GARANCY PASSWORD MANAGEMENT

Erhöhte Sicherheit und verbesserte Produktivität!

GARANCY Password Management dient dem sicheren und einfachen Zugriff von Computern auf verschiedene IT-Plattformen oder Anwendungen in verteilten Systemen.

Die Lösung besteht aus den Komponenten **Password Synchronization und Password Reset** mit umfassend erweitertem Funktionsumfang dieser bewährten Produkte. Sie sorgt für erhöhte Sicherheit und geringere Betriebskosten bei der Verwaltung von Benutzerpasswörtern und dem systemweiten Zugriff in modernen IT Umgebungen und sorgt gleichermaßen für mehr Produktivität am elektronischen Arbeitsplatz.

PASSWORD RESET

Mit GARANCY Password Reset können sich Benutzer **eigenständig authentifizieren und ihr Passwort sicher und komfortabel zurücksetzen**.

Das Produkt überträgt somit im Falle eines vergessenen oder fehlerhaften Passworts die Wiederherstellung des Zugriffs auf alle relevanten Systeme auf den einzelnen Benutzer. Dies entlastet das IT-Fachpersonal und verkürzt die Unterbrechungszeiten für die Endanwender.

GARANCY Password Reset erleichtert es zudem, unternehmensweite Regeln und Richtlinien für die Bildung von Passwörter umzusetzen.

Die flexible und an die Kundenanforderungen anpassbare Infrastruktur erlaubt es, globale und einheitliche Regeln für die Passwortverwaltung zu implementieren. Die Anwendung dokumentiert sämtliche Änderungen an Pass-wörtern und Benutzer-IDs in umfangreichen Audit-Protokollen.

DETAILS

- Zentralisiertes Password Self-Reset für alle angeschlossenen Anwendungen
- Browser-basierte Verwendung für Benutzer und Administratoren
- Der "Helpdesk-Modus" ermöglicht ‚managed Services' mit derselben Anwendung
- Selbst-Registrierungsprozess für Benutzer, um Verwaltungsaufwand zu minimieren
- Optionale Multi-Faktor-Authentifizierung (E-Mail oder SMS-PIN) und
- Festlegung von unternehmensweiten Kennwort Richtlinien und Autorisierung des Passwort Reset

PASSWORD RESET BUSINESS VORTEILE

Kosteneinsparungen	Erhöhte Sicherheit	User Zufriedenheit und verbesserte Produktivität
• Reduzierte Help Desk-Arbeitsbelastung durch das Ausführen von Kennwortrücksetzungen als Self-Service • Reduzierte Leerlaufzeit der Benutzer durch Warten auf die Helpdesk-Ausführung • Reduzierte Arbeitsbelastung durch das Blockieren von Konten nach mehreren fehlgeschlagenen Anmeldungen	• Technische Durchsetzung von Passwortrichtlinien für alle angeschlossenen Systeme • Benutzer haben keine Angst, Passwörter zu vergessen - Erhöhung der Passwort-Sicherheitsstufe • Benutzerfreundlichkeit reduziert die Wahrscheinlichkeit, dass Benutzer Passwörter schreiben	• Benutzer müssen nicht zugeben, ein Passwort vergessen zu haben • Benutzer können Kennwörter zurücksetzen, ohne auf Help Desk zu warten • Weniger Leerlaufzeit der Benutzer / Resets sind jetzt in ihrer Kontrolle

SICHERER UND EINFACHER ZUGRIFF AUF PLATTFORMEN UND ANWENDUNGEN

PASSWORD SYNCHRONIZATION

Die GARANCY Password Synchronisation ermöglicht den Mitarbeitern Zugriff auf verschiedene Plattformen oder Anwendungen mit einem einzigen Passwort. Dabei wird sichergestellt, dass eine **Passwort-änderung in allen gekoppelten Systemen und Anwendungen automatisch synchronisiert** und anwendungs-übergreifend für den Benutzer verfügbar ist.

Password Synchronization stellt somit eine durchgängige Methode für die **plattformüber-greifende Verwaltung zentraler Passwort- und User-ID-Zugriffsattribute** bereit.

Wird ein Passwort auf einem System geändert, aktualisiert die Lösung das Passwort entsprechend für alle relevanten Konten im gesamten Netzwerk. Dadurch verringert sich die Zahl der Passwörter, die sich Mitarbeiter einprägen müssen, da der Zugriff auf die meisten Systeme über ein gemeinsames, synchronisiertes Passwort erfolgt.

Dies reduziert die Passwortkomplexität und senkt die Fälle vergessener Kennwörter deutlich. Gleichzeitig wirkt dies der Gewohnheit vieler Benutzer entgegen, Passwörter zu notieren, und erhöht damit die Sicherheit.

VORTEILE

- Reduzierte Help Desk-Arbeitsbelastung durch Senkung der Anzahl der Passwörter
- Keine Anwenderschulung für den Betrieb des Systems (verglichen mit SSO)
- Wenige Passwörter reduzieren die Wahrscheinlichkeit, dass Benutzer Passwörter schreiben
- Kein zentraler Server zum Hacken für den Masterzugriff
- Verbesserte Benutzerzufriedenheit und Produktivität
- Niedrige Gesamtanzahl der zu speichernden Passwörter
- Automatischer Systembetrieb - Keine Benutzerinteraktion erforderlich
- Kein System / Frontend zu bedienen - System arbeitet im Hintergrund

Beta Systems IAM Software AG

Alt-Moabit 90d | 10559 Berlin | Germany
Tel. +49 (0) 30 726 118-0 | Fax: +49 (0) 30 726 118-800
iam@betasystems.com | www.betasystems-iam.de

Berlin | Köln | Neustadt | Calgary | Washington D.C. | Wien
Paris | Madrid | London | Stockholm | Mailand | Brüssel

Beta Systems Partner: