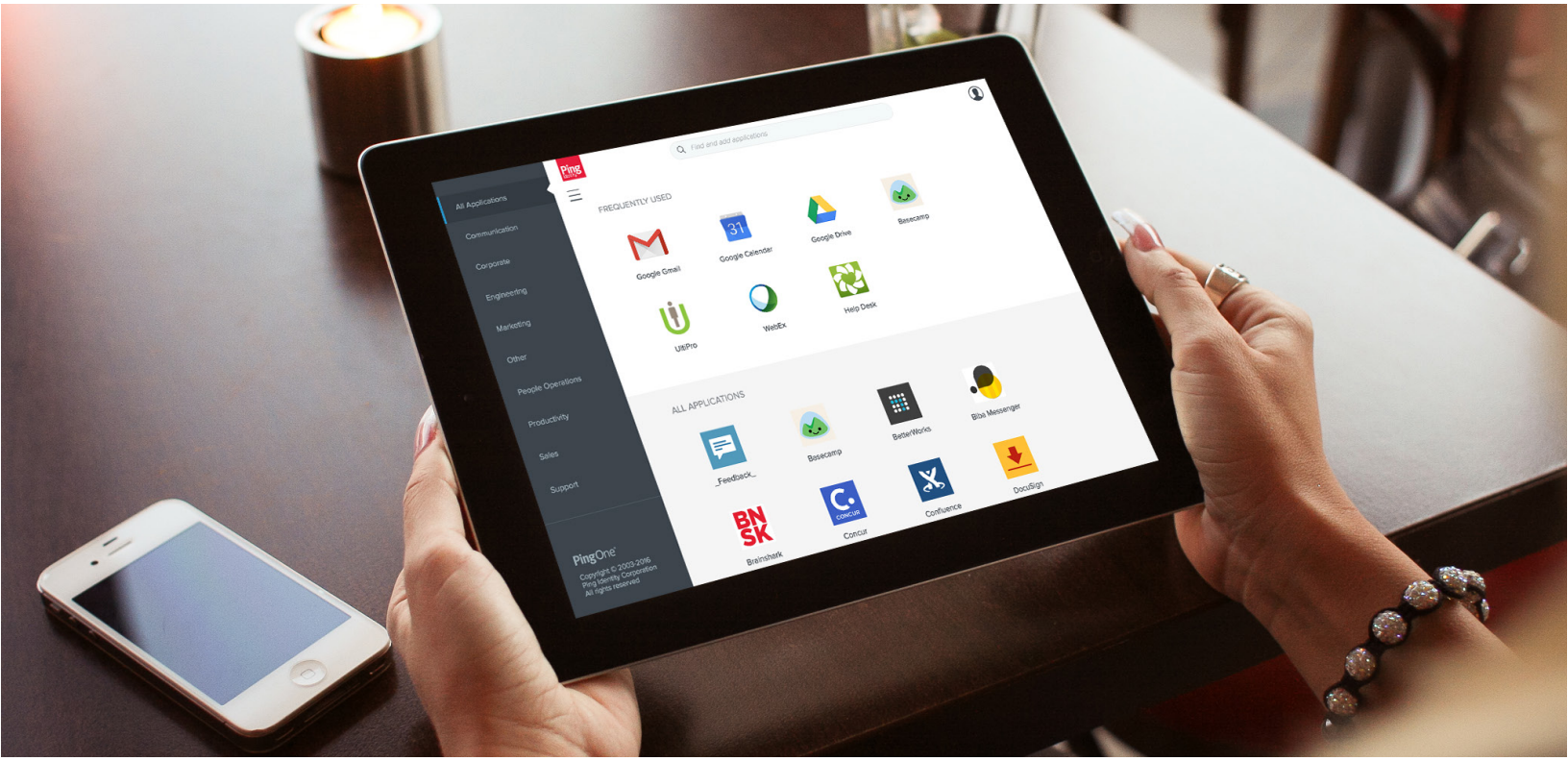
INTEGRATING PING IDENTITY SOLUTIONS WITH GOOGLE IDENTITY SERVICES

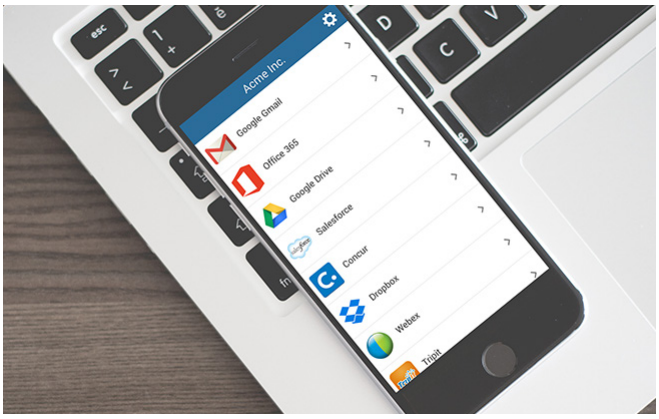
How two technologies work together to add more value to your enterprise



WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY



"Google provides business-critical solutions like serving as the central, secure access point for cloud apps, while also providing infrastructure for these services like the identity directory. I trust Google to play this foundational role, but wouldn't expect it to meet unique needs that fall between the directory and the login. This is where best-of-breed partners like Ping come in to help us solve complex challenges unique to our business."

Justin Slaten
Manager, Enterprise Technology and Client Systems
Netflix

Ping Identity provides a comprehensive platform for identity federation, single sign-on (SSO), multi-factor authentication (MFA) and web and API access security. With complete support for every modern identity standard, including SAML, WS-Trust, OAuth, OpenID Connect (OIDC) and SCIM, Ping offers the most mature and robust identity and access management (IAM) solution available today.

Google identity services, which are a core component of Google Apps for Work, provide a simple and secure mechanism for users to sign on to Google applications such as Google Drive and Gmail. Administrators can easily manage users and devices across their organization, and they can leverage detailed audit and reporting on user activity that might indicate a compromised account or potential data loss.

Ping is an inaugural member of the "Recommended for Google Apps for Work" program, which gives customers the most advanced experience by integrating applications with the Google login, providing secure access and SSO to both SaaS and internal applications running anywhere. Ping was selected by Google based on reliability, extensive support for identity standards and tight integration with Google Apps for Work.

