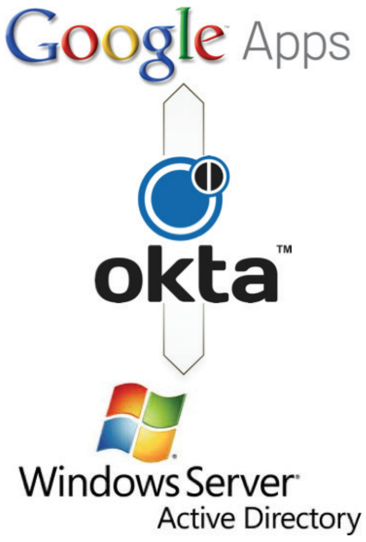
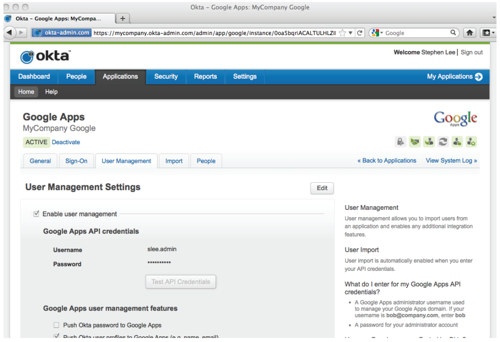
OKTA DATASHEET:

OKTA CLOUD CONNECT FOR GOOGLE APPS

Purpose-Built Active Directory Integration for Google Apps

Single sign-on and automated user management that is simple, scalable, and reliable





Okta – Google Apps: MyCompany Google

https://mycompany.okta-admin.com/admin/app/google/instance/0oa5bqriACALTULHLZIl

Welcome Stephen Lee | Sign out

Google Apps
MyCompany Google
ACTIVE Deactivate

User Management Settings

☑ Enable user management

Google Apps API credentials

Username: slee.admin
Password: **********

Google Apps user management features

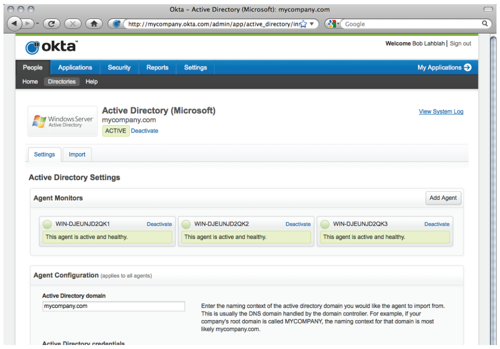
□ Push Okta password to Google Apps
☑ Push Okta user profiles to Google Apps (e.g. name, email)

User Management
User management allows you to import users from an application and enables any additional integration features.

User Import
User import is automatically enabled when you enter your API credentials.

What do I enter for my Google Apps API credentials?
- A Google Apps administrator username used to manage your Google Apps domain. If your username is **bob@company.com**, enter **bob**
- A password for your administrator account

Google Apps SSO and User Management



Okta – Active Directory (Microsoft): mycompany.com

http://mycompany.okta.com/admin/app/active_directory/in

Welcome Bob Lahblah | Sign out

Active Directory (Microsoft)
mycompany.com
ACTIVE Deactivate

Active Directory Settings

Agent Monitors

WIN-DJEUNJD2QK1 – This agent is active and healthy.
WIN-DJEUNJD2QK2 – This agent is active and healthy.
WIN-DJEUNJD2QK3 – This agent is active and healthy.

Agent Configuration (applies to all agents)

Active Directory domain: mycompany.com

Enter the naming context of the active directory domain you would like the agent to import from. This is usually the DNS domain handled by the domain controller. For example, if your company's root domain is called MYCOMPANY, the naming context for that domain is most likely mycompany.com.

Active Directory credentials

Active Directory Homepage

Google Apps for Your Organization

Google Apps has quickly become one of the most popular on-demand business software in the market. In addition to the core web-based email, calendar, and documents, Google Apps seamlessly integrates with a wealth of enterprise applications through Google Marketplace to cover all the business needs for your organization. With this growth comes the need to ensure these users have seamless access via single sign-on (SSO) and that their Google Apps accounts are created, updated, and deactivated on an integrated cycle with the rest of the systems in IT.

Active Directory & Google Apps

For many Google Apps customers, Microsoft Active Directory (AD) is a core piece of the identity management infrastructure. With AD serving as the enterprise directory, user authentication and application access policies around on-premises applications are often tied to users and security groups in AD. Similarly, the ideal Google Apps deployment should be able to tightly integrate with AD. Users should be able to leverage their AD credentials when accessing Google Apps, and the groups assigned to Google Apps users should be based on their AD profile and the security groups they belongs to.

Without native AD integration, administrators must create Google Apps accounts manually for each user by copying AD user profile information to Google Apps, and then manually assign each Google Group associated with each user. Any subsequent user profile changes, such as job title or department, also require manual updates. When users leave the organization, their AD account might be disabled while their Google Apps account is still active—unless administrators manually deactivate the account in a timely manner. These manual processes are inefficient and extremely error-prone; and the hassle extends to users, who must deal with yet another set of credentials stored in Google Apps. Users struggle to manage their passwords and administrators end up spending countless cycles managing password resets.

As a result, user productivity is affected—and the risk of exposing inappropriate access increases.

Okta Cloud Connect for Google Apps

Okta is a 100-percent on-demand, turnkey solution that automates user management and SSO with cloud and web applications. Okta Cloud Connect for Google Apps offers a complete, robust, and easy-to-use AD integration with Google Apps that provides a seamless authentication experience for Google Apps users and automated provisioning and deprovisioning of Google Apps accounts based on AD users and security groups.

- Automated provisioning in Google Apps is based on AD user profile and security groups.
- Users can log in to Google Apps with their AD credentials.
- Organizations can use Integrated Windows Authentication (IWA) for true SSO with Windows domain.
- Automated Google Apps account deprovisioning is triggered directly from AD.

Easy to install & Configure

Okta Cloud Connect for Google Apps is a purpose-built solution that seamlessly integrates Google Apps with Active Directory. With the click of a button, you can download the Okta Active Directory agent and install it on any Windows Server that has access to a Domain Controller. No network or firewall configuration is required.

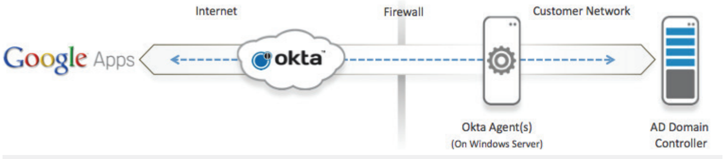
Enabling automated user management for Google Apps is equally simple. Through the Google Apps User Management configuration in Okta, administrators can complete integration in minutes to enable account provisioning, profile updates, and account deprovisioning between AD and your Google Apps instance.

Delegated Authentication & Desktop SSO

With the AD integration completed, a simple configuration change in the Google Apps Single Sign-On setup console enables delegated authentication with Okta through Security Assertion Markup Language (SAML). Google Apps offers the flexibility to enable delegated authentication for a selected group of users based on their IP range. These users can now log in to Google Apps with their AD credentials. With SAML, Google Apps delegates user authentication to Okta where user credentials are entered and verified via the Okta Active Directory agent with the AD server. No password is stored in Google Apps or Okta—the AD server remains the single source for authentication. There's no need for users to remember another password or reset their Google Apps password, because their AD password is their Google Apps password. For users who have already authenticated to the Windows domain with their Windows network login, Okta's support for IWA provides a true single sign-on experience to your Google Apps account.

Automated User Management

Okta Cloud Connect for Google Apps integrates Google Apps with Active Directory and your existing user lifecycle management around AD. Google Apps accounts are automatically provisioned based on AD users and security group membership. As changes are made in Active Directory, Okta ensures that synchronization between AD and Google Apps occurs automatically at configurable intervals so access privileges are always up to date. With Google Apps users authenticating directly against AD, when users are disabled in AD, their access into Google Apps is immediately revoked. Further, Okta will suspend the Google Apps account to prevent access from any other clients or devices—ensuring proper account deactivation in Google Apps.



Integrating AD with Google Apps

Secure Integration

Security is a key component of the Okta Active Directory agent. Communication between the agent and Okta Cloud Connect for Google Apps is protected with SSL encryption. Man-in-the-middle attacks are prevented using server-side SSL certificates. The agent authenticates to the service by first using organization-specific credentials, then exchanging cryptographic keys used for all future communication. Further, any agent's access can be revoked at any time from the service by deactivating its security token.

About Okta

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting. Enterprises everywhere are using Okta to manage access across any application, person or device to increase security, make people more productive, and maintain compliance.

The hundreds of enterprises, thousands of cloud application vendors and millions of people using Okta today also form the foundation for the industry's fastest growing, vendor neutral Enterprise Identity Network.

The Okta team has built and deployed many of the world's leading on-demand and enterprise software solutions from companies including Salesforce.com, PeopleSoft, Microsoft, BMC, Arcsight, Sun, and HP. Okta is backed by premiere venture investors Andreessen Horowitz, Greylock Partners, Khosla Ventures and Sequoia Capital.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.