



Wave EMBASSY® Remote Administration Server (ERAS)

Řízení zabezpečení na základě adresářových služeb pro SED, TPM a BitLocker

Hlavní výhody:

- ✓ **Bezpečnost:** Zvyšuje zabezpečení zařízení díky centrálnímu vynucování zásad, bezpečnému obnovení uživatelského přístupu a ochraně ověřovacích údajů uživatelů a zařízení.
- ✓ **Shoda s bezpečnostní politikou:** Zajišťuje shodu s bezpečnostní politikou prostřednictvím aktivního monitorování, protokolování a reportingu všech událostí spojených s uživateli a zařízeními, v souvislosti s disky s plným šifrováním disků (SED – Self-Encrypting Drives) nebo klientskými Microsoft BitLocker šifrováním a moduly s důvěryhodnou platformou (TPM – Trusted Platform Modules).
- ✓ **Náklady:** Minimalizuje režii IT a náklady na helpdesk spojené se správou, nasazením a údržbou šifrovacích systémů či podporu uživatele.
- ✓ **Přizpůsobivost:** Transparentní ovládací prvek, který se přizpůsobí vaší infrastruktuře, vašim uživatelům a vašim potřebám zabezpečení dnes i v budoucnu.

Centrální správa zabezpečení

Velké i malé organizace chápou, že centrální správa zabezpečení je nezbytnou součástí ochrany jejich sítí a současně kritických informací, které jsou rozhodující pro jejich podnikání. Software Wave poskytuje řízení přístupu na základě zásad, komplexní reporting, integraci adresářových služeb, centrální řízení a obnovování přístupů koncových uživatelů, které společnosti vyžadují pro cenově příznivou implementaci a správu šifrování a ověřování koncových bodů. A co je nejdůležitější, software Wave dává společnosti jistotu, že v případě ztráty nebo krádeže počítače (či jeho pevného disku) jsou její data bezpečně chráněna.

Wave EMBASSY Remote Administration Server

V rámci konvenčních metodik zabezpečení založených na samotném softwaru nelze efektivně ověřovat uživatele a počítače v síti nebo zabezpečit data na ztracených či odcizených laptotech, případně zajistit shodu se zákony. SED, TPM a Microsoft® BitLocker naštěstí poskytují bezpečnější, cenově příznivější a jednodušší způsoby zabezpečení vašich kritických obchodních informací. Tyto technologie však představují pouze polovinu odpovědi. ERAS transformuje SED, TPM a BitLocker na řešení pro šifrování a ověřování v rámci celého podniku doplněním nezbytných centrálních funkcí konfigurace a správy.

Ovladatelnost a řízení

ERAS poskytuje kompletní sadu funkcí pro vzdálené vyhledávání, inicializaci, konfiguraci a správu globálního počítačového vybavení se šifrováním disku SED, TPM a Microsoft BitLocker. Díky nativní integraci s Microsoft Active Directory představuje ERAS prostředek pro centrální poskytování zásad zabezpečení pro koncové body v celém podniku, omezuje přístup k šifrovaným informacím a vzdáleně provádí správu ověřovacích údajů uživatelů a zařízení. Nejdůležitější je to, že díky ERAS mohou organizace prokázat, že splňovaly a splňují předpisy týkající se porušování zabezpečení.

Základní funkce ERAS:

- Modul snap-in Microsoft Management Console (MMC) umožňuje řízení na úrovni jednotlivých uživatelů a skupin
- Plně kompatibilní s Windows Management Instrumentation (WMI)
- Delegovaná správa na základě rolí
- Podpora pro počítače mimo doménu
- Poskytuje objekty zásad skupiny (GPO), skriptování a operace příkazového řádku
- Průvodci nastavením pro SED, TPM a BitLocker

ERAS pro disky s hardwarovým šifrováním (SED)

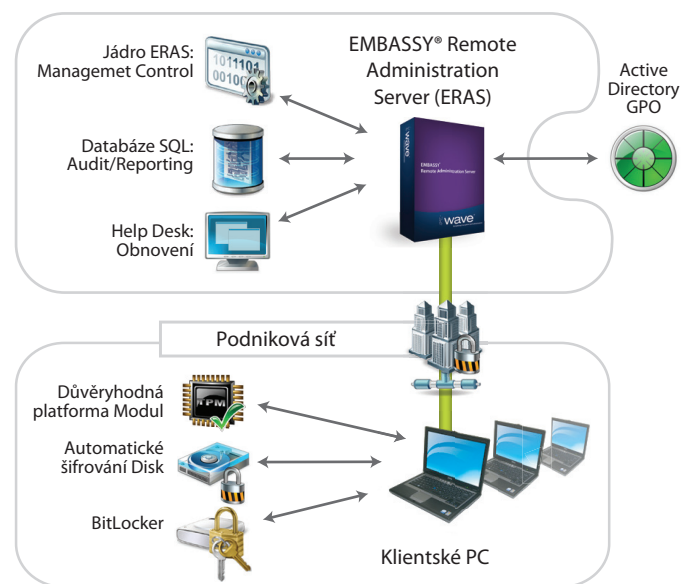
SED jsou nejbezpečnější, nejvýkonnější a nejtransparentnější možností šifrování pro ochranu dat na laptotech. ERAS je jediným řešením řízení, jež umožňuje inicializaci zabezpečení disku, správu uživatelů, uzamčení disku, obnovení uživatelů a bezpečné vymazání pro všechny disky SED se specifikací Opal (mechanické a SSD disky s podporou SED). ERAS navíc nabízí následující:

- Common Access Card (CAC), karta smart card
- Bezpečnou pomoc uživatelům prostřednictvím výzvy/odpovědi
- Synchronizace hesel Windows a jednorázové přihlášení (SSO)
- SSO na základě uživatelského účtu při přihlášení
- Reporty a protokoly zařízení a stavy a události uživatelů
- Ovládání externích SED

ERAS pro moduly s důvěryhodnou platformou (TPM)

TPM představují nejtransparentnější a nejlevnější způsob ochrany uživatelských jmen a rozpoznávání toho, které počítače jsou vaše, a které ne. Místo postupné aktivace TPM na jednotlivých počítačích umožňuje ERAS aktivaci, vlastnictví a správu TPM z centrálního místa. Jakmile jsou TPM zapnuty, můžete pomocí ERAS vytvořit digitální certifikáty na základě hardwaru pro vaše VPN, bezdrátovou síť nebo jiné aplikace s aktivní PKI — eliminují se tak rizika privátních klíčů a zajistí se identita zařízení. ERAS navíc:

- Převádí správu TPM pod kontrolu IT
- Umožňuje resetování hesla TPM pro obnovení uživatele
- Podává hlášení o stavu TPM (aktivní/vlastněný)



ERAS for Microsoft BitLocker

Úzká integrace Microsoft BitLocker s platformami a využívání TPM představuje dobrý začátek pro šifrování disků v organizacích, které používají Windows® 7. Wave ERAS nabízí kompletní sadu funkcí pro automatizaci a zabezpečení konfigurace a správy Microsoft BitLocker. ERAS představuje jednoduchou a intuitivní aplikaci pro nastavování, údržbu a reporting klientů BitLocker — eliminují se tak náklady, složitost a nejistota navrhování vašich vlastních řešení s využitím "domácích" skriptů a úprav adresářů.

ERAS navíc:

- Vynucuje konzistentní nastavení zásad na všech klientech BitLocker
- Zajišťuje obnovování hesel v šifrované databázi
- Monitoruje, protokoluje a reportuje všechny události BitLocker související s aktivací, řízením zásad a přístupem a obnovováním uživatelů
- Zjednodušuje aktivaci TPM pro BitLocker a zachovává TPM pro ověřování uživatelů a zařízení
- Poskytuje jednoduchou a transparentní cestu migrace z BitLocker na disky SED

Technické specifikace

Požadavky na hardware serveru

(pro správu až 2000 účtů)

- Systémový procesor: minimálně: 2 GHz, doporučuje se: 2.5 GHz, 4 Core nebo lepší
- Systémová paměť: doporučuje se 4 GB RAM nebo více
- Volný prostor na disku: minimálně: 10 GB doporučuje se: 40 GB
- 1 GB síťové rozhraní

Operační systém

- Microsoft® Windows® 2003 R2 a vyšší verze, doporučuje se Windows 2008 R2

Kompatibilní serverové komponenty

- Funkční úroveň domény Windows 2003, 2008 nebo 2008 R2
- Microsoft Management Console 3.0
- Group Policy Management Console
- Microsoft SQL Server 2005 a vyšší verze, doporučuje se 2008 nebo vyšší verze
- Microsoft Internet Information Service 6.0 (IIS) nebo IIS 7
- .Net Framework 3.5 a 4.0

Microsoft, Windows a BitLocker jsou buď registrované ochranné známky, nebo obchodní značky skupiny společností Microsoft.

Oficiální distributor pro ČR a SR

Genisoft, a.s.
Strakonická 6
Praha 5 - Lahovičky, 159 00
Česká republika
+420 723 885 032
info@genisoft.cz



Wave Systems EMEA

Německo
Darmstaedter
Landstrasse 87-89,D-60598
Frankfurt, Germany
+49 69 959 32 393
emea@wave.com

Severní Evropa
47 Belgrave Square
London SW1X 8QR, UK
+44 1235 520956
emea@wave.com

**Jižní Evropa,
Afrika & Střední východ**
24 ter, rue Abbé Larose
44190 Gorges, France
+33 2 28 07 42 01
emea@wave.com