epas

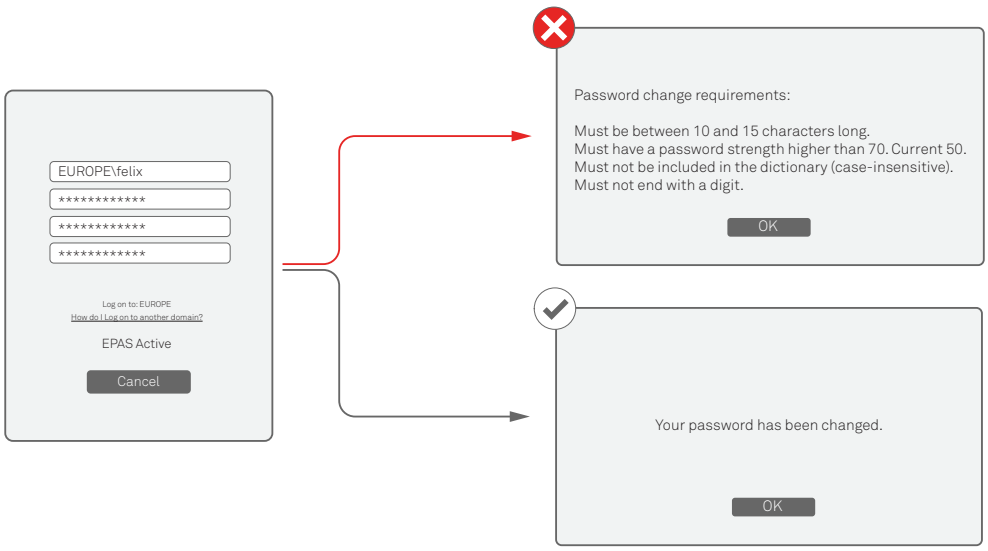
EPAS Enforcer

EPAS Enforcer is a password quality enforcement component, provided as a licensed feature of EPAS.
A single, high availability EPAS instance centrally manages password changes on all supported systems.
The initial release supports Microsoft products; support for additional platforms is currently in development.
EPAS Enforcer for A/D integrates as an LSA filter on the Windows Active Directory domain controllers and ensures that passwords meet defined security requirements when set or changed, in line with a centralized policy mandated by the risk category of the information they protect.
The new password is tested against the EPAS evaluation criteria and is accepted or rejected, depending on the defined security requirements. This means that formerly permitted passwords like “Password123” or “Secret!” are not accepted any longer by the computer.
If the password change attempt is unsuccessful, an optional feature of the EPAS Enforcer displays the failure reasons (e.g. “Password must not be included in a dictionary.”) to the end user.
The security requirements for a password result from the security classification of the data to be protected, based on customer specific measurements.

„With the EPAS Enforcer implemented, we are now able to control that, at the time of password change, a strong password is chosen – strong meaning resilient against real attacks.“

Workflow Password-Change Windows Active Directory

From a technical point of view, there is no difference to a standard Windows A/D installation for domain integrated computers. The EPAS Enforcer integrates seamlessly into the existing environment. Users continue to use the default, built-in Windows password change mechanisms to change passwords.



EPAS

EPAS is a service delivered via on-premises platforms, with no external access, which addresses the topic of weak or predictable passwords on an enterprise scale. EPAS conducts automatic, regular password assessments, helping to maintain secure passwords in large, heterogeneous environments.

A scalable solution, EPAS regularly audits millions of user accounts as well as service and technical accounts in over 30 countries. Objective password strength, length, character composition, and policy compliance, are some of the EPAS measurements.

1. User sends a password change request to the domain controller.
2. The domain controller invokes the EPAS filter, which retrieves additional user information, such as group membership, location and other relevant attributes.
3. The EPAS filter packs the information received and sends it over an encrypted, authenticated channel to the closest EPAS appliance. The EPAS appliance processes the username, group information, and any other known data and checks the password for policy compliance, calculates password strength and performs all other available policy checks defined for that particular account category. The result is returned to the domain controller.
4. The result of the password approval process is sent as a true / false statement to the user workstation.
5. If enabled, an EPAS credential provider installed on the local workstation displays the detailed reasons for a failed password change attempt, without requiring any connections to the EPAS appliance. The message is localized for the specific user language and region.

Sample Policy:

1. Repeatable Characters: Password must not contain a sequence of 3 or more consecutive repeated characters.
2. Length: Password must be between 10 and 15 characters.
3. Sequenced Characters: Password must not contain a sequence of 3 or more sequenced characters, such as usual keyboard sequences (e.g. “asdf”).
4. Strength: Password strength score must be above 70 (structural entropy).
5. Password history: Password must be different from the last 10 used passwords.
6. Dictionary: Password must not be found in a custom dictionary.

„EPAS: A practical, cost efficient, internationally proven solution which employs bleeding edge technology to enable the systematical increase of user account security – state of the art.“

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