OPTICAL AUTHENTICATION SERVICE

A COMPLETE MULTIFACTOR AUTHENTICATION SOLUTION

OPTIMAL IdM

Identity & Access Management

OPTIMAL AUTHENTICATION SERVICE™

AUTHENTICATION AS A SERVICE

The Optimal IdM authentication-as-a-service (AaaS) offering, called The Optimal Authentication Service™ (OAS), is a hosted RESTful web service that provides customers with the ability to perform various types and levels of authentications including single authentication and multi-factor authentication (MFA).

The service may be deployed in any data center and is offered in a multi-tenant environment as well as in an isolated/dedicated environment. OAS can easily integrate into your application using the RESTful call or by using the Optimal IdM .NET SDK or jQuery plugin.

THE OPTIMAL AUTHENTICATION SERVICE PERMITS THE ADDITION OF MULTI-FACTOR AUTHENTICATION

AND CAN BE FULLY INTEGRATED INTO THE OPTIMALCLOUD.

Because this service is available via industry standard REST calls, both web and non-web applications may easily add MFA capabilities, including password-less options. As a MFA service, OAS helps prevent phishing and man-in-the-middle attacks by delivering push notifications to a user’s registered mobile device which optionally works with fingerprint enabled systems. OAS includes other MFA options like Time-based One-Time Password (TOTP) and traditional One-Time Passcodes (OTP) that can be sent via Short Message Service (SMS), Email or voice calls.

Each can be used as a stand-alone option or in conjunction with a complete Identity Access and Management (IAM) program. When integrating with an existing system, you can leverage OTPs via SMS, Email or voice without storing any information about the user in the cloud service. When using TOTP or push notifications, only device information is stored, which reduces the amount of personal identifiable information that is needed. The service can also be used to access applications in a password-less method by sending a push notifications to a mobile device for logins.

THE KEY BENEFITS OF OPTICAL AUTHENTICATION SERVICE (OAS)

BENEFITS

1. Seamlessly add MFA to web and non-web applications

2. Delivery through SMS, Push, TOTP, OTP’s via email, Voice and Fingerprint

3. A hosted RESTful web service

4. The Optimal GINA Plugin offers a flexible and secure solution for securing access to Windows serversIncreased Security and Control

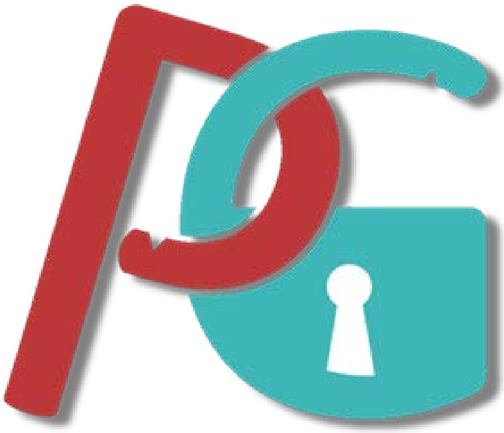
5. Optimal Authenticator available on Google Play and the Apple App Store

Optimal GINA™ Plugin (pGina)

Optimal GINA™ Plugin (pGina) – Accessing Windows Servers, whether in a local data-center or cloud-based, should always require multi-factor authentication (MFA). Until now, it has been a difficult task to setup MFA for server access whether directly through the console or via remote-desktop (RDP). However, with the Optimal GINA™ Plugin for pGina, you can enforce MFA requirements for all server access.

The Optimal Gina plugin along with the Optimal Authentication Service, offers a flexible and secure solution for accessing Windows servers providing state-of-the-art MFA technology leveraging the user's mobile device and PUSH notification technology. Accounts are easily managed in The OptimalCloud™.

pGina also provides the ability to map cloud groups to local server/domain groups when logging in. In fact, users that are configured to login to a given server via The OptimalCoud can automatically have an account created locally and even optionally deleted when they log out.



What is pGina?

pGina is a flexible replacement for the default Windows credential provider (or GINA – Graphical Identification and Authentication library).

The "p" represents "plugins". pGina provides an authentication and authorization framework which supports plugins (e.g. the Optimal GINA Plugin), which extend the capabilities of the default credential provider.

pGina and Multi-Factor Authentication

Plugins are written in managed code and allow for user authentication, authorization and session management. The end result is that you, the administrator, can choose how your users are authenticated, authorized and managed.

The Optimal GINA Plugin extends the pGina framework, allowing administrators to require Multi-Factor Authentication (MFA) for server access.

BENEFITS OF USING THE OPTIMAL GINA PLUGIN

For security reasons access to Windows Servers, whether in a local data-center or cloud-based, should always require multi-factor authentication (MFA).

The Optimal GINA Plugin along with the Optimal Authentication Service, offers a flexible and secure solution for securing access to Windows servers with state-of-the-art MFA technology, leveraging the user's mobile device and PUSH notification technology. Accounts are easily managed in The OptimalCloud™.

The Optimal GINA Plugin also provides the ability to map cloud groups to local server/domain groups for authorization purposes on-the-fly when a user logs in.

Furthermore, the Optimal GINA Plugin can also be configured to dynamically create user accounts locally when the user logs into the server, and optionally deleted their account when they log out.

This dynamic provisioning and de-provisioning can be used to provide an extra level of security, as users will never have a permanent local server account.

The Optimal Authentication Service includes:

- Password-less Access method
- Basic Authentication (username & password)
- Strong-Authentication via E-Mail (MFA)
- Strong-Authentication via SMS/Text Message (MFA)
- Strong-Authentication via VOICE (where a call is placed to a number) (MFA)
- Strong-Authentication via TOTP (MFA)
- Strong-Authentication via PUSH (alert to a mobile device)(MFA)
- Basic Authentication + Strong-Authentication via PUSH (alert to a mobile device) (Fingerprint authentication to iOS and Android)(MFA)
- For more information about authentication-as-a-service, contact Optimal IdM today.

FOR MORE INFORMATION ON OUR PRODUCTS AND SERVICES

VISIT US ONLINE: WWW.OPTIMALIDM.COM

Optimal IdM is a global provider of innovative and affordable identity access management solutions. We partner with our clients to provide comprehensive, fully customizable enterprise level solutions that meet the specific security and scalability needs of their organizations. Optimal IdM offers its solutions both on-premise and in the cloud as a 100% managed service offering. Customers include Fortune 1000 companies, as well as Federal, State and Local Government agencies all over the world.

PRODUCTS

- Virtual Identity Server
- LDAP Proxy Firewall
- VIS for SharePoint
- Optimal Federation & Identity Services
- Optimal People Picker for SharePoint
- VIS for Office 365
- The OptimalCloud
- Cloud Reporting
- Optimal Authentication Service