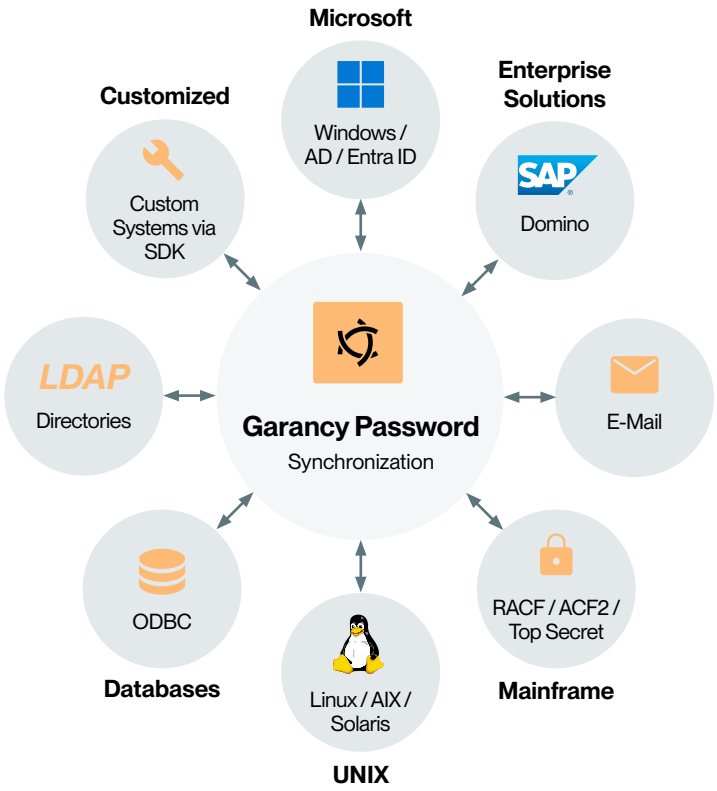
beta systems

Garancy®

Data Sheet – Password Synchronization

Einfacher Zugriff – mit nur einem Passwort

Immer mehr Systeme und Anwendungen verlangen eigene Passwörter und individuelle Richtlinien – für viele Nutzer eine echte Herausforderung. Garancy Password Synchronization schafft hier spürbare Entlastung, indem Passwörter in allen angebundenen Systemen automatisch synchronisiert werden.



Vorteile auf einen Blick

- Ein Passwort für alle Systeme
- Schneller und reibungslose Einführung
- Mühelose Integration in bestehende IT-Umgebungen
- Kosteneffizienter als SSO

Noch mehr Komfort und Effizienz

Kombinieren Sie Garancy Password Synchronization mit dem Modul **Password Reset** für eine nahtlose Nutzererfahrung und noch mehr Effizienz. Nutzer können vergessene Passwörter direkt vom Windows-Login-Bildschirm aus zurücksetzen. Die Sicherheit lässt sich zusätzlich durch Multi-Faktor-Authentifizierung wie SMS- und E-Mail-PINs oder TOTP erhöhen. So entsteht ein konsistentes, sicheres und nutzerfreundliches Passwortmanagement im gesamten Unternehmen.

Ändert ein Nutzer sein Passwort in einem System, wird es überall sofort aktualisiert – schnell, sicher und völlig reibungslos. Statt mehrere Passwörter im Kopf behalten zu müssen, reicht künftig ein einziges. Unternehmen profitieren gleichzeitig von reduziertem Help-Desk-Aufwand und mehr Effizienz. Die Lösung bietet den Komfort eines SSO-Setups, ist aber weniger komplex und deutlich kostengünstiger.

