



Auf einen Blick

Mit ASPR können Mitarbeiter vergessene Passwörter selbständig zurücksetzen – am Arbeitsplatz oder unterwegs, 24 Stunden am Tag, sieben Tage die Woche.

- **Multi-Faktor-Authentifizierung** mit kombinierbaren Anmelde-möglichkeiten
- **Zahlreiche Zielsysteme** durch individuelle Konnektoren anbinden
- **Password Randomizer** zur Generierung von Zufallspasswörtern
- **Password Propagation** überträgt generierte Zufallspasswörter in zahlreiche Zielsysteme
- Mit **ASPR\MobileResponse** am Smartphone ein neues Passwort setzen
- Anbindung an vorhandenes **Service-Portal**
- **Mehrsprachenfähigkeit** der Oberfläche
- **Revisionsicherheit und Compliance** durch Nachvollziehbarkeit und DSGVO-Konformität
- **P³-Abrechnungsmodell**: pay per password, pay per month oder pay per seat

Ihr Nutzen

- Mehr **Effizienz** durch Kostenoptimierung, Aufwandsreduzierung und verschiedene Abrechnungsmöglichkeiten
- Sehr hohe, **messbare Akzeptanz** beim Nutzer
- **Sicherheit und Compliance**
- **Made in Germany** - ASPR wird nach deutschen Qualitäts- und Sicherheitsstandards in München entwickelt und betreut



Trust Seal
www.teletrust.de/itsmig

Leistungsmerkmale

Multi-Faktor-Authentifizierung

Wählen Sie aus verschiedenen Authentifizierungsverfahren, die auch frei kombiniert werden können – für mehr Sicherheit und eine hohe Akzeptanz beim Anwender:

- Frage-/Antwort-Paar
- User-ID und Passwort
- Vier-Augen-Prinzip
- Smartcard / Token

Zahlreiche Zielsysteme

Mit Hilfe von Extensions lässt ASPR sich an eine Vielzahl von Zielsystemen anbinden und kann dadurch ideal an die unternehmensspezifische IT-Infrastruktur angepasst werden:

- MS Active Directory
- IBM z/OS
- Lotus Domino
- OpenLDAP
- SAP
- Unix/Linux





Password Randomizer

Mit dem Password Randomizer schließt ASPR eine potenzielle Sicherheitslücke in SSO-Umgebungen. Hier, aber auch in Smartcard-Umgebungen kommt es häufig vor, dass ein Account ein Password-Never-Expires-Flag erhält. Dies soll Systeme davon abhalten, alle X Tage beim Benutzer ein neues Kennwort abzufragen. Häufig bleibt dabei das letzte Kennwort eines Benutzers mit diesem Flag für immer im System. Um diese Lücke zu schließen, bietet ASPR einen Prozess, der regelmäßig im Hintergrund ein neues Zufallspasswort generiert.

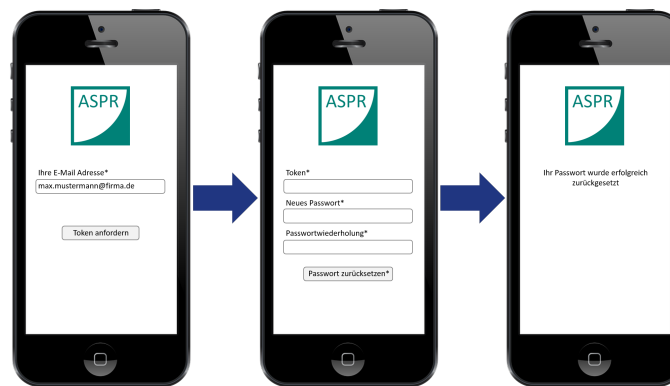
Password Propagation

Ein sicheres Passwort besteht heute durchschnittlich aus 12 bis 15 Zeichen, muss Groß- und Kleinschreibung, mehrere Ziffern sowie Sonderzeichen beinhalten und eine maximale Lebensdauer von 30 Tagen haben. Multiplizieren sich diese Faktoren zudem mit der Vielzahl an Passwörtern, die sich ein Mitarbeiter merken muss, liegt es nahe, dass der Reset-Bedarf bereits heute hoch ist und tendenziell weiter zunimmt. Mit Password Propagation genügt ein Passwort für alle Anwendungen und Systeme. Ein (Master-) Passwort ermöglicht das Weiterreichen neuer Passwörter von AD- oder Host-Systemen an alle angeschlossenen Zielsysteme.

ASPR\MobileResponse

Mit ASPR\MobileResponse erweitern wir den Password Reset Manager um eine mobile Lösung. Das bietet z.B. in Außendienst-Organisationen die Möglichkeit, ein Passwort ohne Einbeziehung des Service Desk zurückzusetzen.

Der Workflow ist einfach, benutzerfreundlich und intuitiv: Hat ein Mitarbeiter unterwegs sein Windows-Passwort vergessen, meldet er sich im Browser seines Smartphones auf der ASPR\MobileResponse-Seite seines Unternehmens an. Nach Eingabe seiner Benutzerkennung wird ihm ein Smart-Token per SMS zugesendet, den er dann eingibt. Anschließend kann er durch zweimalige Eingabe seines neuen Passworts den Reset bestätigen und sich wieder anmelden. Das spart Zeit und Kosten.



Anbindung an ein Service-Portal

ASPR ist auch in Verbindung mit Service-Portalen einsetzbar (z.B. ServiceNow), über die Anwender Kennwörter im Self Service und ohne Einschaltung von Service Desk oder Administrator zurücksetzen bzw. ändern können.

Mehrsprachenfähigkeit

ASPR steht neben deutsch und englisch (Standard) auch in weiteren Sprachen zur Verfügung. Das erhöht die Nutzerakzeptanz und verringert Sprachbarrieren.

Revisionsicherheit und Compliance

Durch vielfältige Attestierungs- und Reporting-Funktionen wird allen Anforderungen einer Revision Rechnung getragen. Unabhängige Experten haben uns bestätigt, dass unser Produkt ASPR EU DSGVO-konform ist.

P³-Abrechnungsmodell

Neben Kauf oder Miete bieten wir eine Abrechnung nach tatsächlich getätigtem Passwort-Reset bzw. -Change. Das bedeutet, Sie gehen kein Risiko bei der Einführung ein, da kein Start-Investment notwendig ist. Außerdem ist der Roll vom ersten Tag der Nutzung berechnen- und nachvollziehbar.

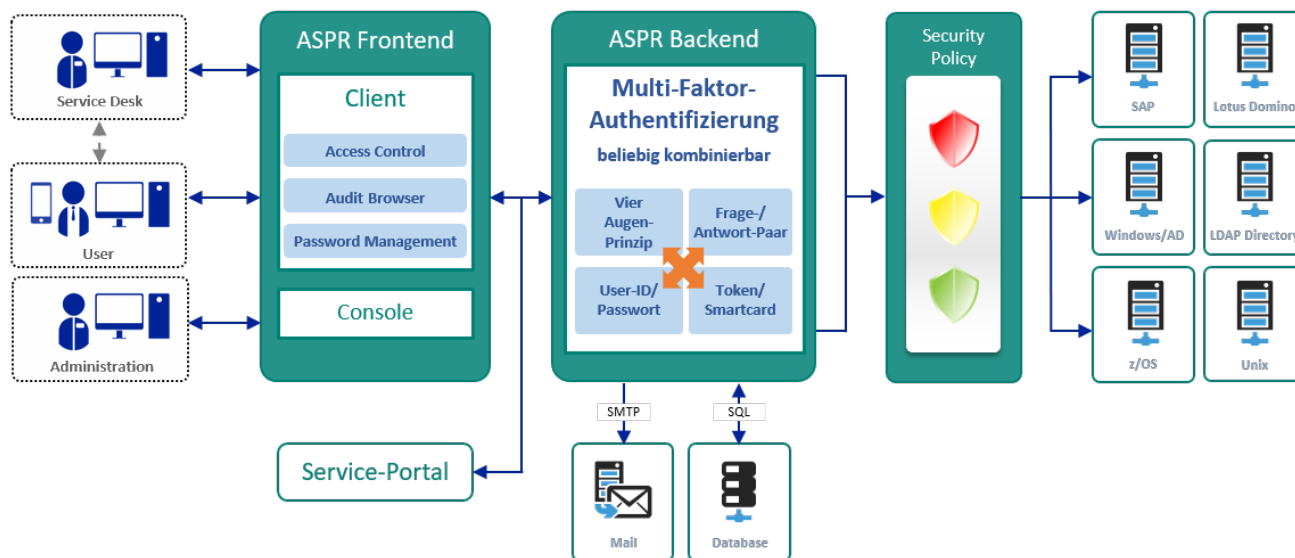


Aufbau

ASPR ist als Web-Anwendung konzipiert und erfordert beim Anwender keinerlei lokale Installation. Das Produkt zeichnet sich durch eine extrem flexible Konfigurierbarkeit aus.

Zum einen können dem User verschiedene Verfahren für die Authentifizierung zur Wahl gestellt werden, was zu einer sehr hohen Akzeptanz bei den Anwendern führt.

Zum anderen können diese Verfahren zur Einhaltung der jeweiligen Security Policy des Zielsystems auch noch untereinander kombiniert werden. In der Praxis führt dies dazu, das z.B. beim Password für Intranet-Applikationen eine einfache Authentifizierung ausreicht, beim Reset des Passwortes für ein SAP-HR-System aber eine 2-Faktor-Authentifizierung verwendet wird.



Sicherheitsaspekte

Bei der Entwicklung der TESIS SYSware-Produkte wurden alle Schutzobjekte betrachtet, die personenbezogene Daten und/oder Daten mit Sicherheitsrelevanz enthalten, z.B.

- Account-Informationen (ID, Anzeigewert)
- Berechtigungen (Account/Identität, Rechte auf Datei/Verzeichnis)
- Stammdaten (Name, Vorname, Abteilung, Personalnummer, Standort, E-Mail-Adresse, Telefon-, Handynummer)

Bei der Festlegung der Informationsobjekte mit personenbezogenen Daten wurden folgende Datenschutzgrundsätze berücksichtigt:

- Die personenbezogenen Daten werden nur zum Zwecke der Servicebereitstellung erfasst (Rechtmäßigkeit gem. EU DSGVO Art. 6, 7)
- Es werden nur für die Verarbeitung unmittelbar erforderliche Daten erfasst (Datenvermeidung und -sparsamkeit, EU DSGVO Art. 5)

Sensible Informationen laufen nur verschlüsselt durch das System. Alle Kommunikationswege sind bereits in der Standardinstallation zwischen den einzelnen Komponenten über SSL abgesichert.





Systemvoraussetzungen

ASPR Frontend

- Applikationsserver: Payara Version 4, Glassfish Version 4 oder Tomcat Version 8
- JDK Version 8
- 16 GB RAM
- 20 GB Speicherplatz
- Zugriff zum ASPR Backend-Server via TCP/IP, Standard-Port: 8885

ASPR Backend

- Windows oder Linux Server
- 16 GB RAM
- 50 GB Speicherplatz
- JRE Version 8
- Zugriff auf eine Datenbank via TCP/IP
- Port abhängig vom Datenbanktyp

Datenbank

- Eines der folgenden Systeme:
 - MS SQL Server ab 2012
 - MySQL ab 5
 - PostgreSQL ab 9

Sonstiges

- Kompatible und aktuelle Treiber für Java
- Zugriff auf einen SMTP-Server, evtl. mit Mail2MSGateway
- Die Firewall-Konfiguration muss Verbindungen des ASPR-Servers erlauben
- Ein privilegiertes Benutzerkonto mit Berechtigung zum Zurücksetzen von Passwörtern

Lieferumfang

Standard

- ASPR mit einer Zielsystem-Anbindung
- Zwei Sprachen (DE und EN)
- Anonymisierte Reports/Statistiken über alle angebundenen Zielsysteme

Optional

- Branding Package (Anpassung an Corporate Design des Kunden)
- Weitere Sprachen
- Anbindung weiterer Zielsysteme
- Mobile Nutzung

Hinweis

Über die reinen Systemvoraussetzungen hinausgehende technische und organisatorische Installationsvoraussetzungen sind einer separaten detaillierten Checkliste zu entnehmen.

