Entrust® Securing Digital Identities & Information

SECURITY ON

Entrust IdentityGuard: Federation Module

Manage & Secure Access to Cloud-Based Services and Networks via Existing User Credentials

Organizations are increasingly moving toward cloud and software-as-a-service (SaaS) applications. In many cases, they are forced to create a new set of identity credentials for end-users and, typically, these identities are based on insecure, outdated username and password approaches.

As organizations move more services to the cloud — such as email, CRM and other applications — the number of user identities grows at an exponential rate.

This leaves end-users with the burden of managing multiple usernames and passwords for each service, not only causing frustration but also hindering security effectiveness. This approach introduces many obstacles.

- Forgotten usernames and passwords, a frustrating experience that drives password reuse, thus reducing overall security
- Adhering to many differing password policies required by the SaaS/cloud provider
- Passwords are a weak form of authentication that have low upfront costs, but a high total cost of ownership (TCO) and inherent security risks

Secure Network Expansion

In addition to cloud access, organizations extend access to their networks with the goal of increasing productivity and streamlining business. But, in doing so, organizations may need to implement an entirely new user-access infrastructure.

Unfortunately, this likely introduces another set of usernames and passwords for end-users to manage. While the use cases of inter- and intra-company access and cloud differ slightly, the constant thread is the need to provide consistent and secure access.

Simple username and password authentication is insufficient protection against unauthorized access to cloud-based services. A strong second factor of authentication is required to properly authenticate individuals accessing cloud-based services to protect from theft or altering of sensitive information.

The type of authenticator used, its strength and total cost may be different depending on what it is protecting, the usability requirements of the officers and budgetary constraints.

Solution Benefits

- Leverage organizational identities to access cloud and inter- and intra-network applications
- Reduce the number of IDs per user
- Single sign-on (SSO) across multiple services
- Integration with SaaS/cloud services (e.g., Microsoft 365, Salesforce.com)
- Standards-based approach simplifies integration (e.g., SAML and OpenID identity providers)
- Strong second-factor authentication to cloud-based services
- Widest range of cost-effective authentication methods to meet unique user requirements
- Flexible to meet current and future security priorities
- Based on award-winning Entrust IdentityGuard software authentication platform

COMPREHENSIVE FEDERATION OF USER IDENTITIES

An extension to the Entrust IdentityGuard software authentication platform, the Entrust IdentityGuard Federation Module allows organizations to manage and secure access to cloud-based services by federating existing user credentials.

The solution enables organizations to federate identities to securely access other networks (e.g., partnering organizations), reducing reliance on usernames and passwords, as well as improving both security and the end-user experience.

Organizations may integrate with some of the most popular cloud-based services (e.g., Microsoft 365, Salesforce.com), which allows end-users to have consistent, simple and secure access to cloud-based services or other organizations.

FEDERATION MODULE: HOW IT WORKS

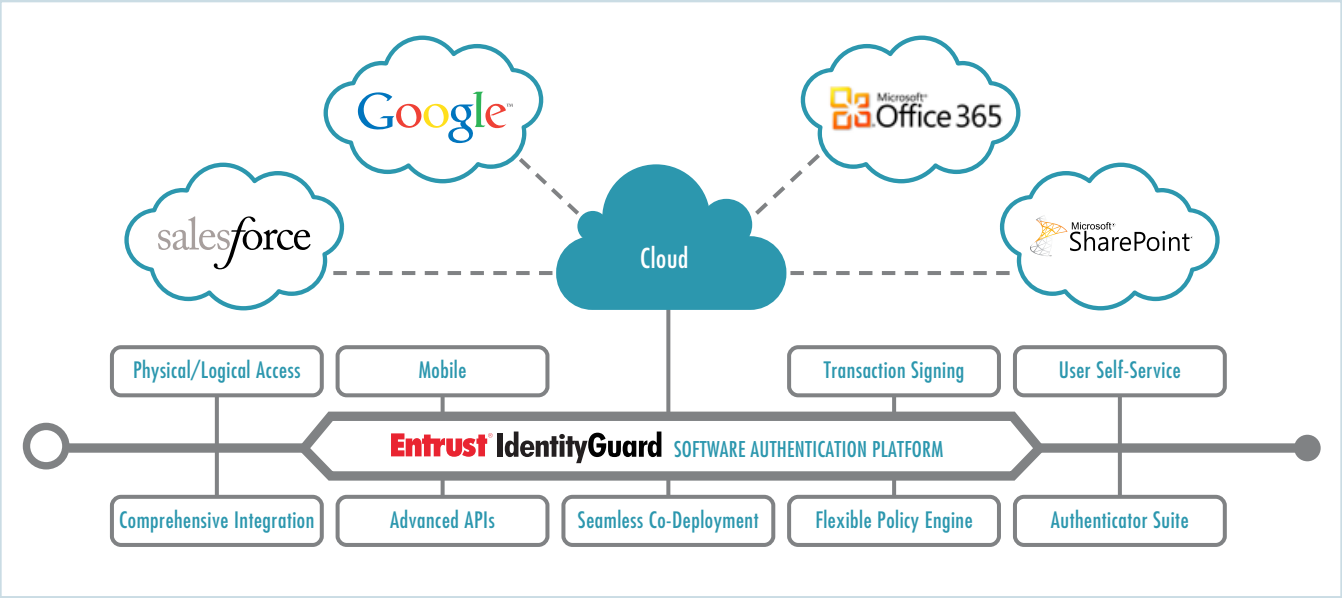
The Entrust IdentityGuard Federation Module enables secure access to a variety of distinct networks — whether they are within the organization or are external (e.g., cloud services, and/or a partnering organization). Simply, organizations require a secure means to access information contained within these entities.