Ping has provided user provisioning and SSO for Google applications for some time, but many customers are choosing to use Google identity services instead of, or in addition to, storing identities in a traditional directory server like Active Directory. Regardless of where identities are stored and managed, integrating Ping solutions with Google identity services provides the most advanced functionality, security and convenience available today.

This paper covers the value and benefits that Google Apps for Work customers can expect by integrating Google identity services with Ping solutions. These benefits include the ability to connect to multiple, disparate directories in addition to the Google directory, expansive support for user provisioning and SSO, advanced identity federation capabilities, unlimited options for MFA and flexible access security for both on-premises and cloud applications.

INTEGRATION OVERVIEW

OPTIONS FOR DEPLOYMENT

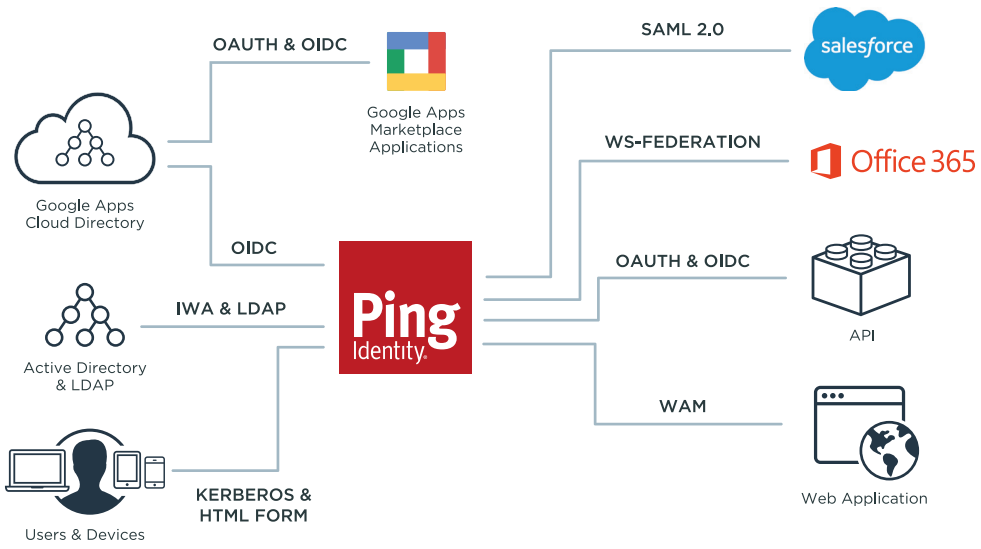
Customers that deploy Ping solutions with Google Apps for Work have two high-level options to choose from when planning their integration: storing identities solely in the Google directory or leveraging a traditional directory server such as Active Directory. Using Google as the sole directory is a simpler option, but customers that already have a directory server or leverage Active Directory in their existing environment can also accelerate their integration to Google Apps by using Ping solutions. Once user accounts are provisioned into the Google directory using Ping's automated user management capabilities, the benefits of Google directory services are immediately available, and the existing directory can be maintained or decommissioned according to the needs of the organization.

CONNECTING GOOGLE IDENTITY SERVICES WITH PING SOLUTIONS

Google identity services can be connected to the Ping Identity Platform using the OIDC support that's built into Google Apps for Work. This modern protocol allows Google identities to be federated into the Ping Identity Platform using standard, secure tokens that also provide the identity attributes required for further SSO and access security. Whether the customer chooses to use Ping's on-premises software or cloud services, the integration uses this same standard protocol, and the configuration only takes a few minutes, allowing organizations to be up and running with advanced SSO and federation capabilities within a few hours instead of days or weeks.

CONNECTING OTHER DIRECTORIES WITH PING SOLUTIONS

Ping's solutions have broad support for integrating with disparate, heterogeneous directories. Tight support with Active Directory and Kerberos is available out of the box, further simplifying the sign-on process for users that have already authenticated to their Windows desktop. Integration with Active Directory and Google directory services can happily coexist, providing flexibility, ease of administration and centralized auditing and reporting for customers that are migrating identities or have requirements for multiple directories. Additionally, Ping supports authentication and attribute retrieval for any LDAP directory server as well as relational database systems, and a rich SDK can be utilized to enable credential validation and attribute retrieval for virtually any directory store—even proprietary and homegrown systems.



SAAS AND INTERNAL SSO

CONNECTING TO SAAS APPLICATIONS

Identity federation protocols such as SAML and OIDC allow users to securely sign on to both internal and third-party applications without additional passwords. Google Apps for Work has some support for SAML and OIDC applications, but Ping has thousands of pre-built integrations, over ten years of experience in identity federation and SSO and 24x7 worldwide customer support. Customers can use a single connection to the Google directory to sign their users onto all of their applications, simply and securely. Administrators use a simple web-based console to configure SaaS applications from a huge catalog, and they can use Google groups to determine which applications users can access. Many SaaS applications can be configured in a completely self-service manner, so that application SSO can be enabled in a matter of minutes without any external or manual intervention. The time to value by implementing Ping solutions for SSO and identity federation can be easily demonstrated, especially in complex or high-traffic environments.

INTERNAL, HOMEGROWN AND PROPRIETARY APPLICATION SSO

In addition to standards-based SaaS applications, Ping has dozens of integrations for homegrown and proprietary applications. Libraries are available for developers for languages such as .NET, Java, PHP and Perl, and simple, REST-based interfaces can be used to enable SSO for internal web applications quickly and easily. Ping also offers full OAuth and OIDC provider capabilities, allowing organizations to generate their own standard tokens for SSO and authorization that are specific to internal applications, including mobile apps and APIs. This way, organizations can enjoy all of the benefits of Google identity services while ensuring the security and integrity of their internal applications, complete with application-scoped authorization controls and full auditing and reporting.

USER PROVISIONING

Much like their SaaS SSO capabilities, Google Apps for Work has some support for user provisioning for SaaS applications. Adding Ping solutions to an organization's environment provides advanced functionality for user provisioning, allowing identity information and attributes to automatically flow from the Google directory into any number of SaaS applications regardless of the mechanisms or APIs available from the service provider.

