SecurAccess – 2FA | jednorázová hesla (OTP)

Autentizace uživatelů k firemním zdrojům by na jedné straně měla splňovat ty nejpřísnější nároky na bezpečnost a na straně druhé zajišťovat komfort uživatelů. Vyváženou kombinaci obou požadavků přináší společnost SecurEnvoy se svým nástrojem SecureAccess, zajišťující bezpečnou autentizaci pomocí jednorázových hesel zasílaných formou SMS, softwarových tokenů a emailů. Uživatelé se již nemusí frustrovat nároky administrátorů na zapamatování náročných hesel. Svoje jednorázové heslo mají vždy při sobě!

Jednoduché nasazení a správa | Na rozdíl od tradičních řešení zajišťujících dvoufaktorovou autentizaci pomocí jednorázových hesel se SecurEnvoy nemusíte provádět žádné výrazné zásahy do Vašeho existujícího IT a celé řešení nasadíte na několik kliknutí. Díky integraci s Vaším Microsoft Active Directory, Novell eDirectory, Sun Directory Server a OpenLDAP zajistíte jednoduše bezpečný přístup všem Vašim zaměstnancům během pár okamžiků.

Úspora nákladů | Velkou výhodou celého řešení je to, že pro autentizaci využívají uživatelé něco, co již vlastní - mobilní telefon. Není tedy nutné dále zvyšovat náklady pořizováním nového hardwaru v podobě tokenů. Stejně tak každý administrátor uvítá absenci časově náročné distribuce hardwarových tokenů, která může zabrat i několik týdnů. SecurEnvoy řešení nasadíte během chvilky a rozeslání hesel se již děje automaticky prostřednictvím SMS nebo softwarový aplikací.

Hesla jsou mrtvá. Ať žije ... | Technologie **OneSwipe** od SecurEnvoy ohlašuje konec hesel, což znamená radikální změnu v přístupu k systémům a informacím v elektronické podobě. SecurEnvoy vyvinul nový nástroj dvoufaktorové autentizace (2FA), která staví na podpoře **NFC** (Near Field Communication) v chytrých telefonech i nových Windows 10. Nyní bude uživateli stačit pouze zadat pin na chytrém telefonu, přiložit ho k zařízení a bude autentizován.

Autentizace pro každého uživatele | Řešení společnosti SecurEnvoy umožňuje výběr, jaký typ autentizace zvolíte pro Vaše uživatele. Máte na výběr z níže uvedených možností:

- ✓ Pre-loaded SMS = uživatel má vždy k dispozici heslo pro další použití dopředu (například pro místa bez GSM signálu jako serverovny).
- ✓ Jednorázová SMS hesla na vyžádání - uživateli se po vyžádání objeví na telefonu a po určité době zmizí (není třeba je mazat).
- ✓ Softwarové tokeny – Aplikace pro smartphony a laptopy
- ✓ One Time Code – uživatel dostává vždy nové jednorázové heslo pro další použití (jak při úspěšné, tak neúspěšné autentizaci).
- ✓ Day Code – heslo je použitelné po definovaný počet dnů, následně uživatel dostává nové, bez ohledu na to, zdali se autentizoval, či nikoliv.
- ✓ Tmp Static Code – definované statické heslo platné po definovanou dobu a po uplynutí doby se vrací zpět na One Time Code či Day Code (nástrojů pro řešení situací, kdy uživatel zapomněl telefon).
- ✓ **NFC** / QR code / wearable – umožňuje využít chytrých hodinek nebo smartphone OTP autentizace s NFC technologií
- ✓ Voice Call – podpora jednorázových hesel zadaných přes pevnou linku.
- ✓ Jednorázová hesla zaslaná přes email – preload, real time, three codes

Klíčové vlastnosti

- ✓ **Vysoká míra zabezpečení** autentizace vzdálených přístupů se zachováním uživatelského komfortu (bez dalších portálů, modifikace stávajících portálů).
- ✓ **Pre-loaded technologie** řešící nedostupnost GSM pokrytí a zpoždění doručení SMS zpráv s jednorázovým heslem.
- ✓ SMS zprávy je možné odesílat pomocí podporovaných **HW GSM bran či webových poskytovatelů SMS služeb.**
- ✓ **Žádné "seed" informace** uložené na serverech výrobce.
- ✓ Jednorázová hesla uložena na zařízení, které si uživatel maximálně chrání - **případná ztráta je odhalena prakticky ihned.**
- ✓ **Rychlé nasazení** řešení do stávající infrastruktury zákazníka.
- ✓ **Celkové snížení nákladů** na provozování celého řešení (snadno a rychle nasaditelné, snadno použitelné, bez client HW/SW).
- ✓ Administrátor definuje, jaký typ tokenů bude pro uživatele dostupný
- ✓ Podpora autentizace do **Windows 8 a Windows server 2012**
- ✓ **Podpora provozování více poskytovatelů SMS služeb současně**

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

6 kroků k otestování SecurEnvoy SecurAccess

Zaujalo Vás řešení SecurEnvoy? Rádi byste si jej vyzkoušeli? Není nic jednoduššího. V šesti následujících krocích naleznete návod jak celé řešení otestovat zcela zdarma a nezabere Vám to více jak hodinu Vašeho času.

