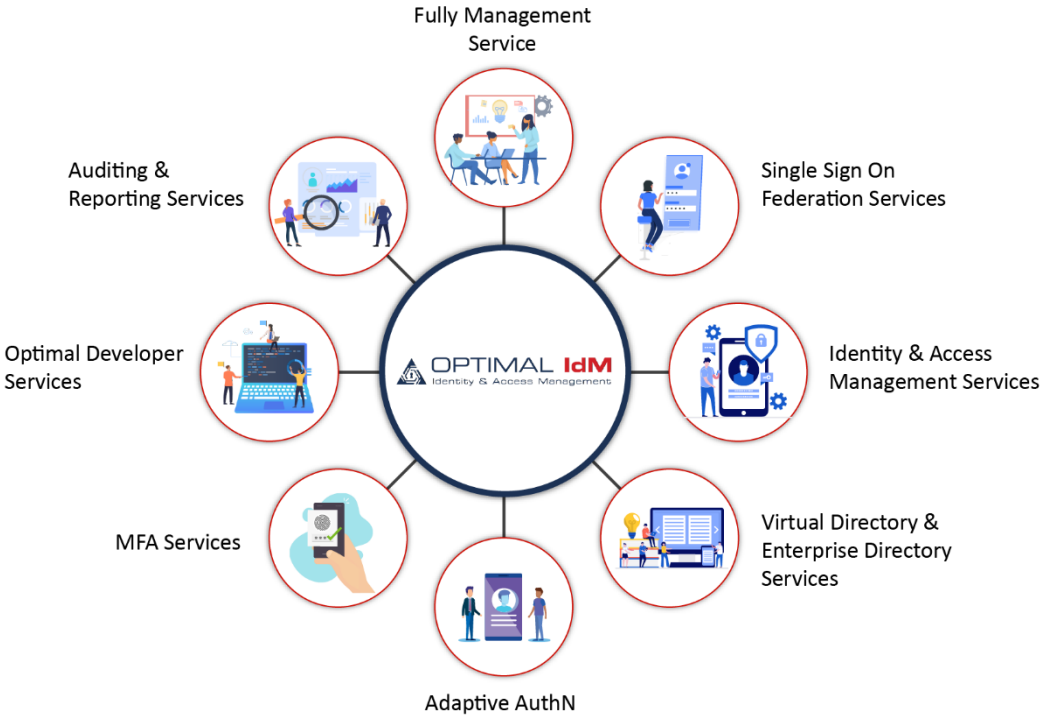
The OptimalCloud v5.0 Deployment Guide

The OptimalCloud v5.0 is a fully cloud-hosted Identity and Access Management platform. The OptimalCloud supports Federation (OAuth2, OpenID Connect, SAML 2.0, and WS-Federation), Identity Management, Multi-Factor Authenticaiton (MFA), Developer Services, Auditing, and Reporting.



This guide shows different deployment options for The OptimalCloud v5.0. To sign up for the OptimalCloud, visit signup.theoptimalcloud.com.

Populating the OptimalCloud with Users

The OptimalCloud has robust Identity Management capabilities. To populate the users in The OptimalCloud there are a number of options:

- Self-registration – users can self-register their accounts. Accounts can be self-registered with OptimalCloud credentials or can be based on a Social Media authentication.
- Administration – an administrator can manually create users. Those users will automatically be sent an email with a one-time link that can be used to set the credentials on their account.

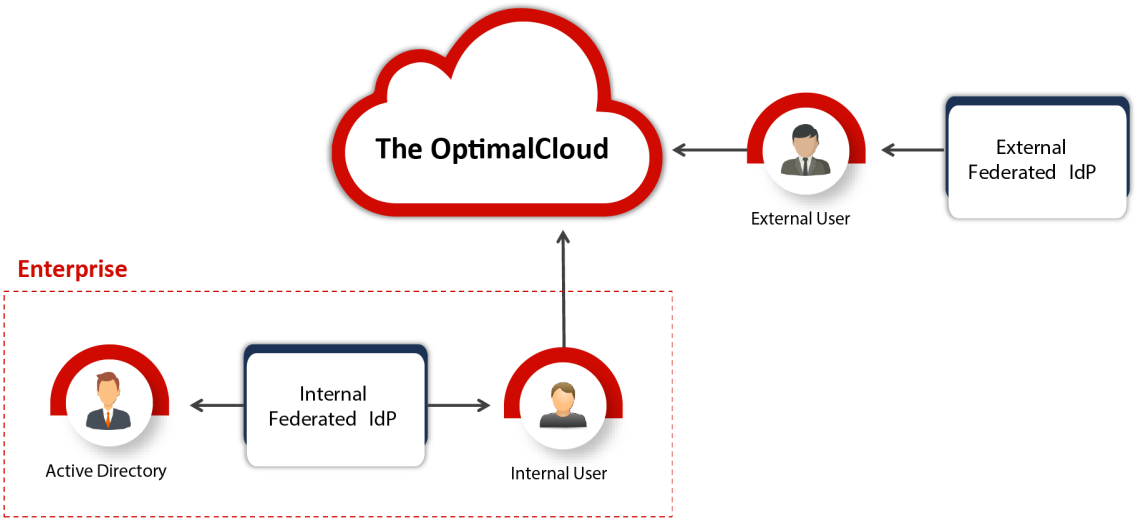
- File Upload – an administrator can upload a CSV file to populate users. The CSV files can optionally contain initial credentials for the new users or the users will automatically be sent an email with a one-time link that can be used to set the credentials on their account.
- Active Directory Synchronization – the Optimal IdM AD Synchronization Agent can be used to synchronize users to the OptimalCloud and also authenticate users in AD based on the cloud login. See Active Directory Synchronization.
- SCIM API – the OptimalCloud supports the System for Cross-domain Identity Management (SCIM) protocol. The OptimalCloud SCIM API can be used to provision users to the OptimalCloud. See SCIM Provisioning.
- Just-in-time (JIT) Provisioning – when a user federates from an external Federated Identity Provider (IdP) and no corresponding user exists in the OptimalCloud, a new user will be created using the federated claims.

User Sign On

When signing into the OptimalCloud the user is first prompted for their user ID. Based on the user ID there are a number of ways the user can authenticate:

- Authenticate with OptimalCloud Credentials – authenticate with a user ID and password registered in The OptimalCloud.
- Authenticate via Social Media – authenticate via a Social Media provider such as Facebook, Google, LinkedIn, or Twitter.
- Authenticate via AD Authentication – authenticate with a user ID and password user interface in the OptimalCloud but authenticate via AD using the Optimal IdM AD Synchronization Agent. See Active Directory Synchronization.
- Authenticate via Federated Identity Provider – authenticate via an external Identity Provider using one of the supported federation protocols such as OAuth2, OpenID Connect, SAML 2.0, or WS-Federation.

When authenticating via Federated Identity Providers, the identity provider to use can be based on Adaptive Authorization rules. For instance choice of Federated Identity Provider can be based on the user's physical location, network, email address, or other attributes about the user.



Authentication Levels

By default there are four authentication levels defined in the OptimalCloud. The OptimalCloud will automatically perform step up authentication based on the current session authentication level when a higher authentication level is required. The default authentication levels are:

- Social – the user has signed into the OptimalCloud using Social Media, such as Facebook, Google, LinkedIn, or Twitter.
- Password – the user has signed into the OptimalCloud using a user ID and password.
- Certificate – the user has signed into the OptimalCloud using client certificate based authentication (PKI).
- Multi-factor Authentication (MFA) – the user has performed MFA.

A minimum authentication level can be defined on a Group, Organization, Application, or Service Provider. Authentication levels can also be defined using Adaptive Authentication rules.

The OptimalCloud supports a number of MFA methods:

- email One-Time-Password (OTP)
- SMS OTP, Voice Message OTP
- Hardware Device
- Typing Behavioral Biometrics.

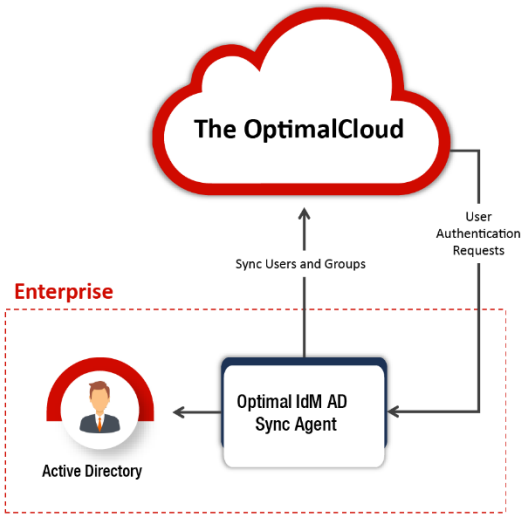
For Hardware Device authentication the OptimalCloud supports all standard TOTP, FIDO, and WebAuthN devices. The OptimalCloud also supports PUSH Notification via the Optimal Authenticator, a free mobile application available for Android and iOS devices.

Note: some MFA options may not be available in your deployment depending on your subscription. If you don't see the options you want, please contact us at info@optimalidm.com.

Active Directory Synchronization

The Optimal IdM AD Synchonization Agent can be used to synchronize Users and Groups from Active Directory (AD) to the OptimalCloud. Optionally, synchronized users can authenticate to the OptimalCloud using their AD user ID and password.

Note: the Optimal IdM AD Synchronization Agent never synchronizes passwords from AD to the OptimalCloud, and only requires standard HTTPS outbound connections (no inbound connections are needed).



SCIM Provisioning

The OptimalCloud SCIM API can be used to provision users and groups to the OptimalCloud. The SCIM API can be used to add, modify, and delete users and groups. The SCIM API can be used to search for users and groups as well as modifying group membership.

The OptimalCloud SCIM API is SCIM v2.0 compliant. For more information about the SCIM specification, see RFC 7644.