



## 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 genullt werden:

The screenshot shows the Group Policy Management console. In the left-hand tree, the 'Default Domain Policy' is selected under the 'Domänen' (Domains) folder. The right-hand pane displays the 'Default Domain Policy' settings. The 'Computerkonfiguration (Aktiviert)' section is expanded, and the 'Richtlinien' (Policies) section is selected. The 'Windows-Einstellungen' (Windows Settings) section is expanded, and the 'Sicherheitseinstellungen' (Security Settings) section is selected. The 'Kontorichtlinien/Kennwortrichtlinien' (Password Policies) section is expanded, and the 'Kontorichtlinien/Kontosperrrichtlinien' (Account Lockout Policies) section is selected. The 'Kontorichtlinien/Kerberos-Richtlinie' (Kerberos Policy) section is also visible. The 'Richtlinie' (Policy) column lists various password and account lockout settings, and the 'Einstellung' (Setting) column shows their current values. A red box highlights the 'Kennwortrichtlinie' (Password Policy) settings, which are currently set to 'Aktiviert' (Enabled).

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

Richtlinie	Einstellung
Kontosperrungsschwelle	3 ungültige Anmeldeversuche
Kontosperrdauer	0 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

Richtlinie	Einstellung
Benutzeranmeldebeschränkungen erzwingen	Aktiviert
Max. Gültigkeitsdauer des Benutzertickets	10 Stunden

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.

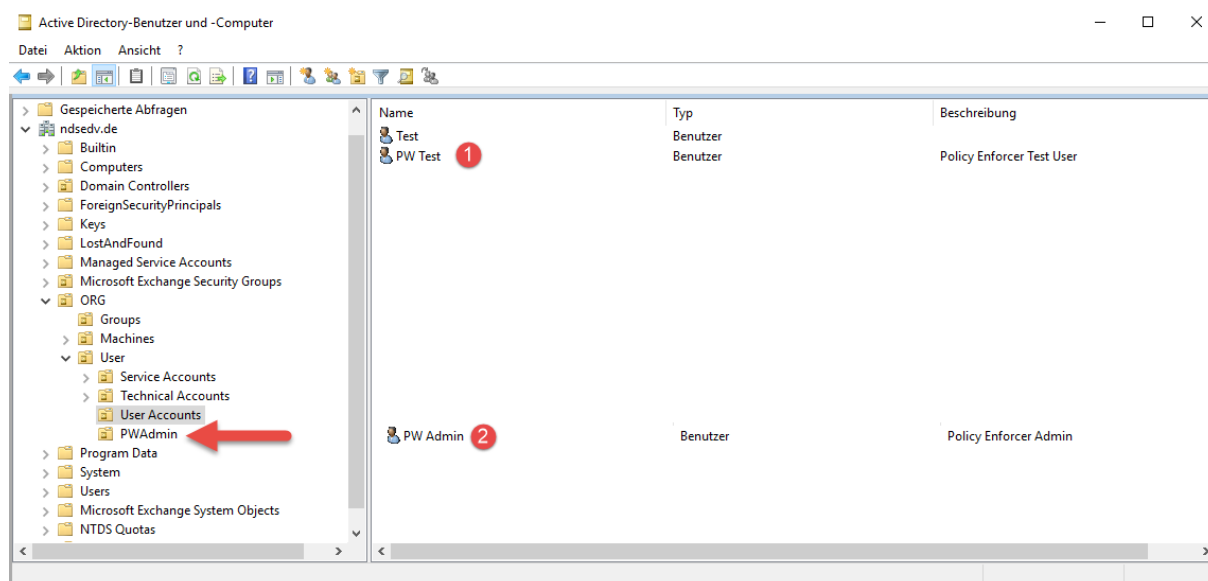
### Ein Hinweis am Rande:

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, das mehrere voneinander getrennte Richtlinien erstellt und zugewiesen werden können.



### 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

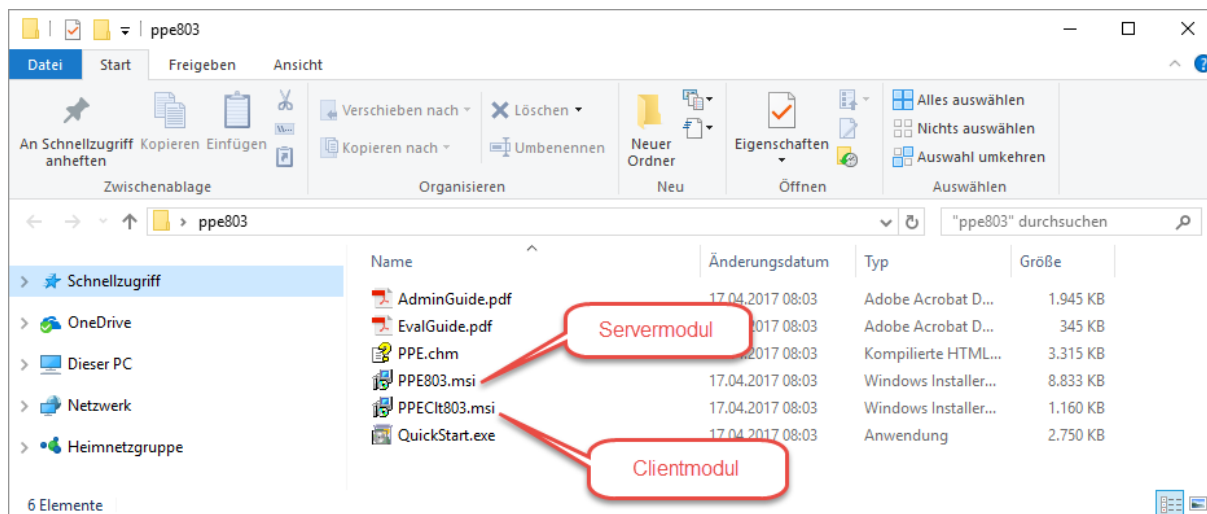


If your firewall performs Stateful Packet Inspection, then only create a rule for the request datagram as the firewall will automatically recognize and allow the response datagram.



## Anixis Password Policy Enforcer

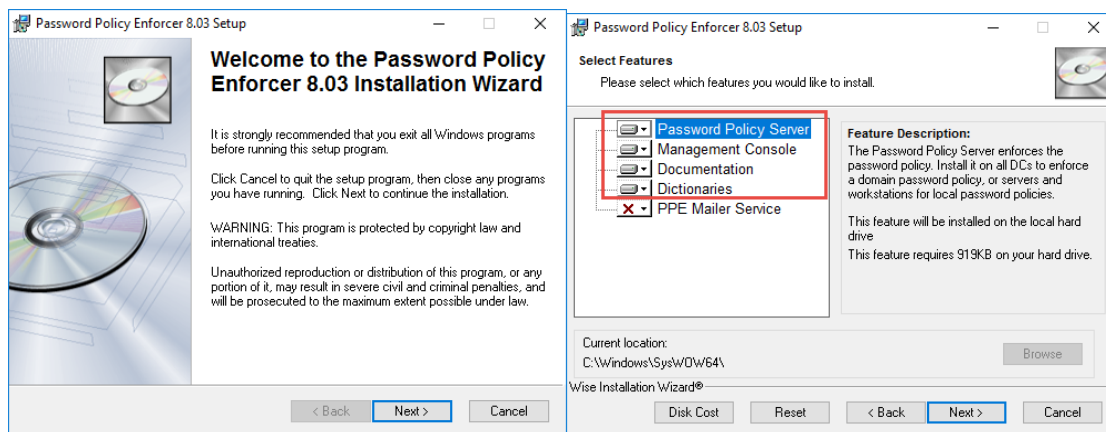
Ich habe das Installation Paket mal zur Veranschaulichung extrahiert um zu zeigen was alles enthalten ist.



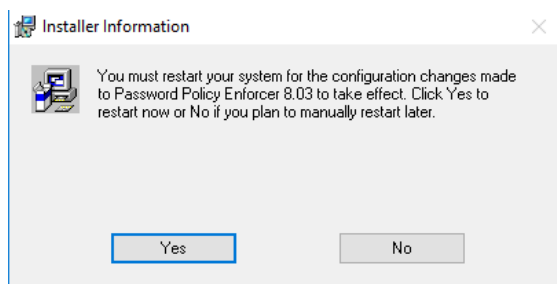
### Systemanforderungen:

- 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.

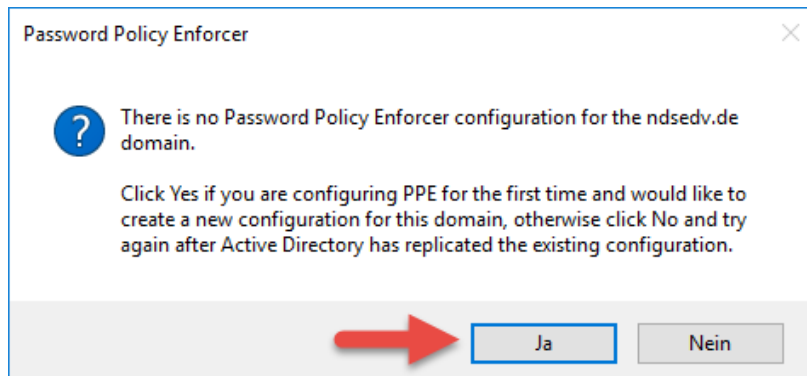


Der Neustart ist zwingend notwendig!

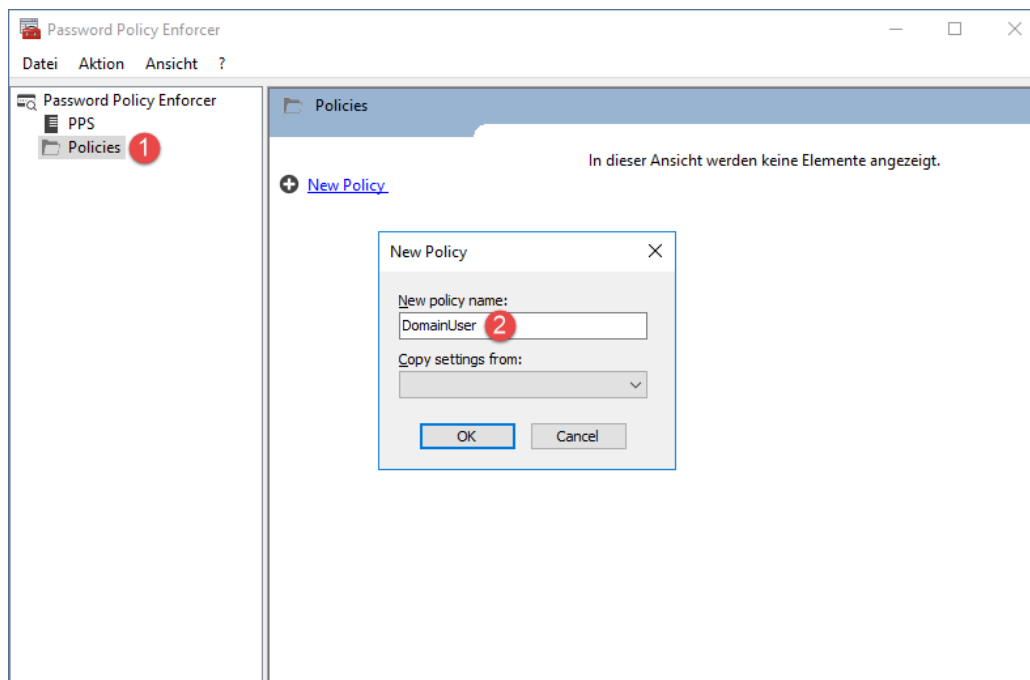


## Anixis Password Policy Enforcer

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



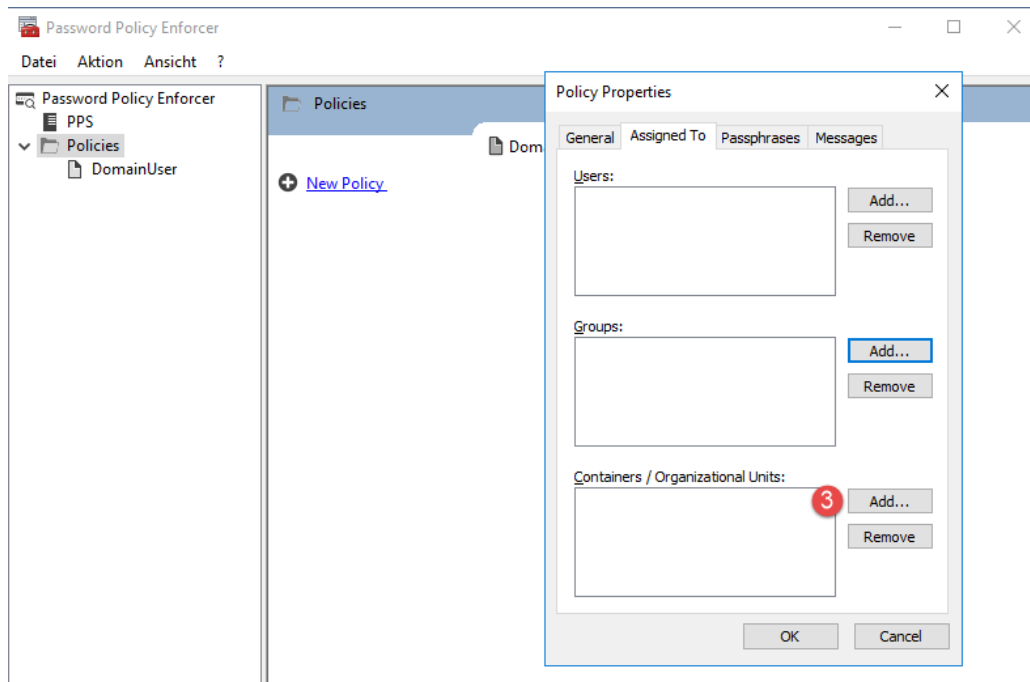
Eine erstellte Regel kann entweder auf einen User, einer Gruppe oder auf eine OU angewendet werden. Es können maximal 256 Regeln erstellt werden.



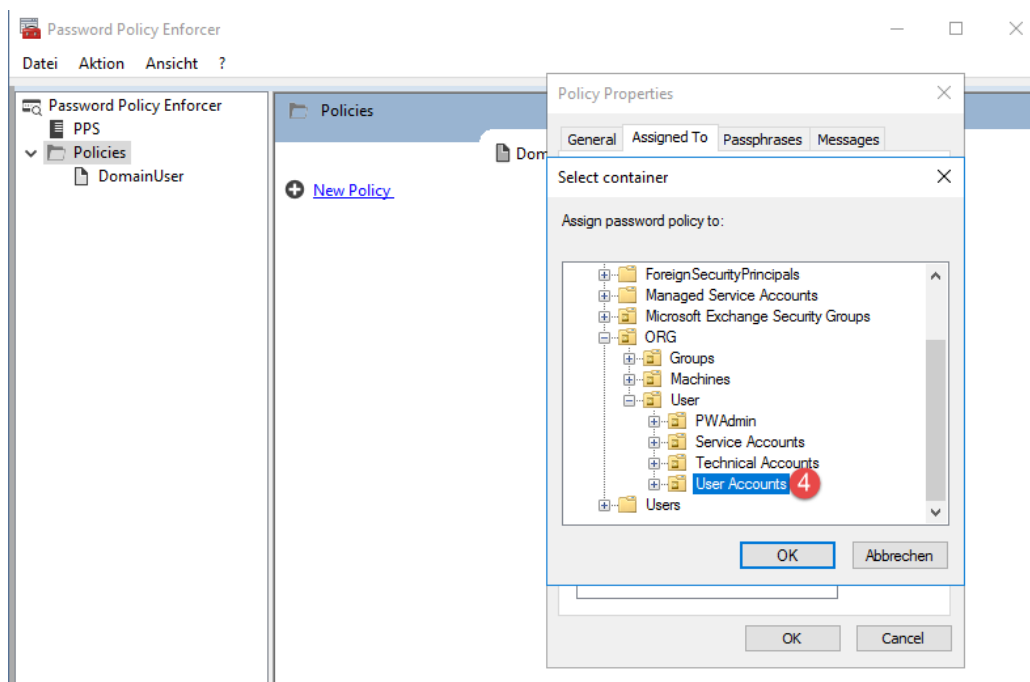


## Anixis Password Policy Enforcer

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



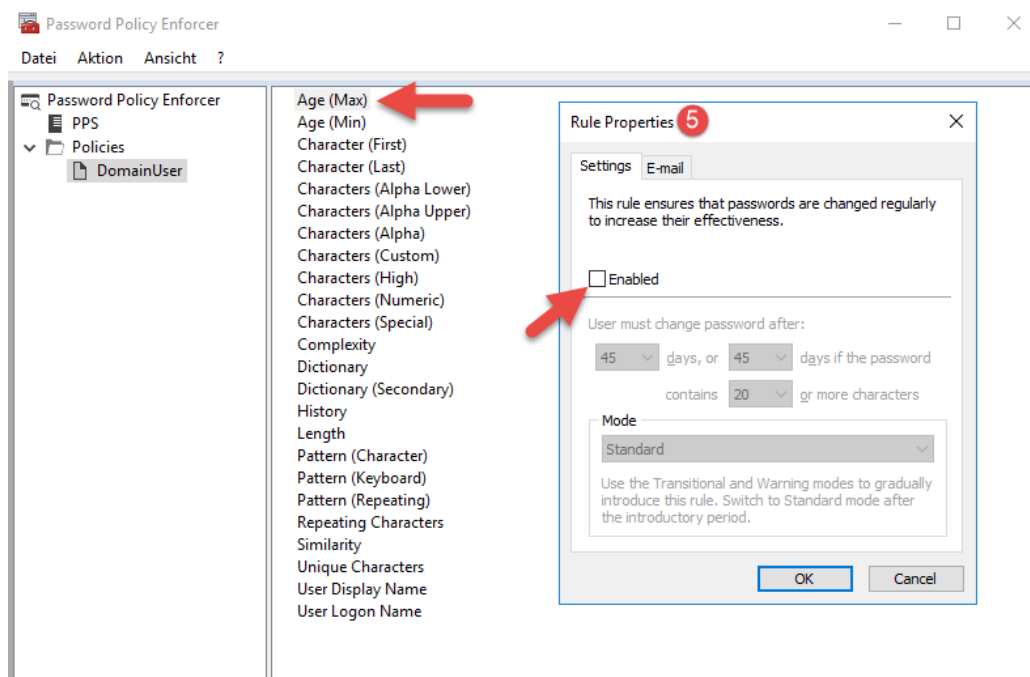
ADD > OU auswählen > OK



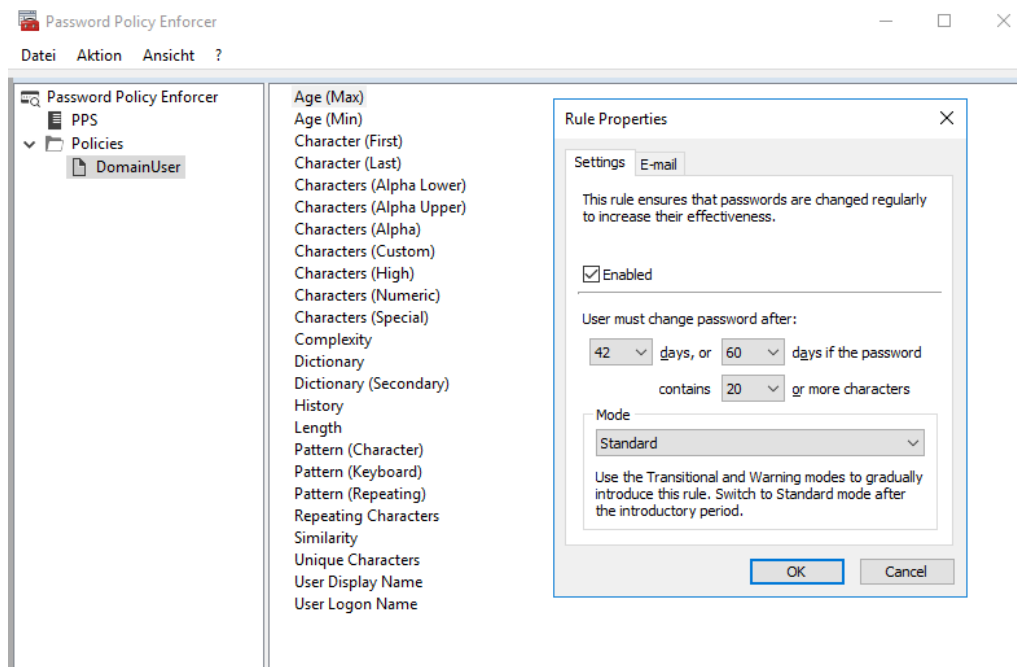


## Anixis Password Policy Enforcer

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



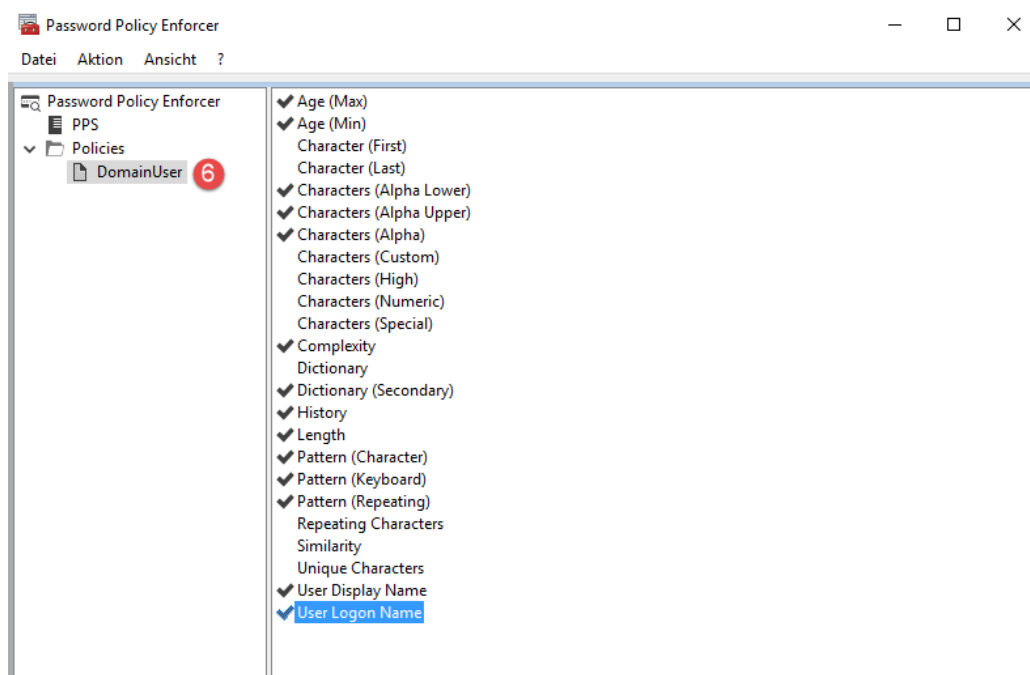
Es ist ganz klar zu erkennen, dass wir mit diesem Produkt wesentlich mehr Möglichkeiten haben als uns die Default Domain Policy anbietet.



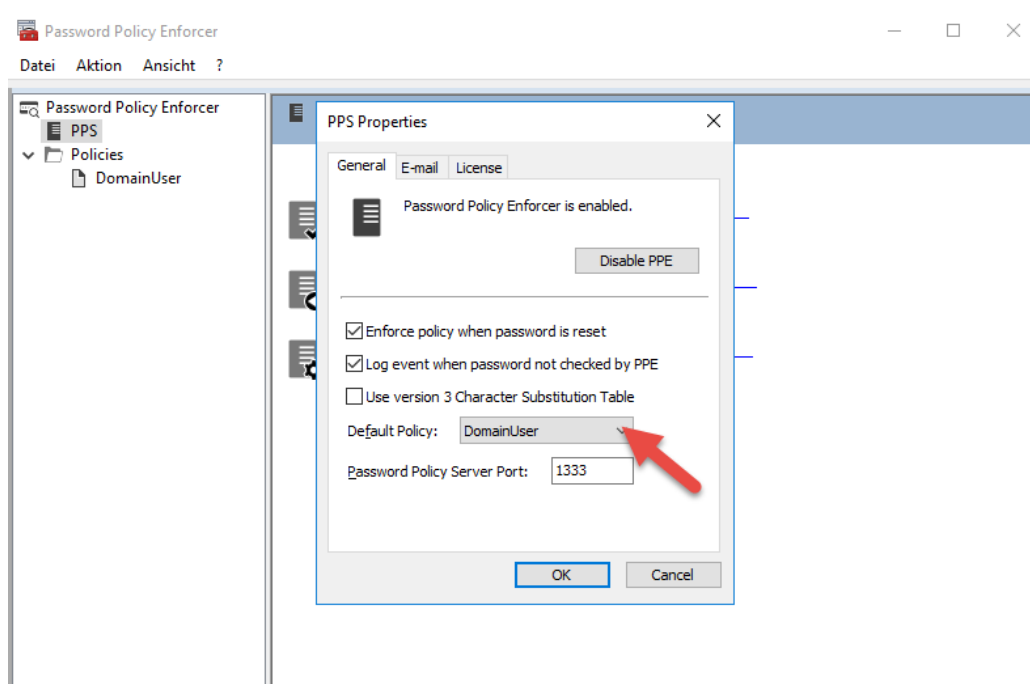


## Anixis Password Policy Enforcer

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



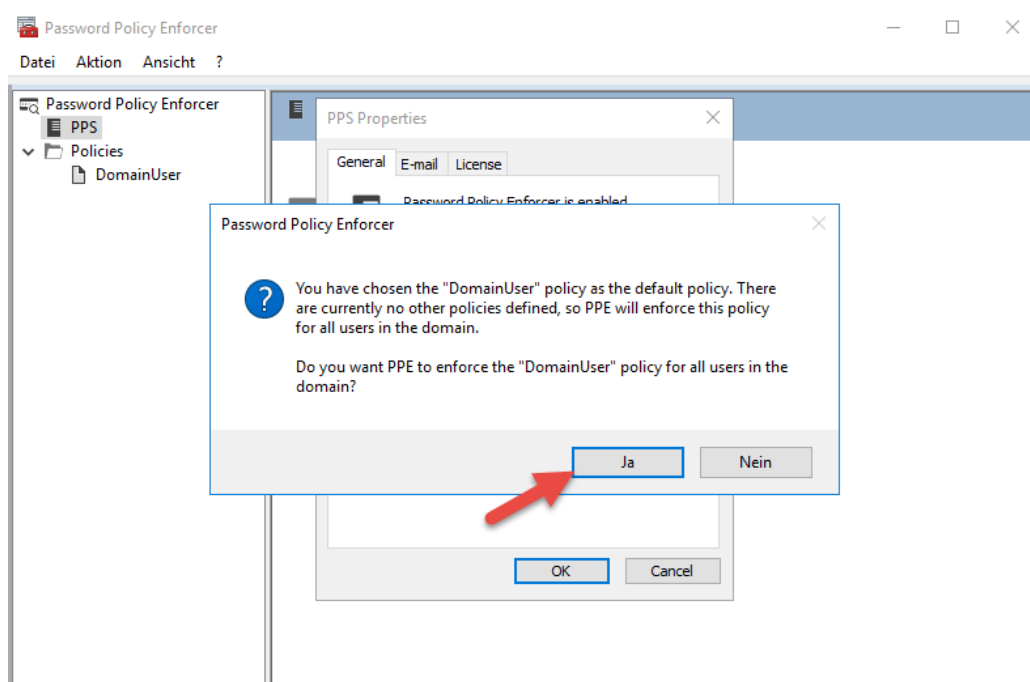
Wir könnten diese Richtlinie auch als Default Policy aktivieren und damit die alte Default Domain Policy ersetzen. Somit könnten z.B. auf Basis dieser Regel weitere folgen.



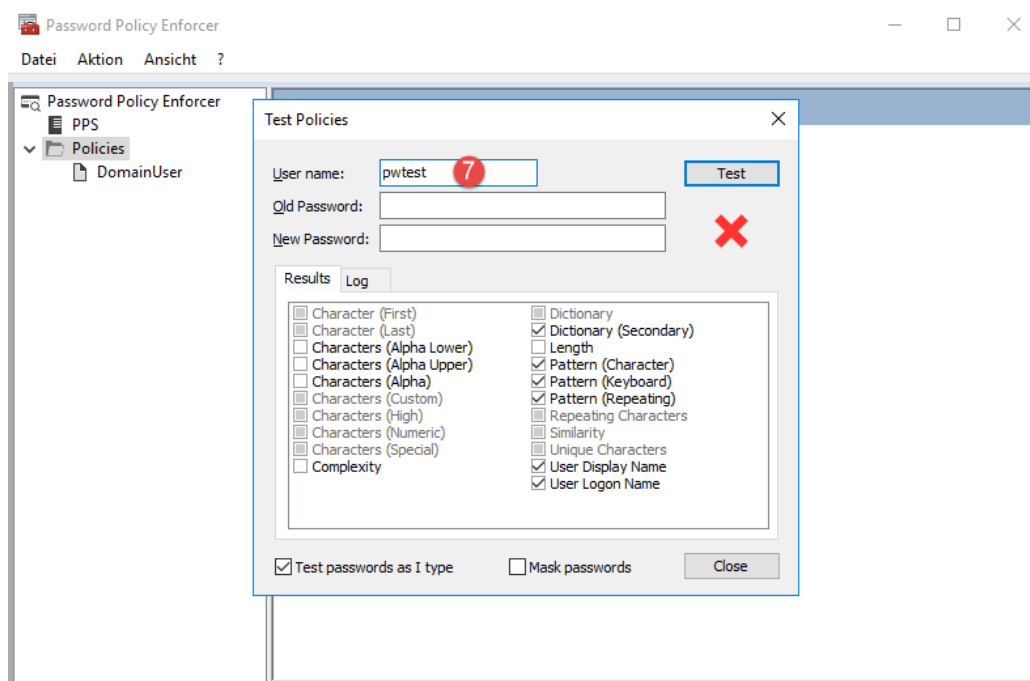


## Anixis Password Policy Enforcer

Ein Konzept sollte vorher erarbeitet worden sein.



Die neue Richtlinie lässt sich nun auch live testen.

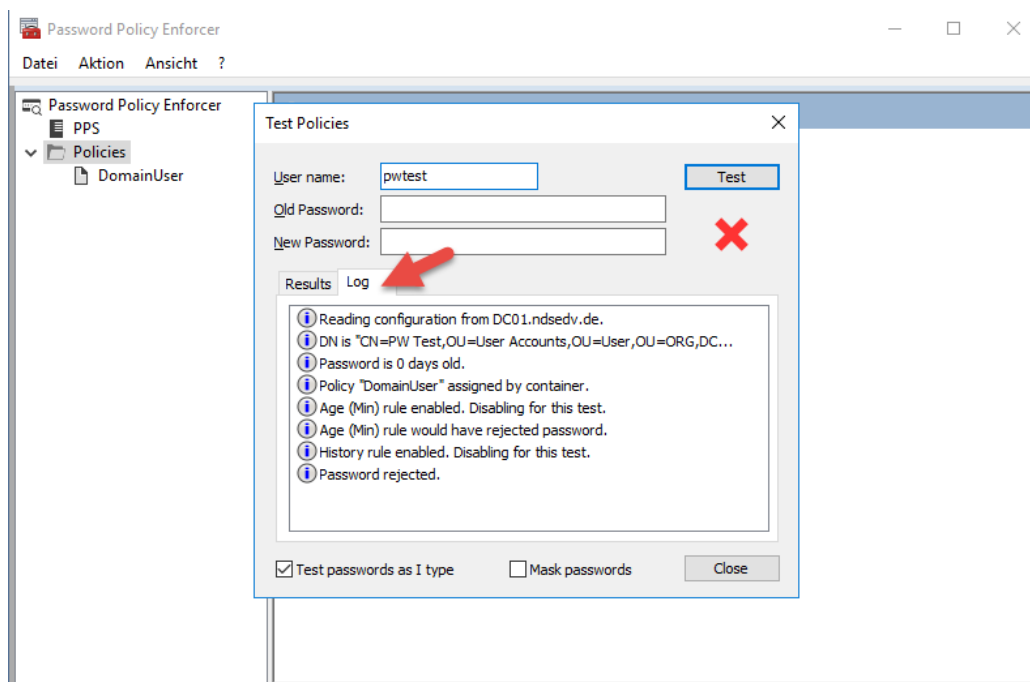






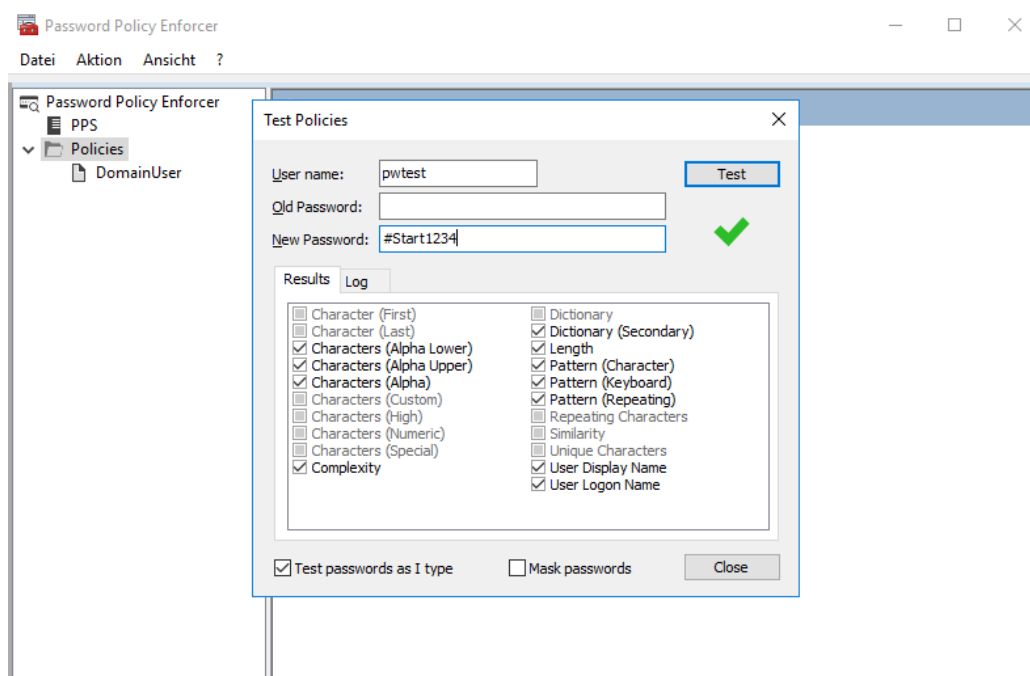
## Anixis Password Policy Enforcer

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.

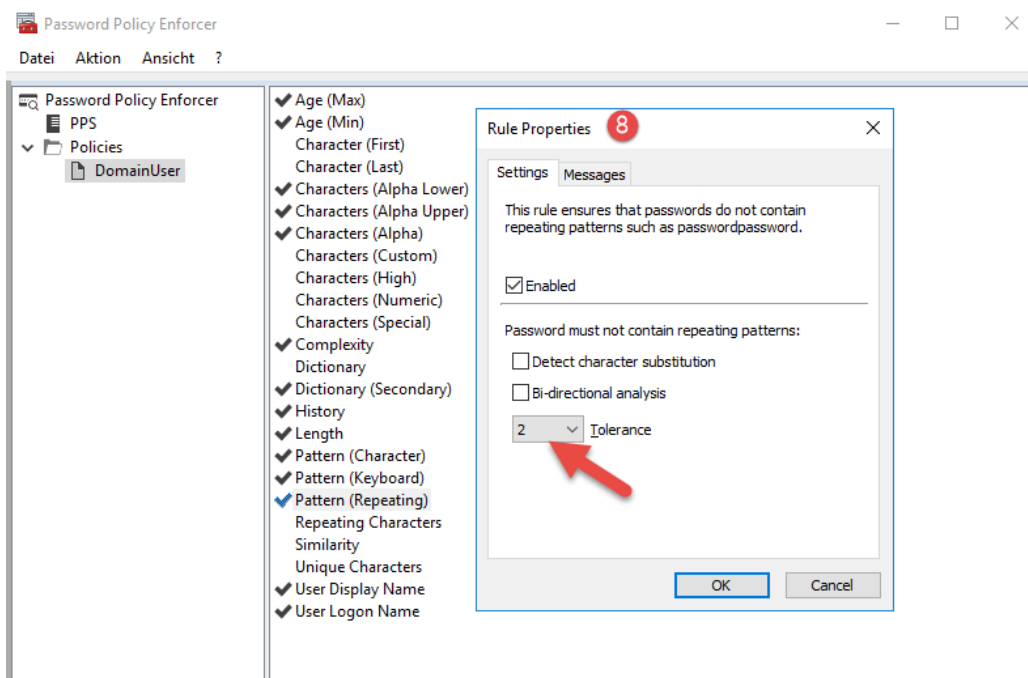
Warum dürfen 4 Zahlen hintereinandergeschrieben werden, ups, das ist nicht sicher, das müssen wir dringend ändern!



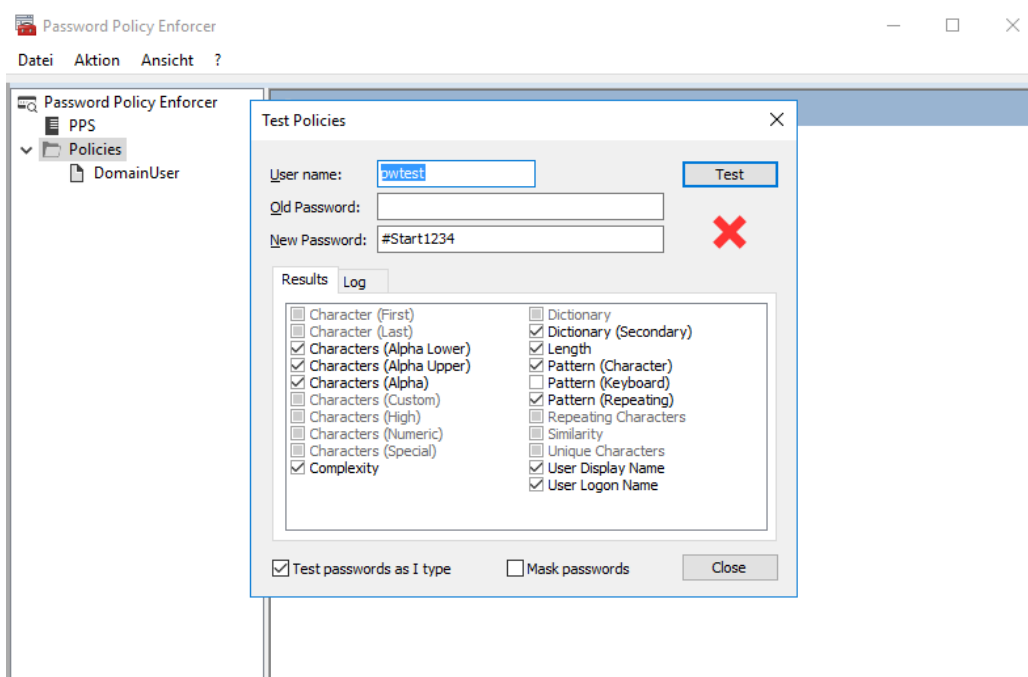


## Anixis Password Policy Enforcer

Ich ändere dafür die Pattern Toleranz von 4 auf 2.



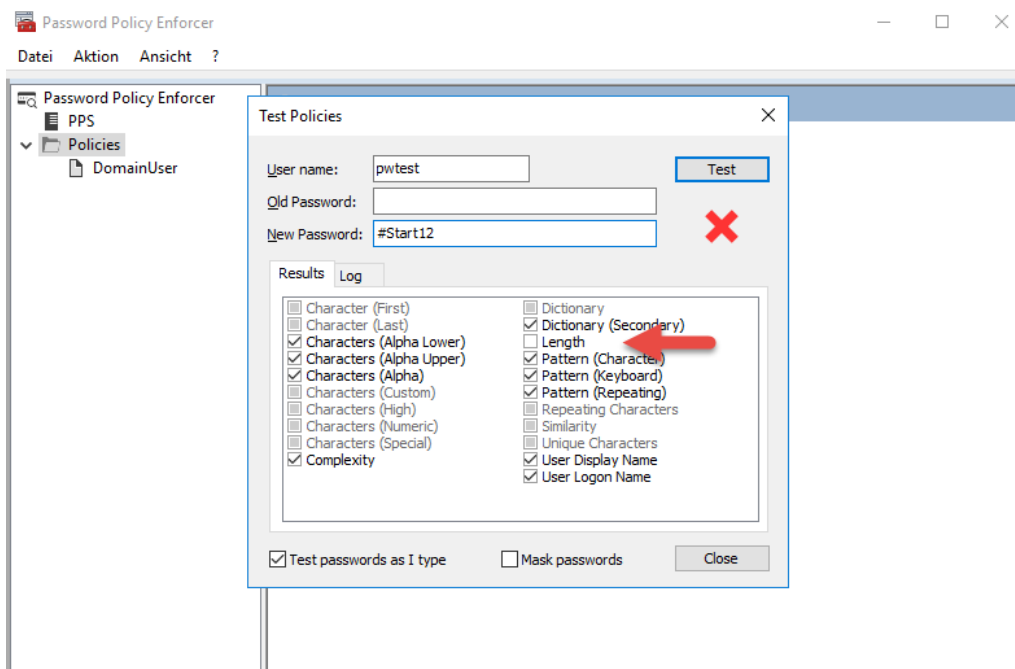
Das Passwort wird jetzt wegen der Toleranz nicht mehr akzeptiert, es sind zu viele Zahlen hintereinander, mehr als die Regel erlaubt.



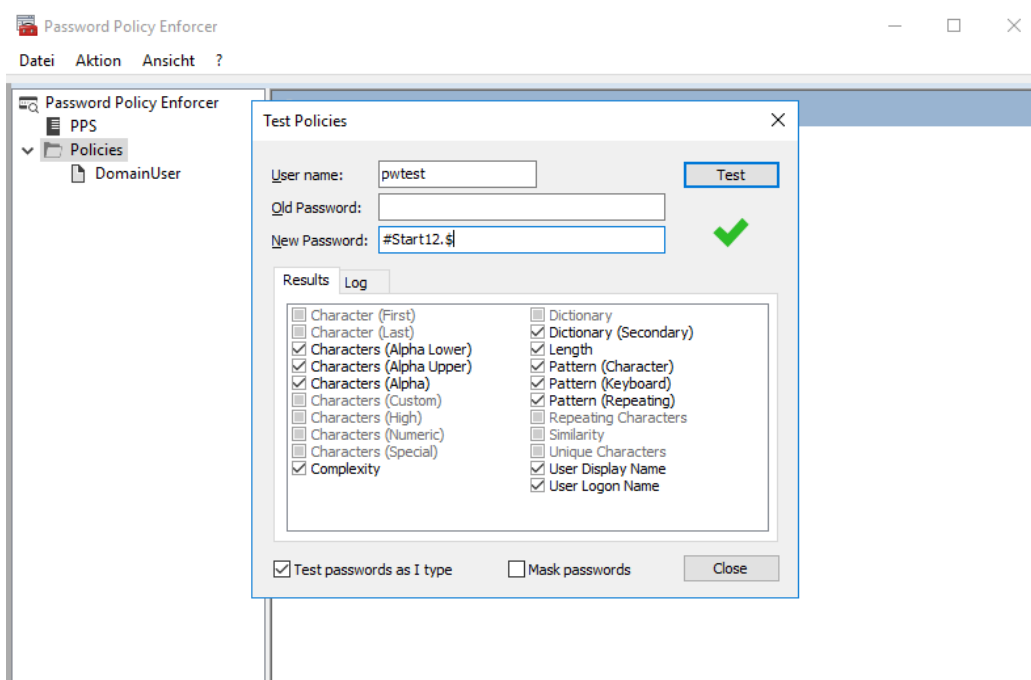


## Anixis Password Policy Enforcer

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.

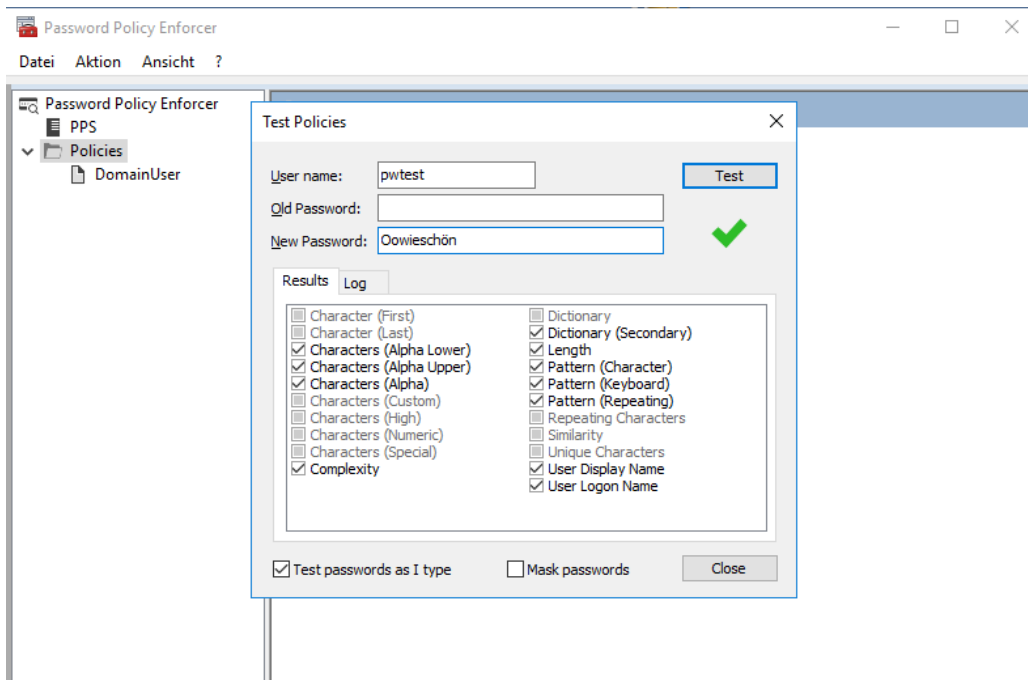




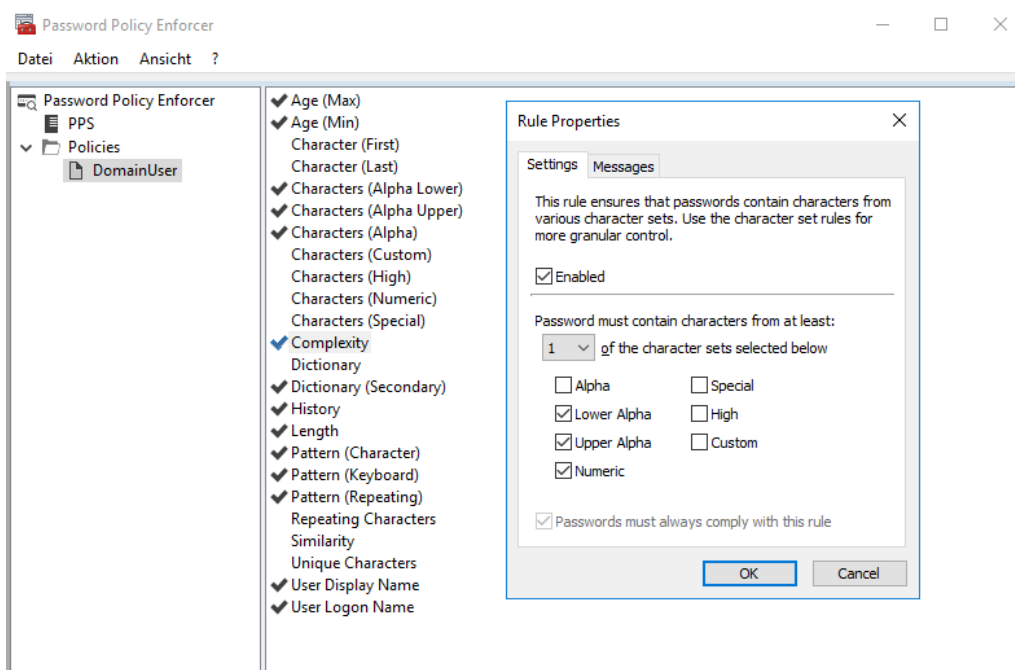
## Anixis Password Policy Enforcer

**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 Passworllänge zu erreichen.



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

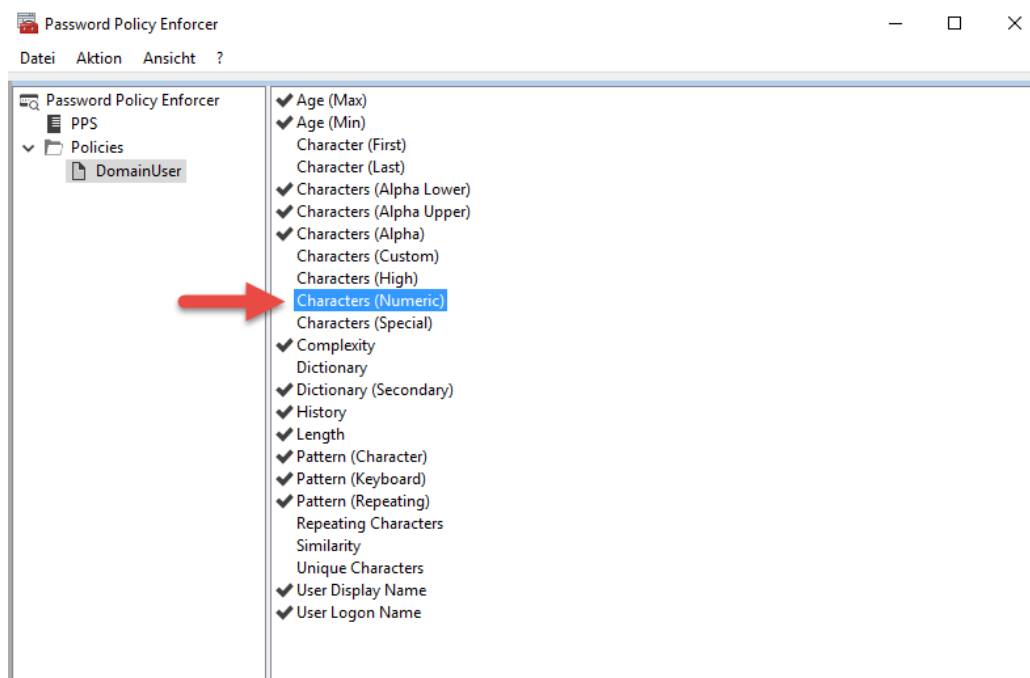


Ich hatte doch die Regel Numeric nicht aktiviert und somit werden auch keine Zahlen erwartet. ;-)

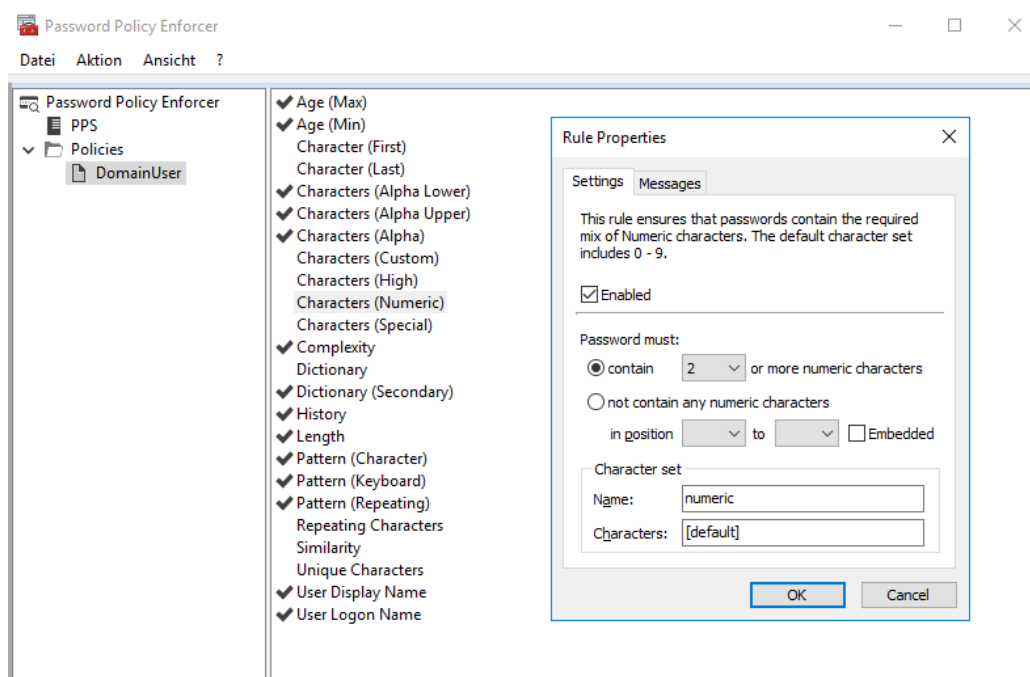


## Anixis Password Policy Enforcer

Das holen wir jetzt nach.



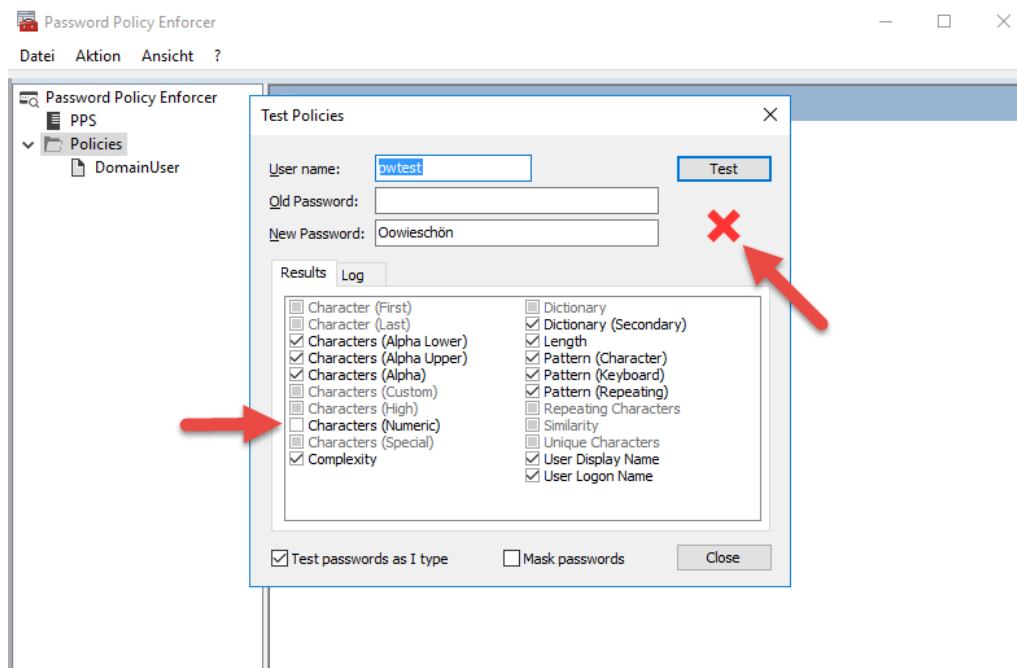
Info: Die Komplexitätsregel ist eine untergeordnete Funktion die nur dann richtig funktioniert wenn auch alle Abhängigkeiten aktiviert sind.



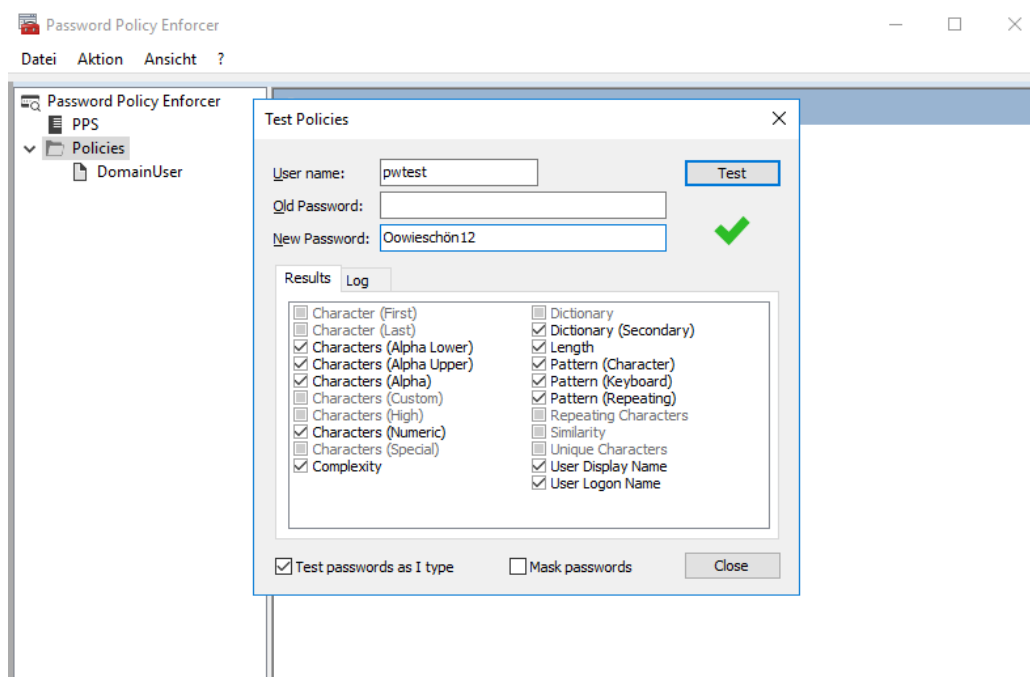


## Anixis Password Policy Enforcer

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.

Kennwort ändern

NDSEDEV\admin

.....

.....

.....

Anmelden an: NDSEDEV

[Wie melden Sie sich an einer anderen Domäne an?](#)

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

Kennwort ändern

NDSEDEV\pwadmin

Altes Kennwort

Neues Kennwort

Kennwort bestätigen

Anmelden an: NDSEDEV

[Wie melden Sie sich an einer anderen Domäne an?](#)

Komplexität :

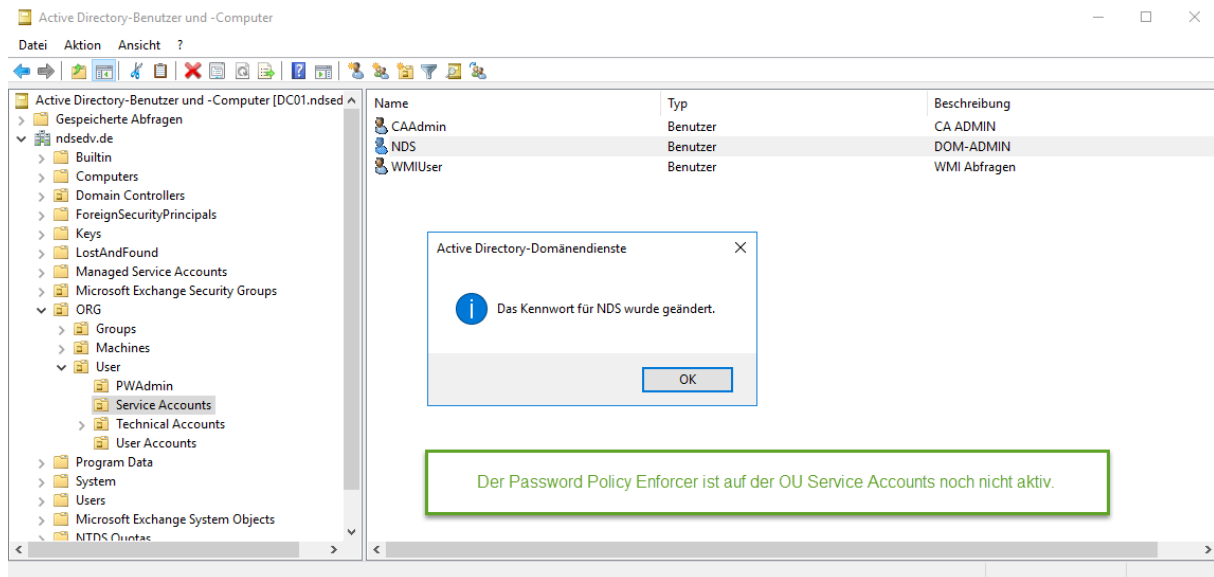
- not match one of your last 24 passwords
- not be similar to your current password
- not be similar to your logon name
- not be similar to your name
- not be similar to common passwords
- contain an upper alpha character
- contain a lower alpha character
- contain at least 2 numeric characters
- contain 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



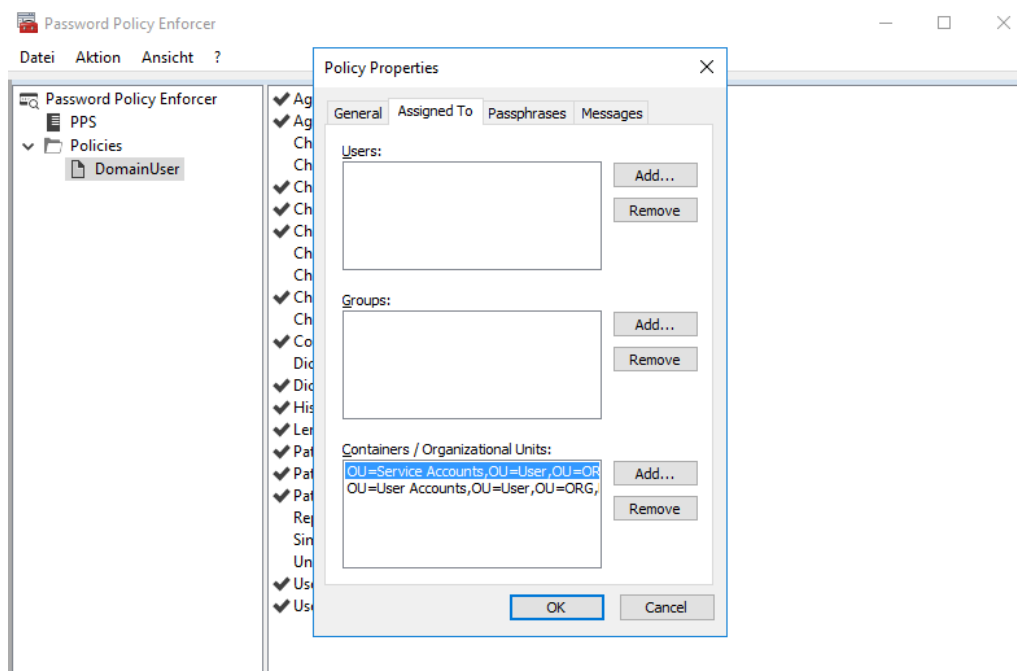


## Anixis Password Policy Enforcer

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.



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

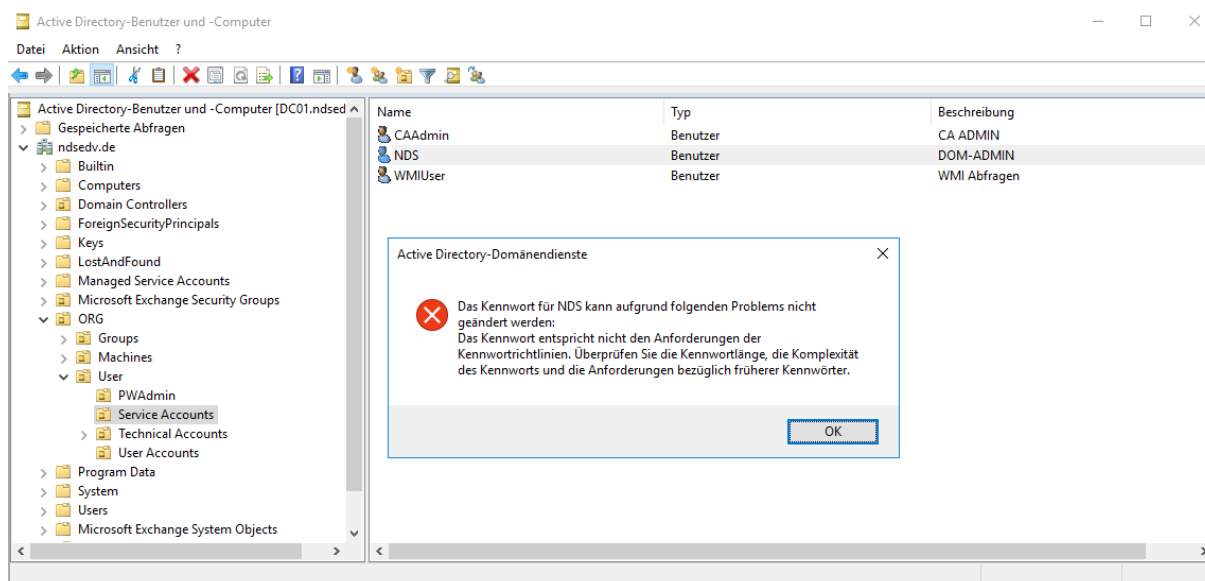




## Anixis Password Policy Enforcer

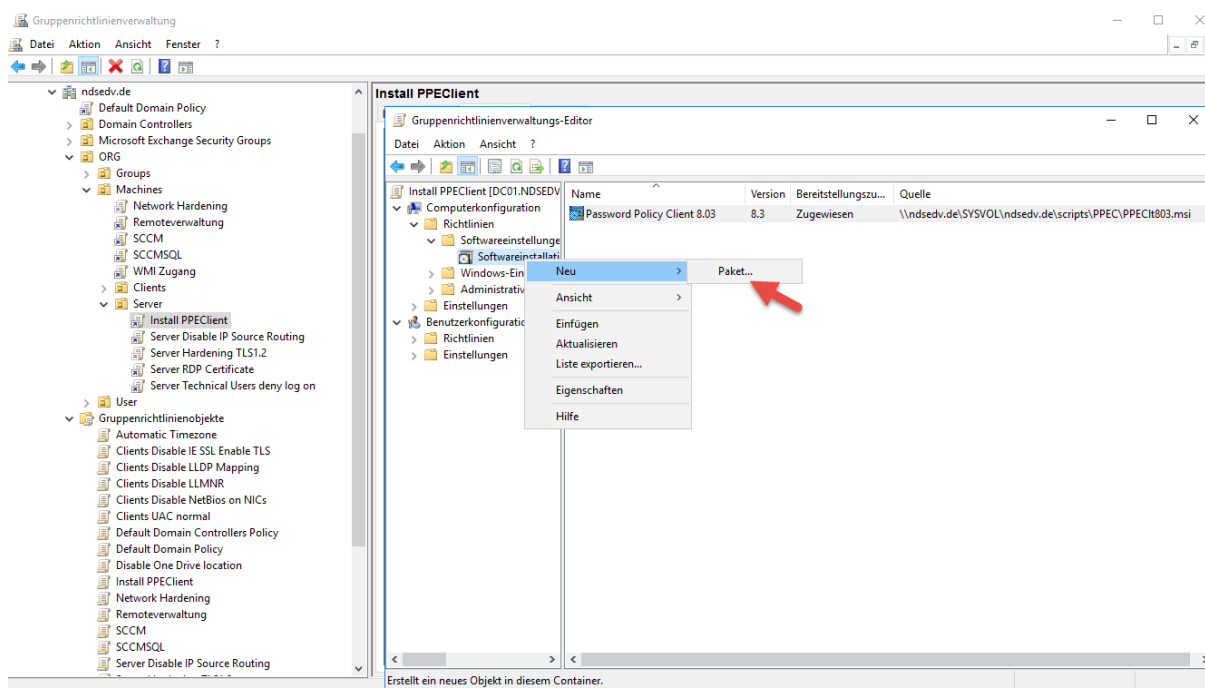
Erstaunlich. Auch der Admin hat sich an die gültige Richtlinie zu halten. TOP!

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



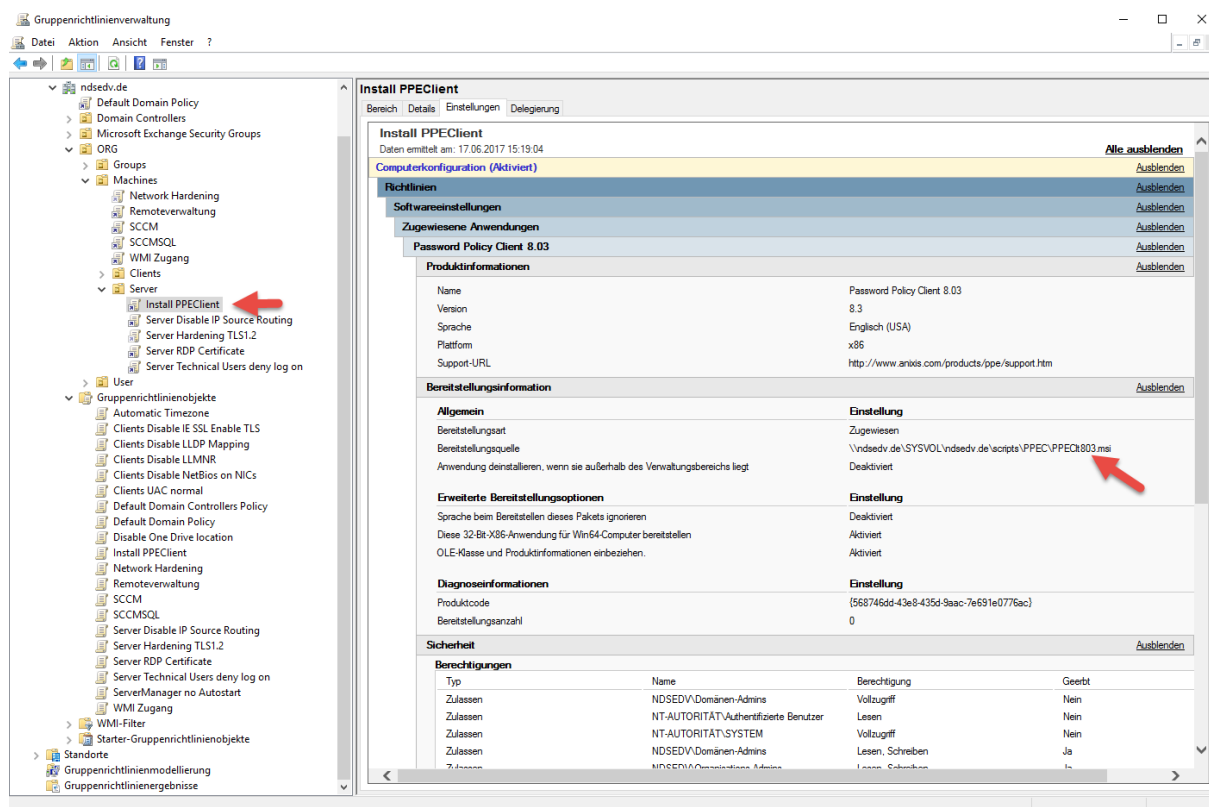
Automatische Verteilung des Client Moduls über eine Gruppenrichtlinie.  
Neue GPO erstellen und das Paket per UNC Pfad einbinden.

C:\Windows\SYSVOL\sysvol\ndsedv.de\scripts\PPEC\PPECIt803.msi

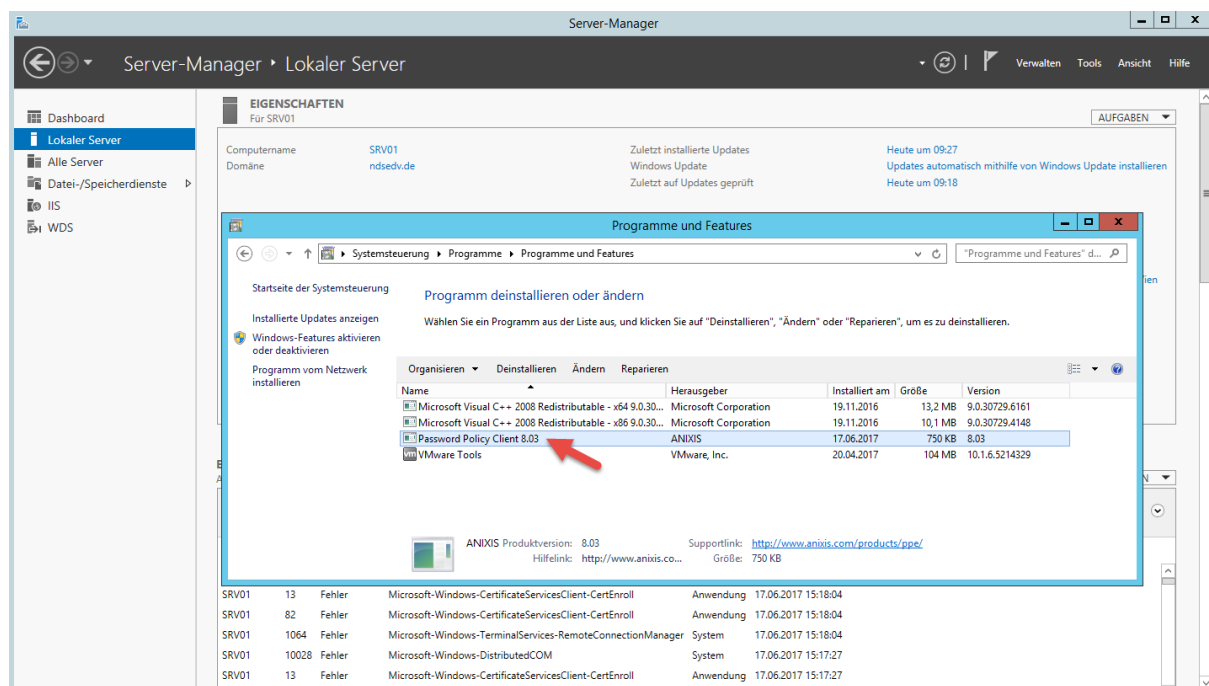




# Anixis Password Policy Enforcer



Nach einem Neustart erhalten die Clientsysteme das Paket automatisch.





# Anixis Password Policy Enforcer

## Troubleshooting:

Das Ereignisprotokoll ist sehr aussagekräftig und gibt Hinweise auf Lösungen.

Event Viewer (Ereignisanzeige) - Windows-Protokolle > System > Anwendungs- und Dienstprotokolle > Active Directory-Webdienste > Password Policy Enforcer

Anwendung	Anzahl von Ereignissen: 4/221			
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	ESNT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	105	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	102	Allgemein
Warnung	17.06.2017 12:06:28	Password Policy Enforcer	2155	Keine

**Ereignis 2108, Password Policy Enforcer**

Allgemein Details

Protokollname: Anwendung  
Quelle: Password Policy Enforcer  
Ereignis-ID: 2108  
Ebene: Warnung  
Benutzer: Nicht zutreffend  
Vorgangcode:  
Weitere Informationen: [Onlinehilfe](#)

Event Viewer (Ereignisanzeige) - Windows-Protokolle > System > Anwendungs- und Dienstprotokolle > Active Directory-Webdienste > Password Policy Enforcer

Anwendung	Anzahl von Ereignissen: 4/221			
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	ESNT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	105	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	102	Allgemein
Warnung	17.06.2017 12:06:28	Password Policy Enforcer	2155	Keine

**Ereignis 2105, Password Policy Enforcer**

Allgemein Details

Protokollname: Anwendung  
Quelle: Password Policy Enforcer  
Ereignis-ID: 2105  
Ebene: Warnung  
Benutzer: Nicht zutreffend  
Vorgangcode:  
Weitere Informationen: [Onlinehilfe](#)

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

Event Viewer (Ereignisanzeige) - Windows-Protokolle > System > Anwendungs- und Dienstprotokolle > Active Directory-Webdienste > Password Policy Enforcer

Anwendung	Anzahl von Ereignissen: 4/222			
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	ESNT	326	Allgemein
Informationen	17.06.2017 12:07:17	ESNT	105	Allgemein
Informationen	17.06.2017 12:06:28	Password Policy Enforcer	2155	Keine

**Ereignis 2155, Password Policy Enforcer**

Allgemein Details

Protokollname: Anwendung  
Quelle: Password Policy Enforcer  
Ereignis-ID: 2155  
Ebene: Warnung  
Benutzer: Nicht zutreffend  
Vorgangcode:  
Weitere Informationen: [Onlinehilfe](#)

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](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=ndsedv,DC=de"
Verbindung mit "DC01.ndsedv.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.

The 'Rule Properties' dialog box has two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active. It contains the following text: 'This rule ensures that passwords do not contain character patterns such as abcde.' Below this is a checked checkbox labeled 'Enabled'. A horizontal line separates this from the section 'Password must not contain character patterns:', which contains two unchecked checkboxes: 'Detect character substitution' and 'Bi-directional analysis'. Below these is a dropdown menu showing '4' and the label 'Tolerance'. At the bottom right is a button labeled 'Character Patterns'. At the very bottom are 'OK' and 'Cancel' buttons.

The 'Character Patterns' dialog box has a title bar with a close button. It contains the text 'Select enabled character patterns' above a list box. The list box contains two items, both with checked checkboxes: 'English Alphabet (a-z)' and 'Numerals (0-9)'. At the bottom are 'OK' and 'Cancel' buttons.



## 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.

The screenshot shows the 'Rule Properties' dialog box for the Complexity rule. The 'Settings' tab is active. The rule is enabled. The description states: 'This rule ensures that passwords contain characters from various character sets. Use the character set rules for more granular control.' The configuration shows '1' of the character sets selected below. The selected character sets are: Lower Alpha, Upper Alpha, Numeric, Special, and High. The 'Alpha' and 'Custom' options are not selected. A checkbox at the bottom indicates 'Passwords must always comply with this rule' is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

### 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.

The screenshot shows the 'Rule Properties' dialog box for the Dictionary rule. The 'Settings' tab is active. The rule is enabled. The description states: 'This rule ensures that passwords are not vulnerable to a dictionary cracking attack.' The configuration shows 'Password must not exist in dictionary file:' with several options: 'Detect inclusion of non-alpha characters' (checked), 'Detect character substitution' (unchecked), 'Bi-directional analysis' (unchecked), and 'Wildcard analysis' (unchecked). A 'Tolerance' dropdown is set to '4'. The 'Dictionary file' path is 'C:\Program Files (x86)\Password Policy Enforcer\my'. There are 'Sort' and 'Browse' buttons next to the path. The 'OK' and 'Cancel' buttons are at the bottom right.



## 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.

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The title bar says 'Rule Properties' with a close button. Inside, there are two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active and contains the following text: 'This rule ensures that passwords begin with an appropriate character.' Below this is a checkbox labeled 'Enabled' which is checked. Further down, it says 'Password must:' followed by two radio buttons: 'begin' (selected) and 'not begin'. Below the radio buttons is the text 'with a character from the selected character sets'. There are seven checkboxes for character sets: 'Alpha', 'Lower Alpha', 'Upper Alpha', 'Numeric', 'Special' (checked), 'High', and 'Custom'. At the bottom are 'OK' and 'Cancel' buttons.

History:

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

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The title bar says 'Rule Properties' with a close button. Inside, there are two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active and contains the following text: 'This rule ensures that passwords are not the same as a recently used password.' Below this is a checkbox labeled 'Enabled' which is checked. Further down, it says 'Password must not be the same as:' followed by two radio buttons: 'one of the last' (selected) and 'a password used in the last'. The 'one of the last' option has a dropdown menu showing '24' and the text 'passwords'. The 'a password used in the last' option has a text input field showing '365' and the text 'days'. At the bottom, there is an unchecked checkbox labeled 'Enforce this rule when a password is reset'. At the bottom are 'OK' and 'Cancel' buttons.





## 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!

The 'Rule Properties' dialog box has two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active. It contains the following information:

- A description: "This rule ensures that passwords do not contain keyboard patterns such as qwerty."
- An 'Enabled' checkbox, which is checked.
- A section titled 'Password must not contain:' with a dropdown menu set to 'Horizontal' and the text 'keyboard patterns'.
- Three checkboxes for detection options:
  - ☐ Detect direction change
  - ☒ Detect key repeat
  - ☐ Detect key skip
- A 'Tolerance' dropdown menu set to '2'.
- A 'Keyboard Layouts' button.
- 'OK' and 'Cancel' buttons at the bottom.

The 'Keyboard Layouts' dialog box has a title bar with a close button. It contains the following information:

- A title: "Select enabled keyboard layouts:"
- A list of keyboard layouts with checkboxes:
  - ☐ Canadian French
  - ☐ French
  - ☐ United Kingdom
  - ☒ United States
  - ☐ United States International
- 'OK' and 'Cancel' buttons at the bottom.



## Anixis Password Policy Enforcer

Last Character:

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

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The title bar says 'Rule Properties' with a close button. Inside, there are two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active and contains the following text: 'This rule ensures that passwords end with an appropriate character.' Below this is a checkbox labeled 'Enabled' which is checked. Further down, it says 'Password must:' followed by two radio buttons: 'end' (which is selected) and 'not end'. Below these is the text 'with a character from the selected character sets'. There are seven checkboxes for character sets: 'Alpha', 'Lower Alpha', 'Upper Alpha', 'Numeric' (which is checked), 'Special', 'High', and 'Custom'. At the bottom are 'OK' and 'Cancel' buttons.

Length:

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

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The title bar says 'Rule Properties' with a close button. Inside, there are two tabs: 'Settings' and 'Messages'. The 'Settings' tab is active and contains the following text: 'This rule ensures that passwords meet the minimum and maximum length requirements.' Below this is a checkbox labeled 'Enabled' which is checked. Further down, it says 'Password must contain:'. There are four radio button options: 'at least' (selected) with a dropdown menu showing '10' and the text 'characters'; 'no more than' with a dropdown menu and the text 'characters'; 'between' with two dropdown menus and the text 'and characters'; and 'exactly 7 or 14 characters'. At the bottom are 'OK' and 'Cancel' buttons.



## 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.

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The 'E-mail' sub-tab is also visible. The text inside reads: 'This rule ensures that passwords are changed regularly to increase their effectiveness.' Below this is a checked checkbox labeled 'Enabled'. The main configuration section is titled 'User must change password after:'. It contains three dropdown menus: the first is set to '42' with the unit 'days', the second is set to '60' with the unit 'days' and the text 'if the password contains', and the third is set to '20' with the unit 'or more characters'. Below this is a 'Mode' dropdown menu set to 'Standard'. A note at the bottom of the configuration area says: 'Use the Transitional and Warning modes to gradually introduce this rule. Switch to Standard mode after the introductory period.' At the bottom of the dialog are 'OK' and 'Cancel' buttons.

### 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.

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The 'Messages' sub-tab is also visible. The text inside reads: 'This rule ensures that passwords are used for a minimum duration, stopping users from quickly cycling through a series of passwords.' Below this is a checked checkbox labeled 'Enabled'. The main configuration section is titled 'User cannot change password for at least:'. It contains a dropdown menu set to '1' with the unit 'days'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.



## Anixis Password Policy Enforcer

### Repeating Characters:

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

Rule Properties

Settings Messages

This rule ensures that passwords do not contain repeating character patterns such as aaaa.

☒ Enabled

Password must not contain more than:

3 consecutive repeating characters

OK Cancel

### 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).

Rule Properties

Settings Messages

This rule ensures that passwords do not contain repeating patterns such as passwordpassword.

☒ Enabled

Password must not contain repeating patterns:

☐ Detect character substitution

☐ Bi-directional analysis

2 Tolerance

OK Cancel



## 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.

Rule Properties

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

### Unique Character:

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

Rule Properties

Settings Messages

This rule ensures that passwords contain a minimum number of unique characters.

☒ Enabled

Password must contain at least:

5 unique characters

OK Cancel



## 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.

Rule Properties

Settings Messages

This rule ensures that passwords are not similar to a user's display name.

☒ Enabled

Password must not be similar to user display name:

☐ Detect character substitution

☐ Bi-directional analysis

4 Tolerance

OK Cancel

User Logon Name.

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

Rule Properties

Settings Messages

This rule ensures that passwords are not similar to a user's logon name.

☒ Enabled

Password must not be similar to user logon name:

☐ Detect character substitution

☐ Bi-directional analysis

4 Tolerance

OK Cancel



## Anixis Password Policy Enforcer

Meine empfohlenen Einstellungen:

Age Max:

Rule Properties

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

Age Min:

Rule Properties

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

Character (Alpha Lower):

The screenshot shows the 'Rule Properties' dialog box for the 'Alpha Lower' rule. The 'Settings' tab is active. The rule is enabled. The 'Password must:' section has the 'contain' radio button selected, with a value of '1' in the dropdown. The 'Character set' section has 'Name' set to 'lower alpha' and 'Characters' set to '[default]'. The 'OK' button is highlighted.

Rule Properties

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 1 or more lower alpha characters

☐ not contain any lower alpha characters

in position to ☐ Embedded

Character set

Name: lower alpha

Characters: [default]

OK Cancel

Character (Alpha Upper):

The screenshot shows the 'Rule Properties' dialog box for the 'Alpha Upper' rule. The 'Settings' tab is active. The rule is enabled. The 'Password must:' section has the 'contain' radio button selected, with a value of '1' in the dropdown. The 'Character set' section has 'Name' set to 'upper alpha' and 'Characters' set to '[default]'. The 'OK' button is highlighted.

Rule Properties

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 1 or more upper alpha characters

☐ not contain any upper alpha characters

in position to ☐ Embedded

Character set

Name: upper alpha

Characters: [default]

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 2 or more numeric characters

☐ not contain any numeric characters

in position to ☐ Embedded

Character set

Name: numeric

Characters: [default]

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:

1 of the character sets selected below

☐ Alpha ☒ Special

☒ Lower Alpha ☐ High

☒ Upper Alpha ☐ Custom

☒ Numeric

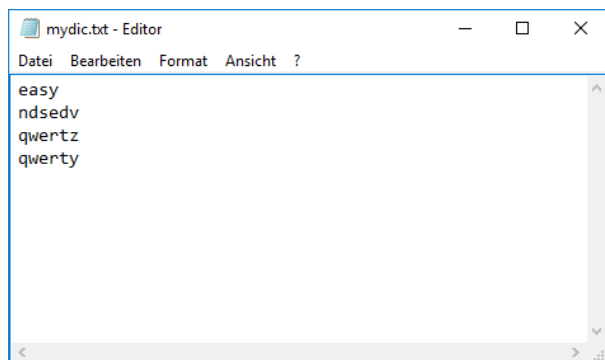
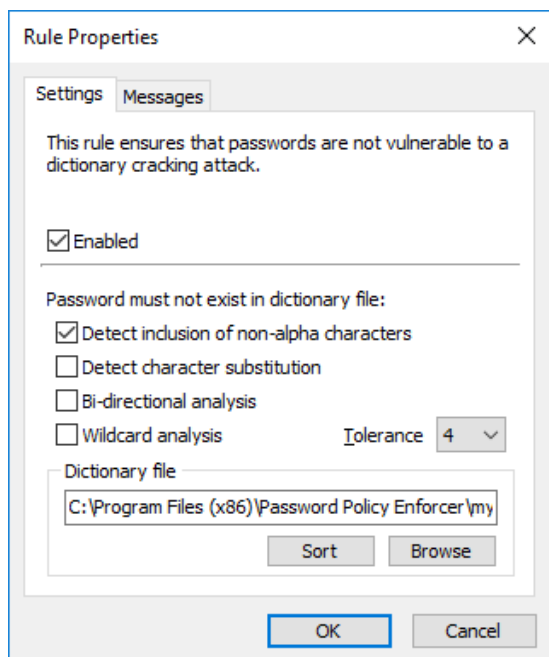
☒ Passwords must always comply with this rule

OK Cancel

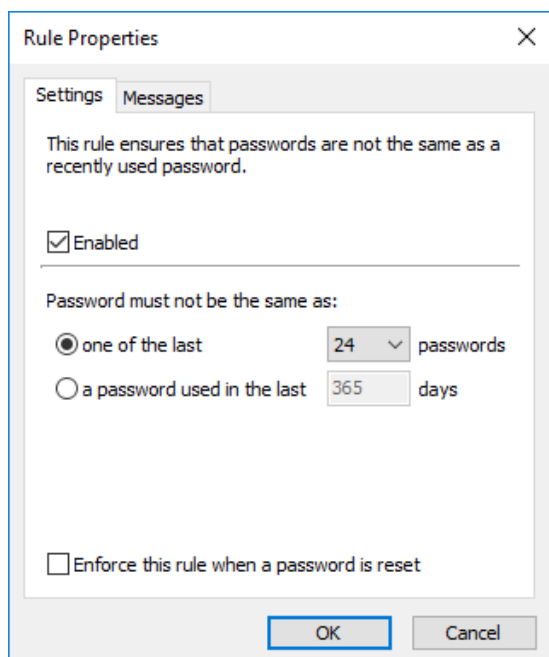


## Anixis Password Policy Enforcer

Dictionary:



History:





## Anixis Password Policy Enforcer

Length:

Rule Properties

Settings Messages

This rule ensures that passwords meet the minimum and maximum length requirements.

☒ Enabled

Password must contain:

☒ at least 10 characters

☐ no more than characters

☐ between and characters

☐ exactly 7 or 14 characters

OK Cancel

Pattern (Keyboard):

Rule Properties

Settings Messages

This rule ensures that passwords do not contain keyboard patterns such as qwerty.

☒ Enabled

Password must not contain:

Horizontal keyboard patterns

☐ Detect direction change

☒ Detect key repeat

☐ Detect key skip

2 Tolerance

Keyboard Layouts

OK Cancel



## Anixis Password Policy Enforcer

Pattern (Repeating):

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The 'Messages' tab is also visible. The text inside the dialog reads: 'This rule ensures that passwords do not contain repeating patterns such as passwordpassword.' Below this, there is a checkbox labeled 'Enabled' which is checked. Underneath, it says 'Password must not contain repeating patterns:'. There are two unchecked checkboxes: 'Detect character substitution' and 'Bi-directional analysis'. Below these is a dropdown menu showing the number '2' and the word 'Tolerance'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Repeating Characters:

The screenshot shows the 'Rule Properties' dialog box with the 'Settings' tab selected. The 'Messages' tab is also visible. The text inside the dialog reads: 'This rule ensures that passwords do not contain repeating character patterns such as aaaa.' Below this, there is a checkbox labeled 'Enabled' which is checked. Underneath, it says 'Password must not contain more than:'. There is a dropdown menu showing the number '3' followed by the text 'consecutive repeating characters'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.



## Anixis Password Policy Enforcer

Similarity:

Rule Properties

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

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

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