1. Stažení produktu

Z adresy http://www.securenvoy.com/trial.aspx si stáhněte zkušební verzi řešení. Na úvodní stránce vyplníte kontaktní informace a na Vámi zadanou emailovou adresu dorazí testovací licenční klíč, v rámci kterého je i kredit 50 SMS web SMS poskytovatele AQL)

2. Nezbytné prostředí

Nutností pro testování je mít k dispozici Windows 2003|2008|2008R2|2012 Server s IIS

3. Instalace

Na připravený Windows server nainstalujeme SecurEnvoy, po instalaci se spustí config wizard, ve kterém ve čtyřech krocích nastavíte vše potřebné.

a. Provázání se stávající nebo testovací podporovanou adresářovou strukturou (Microsoft Active Directory, Novell E-Directory, Sun Directory Server, OpenLDAP, Microsoft ADAM)
b. Nastavení poštovního serveru
c. Nastavení web SMS poskytovatele AQL [50 free SMS] (případně provázat s podporovanou HW GSM bránou a vlastní SIM)
d. Konfigurace portu pro RADIUS server

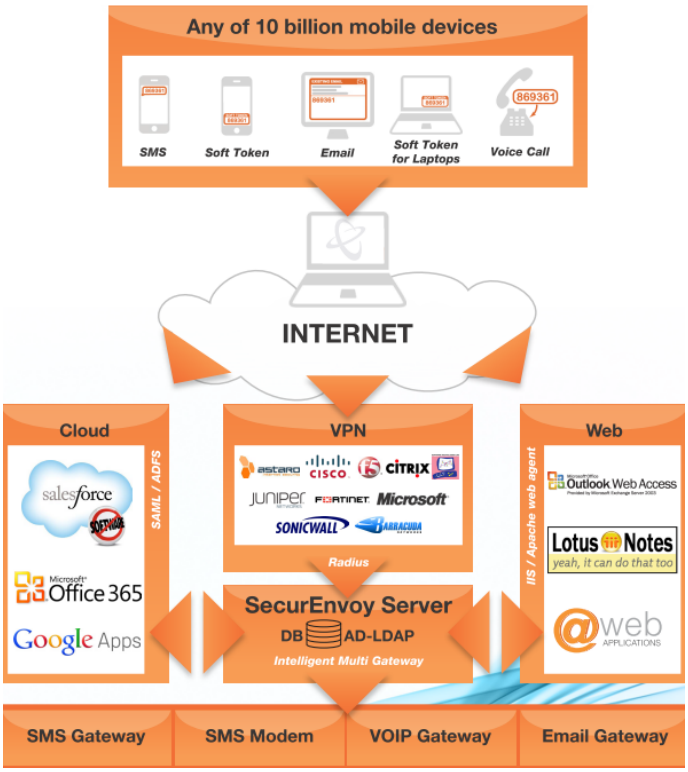
4. Administrace řešení

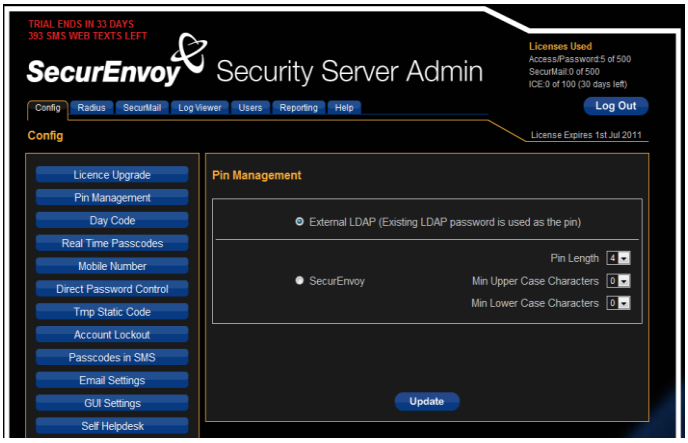
Veškerá administrace řešení je prováděna přes webové GUI SecurEnvoy. Ve kterém po přihlášení v záložce RADIUS provážete se stávajícím VPN řešením

5. Nasazení mezi uživatele

a. Přejdete do záložky Users, kde bude dostupný seznam uživatelů z definované adresářové struktury (AD aj).
b. Autorizujete definované uživatele pro využití SMS autentizace (dostupný také deployment nástroj pro společnosti s větším počtem uživatelů).
c. Uživateli dorazí první jednorázové heslo pro přihlášení do VPN (jako PIN je defaultně nastaveno heslo z domény).

6. Po dokončení testování je možné z testovací verze přejít na ostrou pouhou výměnnou licenčního klíče.





COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz