Two-Factor Authentication Solution for Enterprises

Devolutions

SAAS vs ENTRUST IDENTITYGUARD vs MICROSOFT AZURE MULTI-FACTOR AUTHENTICATION

Last week we did an updated review of 2FA solutions that was targeted toward single users, but what about company-wide solutions? With businesses falling victim to brute-force attacks targeting physical and logical infrastructures, mobile platforms and user identities, **an extra layer of security is integral to protect from all of those threats**.

To help you choose 2FA solutions for your enterprise we've compared three popular solutions: SAAS, Entrust IdentityGuard and Microsoft Azure Multi-Factor Authentication.

SAASPASS IS KNOWN FOR ITS HIGH LEVEL OF SECURITY AND MULTI-FACTOR AUTHENTICATION. IT EASILY REPLACES THE USE OF PASSWORDS ACROSS THE BOARD.

WHAT WE LOVE

APP SECURITY: The SAASPASS application offers a high level of protection like the touch ID support, fingerprint support on Android, 4 or 6 digit PIN options and a pattern support on Android devices. With all of that, SAASPASS is always protected against brute force attacks.

RECOVERY: You can setup recovery for your SAASPASS ID in case you've lost your phone and not cloned it onto multiple devices. You can also add additional security measures for your recovery by going to the Recovery menu under Settings.

SECURE SINGLE SIGN-ON FOR ACTIVE DIRECTORY: As an administrator you can set up SAASPASS two-factor authentication and secure single sign-on for your Microsoft Active Directory company domain smoothly. You can add SAASPASS to all your on-premises assets controlled by Active Directory.

VPN WITH 2FA: Easily integrate your 2FA solution directly into your VPN. Secure tunneling is now safer than ever with static passwords being replaced by randomly generated dynamic passcodes.

WHERE IT NEEDS IMPROVEMENT

The set-up is somewhat **confusing**. It can take a little while to figure out the process at times.

WHO IT'S FOR

With their wide range of options and the Active Directory solution, SAASPASS would **fulfill the needs of multiple companies both big and small.**

SAASPASS offers different pricing options depending on which plan you wish to use. It is **completely free for personal use. For companies over 150 employees, there are plans ranging from $20 to $60 per employee per year.**

Entrust IdentityGuard

ENTRUST IDENTITYGUARD IS A 2FA APPLICATION, SERVER, SMARTCARD MANAGER, BIOMETRICS SERVER AND A VERSATILE AUTHENTICATION PLATFORM THAT ENABLES ORGANIZATIONS TO DEPLOY STRONG AUTHENTICATION THROUGHOUT AN ENTERPRISE.

WHAT WE LOVE

EASY FOR USERS: End-users are more and more confused by all the security measures they have to manage, like credentials, IDs, badges, and tokens. Entrust allows you to have a Jack-of-all-trades helping you to eliminate the confusion by reducing the number of credentials users must have for physical or logical access.

AUTHENTICATION METHODS: Entrust IdentityGuard offers a wide variety of supported authentication methods ranging from mobile OTP, soft and hard token and grid cards, as well as smartcards, USB and OTP tokens, SMS, QR Code, Mobile Smart Credentials and more.

INTEGRATION AND DEPLOYMENT: Entrust's open API architecture allows for tight integration with today's leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors. This enables Entrust IdentityGuard to work with new and existing enterprise implementations, offering seamless integration with existing directories.

SINGLE SOFTWARE PLATFORM: Entrust IdentityGuard allows businesses to distribute smartcards, digital certificates, mobile-based smart credentials and a full range of strong authentication options from a single software platform.

WHERE IT NEEDS IMPROVEMENT

There is quite a big learning curve for the administrators, so it can be time consuming to get the whole process started. Budget-wise, the smart card readers and biometric scanners don't come with the licenses and can increase the overall cost.

WHO IT'S FOR

Entrust IdentityGuard is meant for enterprises, not for personal use. It is an efficient tool to use when wanting to manage authentication devices and identities from a single-platform.

The price is around **$8 per user** and **$3.75 per user above 25,000 users.**

Azure MFA

AZURE MULTI-FACTOR AUTHENTICATION REDUCES ORGANIZATIONAL RISK AND HELPS SAFEGUARD ACCESS TO DATA AND APPLICATIONS BY PROVIDING AN EXTRA LEVEL OF AUTHENTICATION. IT OFFERS A STRONG AUTHENTICATION THROUGH A WIDE RANGE OF VERIFICATION METHODS.

WHAT WE LOVE

ALERTS AND REAL-TIME MONITORING: Azure helps you protect your business with high security monitoring and machine-learning-based reports identifying inconsistent sign-in patterns. The real-time alerts will inform your IT department of any possible threats or any suspicious account credentials.

DEPLOY ON-PREMISES OR ON AZURE: It uses the power of the cloud and integrates with your on-premises Active Directory and custom application. This protection is even extended to your high-volume, mission-critical scenarios.

USE WITH OFFICE 365: It helps secure access to your Office 365 applications at no additional cost. It is also available with Azure Active Directory Premium and thousands of SaaS applications, including Salesforce, Dropbox, and more.

HIGH LEVEL OF SECURITY: Azure Multi-Factor Authentication offers strong and secure authentication using the highest industry standards.

WHERE IT NEEDS IMPROVEMENT

The initial deployment can be **confusing and challenging** depending on the internal setup, and especially when diverging from standard use cases.

WHO IT'S FOR

Azure can be quite expensive but if you have Office 365, Active Directory or if your solution falls within their standard use cases then it is a wise investment. On the other hand, if you need a lot of customization it would probably be better to go for another solution or to create a custom solution.

- **Per user consumption-based:** $1.70 per month (unlimited authentications)
- **Per authentication consumption-based:** $1.70 per 10 authentications
- **Per user annual model (Direct):** $1.70 per month (unlimited authentications)

CONCLUSION

And there you go folks! We know we have only taken a look at the tip of the iceberg when it comes to 2FA enterprise-wide solution, but don't worry eventually we will include even more solutions. Let's not forget that the implementation of an extra layer of security, like multifactor authentication, is a must for your company and is something that should never be taken lightly! We hope this will help you choose the right solution for you and your company!

Here is a table for a quick overview of some advanced options supported by the different 2 Factor Authentication applications.

	SAASPASS	Entrust IdentityGuard	Azure MFA
Mobile	✓	✓	✓
Desktop	✓	✓	✓
Cloud	✓	✓	✓
VPN 2FA	✓	✓	✓
Offline Mode	✓	✓	✓
SDK Support	✓	✓	✓*
RDM Integration			✓

Share with us which solution you are using by participating in our poll and have a chance to win a 25$ Amazon gift certificate.