SPECOPS PASSWORD POLICY
Datenblatt

Die Specops Password Policy unterstützt Sie bei der Erhöhung der Passwortsicherheit in Ihrer Microsoft Active Directory. Die Lösung erweitert in einer Active Directory-Umgebung die Fähigkeit eines Domänen Controllers, Anforderungen an Passwortsicherheit nach dem aktuellen Stand der Technik durchzusetzen. Durch Nutzung von Gruppenrichtlinien zur Konfiguration, wird die einfache Verwaltung von individuellen Passwortrichtlinien innerhalb einer Domäne ermöglicht. Die Specops Password Policy ermöglicht unter anderem das Blockieren von kompromittierten Passwörtern, das Anlegen von individuellen Wörterbüchern und die Verwendung von Passphrasen, mit deren Hilfe Sie starke Kennwörter unter Wegfall der Komplexität erzeugen können. Zusätzlich können Sie mit dem längenbasierten Kennwort-Ablaufdatum einen Prozess einführen, der Ihre Anwender für die Auswahl längerer Kennwörter mit einem späteren Ablaufdatum belohnt.

Mit einem segmentierten Ansatz können Sie die Anforderungen an Passwort-Sicherheit verschiedener Benutzergruppen basierend auf den jeweiligen Schutzklassen der Daten konfigurieren. Setzen Sie für Benutzer, die Zugang zu streng vertraulichen Informationen haben, sehr starke Kennwörter durch, ohne dabei die Benutzerfreundlichkeit für Anwender mit weniger Berechtigungen zu beeinträchtigen.

Erfüllen Sie regulatorische Anforderungen (z.B. BSI Grundschutz ORP.4.A23) durch das Blockieren von mehr als 2,4 Milliarden kompromittierter Kennwörter sowie von Passwörtern, die bei aktuellen Password Spraying-Angriffen verwendet werden. Erhöhen Sie die Sicherheit, indem Sie die Erstellung von leicht erratbaren Passwörtern basierend auf Begriffen im Umfeld Ihrer Organisation über eigene Wörterbücher blockieren.

FEATURES IM VERGLEICH	SPECOPS PASSWORD POLICY	ACTIVE DIRECTORY PASSWORD POLICY	AZURE AD PASSWORD PROTECTION
Wörterbuchangriffe & Passwort-Leaks Sie können ein Passwort-Wörterbuch (eine Datei mit häufig verwendeten bzw. kompromittierten Passwörtern) verwenden, um zu verhindern, dass Benutzer Passwörter erstellen, die leicht erratbar oder bereits kompromittiert sind.			
Unterstützt Erstellung von eigenen Wörterbuchlisten	Ja	Nein	Ja [1]
Verhindert Verwendung von kompromittierten Kennwörtern (laut Empfehlung von Organisationen wie BSI, NIST oder NCSC)	Ja	Nein	Teilweise[2]
Identifiziert bereits verwendete, kompromittierte Passwörter[3]	Ja	Nein	Nein
Verhindert auch die teilweise Verwendung von Wörtern aus der Wörterbuchliste	Ja	Nein	Nein
Erkennt und blockiert Varianten[4] der Wörter aus den Wörterbuchlisten	Ja	Nein	Nein

[1] Limitiert auf bis zu 1000 Begriffen, mindestens 4 Zeichen pro Eintrag
[2] Es werden nur Basisbegriffe aus der globalen Liste, bzw. Begriffe aus der eigenen Wortliste verwendet, 3rd Party Breach PW Listen können nicht eingebunden werden
[3] Die Erkennung basiert auf den gespeicherten Hashwerten der Kennwörter in Active Directory – die Kennwörter selbst werden hierfür nicht entschlüsselt
[4] Der Versuch, Buchstaben durch ähnlich aussehende Zeichen zu ersetzen (Leetspeak) wird erkannt, z.B. würde „B3rlin“ blockiert werden, selbst wenn lediglich „Berlin“ im Wörterbuch aufgeführt ist

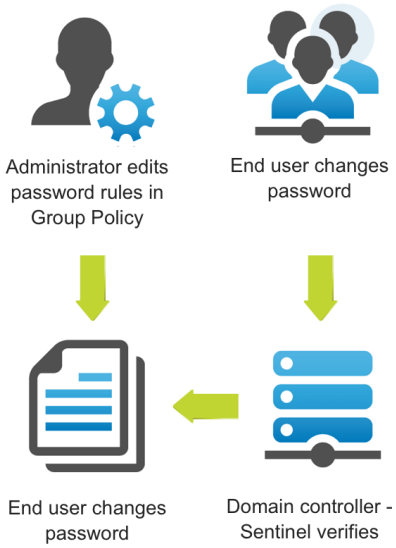
FEATURES IM VERGLEICH	SPECOPS PASSWORD POLICY	ACTIVE DIRECTORY PASSWORD POLICY	AZURE AD PASSWORD PROTECTION
Passwort Komplexität & Schutz vor Verwendung vorhersehbarer Muster Komplexität definiert die Anforderungen an den Zeichenraum, der in einem Kennwort zu verwenden ist, d.h. Klein- und Großbuchstaben, Ziffern und Sonderzeichen. Komplexität hat jedoch einen geringeren Einfluss auf die Stärke eines Passworts als dessen Länge. Anwender verwenden oftmals bekannte Muster bei der zeitgesteuerten Kennwortänderung, die zu vorhersehbaren Kennwörtern führen.			
Blockiert die Verwendung von Teilen des Vor- oder Nachnamens eines Benutzers	Ja	Nein	Nein
Blockiert Ziffern am Ende oder Anfang eines Passworts	Ja	Nein	Nein
Blockiert aufeinanderfolgende identische Zeichen	Ja	Nein	Nein
Erlaubt die granulare Definition der zu verwendenden Zeichenklassen und die minimale Anzahl der Zeichen pro Klasse	Ja	Nein	Nein
Unterstützung von Passphrasen	Ja	Nein	Nein
Erlaubt Definition einer Mindestanzahl von Zeichen, um die sich das neue vom alten Kennwort unterscheiden muss	Ja	Nein	Nein
Blockiert die Wiederverwendung von Teilen des alten Kennworts	Ja	Nein	Nein

WICHTIGE FUNKTIONEN IM VERGLEICH	SPECOPS PASSWORD POLICY	ACTIVE DIRECTORY PASSWORD POLICY	AZURE AD PASSWORD PROTECTION
Ablauf von Passwörtern			
E-Mail-Benachrichtigung über den bevorstehenden Ablauf von Passwörtern	Ja	Nein	Nein
Unterstützung von Längenbasiertem Kennwortablaufdatum[5]	Ja	Nein	Nein
Zusätzliche Features			
Spezielles Reporting Tool[6] zu verwendeten Passwortrichtlinien	Ja	Nein	Nein
Dynamisches Benutzer-Feedback bei der Passwortänderung auf dem Client Computer	Ja	Nein	Nein
Benutzerdefinierte Meldung bei Passwortänderungen für Endnutzer	Ja	Nein	Nein
Integration in das Kontext-Menü von Active Directory User and Computers[7]	Ja	Nein	Nein

[5] Das Längenbasierte Kennwortablaufdatum ist ein „Belohnungssystem“, das das Kennwort umso später ablaufen lässt, je länger es gewählt wird.
[6] Specops Password Auditor
[7] Microsoft Management Console (MMC) Snap-In

Wie ist die Funktionsweise?

Die Specops Password Policy ist ein Passwort Filter[8], der auf jedem Domänen Controller einer Active Directory Domäne zusätzlich installiert wird und mit bereits bestehenden Passwortrichtlinien nahtlos zusammenarbeitet. Specops Password Policy wird mit Hilfe von Gruppenrichtlinien konfiguriert und umfasst die folgenden Komponenten:.



Administrator-Tool: Konfiguriert die Specops Password Policy in der Domäne und ermöglicht die Erstellung und Konfiguration von Passwortanforderungen in Gruppenrichtlinien (GPOs).

Sentinel: Setzt die Anforderungen an ein neues Passwort für ein bestimmtes Benutzerkonto bei Änderung oder Zurücksetzen durch. Bei dem Specops Password Policy Sentinel handelt es sich um den eigentlichen Passwortfilter auf jedem Domänen Controller.

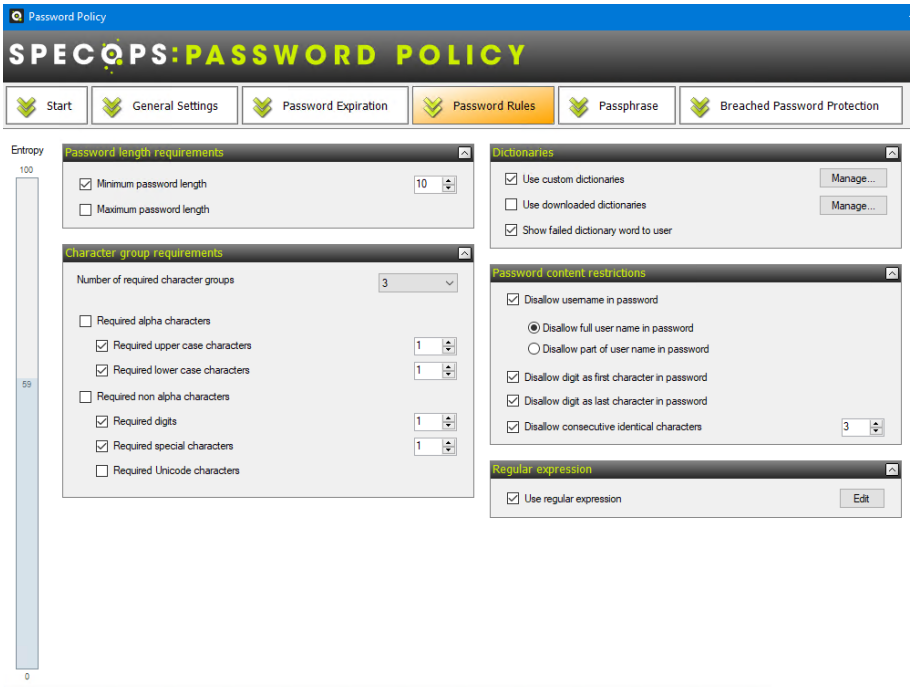
Arbiter: Der Specops Password Policy Arbiter wird auf einem dedizierten Server[9] installiert und stellt sicher, dass das soeben gewählte Kennwort nicht bereits kompromittiert ist. Hierzu wird gegen eine Daten-Basis von mehr als 2,4 Milliarden kompromittierten Kennwörtern, bzw. deren Hashes geprüft.[10]

Client (optional): Der Specops Authentication Client zeigt die einzelnen Kriterien der für einen Benutzer geltenden Passwortrichtlinie beim Ändern des Kennworts[11] an. Darüber hinaus benachrichtigt der Client den Anwender, wenn das Passwort in Kürze abläuft.

[8] https://docs.microsoft.com/en-us/windows/win32/secmgmt/password-filters
[9] Dieser Server muss Mitglied der Domäne sein, in der sich die Benutzerkonten befinden.
[10] Bei dieser Prüfung wird weder das Kennwort noch dessen Hash über das Internet übertragen. Es ist einem Dritten bei dieser Prüfung unmöglich, Kenntnis über das zu prüfende Passwort zu erlangen.
[11] Erfordert Windows 10, bzw. Windows Server 2016 oder höher. Bei älteren Windows Versionen werden nicht befolgte Kriterien erst mit der Meldung über einen erfolglosen Versuch, das Kennworts zu ändern, angezeigt

Wie sieht Specops Password Policy aus?

Administrator Client: Konfiguration der Richtlinie

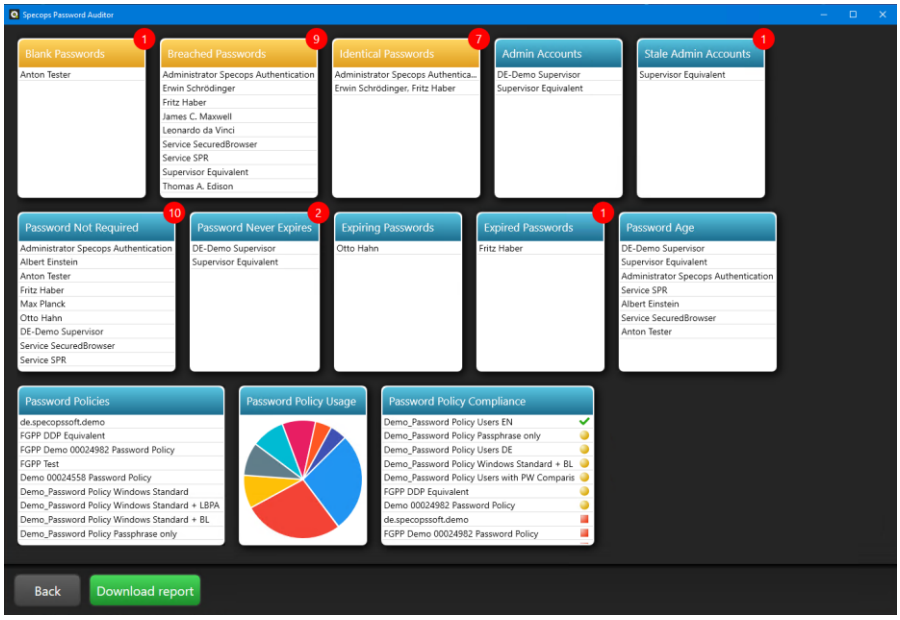


Die Anforderungen an Passwörter werden als Gruppenrichtlinie konfiguriert.

Typischerweise wird eine Organisation drei Basisrichtlinien erstellen:

1. Benutzer
2. Administratoren
3. Service-Konten

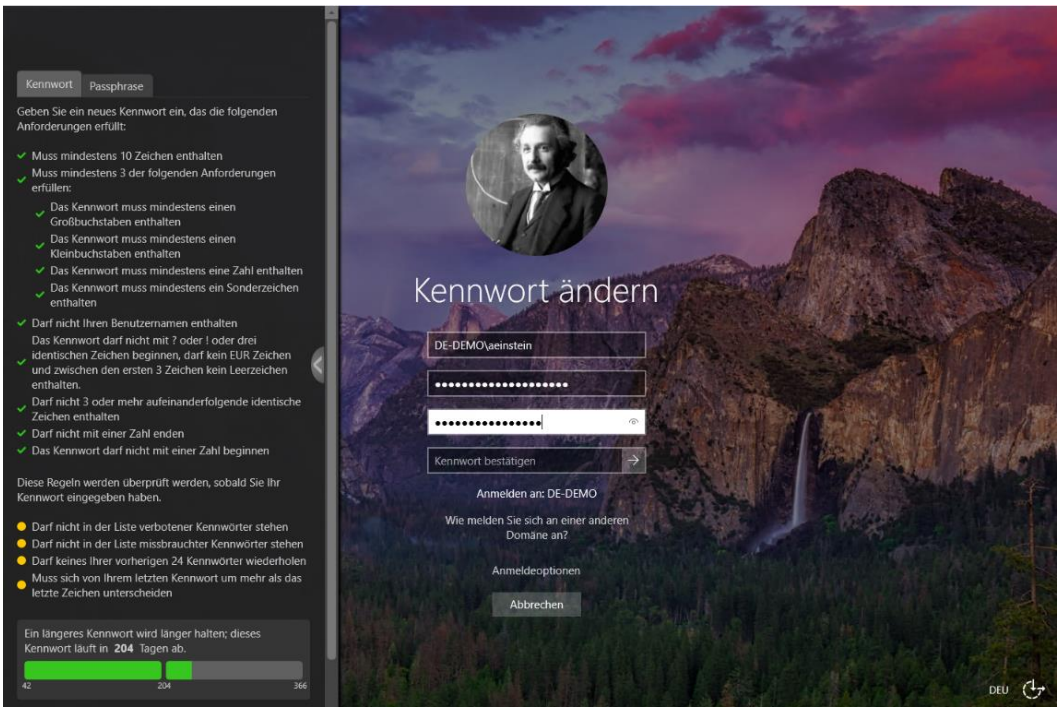
Specops Password Auditor: Bewertung des IST-Standes



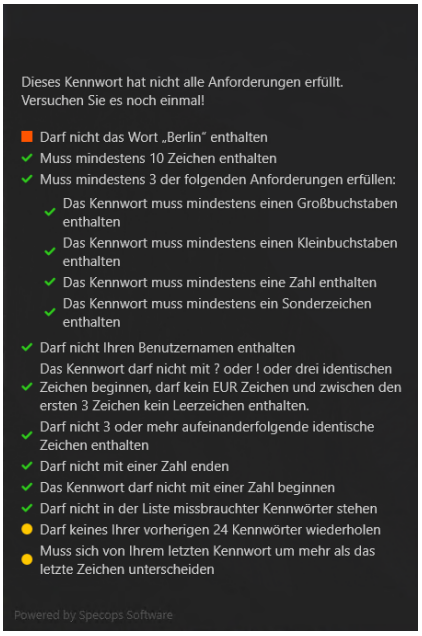
Der Specops Password Auditor scannt und identifiziert passwortrelevante Schwachstellen.

Die Scanergebnisse umfassen mehrere interaktive Berichte mit Benutzer- und Richtlinieninformationen sowie einen PDF-Export zur gemeinsamen Nutzung.

Anwender: Transparenz bei der Kennwortänderung



Durch das Dynamisches Feedback bei der Passwortänderung sieht der Anwender noch während der Eingabe des neuen Kennworts, ob dieses den festgelegten Anforderungen entspricht.



Sollte das Kennwort aufgrund der Verwendung von unerwünschten Begriffen oder im Fall einer erkannten Kompromittierung zurückgewiesen werden, wird dies ebenfalls im Feedback mitgeteilt.

Warum entscheiden sich Kunden für Specops?

„Wenn Sie Ihre Passwörter im Active Directory verstärken möchten, sollten Sie unbedingt die Specops Password Policy in Betracht ziehen. Sie ist einfach und intuitiv zu bedienen und funktioniert wie versprochen.“ *Vlatko Kosturjak, Sicherheitsberater* https://www.helpnetsecurity.com/2018/11/19/review-specops-password-policy/

„Durch die Erstellung einer Wörterbuchliste mit gängigen Wörtern können wir verhindern, dass leicht vorhersehbare Wörter wie „Tombola“ oder „Bingo“ verwendet werden. Wir können Benutzer daran hindern, einen Teil ihres Namens zu verwenden oder das letzte Passwort einfach zu wiederholen – z. B. password1 zu password2.“ *Tom Blackburn, Jr. Operational Support Engineer bei Tombola* https://specopssoft.com/blog/tombolas-review-of-specops-password-policy-and-ureset/

„Die Specops Password Policy lässt sich auf beliebigen GPO-Ebenen, Computern, Benutzern oder Gruppen anwenden und bietet den zusätzlichen Vorteil erweiterter Optionen zu Passwortrichtlinien, einschließlich der Verwendung von Passphrasen.“ *Timothy Warner, Microsoft Cloud and Datacenter Management (MVP)* https://4sysops.com/archives/specops-password-policy-enterprise-password-security/

„Das Tool ist sehr benutzerfreundlich, lässt sich schnell installieren und nutzt bestehende Windows-Verwaltungsabläufe zur Umsetzung individueller Passwortrichtlinien. Systemadministratoren werden feststellen, dass die Integration der Specops Password Policy sehr wenig Zeit und Aufwand in Anspruch nimmt und die Lernkurve für die Nutzung des Produkts minimal ist.“ *Richard Hicks, Microsoft Cloud and Datacenter Management (MVP)* http://techgenix.com/product-review-specops-password-policy/

„Die neuen Wörterbuchfunktionen geben Administratoren noch mehr Kontrolle über die Passwörter der Benutzer und steigern zweifelsohne die Sicherheit dieser Passwörter.“ *Brien Posey, 15-facher Microsoft MVP* http://techgenix.com/review-of-specops-password-policy/

Demo von Specops Password Policy anfordern

Möchten Sie wissen, wie Specops Password Policy und Breached Password Protection in Ihrer Umgebung funktionieren? Klicken Sie hier, um noch heute eine Demo- oder Testversion zu erhalten.