Funktionsumfang

Bereitstellung und Integration

- Nahtlose Implementierung für Windows, z/OS, UNIX und IBM i
- Flexible Anbindung von nicht-standardisierten Systemen über das integrierte Software Development Kit (SDK)
- Schnelle Bereitstellung, die den Time-to-Value verkürzt – auch in komplexen Umgebungen

Sicherheit und Compliance

- Durchgängige Absicherung dank verschlüsselter und authentifizierter TLS-Kommunikation
- Verbesserte Passworthygiene mit Blacklist-Support für Windows und Mainframe
- Vollständige Audit-Trails für lückenlose Nachvollziehbarkeit aller Passwortaktivitäten

Intelligentes Password Management

- Konsistente Durchsetzung von Passwortregeln und Komplexitätsanforderungen über alle angebundenen Systeme hinweg

Unterstützte Systeme

- **Mainframe:** RACF, ACF2, Top Secret
- **Microsoft:** Active Directory / EntraID, Office 365, Windows
- **Unix:** Linux, IBM AIX, Solaris
- IBM i
- SAP
- LDAP
- Domino
- Garancy Identity Manager (ISEC)
- ODBC (MS SQL, Oracle, Teradata)
- SDK für individuelle Systeme

beta systems

Beta Systems IAM Software AG
Ernst-Reuter-Platz 6, 10587 Berlin

Tel. +49 (0) 30 726 118-0
www.betasystems.com, info-iam@betasystems.com

Produktdetails

Erhöhte Benutzerzufriedenheit durch nahtlose Hintergrundprozesse

Garancy Password Synchronization arbeitet unauffällig im Hintergrund und liefert dabei spürbare Vorteile. Nutzer müssen nicht länger mehrere Passwörter verwalten und behalten in der Regel nur noch ein einziges sicheres Kennwort.

Die Lösung sorgt für einheitliche, unternehmensweite Passwortrichtlinien, unterstützt mehrere Instanzen derselben Anwendung – zum Beispiel ein gemeinsames Passwort für alle SAP-Systeme – und lässt sich schnell einführen. Ändert sich ein Passwort oder der Account-Status in einem angebundenen System, werden die Updates auch in allen anderen verwalteten Systemen umgesetzt – schnell, zuverlässig und transparent. Admins ordnen lediglich die jeweiligen Accounts eines Users zu, auch wenn unterschiedliche Namenskonventionen genutzt werden.

Umfassende Synchronisation in Windows-Umgebungen

Die Plattform synchronisiert nicht nur Passwörter, sondern gleicht auch Account-Attribute ab. Wird ein User gesperrt, können verbundene Konten automatisch mitgesperrt werden.

Alle Änderungen werden in Echtzeit erkannt und sicher übertragen. Die Password Rule Authority (PRA) prüft jede Passwortänderung anhand der definierten Richtlinien, bevor die Synchronisation erfolgt. Das gewährleistet Konsistenz und hohe Sicherheit.

Mühelos über alle Plattformen hinweg

Garancy Password Synchronization verbindet unterschiedliche IT-Landschaften – von Windows, z/OS, IBM i und UNIX bis LDAP, SAP, Domino und großen Datenbankplattformen. Alle Mainframe-Sicherheitssysteme (RACF, ACF2 und Top Secret) werden vollständig unterstützt.

Änderungen erfolgen über verschlüsselte, authentifizierte Kanäle und sorgen so für einen durchgehend sicheren und regelkonformen IT-Betrieb.

Bereit für jedes System – ob Standard oder Individuallösung

Die Lösung passt sich der Entwicklung Ihrer Infrastruktur an. Mit dem Windows SDK sowie APIs und Exit Points für z/OS und UNIX können sogar individuelle und Legacy-Anwendungen eingebunden werden. Die Systeme erkennen Passwortänderungen automatisch und übertragen sie zuverlässig – für eine harmonisierte Passwortverwaltung in allen Anwendungen und Plattformen.

Bereit für den nächsten Schritt?

Kontaktieren Sie uns, um mehr über unsere IAM-Lösung zu erfahren – wir freuen uns auf Ihre Anfrage.

Schreiben Sie uns eine E-Mail an **info-iam@betasystems.com** oder melden Sie sich telefonisch unter **+49 (0) 30 726 118-0**.

www.betasystems.com/de/produkte/garancy