Leverage Existing Digital IDs

The Federation Module allows users to leverage existing corporate IDs to access specific external network segments and cloud-based services — all without having to introduce or issue another set of identity credentials. The solution is based on industry-wide standards such as SAML and OpenID, allowing organizations the assurance of integration, compatibility and future extensibility.

Extend Security Investment

Unlike other federation solutions on the market, Entrust's federation module is based on the award-winning Entrust IdentityGuard software authentication platform, which enables organizations to inherit the strong identity offerings already provided by the platform.



AWARD-WINNING AUTHENTICATION PLATFORM

Entrust IdentityGuard secures cloud and network access for many of the world's leading enterprises, governments and financial institutions. It serves as an organization's single comprehensive user authentication platform and authenticates identities prior to accessing sensitive cloud-based services or computer networks.

All Authenticators, One Platform

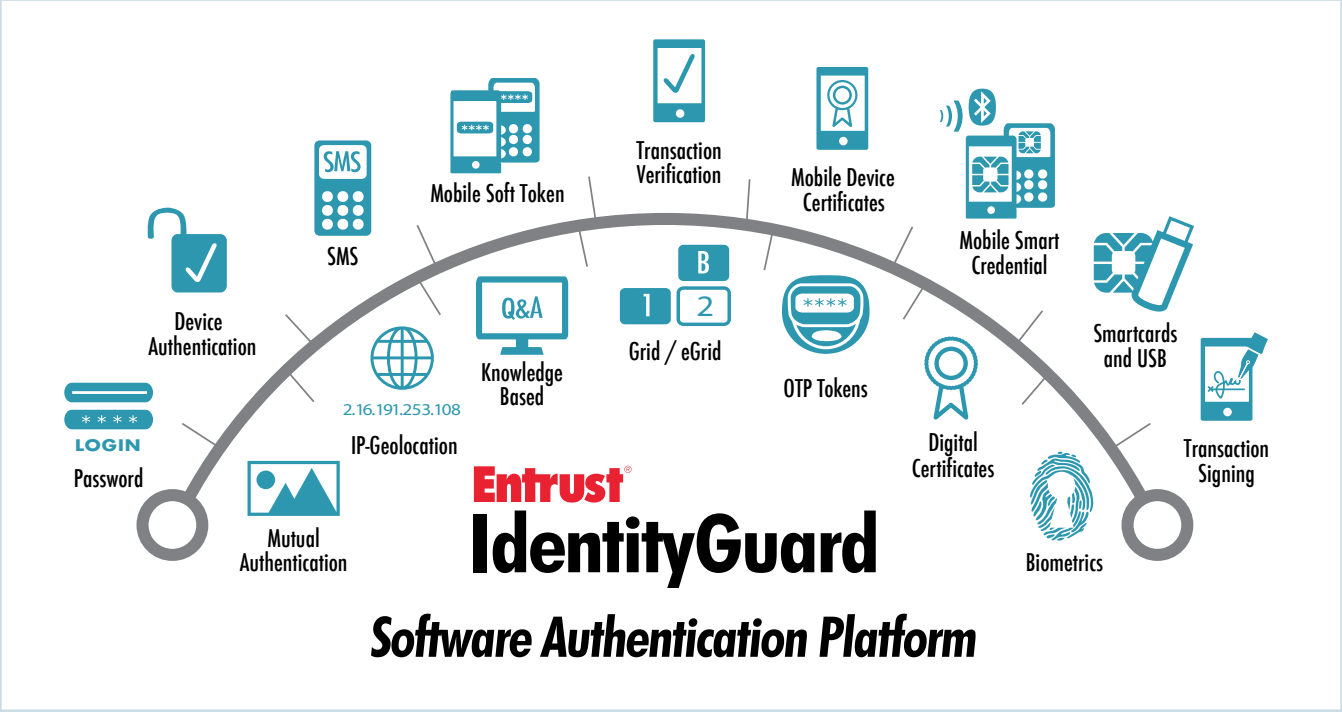
Entrust IdentityGuard offers a broad range of user authentication methods including physical (e.g., a one-time-passcode token or grid card), mobile- and smartcard-based, or online (e.g., passwords plus questions and answers).

Organizations may deploy authentication methods that are convenient and simple to use, ensure strong user authentication of the user, and meet the budgetary requirements of the organization.

Evolve to Address New Risks

This approach provides a single point of administration, regardless of the authentication option or combination of options deployed.

Organizations are able to evolve and change authentication methods over time as the risks and the operating environment change.



Entrust's flagship authentication solution, Entrust IdentityGuard continues to lead the industry as one of the most robust software authentication platforms, delivering an unmatched breadth of capabilities and flexibility to meet the most demanding security environments.

Evaluating Security Needs

The traditional authentication method — a user providing their username and password — is proven to be ineffective in preventing unauthorized access. Entrust IdentityGuard allows organizations to require additional authentication prior to network access.

All users are not created equal — nor do they need the same access. Entrust provides a range of authentication methods to ensure an organization's unique requirements are met. The type of authenticators used is based on an evaluation of the organization and their requirements.

Once issued, this second factor of authentication will be required (in addition to their username and password) when a user attempts to access a secure network. This helps strongly authenticate the identity of the individual and prevent unauthorized access.

Internal Security Evaluation

- How sensitive is the information you are protecting?
- What is the risk of a breach?
- Who will be using the authenticator and what are their unique requirements?
- Do you want authentication to be transparent to the user or can the user carry a physical device?
- Can you leverage the user's mobile device?
- Do you want to use the same authenticator for physical access?

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects.

Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information on Entrust's comprehensive portfolio of identity-based security solutions, contact the representative in your area at **888-690-2424** or visit **entrust.com/federation**.

About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Entrust® Securing Digital Identities & Information

24640/12-12