CODE42

Tech Specs | **Product**

# Code42 Identity Management Options

User authentication and management can be conducted manually within enterprise applications, but most organizations prefer to take a standardized approach to identity management. This allows IT and security teams to maintain one point of reference in order to minimize administrative burden and prevent errors in the user onboarding and offboarding process. Read on to learn about how Code42 approaches identity management within its cloud deployment models.

## Defining identity management actions

Code42 uses two terms to describe the sets of identity management actions that can be taken within the product: authentication and provisioning.

- **Authentication** is the process of identifying and verifying users in order to provide them with access to Code42.
- **Provisioning** allows you to automatically manage users in your Code42 environment. This includes adding or deactivating users, moving users to appropriate organizations and applying roles to users. Within Code42, organizations determine what data is collected and what policies are applied to a given user. Roles determine the Code42 permissions assigned to a given user.

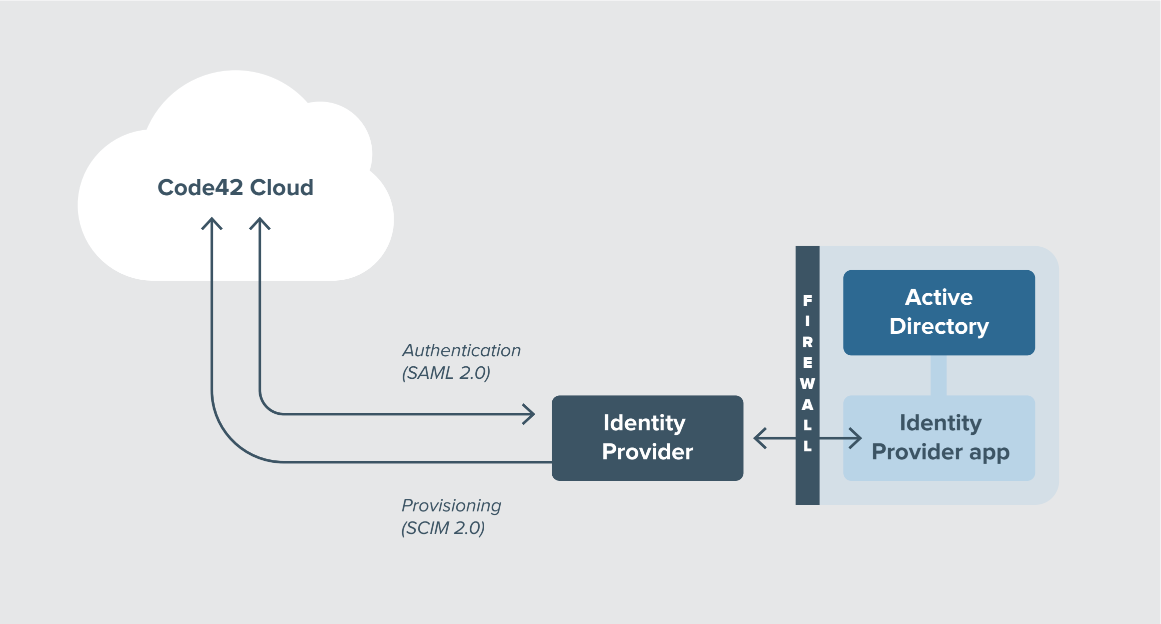
## Automating identity management in Code42 cloud deployments

Authentication and provisioning can be manually performed by administrators within the Code42 product, but Code42 recommends two best practice configurations for customers who prefer to automate identity and user management in their cloud environment. Automation enables better integration into existing corporate processes.

Integrate Code42 with an identity management provider to perform:

Authentication via SAML 2.0

Provisioning via SCIM 2.0



## Configuration 1

### Integration with identity management provider

#### Benefits

Streamlines administration by maintaining an organization's existing identity management provider as the single source of truth for user authentication and management

#### Technical requirements

Code42 supports the following standards for identity management:

SAML 2.0 protocol for authentication, SCIM 2.0 protocol for provisioning

#### Considerations

Companies who have not standardized on an identity management solution can get a fully functioning Okta Identity Provider instance for use with Code42 at no additional charge

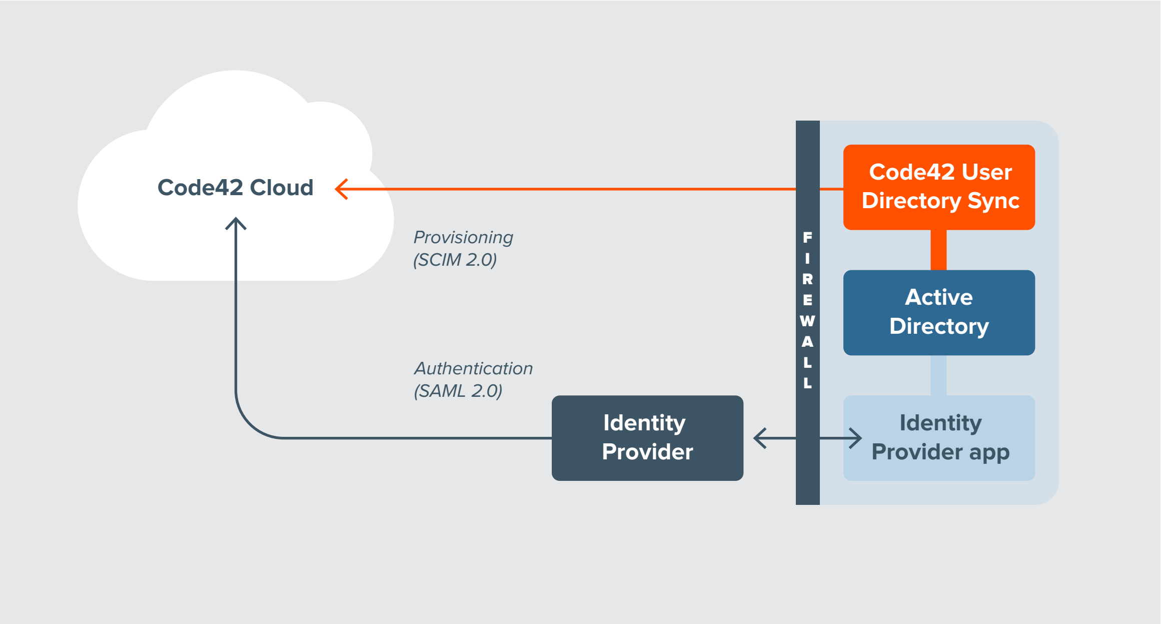
Code42 offers a second configuration for customers who have complex identity management requirements or whose chosen identity management provider does not support SCIM 2.0 for provisioning

#### Example identity management vendors

Okta Ping Identity OneLogin

Integrate Code42 with an identity management provider to perform authentication via SAML 2.0

Integrate your locally hosted directory services with Code42 User Directory Sync to perform automated user provisioning



## Configuration 2

### Integration with identity management provider and Code42 User Directory Sync

### Benefits

Integrates with locally hosted directory services for customers who have complex identity management requirements or whose chosen identity management provider does not support the SCIM 2.0 protocol necessary for Code42 provisioning

### Technical requirements

- Code42 supports SAML 2.0 for authentication via Identity Providers
- User Directory Sync will be implemented by the Code42 Professional Services team as part of the customer deployment
- User Directory Sync requires an LDAP service user and password to read the customer's directory tree
- The Code42 customer must install User Directory Sync on a physical or virtual server (Windows or Linux) that has network access to the customer's directory server
- User Directory Sync uses configurable scripts to align a customer's directory to Code42

### Considerations

Companies who have not standardized on an identity management solution can get a fully functioning Okta Identity Provider instance for use with Code42 at no additional charge

### Example identity management vendors

The following are examples of identity management vendors that could be used for authentication when Code42's User Directory Sync is used for provisioning:

Okta
Duo
Azure AD
OneLogin
Ping Identity
Google SSO
Active Directory Federation Services (ADFS)
InCommon

## What is Code42 User Directory Sync?

User Directory Sync allows you to securely and automatically provision users in your environment. Once enabled, Code42 creates new users, removes deactivated users, manages organizational assignments and updates user roles and permissions based on scheduled syncs with your locally hosted directory services, such as Microsoft Active Directory.

## Why Code42 User Directory Sync does not perform authentication

In order to directly perform authentication using LDAP in a cloud deployment, Code42 would need to compromise our data security standards. Because Active Directory sits behind a firewall, our customers would have to open an inbound firewall port in order for Code42 to connect. Not only would this be a security concern for most organizations, but this would also compromise the availability of the Code42 service when the customer performs network maintenance. Additionally, it would cause Active Directory passwords to go through Code42 servers, leaving the potential for them to be logged in our system. Rather than follow these non-standard protocols, Code42 has chosen to follow industry best practices by integrating with purpose-built identity management providers for authentication, while still providing a solution for customers who need to manage user provisioning via a locally hosted directory service.

## Conclusion

No matter which configuration your organization chooses, you can be confident that Code42 will help you streamline identity management in order to minimize administrative burden and prevent errors in the user onboarding and offboarding process.

FOR MORE INFORMATION: CODE42.COM/CONTACT

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM