epas

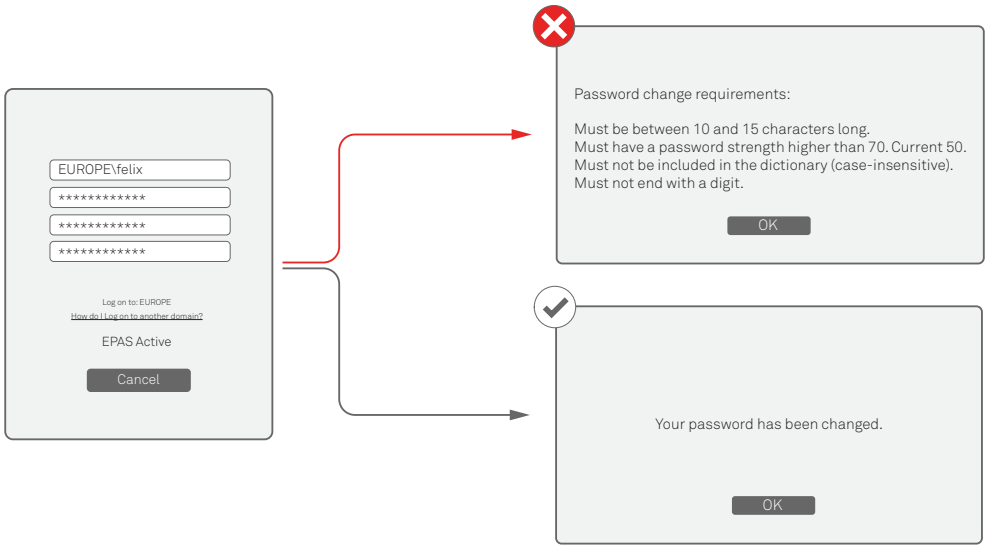
EPAS Enforcer

Der EPAS Enforcer ist ein in EPAS verfügbares Modul zum Password Quality Enforcement. Eine einzelne, hoch verfügbare EPAS Instanz verwaltet zentral Passwort-Changes aller unterstützten Systeme.
Das aktuelle Release unterstützt Microsoft Produkte. Support für weitere Plattformen befindet sich bereits in der Entwicklung.
Der EPAS Enforcer wird als LSA Filter in die Domain Controller einer Microsoft A/D Umgebung integriert und prüft bei neu gesetzten Passwörtern und Password-Changes, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht.
Die Sicherheitsanforderungen für ein Passwort ergeben sich aus kundenspezifischen und gruppenspezifischen Sicherheitseinstufungen sowie der Risikokategorie der zu schützenden Daten. Das neue Passwort wird mittels der EPAS eigenen Bewertungsmechanismen evaluiert und auf seine Widerstandsfähigkeit gegen echte Angriffe geprüft.
Für den Endbenutzer heißt das, dass früher erlaubte Passwörter wie „Passwort123“ oder „Geheim!“ nicht mehr akzeptiert werden.
Ist der Passwortwechsel nicht erfolgreich, so ermöglicht ein optionales Feature im EPAS Enforcer, dass Benutzer über die Gründe für fehlgeschlagene Passwortänderungen informiert werden (z.B.: „Das Passwort darf nicht in einem Wörterbuch enthalten sein.“).

„Mit dem EPAS Enforcer stellen wir schon beim Passwort-Change sicher, dass es tatsächlich ein starkes Passwort ist – stark heißt, widerstandsfähig gegen reale Angriffe.“

Workflow Password-Change Windows Active Directory

Technisch gesehen besteht für in diese Domain eingebundene Rechner und Systeme kein Unterschied zu einer Standard Windows A/D Installation. Der EPAS Enforcer integriert sich nahtlos in das System. Ein User verwendet den bekannten Standard-Windows Mechanismus, um das Passwort zu ändern.



EPAS

EPAS ist eine „On-Premises“ Lösung ohne externen Zugriff, die das Problem von schwachen und vorhersehbaren Passwörtern unternehmensweit angeht.
EPAS führt automatische und regelmäßige Prüfungen der unternehmensweiten Passwort-Qualität durch und hilft dabei, sichere Passwörter in großen und heterogenen Umgebungen durchzusetzen. EPAS ist skalierbar und auditiert regelmäßig Millionen von User Accounts sowie technische Accounts. Objektive Passwortstärke, Länge, Zusammensetzung der Zeichen sowie Policy Compliance sind einige der Bewertungskriterien von EPAS.
Die Lösung kommt bereits in über 30 Ländern zum Einsatz.

1. User sendet Anfrage zur Passwortänderung an den Domain Controller.
2. Der Domain Controller aktiviert den EPAS Filter, welcher zusätzliche User Informationen abruft, wie zum Beispiel Gruppenzugehörigkeit, Standort und andere relevante Eigenschaften.
3. Der EPAS Filter fasst alle abgerufenen Informationen zusammen und sendet sie über eine verschlüsselte, authentifizierte Verbindung zur nahegelegensten EPAS Appliance. Die EPAS Appliance überprüft Username, Gruppeninformationen und Passwort auf Policy Compliance, berechnet die Passwortstärke und führt alle anderen konfigurierten Prüfungen, die für diese spezielle Account-Kategorie definiert sind, aus. Das Ergebnis wird an den Domain Controller zurück geschickt.
4. Das Ergebnis des Passwort-Genehmigungs-Prozesses wird als true / false Statement zum Arbeitsplatzrechner gesendet.
5. Falls aktiviert zeigt ein auf dem Arbeitsplatzrechner installierter EPAS Credential Provider den Grund für einen gescheiterten Passwortänderungs-Versuch im Detail auf, ohne dabei eine Verbindung mit der EPAS Appliance zu benötigen. Die Benachrichtigung ist an die entsprechende Sprache und Region des Users angepasst.

Beispiel einer Policy:

1. Zeichenwiederholung: Das Passwort darf keine Zeichenfolgen aus 3 oder mehr aufeinanderfolgenden, gleichen Zeichen enthalten.
2. Länge: Das Passwort muss zwischen 10 und 15 Zeichen lang sein.
3. Aufeinanderfolgende Zeichen: Das Passwort darf keine Zeichenfolgen aus 3 oder mehr aufeinanderfolgende Zeichenfolgen, wie Tastatur-Reihenfolgen (z.B. „asdf“), enthalten.
4. Stärke: Die Passwortstärke muss > 70 sein.
5. Passwort Verlauf: Das Passwort muss sich von den letzten 10 verwendeten Passwörtern unterscheiden.
6. Wörterbuch: Das Passwort darf nicht in einem unternehmensspezifischen Wörterbuch gefunden werden.

„EPAS: Eine praxisgerechte, kostengünstige, international bewährte Lösung, die Spitzentechnologie einsetzt, um die Sicherheit von Benutzerkonten systemisch zu erhöhen – Stand der Technik.“

DETACK GmbH
Königsallee 43
71638 Ludwigsburg
Phone: +49 7141 125-150
Fax: +49 7141 125-155
info@detack.de
www.epas.de

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig