



Anixis Password Policy Enforcer

Die aktuellen Anforderungen an ein starkes Passwort kann über die Default Domain Policy nicht mehr erreicht werden.

Aus diesem Grund benötigen wir für die Durchsetzung ein Drittanbieter Tool. In diesem Fall greife ich auf den Policy Enforcer zurück.

<https://anixis.com/default.htm>

Bevor wir den PPE einsetzen können, müssen wir ein paar Vorbereitungen treffen.

Die aktuelle Kennwortrichtlinie die über die DDP geforced wird sollte deaktiviert werden. Folgende Einstellungen können genutzt werden:

Richtlinie	Einstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingt gespeicherte Kennwörter	24 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	42 Tage
Minimale Kennwortlänge	8 Zeichen
Minimales Kennwortalter	1 Tage

Der Grund liegt in der Erfüllung der Richtlinien. Wenn 2 Richtlinien aktiv sind, so muss das eingerichtete/geänderte Passwort einmal der Richtlinie der DDP entsprechen so wie der des Password Policy Enforcers. Wenn jedoch die Einstellungen der DDP in das PPE Regelwerk übernommen werden und diese sich decken, ist alles in Ordnung.

Ein Hinweis am Rande:

Der Password Policy Enforcer erweitert nicht, wie viele glauben, das Active Directory Schema!



Anixis Password Policy Enforcer

Dann richte ich zum Test noch 2 neue Domänen-Benutzer ein. Der 2. Benutzer ist nur demonstrativ und soll zeigen, dass mehrere voneinander getrennte Richtlinien erstellt und zugewiesen werden können.

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. On the left, the navigation pane lists various Active Directory containers and objects. In the center, a table displays two user accounts:

Name	Typ	Beschreibung
PW Test	Benutzer	Policy Enforcer Test User
PW Admin	Benutzer	Policy Enforcer Admin

A red arrow points to the 'User Accounts' node in the navigation pane, and a red circle with the number '1' is placed over the 'PW Test' row in the table. Another red arrow points to the 'PW Admin' account in the table, and a red circle with the number '2' is placed over it.

Kommen wir nun zur Softwareinstallation.

Das Produkt besteht aus 2 Softwaremodulen. Der eine Teil wird auf den Servern (Domain Controllern) installiert und der andere Teil optional auf alle Client Systeme im Netzwerk egal ob Member Server oder Workstation. Das Servermodul sorgt für die Durchsetzung der noch zu erstellenden Richtlinien, wobei das Clientmodul den User bei der Änderung des Passworts nur unterstützt, in dem die Komplexität des Passworts angezeigt wird.

Sollte dieses Modul zum Einsatz kommen, muss auf den Domain Controllern/Netzwerk der **UDP Port 1333** freigeschaltet werden! Hinweis: Der Port ist änderbar.

The Password Policy Client initiates a request by sending a datagram with the following attributes to the Password Policy Server:

Protocol	UDP
Source address	Client computer IP address
Source port	Any
Destination address	Domain controller IP address
Destination port	1333

The Password Policy Server responds by sending a datagram with the following attributes back to the Password Policy Client:

Protocol	UDP
Source address	Domain controller IP address
Source port	1333
Destination address	Client computer IP address
Destination port	Any

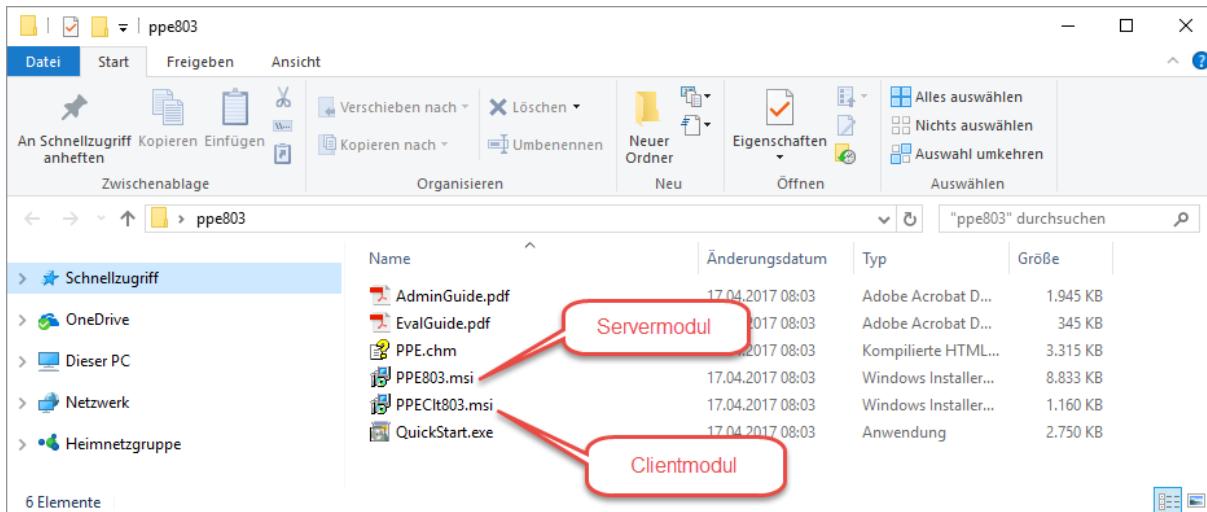


If your firewall performs Stateful Packet Inspection, then only create a rule for the request datagram as the firewall will automatically recognize and allow the response datagram.



Anixis Password Policy Enforcer

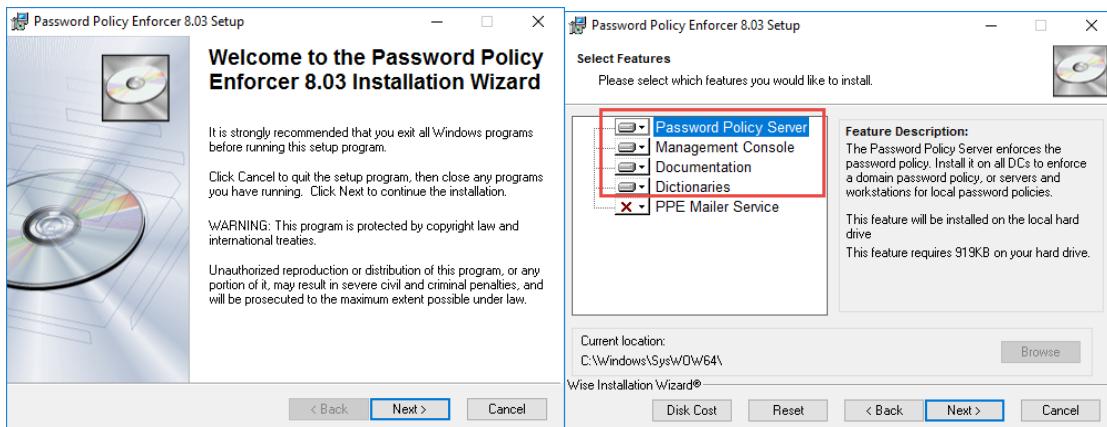
Ich habe das Installation Paket mal zur Veranschaulichung extrahiert um zu zeigen was alles enthalten ist.



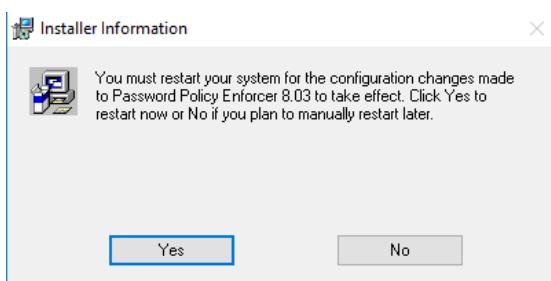
Systemanforderungen:

- Windows Server 2003 > Windows Server 2016
- Windows XP > Windows 10
- 15 MB Festplattenplatz
- 4 MB RAM

Als erstes installieren wir das Servermodul auf den Domain Controllern.



Der PPE Mailer ist ein Service um die User an die bevorstehende Passwortänderung zu informieren.

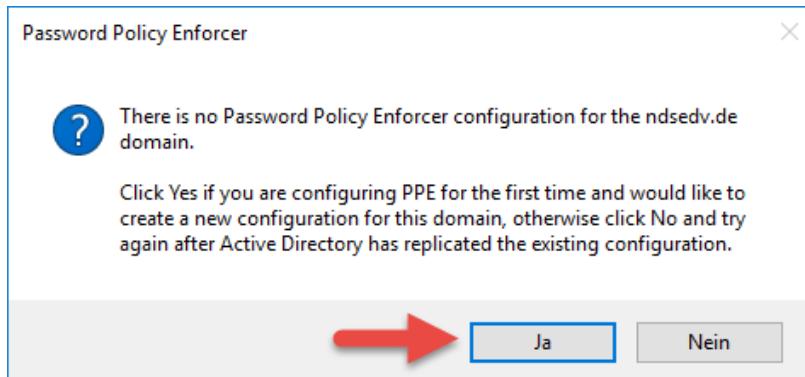


Der Neustart ist zwingend notwendig!

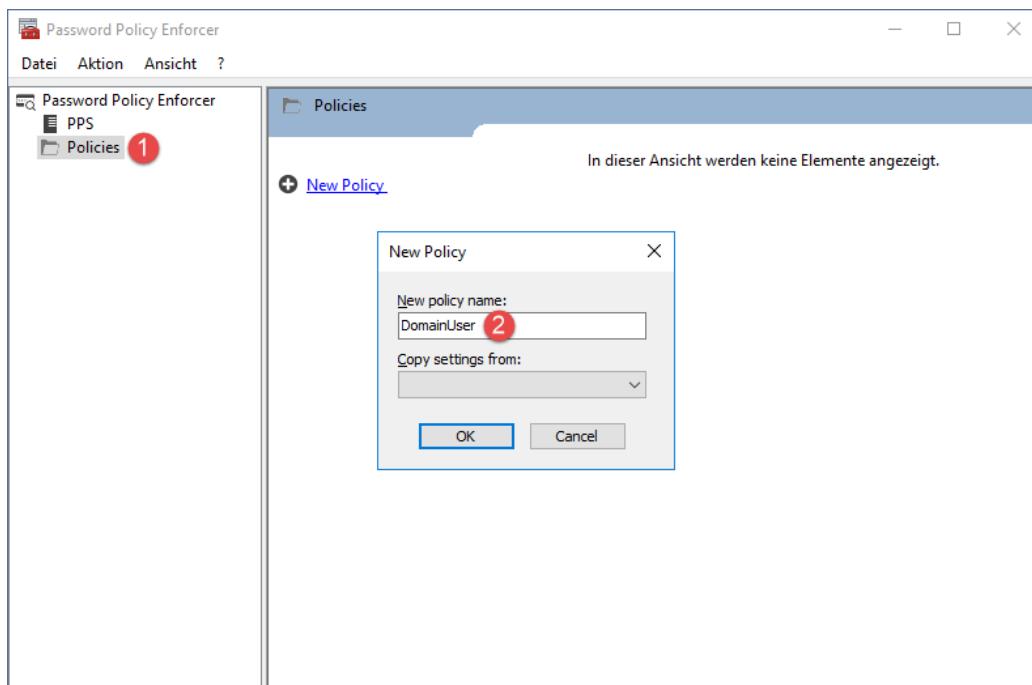


Anixis Password Policy Enforcer

Nach dem Neustart starten wir den Password Policy Enforcer und erstellen als erstes eine neue Regel (Set).



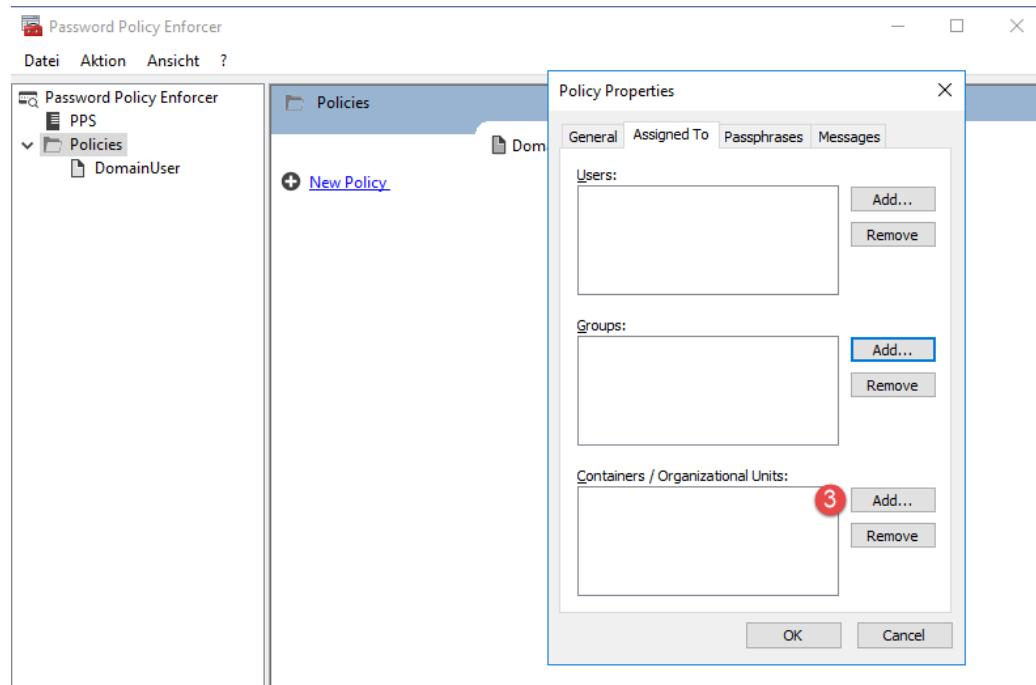
Eine erstellte Regel kann entweder auf einen User, einer Gruppe oder auf eine OU angewendet werden. Es können maximal 256 Regeln erstellt werden.



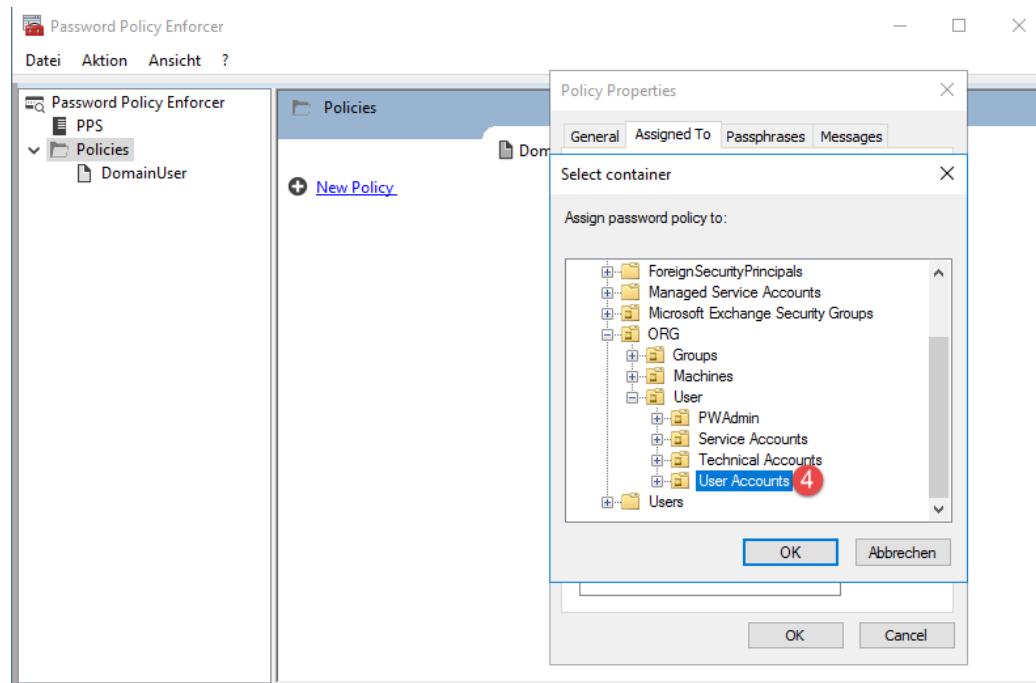


Anixis Password Policy Enforcer

In diesem Fall werde ich die erste Richtlinie auf die **OU = User Accounts** anwenden, in der mein Test User (PW Test) enthalten ist.



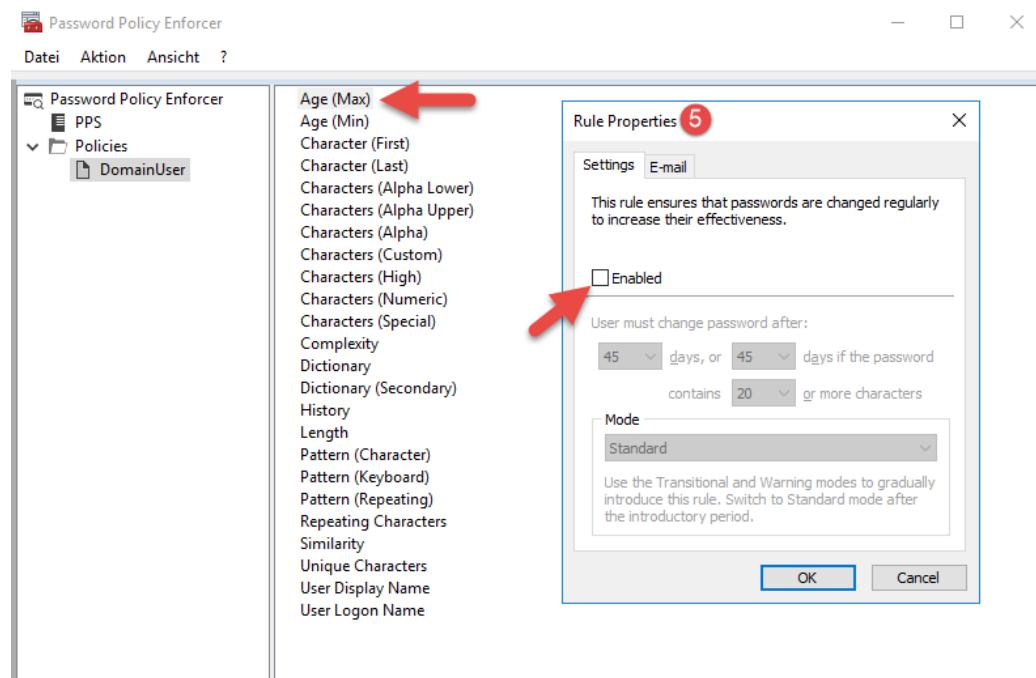
ADD > OU auswählen > OK



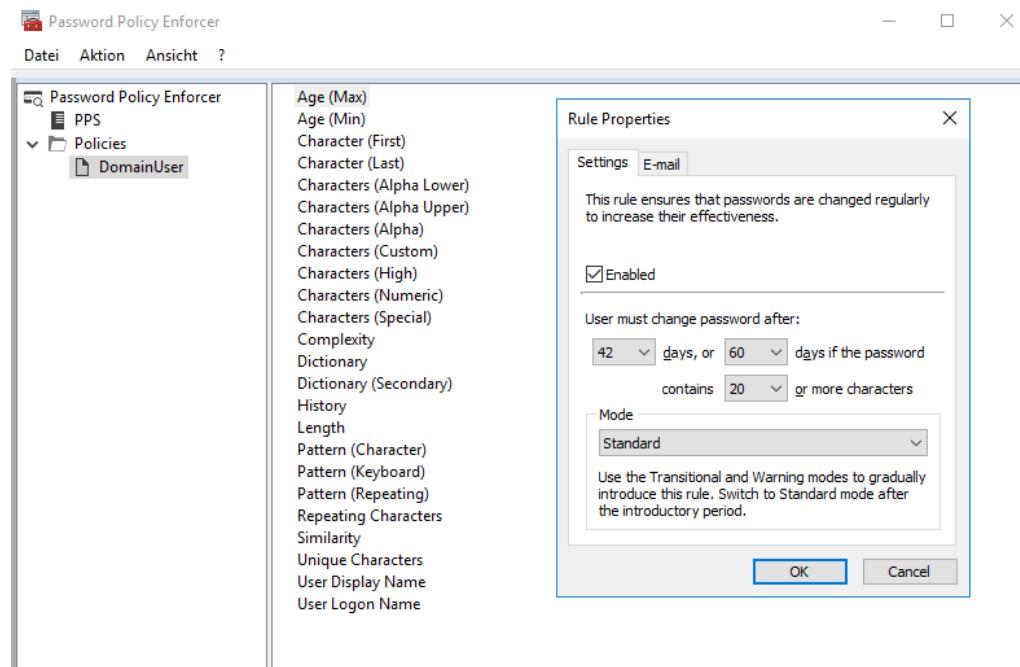


Anixis Password Policy Enforcer

Kommen wir nun zum wichtigsten Teil der Konfiguration, der Richtlinienoptionen. Über einen Doppelklick auf die einzelnen Optionen können individuelle Einstellungen vorgenommen werden.



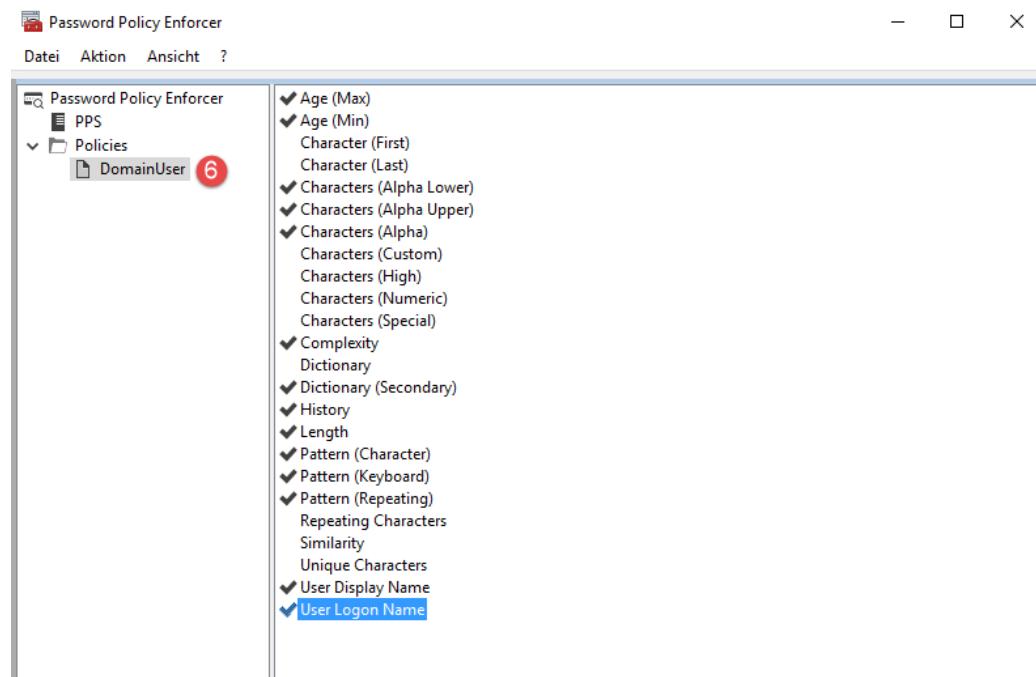
Es ist ganz klar zu erkennen, dass wir mit diesem Produkt wesentlich mehr Möglichkeiten haben als uns die Default Domain Policy anbietet.



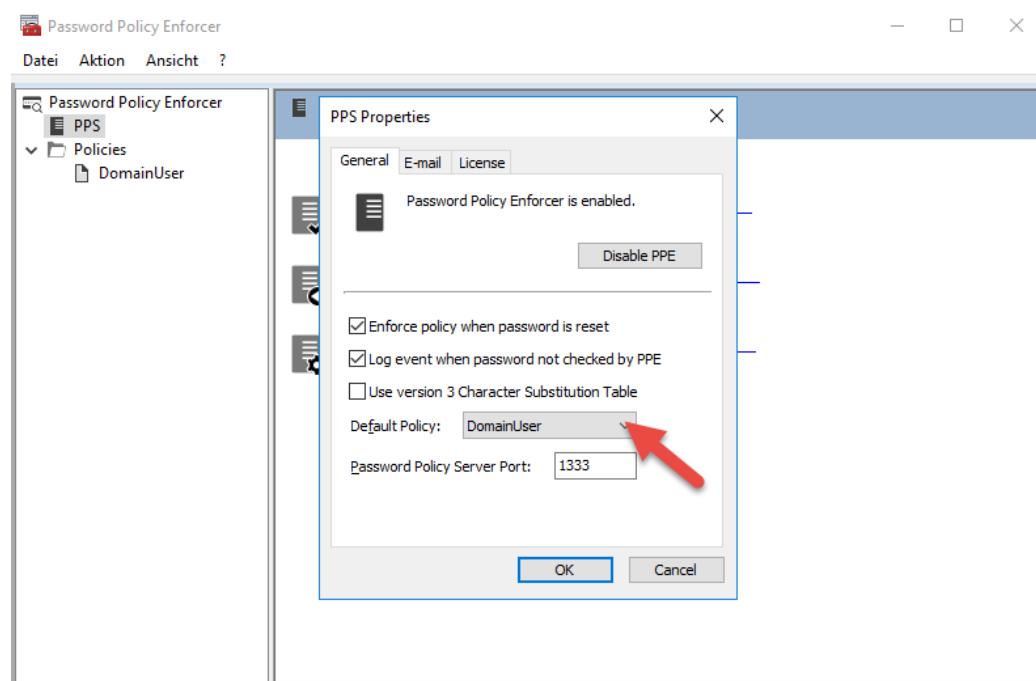


Anixis Password Policy Enforcer

Ich habe bewusst die Numeric Option weggelassen, später mehr dazu.



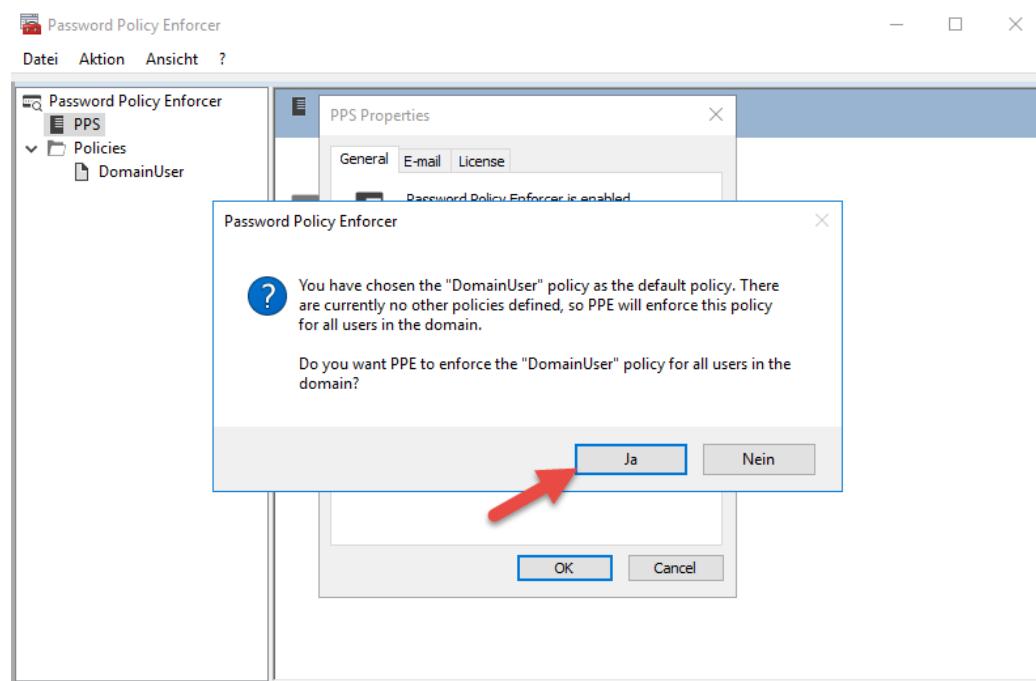
Wir könnten diese Richtlinie auch als Default Policy aktivieren und damit die alte Default Domain Policy ersetzen. Somit könnten z.B. auf Basis dieser Regel weitere folgen.



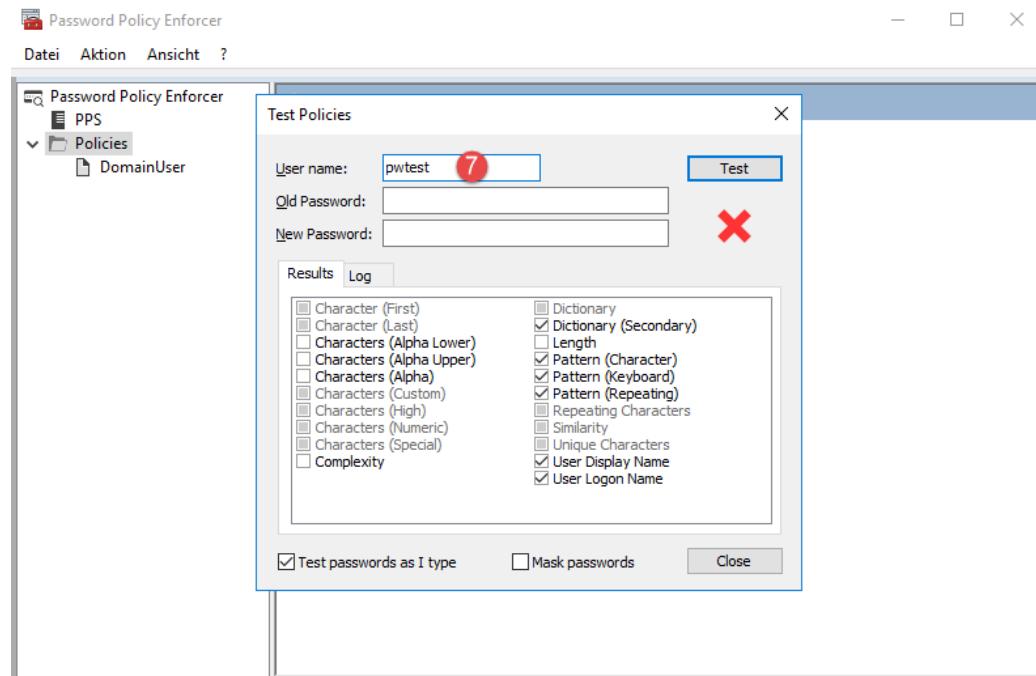


Anixis Password Policy Enforcer

Ein Konzept sollte vorher erarbeitet worden sein.



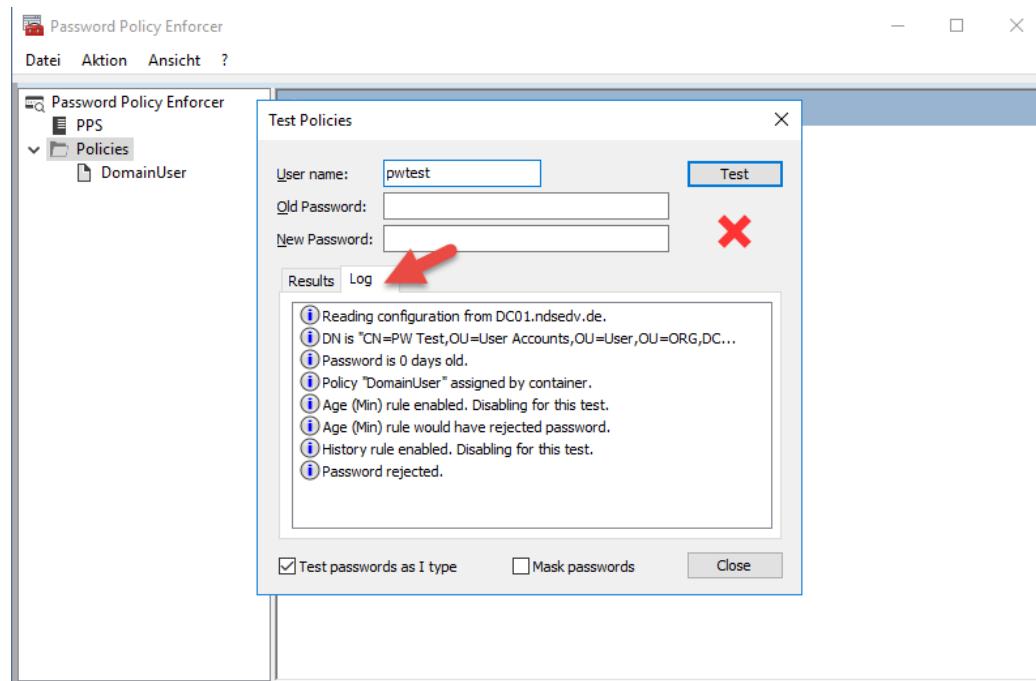
Die neue Richtlinie lässt sich nun auch live testen.





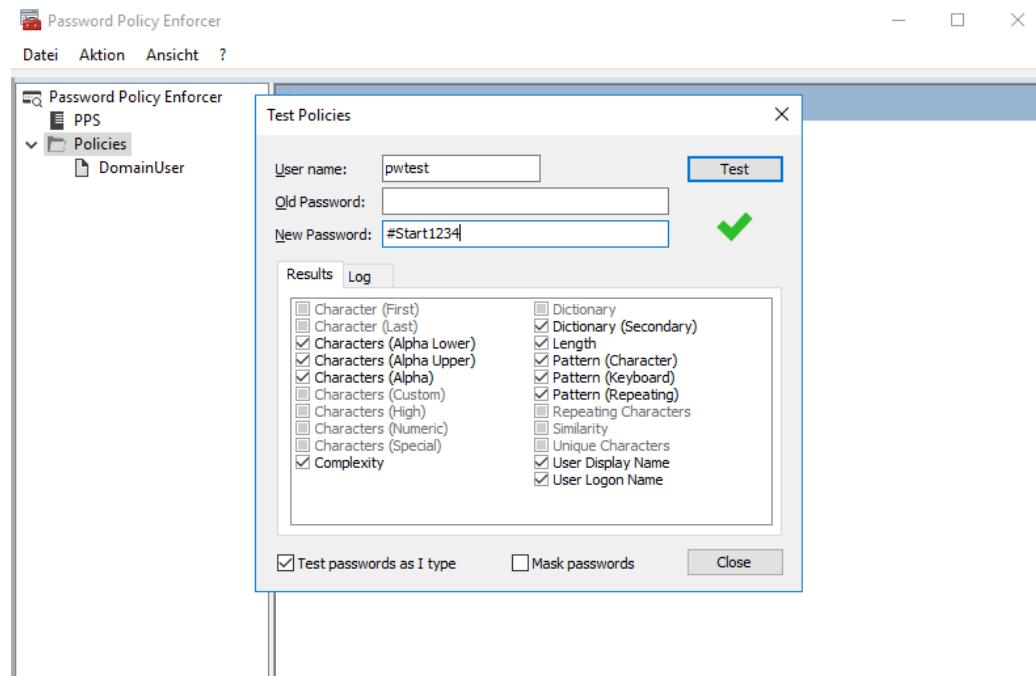
Anixis Password Policy Enforcer

Über das **Log** sehen wir die Eigenschaften die auf den User wirken.



Starten wir einen Test. Das Passwort #Start1234 entspricht nun unserem Regelwerk. Es enthält das was wir konfiguriert und aktiviert haben.

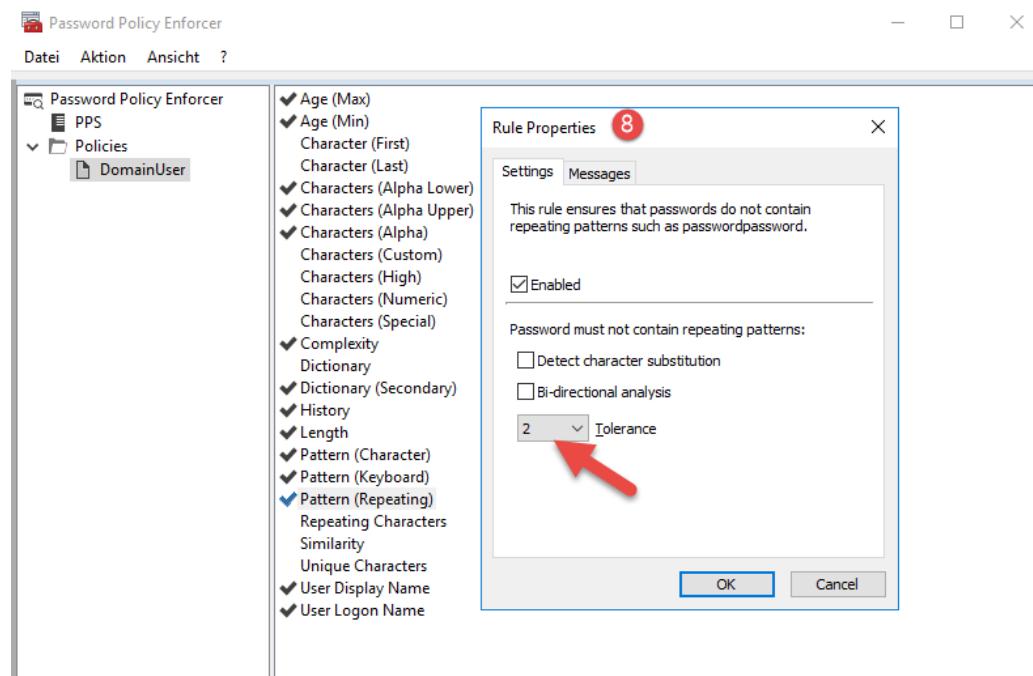
Warum dürfen 4 Zahlen hintereinander geschrieben werden, ups, das ist nicht sicher, das müssen wir dringend ändern!



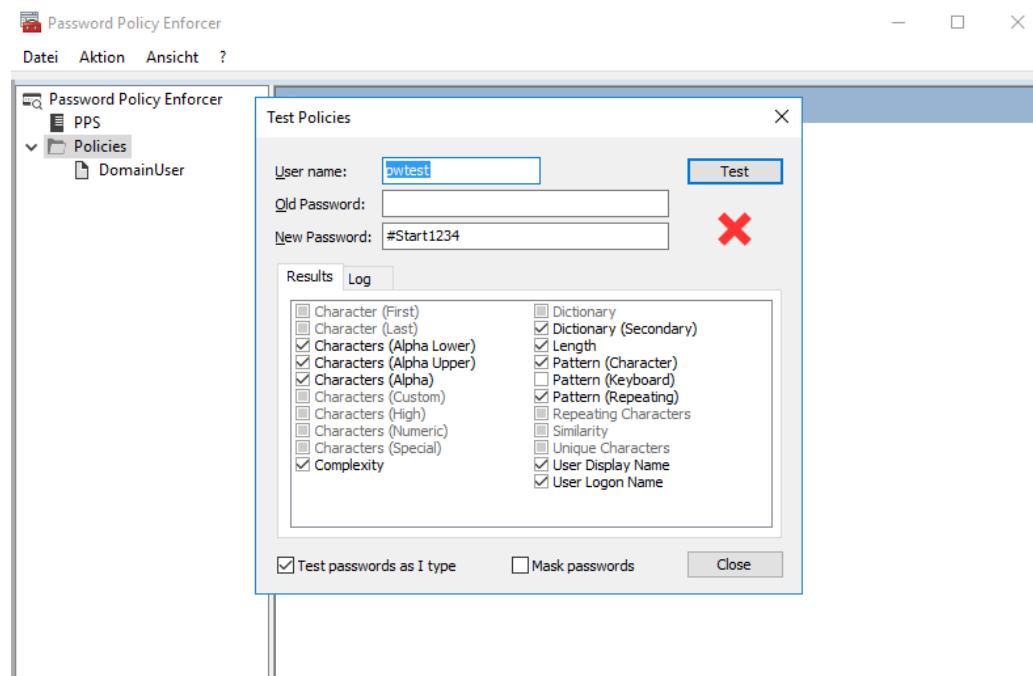


Anixis Password Policy Enforcer

Ich ändere dafür die Pattern Toleranz von 4 auf 2.



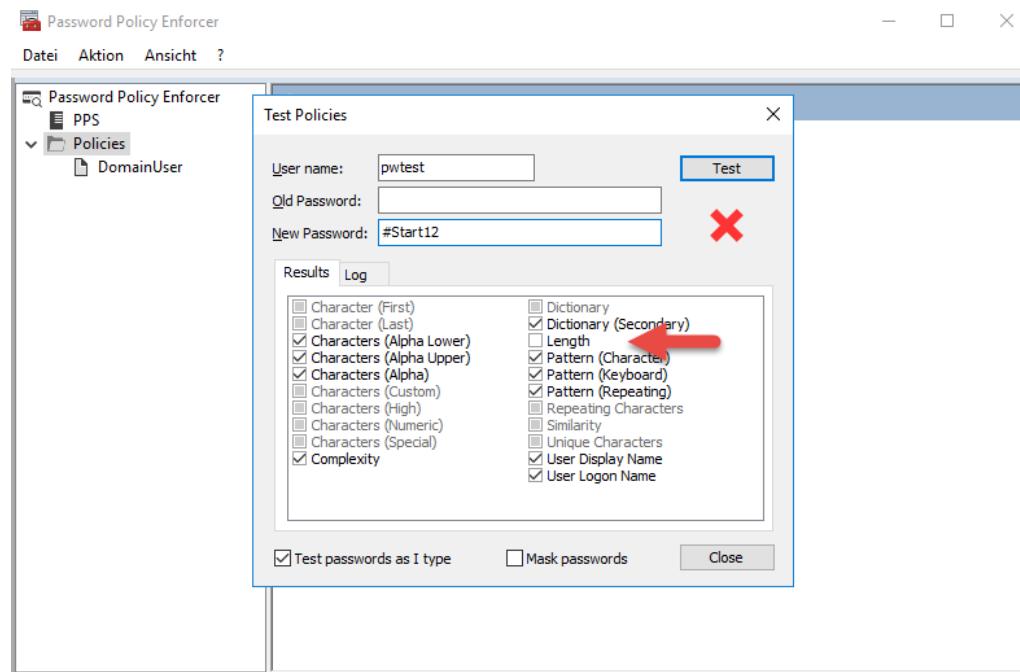
Das Passwort wird jetzt wegen der Toleranz nicht mehr akzeptiert, es sind zu viele Zahlen hintereinander, mehr als die Regel erlaubt.



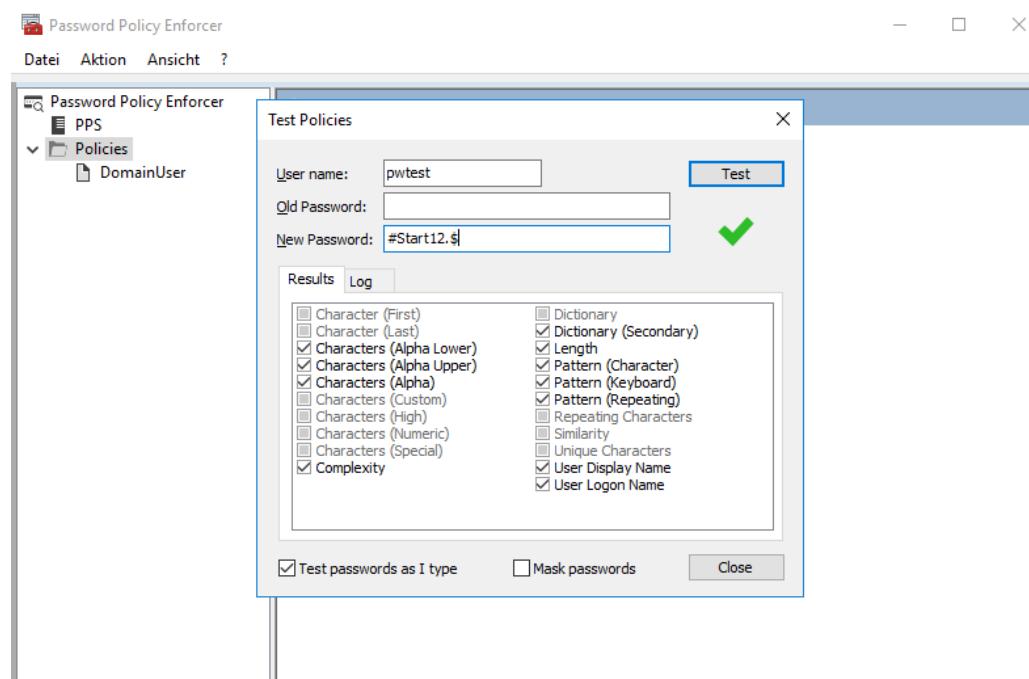


Anixis Password Policy Enforcer

Ziehen wir 2 Zahlen zurück ist das Passwort nun nicht mehr lang genug. Ok.



Wir fügen dem Passwort 2 weitere Sonderzeichen hinzu und es entspricht nun wieder dem Gesamtregelwerk.





Anixis Password Policy Enforcer

Oowieschön enthält keine Zahlen und bekommt einen grünen Haken?! Warum wird das Passwort eigentlich akzeptiert?

Gerade eben haben wir doch noch mit Zahlen gearbeitet, ja richtig, diese dienten aber nur als Füllzweck um die vorgegebene Passwortlänge zu erreichen.

The screenshot shows the 'Test Policies' dialog box. In the 'User name:' field, 'pwtest' is entered. In the 'Old Password:' field, the password 'Oowieschön' is entered. A green checkmark icon is displayed next to the 'New Password' field. Below the fields, there are two tabs: 'Results' (selected) and 'Log'. The 'Results' tab lists various complexity rules: Character (First), Character (Last), Characters (Alpha Lower), Characters (Alpha Upper), Characters (Alpha), Characters (Custom), Characters (High), Characters (Numeric), Characters (Special), Complexity, Dictionary, Dictionary (Secondary), Length, Pattern (Character), Pattern (Keyboard), Pattern (Repeating), Repeating Characters, Similarity, Unique Characters, User Display Name, and User Logon Name. Most of these rules have checkboxes checked. At the bottom of the dialog are two checkboxes: 'Test passwords as I type' (checked) and 'Mask passwords' (unchecked). There are also 'Close' and 'Test' buttons.

Es liegt nicht an der Complexity, die ist korrekt eingestellt. Do you remember?

The screenshot shows the 'Rule Properties' dialog box for the 'Complexity' rule. The 'Settings' tab is selected. The text area states: 'This rule ensures that passwords contain characters from various character sets. Use the character set rules for more granular control.' Below this, the 'Enabled' checkbox is checked. Under 'Password must contain characters from at least:' a dropdown menu shows '1' and 'of the character sets selected below'. A grid of checkboxes allows selecting character sets: Alpha, Special, Lower Alpha, High, Upper Alpha, Custom, and Numeric. The 'Upper Alpha' and 'Numeric' checkboxes are checked. At the bottom right are 'OK' and 'Cancel' buttons. On the left side of the main window, the tree view shows 'PPS', 'Policies', and 'DomainUser' under 'Policies'.

Ich hatte doch die Regel Numeric nicht aktiviert und somit werden auch keine Zahlen erwartet. ;-)



Anixis Password Policy Enforcer

Das holen wir jetzt nach.

The screenshot shows the 'Password Policy Enforcer' application window. On the left, there's a navigation pane with 'PPS' and 'Policies' expanded, showing 'DomainUser'. The main pane lists various policy rules with checkboxes. A red arrow points to the 'Characters (Numeric)' rule, which is highlighted with a blue selection bar at the bottom of the list.

- ✓ Age (Max)
- ✓ Age (Min)
- ✓ Character (First)
- ✓ Character (Last)
- ✓ Characters (Alpha Lower)
- ✓ Characters (Alpha Upper)
- ✓ Characters (Alpha)
- ✓ Characters (Custom)
- ✓ Characters (High)
- Characters (Numeric)** (highlighted)
- ✓ Characters (Special)
- ✓ Complexity
- ✓ Dictionary
- ✓ Dictionary (Secondary)
- ✓ History
- ✓ Length
- ✓ Pattern (Character)
- ✓ Pattern (Keyboard)
- ✓ Pattern (Repeating)
- Repeating Characters
- Similarity
- Unique Characters
- ✓ User Display Name
- ✓ User Logon Name

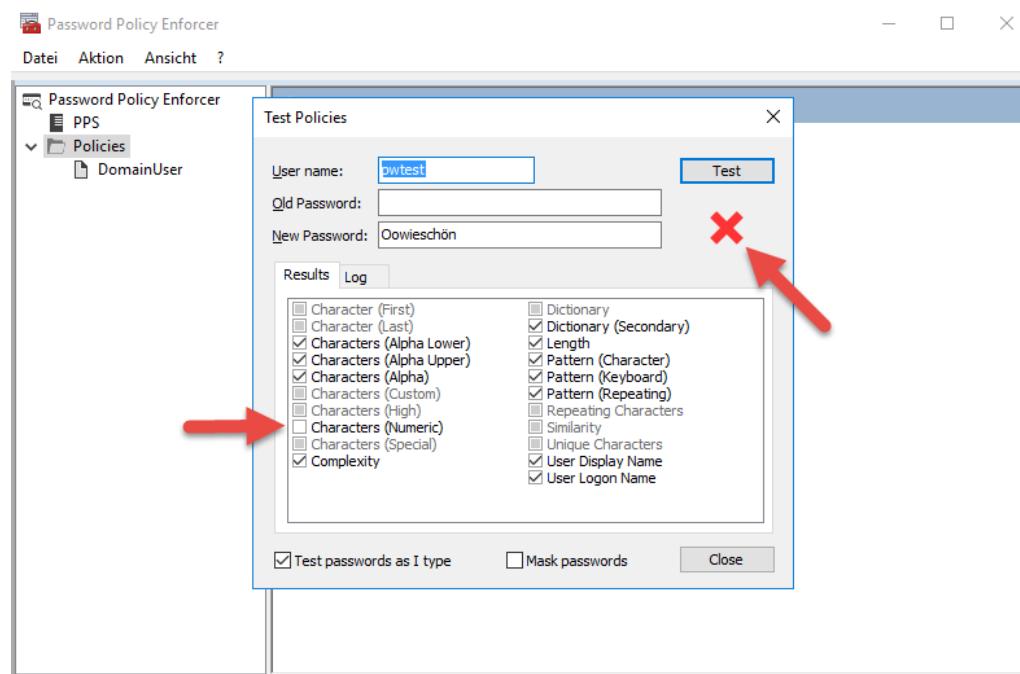
Info: Die Komplexitätsregel ist eine untergeordnete Funktion die nur dann richtig funktioniert wenn auch alle Abhängigkeiten aktiviert sind.

The screenshot shows the 'Password Policy Enforcer' application window with the 'Rule Properties' dialog open over the main interface. The dialog is titled 'Rule Properties' and has two tabs: 'Settings' (selected) and 'Messages'. The 'Settings' tab contains a description: 'This rule ensures that passwords contain the required mix of numeric characters. The default character set includes 0 - 9.' Below this, there's a checked checkbox labeled 'Enabled'. Under 'Password must:', there are two radio button options: 'contain 2 or more numeric characters' (selected) and 'not contain any numeric characters'. There's also a 'Character set' section with a 'Name:' field containing 'numeric' and a 'Characters:' field containing '[default]'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

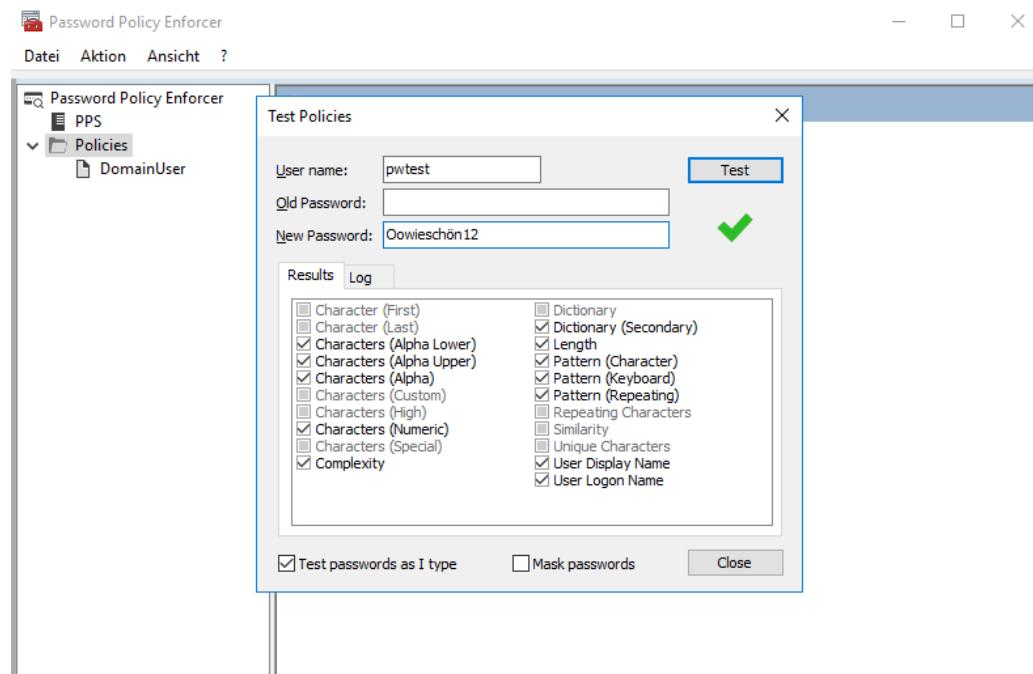


Anixis Password Policy Enforcer

Erneuter Versuch, nun werden auch Zahlen erwartet.



Ich denke diesen Abschnitt haben wir genug behandelt....





Anixis Password Policy Enforcer

... kommen wir zum Client.

Den automatisierten roll-out des Client Moduls behandeln wir später. Die neue Policy ist nun aktiv und scharf.

So sieht das Kennwort ändern Feld aus, wie wir es von Server 2016 oder Windows 10 kennen. Das Passwort muss ab sofort der neuen Richtlinie entsprechen, aber wie sieht diese aus eigentlich?!



Nachdem das Clientmodul installiert wurde, bekomme wir auch einen Hinweis darauf, was die Richtlinie von uns erwartet.





Anixis Password Policy Enforcer

Die Ansicht bei einem Server 2012 R2 ohne Client Modul.

The screenshot shows a Windows-style password change dialog. It features a user icon on the left and a title 'Kennwort ändern' at the top right. Below the title are four input fields: the current password ('NDSEDV\admin'), the old password ('*****'), the new password ('*****'), and a confirmation field ('*****'). To the right of the fields are two buttons: a blue eye icon for viewing the password and a blue arrow icon for saving it. Below the fields is a link 'Anmelden an: NDSEDV' with a hand cursor icon. At the bottom, there's a question 'Wie melden Sie sich an einer anderen Domäne an?' and a blue arrow button.

Die Ansicht bei einem Server 2012 R2 mit installiertem Client Modul.

This screenshot shows the same password change dialog as above, but with additional complexity rules displayed below the input fields. The rules are listed under the heading 'Komplexität:' and include:

- not match one of your last 24 passwords
- not be similar to your current password
- not be similar to your logon name
- not be similar to your name
- not be similar to common passwords
- contain an upper alpha character
- contain a lower alpha character
- contain at least 2 numeric characters
- contain at least 1 of these character types:
 - upper alpha
 - lower alpha
 - numeric
 - special
- not contain a keyboard pattern like qwerty
- not contain a repeating pattern like abcabc
- not contain a repeating character like aaa
- contain at least 10 characters



Anixis Password Policy Enforcer

Der Policy Enforcer funktioniert übergreifend. Auch der Admin ist nicht in der Lage ein Passwort gegen die eingereichte und zugewiesene Richtlinie zu vergeben. Zurzeit ist die Richtlinie noch nicht zugewiesen, es kann ein beliebiges Passwort vergeben werden.

The screenshot shows the Windows Active Directory Users and Computers interface. In the center, a modal dialog box titled "Active Directory-Domänen Dienste" displays the message: "Das Kennwort für NDS wurde geändert." (The password for NDS was changed). Below the dialog, a green message box states: "Der Password Policy Enforcer ist auf der OU Service Accounts noch nicht aktiv." (The Password Policy Enforcer is not active in the OU Service Accounts). The left navigation pane shows various Active Directory containers and objects like "Gespeicherte Abfragen", "Builtin", "Computers", etc.

Verknüpfe die Richtlinie nun auf die **OU = Service Accounts** und werde als Domänen-Admin versuchen das Passwort erneut zu ändern.

The screenshot shows the "Policy Properties" dialog for the "DomainUser" policy. The "Assigned To" tab is selected. Under "Containers / Organizational Units:", the value "OU=Service Accounts,OU=User,OU=ORG" is listed. Other entries in the list include "OU=User Accounts,OU=User,OU=ORG" and "OU=Users,OU=User,OU=ORG". The "OK" button is highlighted at the bottom of the dialog.



Anixis Password Policy Enforcer

Erstaunlich. Auch der Admin hat sich an die gültige Richtlinie zu halten. TOP!

(Hatte jetzt bewusst ein Sonderzeichen weggelassen obwohl dieses erwartet wird.)

The screenshot shows the Windows Active Directory Users and Computers interface. On the left, a tree view shows the structure of the domain 'ndsedv.de'. On the right, a table lists users with their types and descriptions. The 'NDS' user is listed as a 'Benutzer' (User) with the description 'DOM-ADMIN'. A modal dialog box titled 'Active Directory-Domäendienste' displays an error message: 'Das Kennwort für NDS kann aufgrund folgenden Problems nicht geändert werden: Das Kennwort entspricht nicht den Anforderungen der Kennwortrichtlinien. Überprüfen Sie die Kennwortlänge, die Komplexität des Kennworts und die Anforderungen bezüglich früherer Kennwörter.' (The password for NDS cannot be changed due to the following problems: The password does not meet the requirements of the password policy. Check the password length, complexity, and requirements regarding previous passwords.)

Automatische Verteilung des Client Moduls über eine Gruppenrichtlinie.
Neue GPO erstellen und das Paket per UNC Pfad einbinden.

C:\Windows\SYSVOL\sysvol\ndsedv.de\scripts\PPEC\PPEClt803.msi

The screenshot shows the Group Policy Management Editor. On the left, a tree view shows the group policy objects (GPOs) under 'ndsedv.de'. On the right, the 'Install PPECClient' GPO is selected. In the center, a list of policy items is shown. A context menu is open over one of the items, with the 'Paket...' option highlighted by a red arrow. The menu also includes 'Neu', 'Ansicht', 'Einfügen', 'Aktualisieren', 'Liste exportieren...', 'Eigenschaften', and 'Hilfe'.



Anixis Password Policy Enforcer

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays a hierarchy of Group Policies, including 'nsedv.de', 'Default Domain Policy', 'Domain Controllers', 'Microsoft Exchange Security Groups', 'ORG', 'Groups', 'Machines', 'Software', 'Clients', 'Server', and 'User'. Under 'Server', there is a policy named 'Install PPEClient' with a red arrow pointing to it. The main pane shows the 'Install PPEClient' policy details. In the 'Computer Configuration (Aktiviert)' tab, the 'Richtlinien' section is selected. The 'Produktinformationen' table shows 'Name: Password Policy Client 8.03', 'Version: 8.3', 'Sprache: Englisch (USA)', 'Plattform: x86', and 'Support-URL: http://www.anixis.com/products/ppe/support.htm'. The 'Bereitstellungsinformation' section includes 'Allgemein' and 'Erweiterte Bereitstellungsoptionen' tables. A red arrow points to the 'Bereitstellungsart' table, specifically to the 'Zugewiesen' row which contains the path '\\\nsedv.de\SYSVOL\nsedv.de\scripts\PPEC\PPCE803.msi'. The 'Diagnoseinformationen' and 'Sicherheit' sections are also visible.

Nach einem Neustart erhalten die Clientsysteme das Paket automatisch.

The screenshot shows the Windows Server Manager interface. The left sidebar shows 'Dashboard', 'Lokaler Server', 'Alle Server', 'Datei-/Speicherdiene...', 'IIS', and 'WDS'. The main area shows the 'EIGENSCHAFTEN' (Properties) for 'SRV01'. The 'Programme und Features' (Programs and Features) window is open, displaying a list of installed programs. The 'Password Policy Client 8.03' entry is highlighted with a red arrow. The properties for this program are shown at the bottom of the window: 'ANIXIS', 'Version: 8.03', 'Supportlink: http://www.anixis.com/products/ppe/', and 'Hilfeline: http://www.anixis.co...'. Below the main window, a table lists various system components and their status.

System Component	Status	Description	Details
SRV01	13 Fehler	Microsoft-Windows-CertificateServicesClient-CertEnroll	Anwendung 17.06.2017 15:18:04
SRV01	82 Fehler	Microsoft-Windows-CertificateServicesClient-CertEnroll	Anwendung 17.06.2017 15:18:04
SRV01	1064 Fehler	Microsoft-Windows-TerminalServices-RemoteConnectionManager	System 17.06.2017 15:18:04
SRV01	10028 Fehler	Microsoft-Windows-DistributedCOM	System 17.06.2017 15:17:27
SRV01	13 Fehler	Microsoft-Windows-CertificateServicesClient-CertEnroll	Anwendung 17.06.2017 15:17:27



Anixis Password Policy Enforcer

Troubleshooting:

Das Ereignisprotokoll ist sehr aussagekräftig und gibt Hinweise auf Lösungen.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs, and the right pane shows a detailed view of a selected event. The event details are as follows:

Ebene	Datum und Uhrzeit	Quelle	Event-ID	Aufgabenkategorie
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2108	Keine
Warnung	17.06.2017 12:24:15	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:15:37	Password Policy Enforcer	2105	Keine
Informationen	17.06.2017 12:10:26	LoadPerf	1000	Keine
Fehler	17.06.2017 12:10:25	PerfNet	2006	Keine
Informationen	17.06.2017 12:07:17	ESENT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESENT	105	Allgemein
Informationen	17.06.2017 12:07:17	ESENT	102	Allgemein
Warnung	17.06.2017 12:06:28	Password Policy Enforcer	2155	Keine

Event 2108, Password Policy Enforcer

Allgemein Details

Protocol name: Anwendung
Source: Password Policy Enforcer Protocol time: 17.06.2017 12:25:11
Event ID: 2108 Task category: None
Level: Warning Keyword: Classic
User: Not applicable Computer: DC01.ndsedv.de
Action code: Further information: [Onlinehelp](#)

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs, and the right pane shows a detailed view of a selected event. The event details are as follows:

Ebene	Datum und Uhrzeit	Quelle	Event-ID	Aufgabenkategorie
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2108	Keine
Warnung	17.06.2017 12:24:15	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:15:37	Password Policy Enforcer	2105	Keine
Informationen	17.06.2017 12:10:26	LoadPerf	1000	Keine
Fehler	17.06.2017 12:10:25	PerfNet	2006	Keine
Informationen	17.06.2017 12:07:17	ESENT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESENT	105	Allgemein
Informationen	17.06.2017 12:07:17	ESENT	102	Allgemein
Warnung	17.06.2017 12:06:28	Password Policy Enforcer	2155	Keine

Event 2105, Password Policy Enforcer

Allgemein Details

Protocol name: Anwendung
Source: Password Policy Enforcer Protocol time: 17.06.2017 12:15:37
Event ID: 2105 Task category: None
Level: Warning Keyword: Classic
User: Not applicable Computer: DC01.ndsedv.de
Action code: Further information: [Onlinehelp](#)

Fehlendes Attribut setzen: ldifde -i -f History.ldf -c "DC=X" "DC=nds-edv,DC=de"

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs, and the right pane shows a detailed view of a selected event. The event details are as follows:

Ebene	Datum und Uhrzeit	Quelle	Event-ID	Aufgabenkategorie
Warnung	17.06.2017 13:20:20	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:25:11	Password Policy Enforcer	2108	Keine
Warnung	17.06.2017 12:24:15	Password Policy Enforcer	2155	Keine
Warnung	17.06.2017 12:15:37	Password Policy Enforcer	2105	Keine
Informationen	17.06.2017 12:10:26	LoadPerf	1000	Keine
Fehler	17.06.2017 12:10:25	PerfNet	2006	Keine
Informationen	17.06.2017 12:07:17	ESENT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESENT	105	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	102	Allgemein

Event 2155, Password Policy Enforcer

Allgemein Details

Protocol name: Anwendung
Source: Password Policy Enforcer Protocol time: 17.06.2017 13:20:20
Event ID: 2155 Task category: None
Level: Warning Keyword: Classic
User: Not applicable Computer: DC01.ndsedv.de
Action code: Further information: [Onlinehelp](#)

**Das Attribut muss im AD neu angelegt werden
ldifde -i -f History.ldf -c "DC=X" "DC=nds-edv,DC=de"**

https://anixis.com/doc/ppe60ag/History_Rule.html#wp9000608



Anixis Password Policy Enforcer

```
Administrator: Eingabeaufforderung

C:\Program Files (x86)\Password Policy Enforcer>ldifde -i -f History.ldf -c "DC=X" "DC=ndsevd,DC=de"
Verbindung mit "DC01.ndsevd.de" wird hergestellt.
Anmelden als aktueller Benutzer unter Verwendung von SSPI
Das Verzeichnis wird aus der Datei "History.ldf" importiert.
Die Einträge werden geladen.....
3 Einträge wurden erfolgreich geändert.

Der Befehl wurde einwandfrei durchgeführt.

C:\Program Files (x86)\Password Policy Enforcer>
```

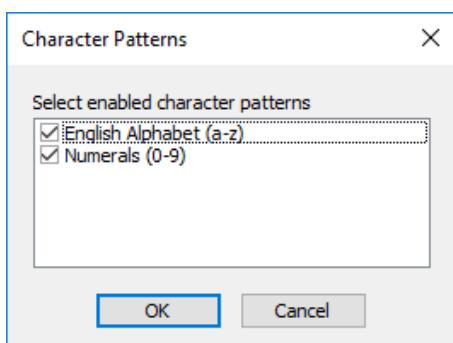
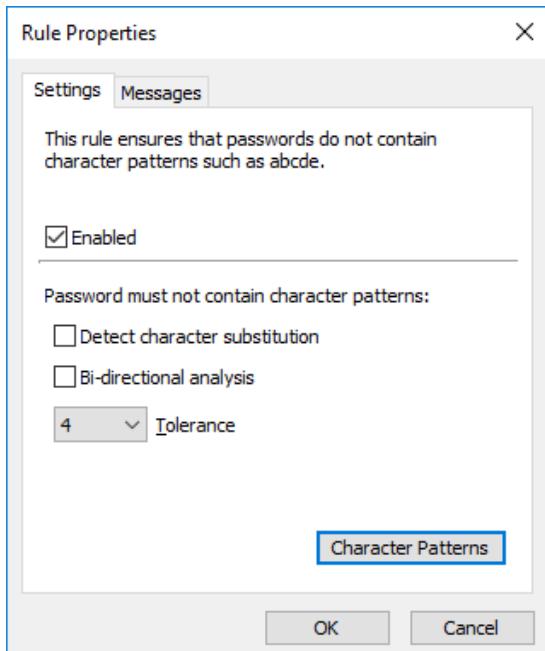


Anixis Password Policy Enforcer

Details zu den Regeln:

Character Pattern:

Die Zeichenmusterregel lehnt Passwörter ab, die die Zeichenmuster wie z.B. „abcde“ oder „12345“ enthalten. Die Muster können einzeln oder kombiniert eingesetzt und konfiguriert werden. Auch die Toleranz wie viele Zeichen hintereinanderstehen dürfen kann eingestellt werden.

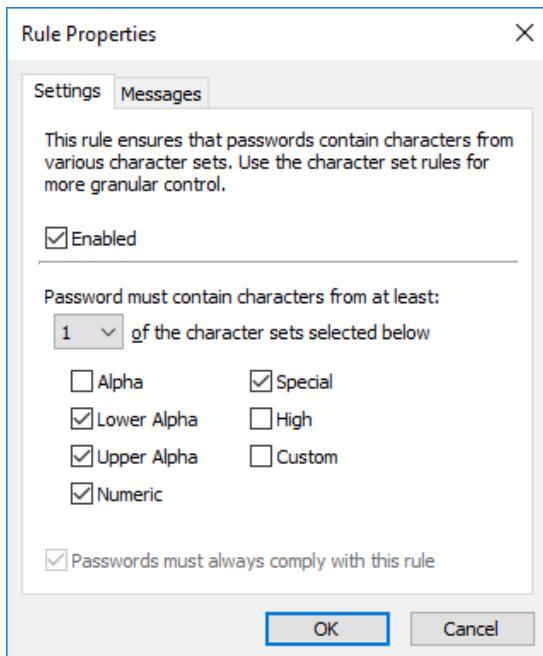




Anixis Password Policy Enforcer

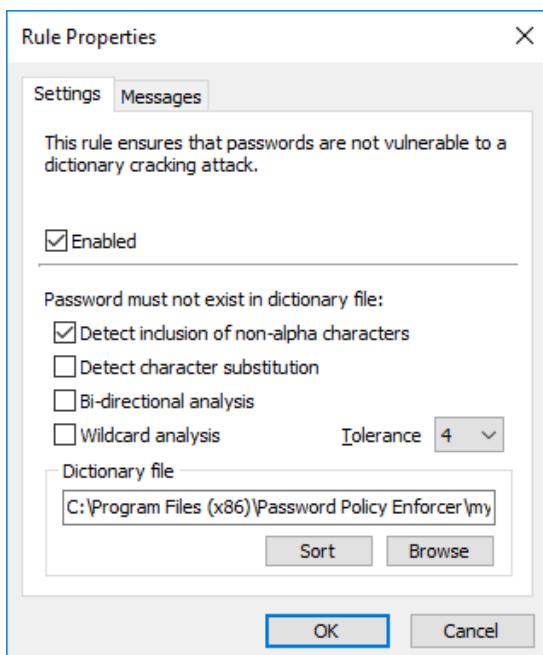
Complexity:

Die Komplexitätsregel lehnt Passwörter ab, die keine Zeichen aus einer Vielzahl von Zeichensätzen enthalten. Die erforderliche Anzahl und Auswahl von Zeichensätzen sind konfigurierbar.



Dictionary:

Die Wörterbuchregel lehnt Passwörter ab, die anfällig für Hackerangriffe sind. Hierbei wird ein lokales Wörterbuch verwendet, indem der PPE dieses einliest und mit den Passwörtern vergleicht. Diese Regel erkennt partielle Übereinstimmungen mit einem Passwort und kann Zeichensubstitutionen (ersetzen von \$ durch S), Bidirektional und eine Zeichenumkehr erkennen.





Anixis Password Policy Enforcer

First Character:

Diese Regel lehnt Passwörter ab, die nicht mit einem entsprechenden Zeichen beginnen. Mehrere Zeichensätze können als gültig oder ungültig erklärt werden.

Rule Properties X

Settings Messages

This rule ensures that passwords begin with an appropriate character.

Enabled

Password must:

begin not begin

with a character from the selected character sets

Alpha Special
 Lower Alpha High
 Upper Alpha Custom
 Numeric

OK Cancel

History:

Die Historienregel lehnt Passwörter ab, die kürzlich bereits verwendet wurden.

Rule Properties X

Settings Messages

This rule ensures that passwords are not the same as a recently used password.

Enabled

Password must not be the same as:

one of the last passwords
 a password used in the last days

Enforce this rule when a password is reset

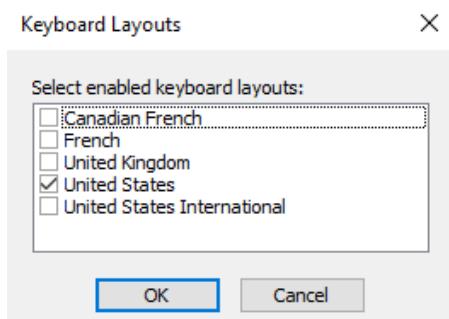
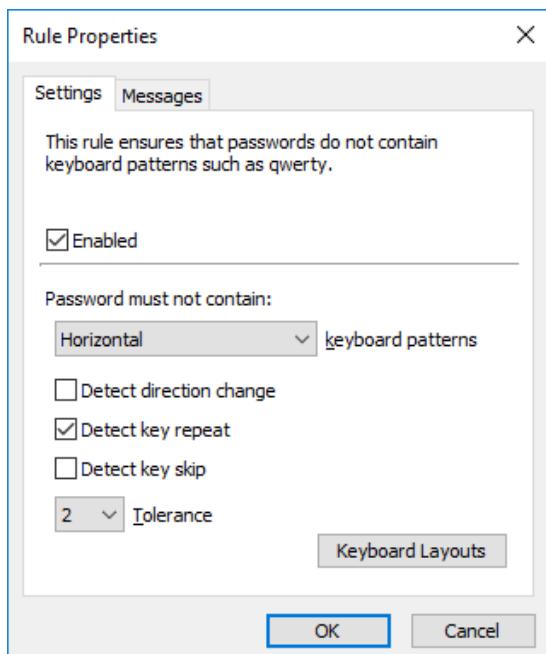
OK Cancel



Anixis Password Policy Enforcer

Keyboard Pattern:

Die Tastatur Pattern-Regel lehnt Passwörter ab, wie z.B. qwerty oder asdfg. Das Tastaturlayout kann für ein Land bestimmt werden. An dieser Stelle muss ich leider sagen das die deutsche Tastatur nicht unterstützt wird. Die Alternative wäre die Dictionary!

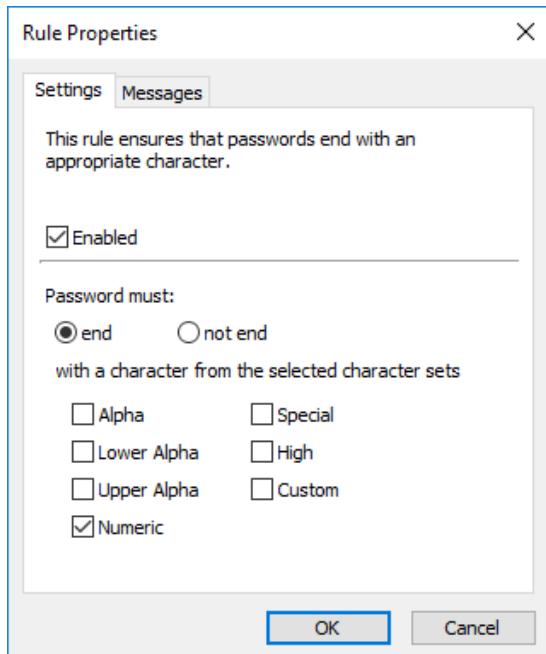




Anixis Password Policy Enforcer

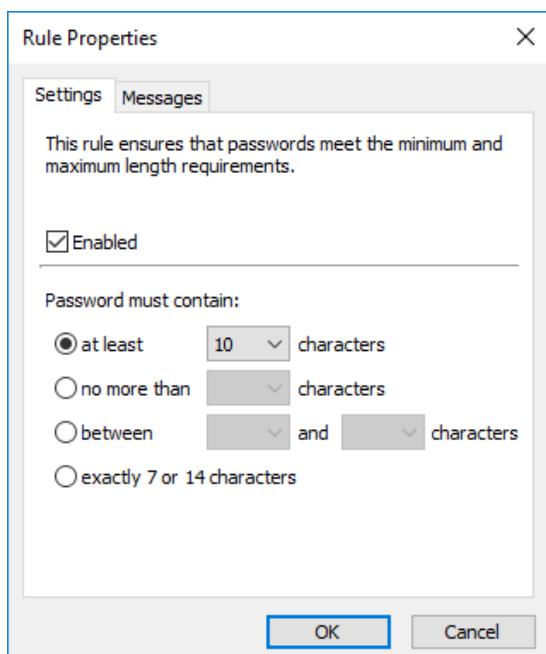
Last Character:

Die letzte Zeichenregel lehnt Passwörter ab die nicht mit einem entsprechenden Zeichen enden.



Length:

Die Längenregel lehnt Passwörter an die zu wenig oder zu viele Zeichen enthält.





Anixis Password Policy Enforcer

Maximum Age:

Die maximale Altersregel zwingt den Benutzer, das Passwort regelmäßig zu ändern. Wie in diesem Beispiel alle 42 Tage. Ist das Passwort aber 20 Zeichen lang, so wird der Benutzer erst nach 60 Tagen gezwungen sein Passwort zu ändern.

Rule Properties X

Settings E-mail

This rule ensures that passwords are changed regularly to increase their effectiveness.

Enabled

User must change password after:

42 days, or 60 days if the password contains 20 or more characters

Mode

Standard

Use the Transitional and Warning modes to gradually introduce this rule. Switch to Standard mode after the introductory period.

OK Cancel

Minimum Age:

Die Mindestalter Regel stoppt den Benutzer vor einer mehrmaligen Änderung des Passwortes an x Tagen. Außerdem schützt es die schnelle Umgehung der History.

Rule Properties X

Settings Messages

This rule ensures that passwords are used for a minimum duration, stopping users from quickly cycling through a series of passwords.

Enabled

User cannot change password for at least:

1 days

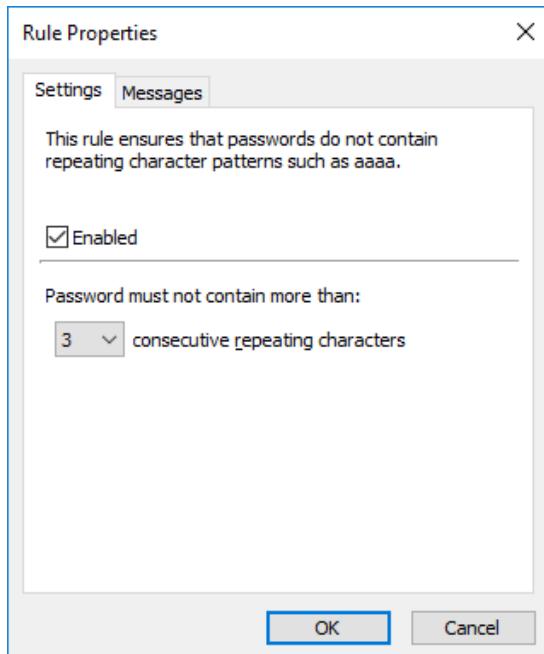
OK Cancel



Anixis Password Policy Enforcer

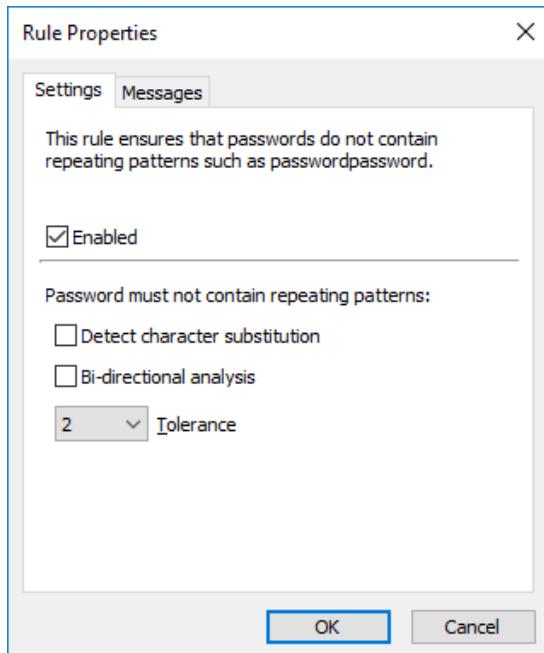
Repeating Characters:

Diese Regel lehnt Passwörter ab, die eine übermäßige Zeichenwiederholung enthält, wie z.B. aaa, bbb usw.



Repeating Pattern:

Diese Regel erkennt wiederholte Muster und lehnt Passwörter ab wie z.B. Passw0rdPassw0rd. Auch hier gibt es die Option der bidirektionalen Erkennung und der Zeichensubstitutionen (ersetzen von \$ durch S).

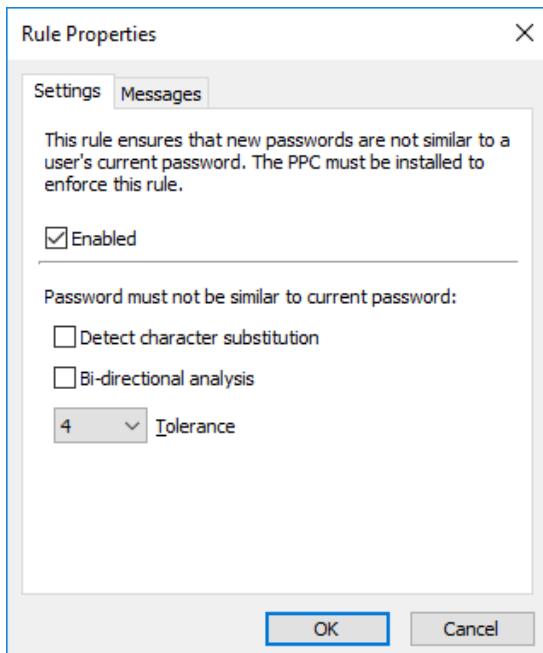




Anixis Password Policy Enforcer

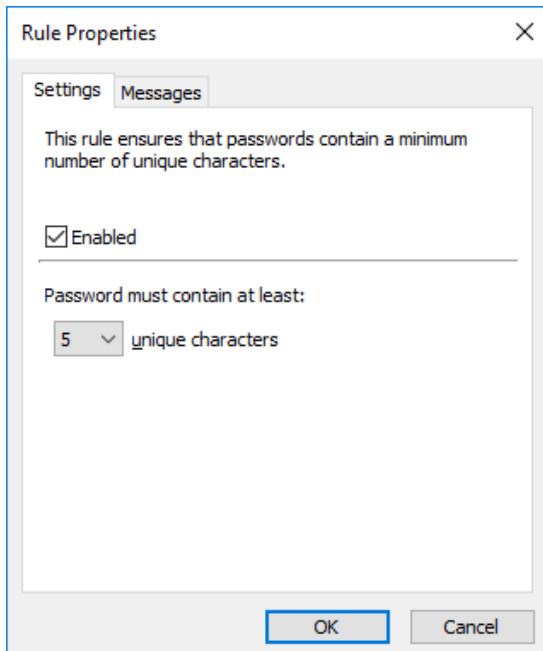
Similarity:

Die Ähnlichkeitserkennung lehnt Passwörter ab, die dem alten ähneln. Wie z.B. Password1 oder Password2. Dafür muss die Client Software (PPC) installiert sein, siehe oben.



Unique Character:

Diese Regel lehnt Passwörter ab, die keine minimale Anzahl von eindeutigen Zeichen enthält.

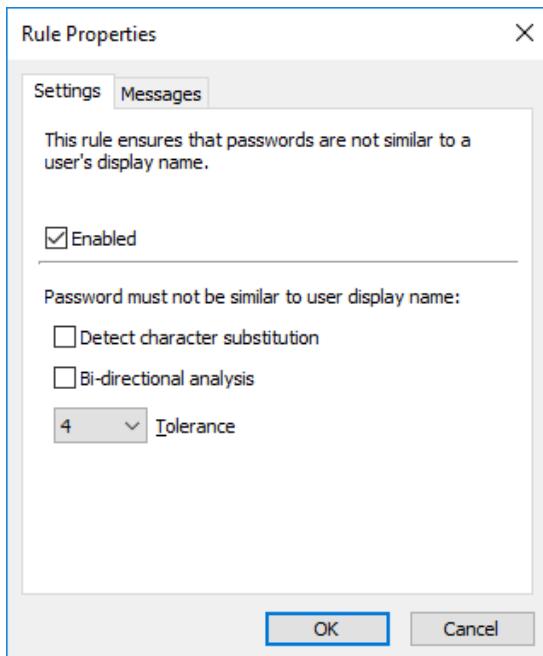




Anixis Password Policy Enforcer

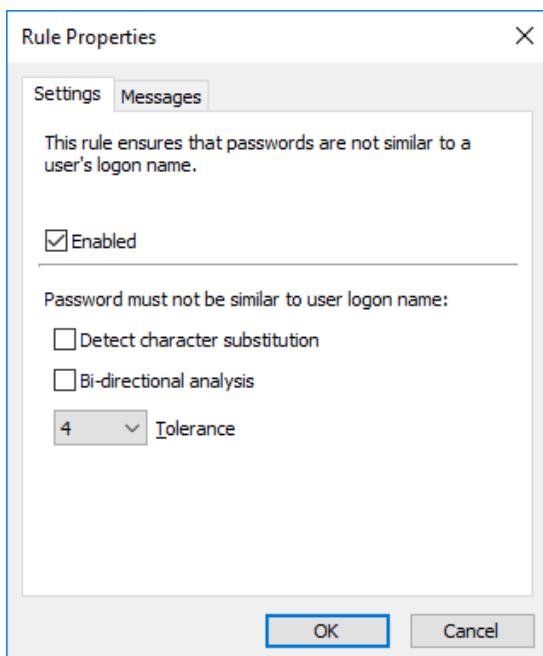
User Display Name:

Die Regel Benutzer Anzeigename lehnt Passwörter ab, die sich mit dem Anzeigenamen im Active Directory ähneln. Zu den Optionen gehören Match-Toleranz, Zeichensatzerkennung und die bidirektionale Analyse.



User Logon Name.

Die Regel Benutzer Anmeldename lehnt Passwörter ab, die sich mit dem Anmeldenamen im Active Directory ähneln. Zu den Optionen gehören auch hier die Match-Toleranz, Zeichensatzerkennung und die bidirektionale Analyse.





Anixis Password Policy Enforcer

Meine empfohlenen Einstellungen:

Age Max:

Rule Properties X

Enabled

User must change password after:

42 days, or 60 days if the password contains 20 or more characters

Mode

Standard

Use the Transitional and Warning modes to gradually introduce this rule. Switch to Standard mode after the introductory period.

OK Cancel

Age Min:

Rule Properties X

Enabled

User cannot change password for at least:

1 days

OK Cancel



Anixis Password Policy Enforcer

Character (Alpha Lower):

Rule Properties X

Settings Messages

This rule ensures that passwords contain the required mix of Lower Alpha characters. The default character set includes a - z.

Enabled

Password must:

contain or more lower alpha characters
 not contain any lower alpha characters
in position to Embedded

Character set

Name:
Characters:

OK Cancel

Character (Alpha Upper):

Rule Properties X

Settings Messages

This rule ensures that passwords contain the required mix of Upper Alpha characters. The default character set includes A - Z.

Enabled

Password must:

contain or more upper alpha characters
 not contain any upper alpha characters
in position to Embedded

Character set

Name:
Characters:

OK Cancel



Anixis Password Policy Enforcer

Character (Numeric):

Rule Properties

Settings Messages

This rule ensures that passwords contain the required mix of Numeric characters. The default character set includes 0 - 9.

Enabled

Password must:

contain or more numeric characters
 not contain any numeric characters

in position to Embedded

Character set

Name:
Characters:

OK Cancel

Complexity:

Rule Properties

Settings Messages

This rule ensures that passwords contain characters from various character sets. Use the character set rules for more granular control.

Enabled

Password must contain characters from at least:

of the character sets selected below

Alpha Special
 Lower Alpha High
 Upper Alpha Custom
 Numeric

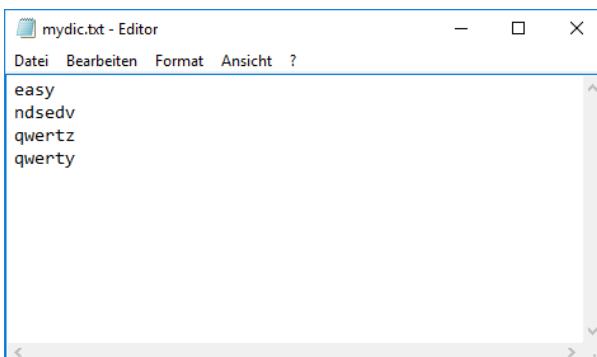
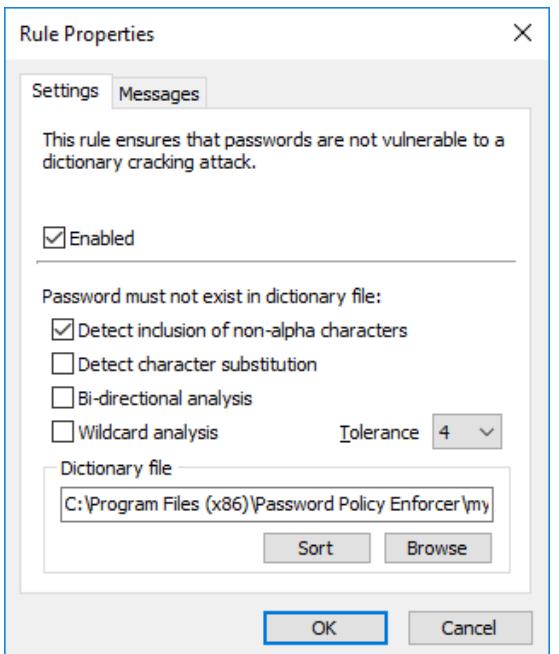
Passwords must always comply with this rule

OK Cancel

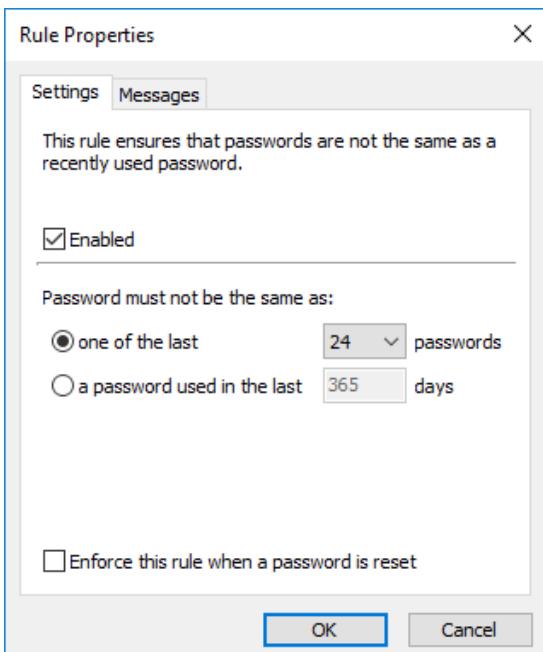


Anixis Password Policy Enforcer

Dictionary:



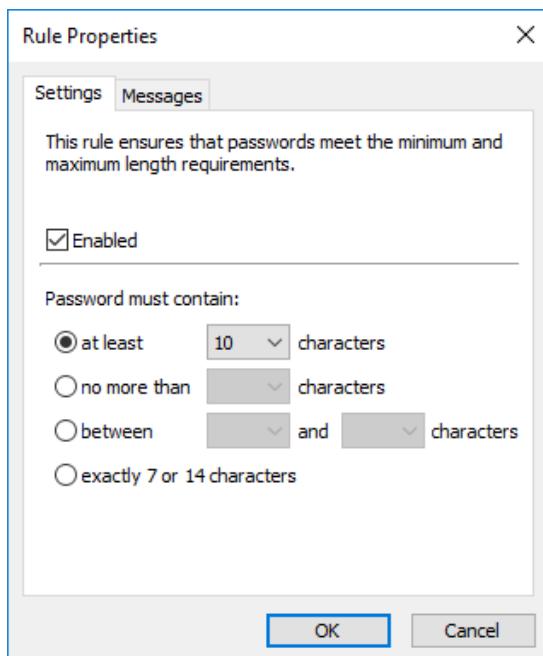
History:



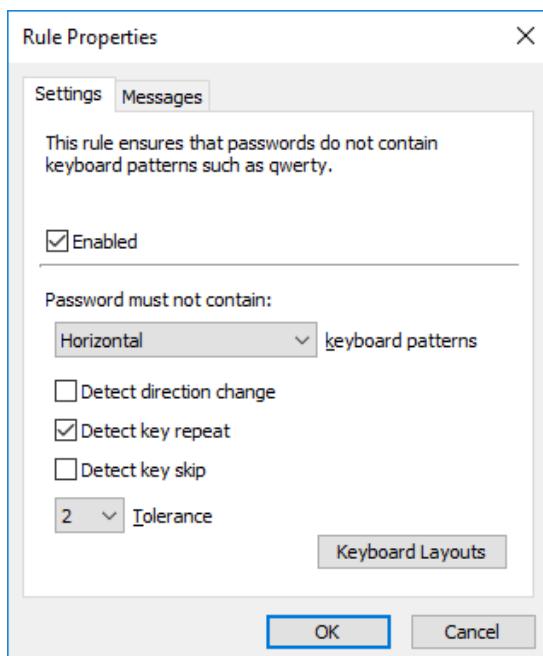


Anixis Password Policy Enforcer

Length:



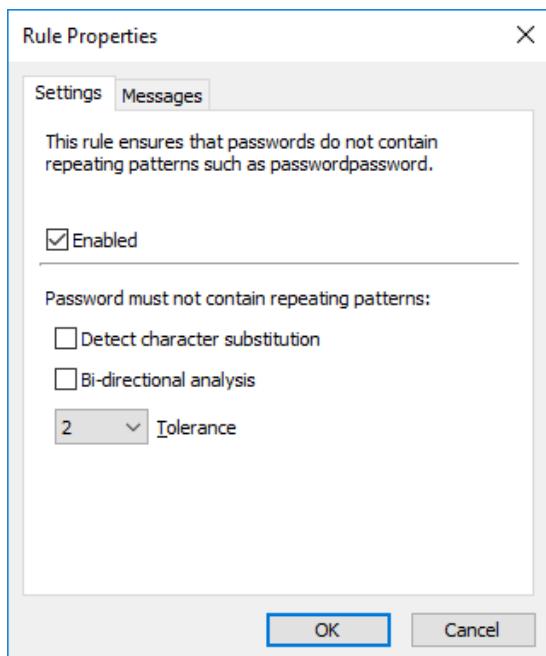
Pattern (Keyboard):



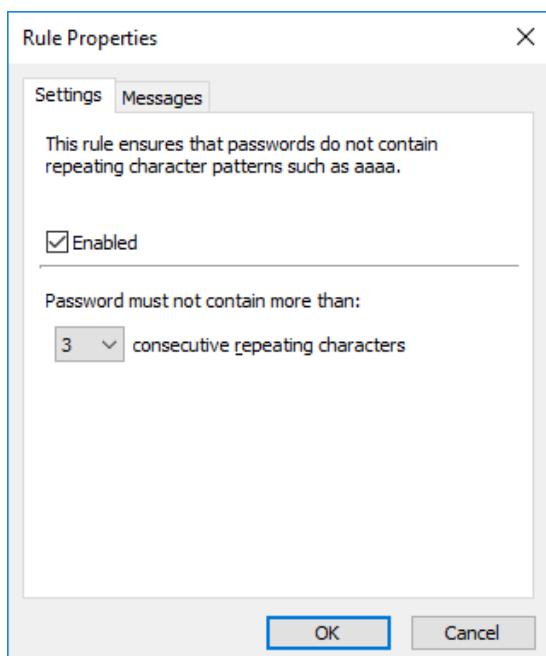


Anixis Password Policy Enforcer

Pattern (Repeating):



Repeating Characters:





Anixis Password Policy Enforcer

Similarity:

Rule Properties X

Settings Messages

This rule ensures that new passwords are not similar to a user's current password. The PPC must be installed to enforce this rule.

Enabled

Password must not be similar to current password:

Detect character substitution
 Bi-directional analysis
4 Tolerance

OK Cancel

Age Max:

Rule Properties X

Settings E-mail

This rule ensures that passwords are changed regularly to increase their effectiveness.

Enabled

User must change password after:

42 days, or 60 days if the password contains 20 or more characters

Mode
Standard

Use the Transitional and Warning modes to gradually introduce this rule. Switch to Standard mode after the introductory period.

OK Cancel



Anixis Password Policy Enforcer

Age Min:

Rule Properties X

Settings Messages

This rule ensures that passwords are used for a minimum duration, stopping users from quickly cycling through a series of passwords.

Enabled

User cannot change password for at least:

1 days

OK Cancel