OTHER PROVISIONING CAPABILITIES

Ping solutions provide both scheduled provisioning and just-in-time provisioning, enabling user creation as users are added to groups or during the first SSO operation. These advanced provisioning capabilities are available for both SaaS applications and internal applications using both proprietary and standard mechanisms. Deprovisioning of users is also available if the application or service provider supports it, disabling or deleting user accounts in the remote application as the user is off-boarded—enhancing security as well as controlling costs.

INBOUND AND OUTBOUND PROVISIONING USING SCIM

Ping has been heavily involved with standard provisioning protocols for years, and full SCIM support is built into the Ping Identity Platform. This allows organizations to provide outbound provisioning of user data to any SCIM-compliant service provider as well as inbound provisioning to internal databases or directory servers. This enables easy synchronization of user data across disparate directories and services, avoiding time-consuming and error-prone manual provisioning processes.

MULTI-FACTOR AUTHENTICATION

GOOGLE TWO-STEP VERIFICATION

Google Apps for Work includes the ability to protect accounts by requiring users to enter a one-time passcode (OTP) when they sign on. Administrators can choose to turn on two-step verification for their domain at any time. The Google Authenticator app, which is used to generate these codes, is available for many mobile platforms and provides adequate security and ease of use for many organizations.

MOBILE MFA

PingID is Ping's mobile MFA solution, and it allows organizations to enable MFA at sign-on or during a step-up authentication for specific groups or applications. A notification is sent to the user's mobile phone, and a simple swipe or fingerprint provides authentication. Additionally, alternate MFA mechanisms can be used to provide OTPs through SMS, voice, email or a desktop application as well as via YubiKey hard tokens. Advanced options for both pairing devices and determining the need for MFA ensure the highest levels of security while providing a frictionless user experience, which aids both adoption and productivity. PingID is centrally managed as a cloud service, and administrators can enable device requirements and conditions (such as restricting rooted devices) as well as define policies for MFA from a simple, web-based administration console. PingID can also be leveraged for VPNs and SSH, and it can be applied to applications through a comprehensive API.

OTHER MFA OPTIONS

Ping solutions can also integrate with a number of third-party MFA solutions, and these solutions can easily be combined in the platform. For organizations that have already deployed MFA or wish to support multiple solutions, Ping can centralize management and auditing for these solutions as well as integrate them with both Google directory accounts and other disparate directories. This functionality can also assist with the migration from expensive hard token solutions, giving organizations the ability to migrate to modern MFA according to their own schedules instead of as a complete rip and replace. A full SDK for credential validation provides support for homegrown or obscure MFA solutions.

WEB AND API ACCESS SECURITY

In addition to SSO and MFA, the Ping Identity Platform provides modern access security for applications deployed both on-premises and in the cloud. Ping's access security solution supports attribute and group-based access control through medium-grained policies that are used to protect both web applications and APIs. Deployed as a reverse proxy or as a standalone policy server with web server agents, Ping's solution leverages OIDC to completely replace proprietary, legacy web access management (WAM) solutions or integrate with them through token mediation, trading standard OIDC tokens for proprietary ones. Organizations can again choose to migrate their applications at their own pace, and developers have a standard method of applying security and control to their applications since both authentication and access policies are managed through Ping's centralized platform. Ping's solution allows Google Apps for Work users to securely access even the largest, most complex web and mobile environments with full auditing and visibility for administrators. This modern access security can also be extended to any of the directories or federation partners that are integrated with the platform, providing security for customers and partners as well as the internal workforce, regardless of where their identities are stored.

MOBILE DEVICE MANAGEMENT (MDM)

Google Apps for Work includes MDM for Android, iOS, Windows Phone and smartphones and tablets using Microsoft® Exchange ActiveSync®. Google's MDM eliminates the need for third-party management solutions, and administrators can enforce device policies, encrypt data and remotely lock or wipe lost or stolen devices through the Google management console. By combining Google MDM with Ping's identity federation and access security capabilities, organizations can implement a truly comprehensive, end-to-end program that secures applications, protects devices and enables users, even if they choose to work from their personal phones or tablets.

CONCLUSION

Ping provides 24x7 support, online and on-site training and frequent webinars and events, including the annual Cloud Identity Summit. If you have any questions about Ping's solutions or capabilities or would like a technical overview or demonstration, don't hesitate to contact us.

#3034 | 08.22 | v00a