Anixis Password Policy Enforcer

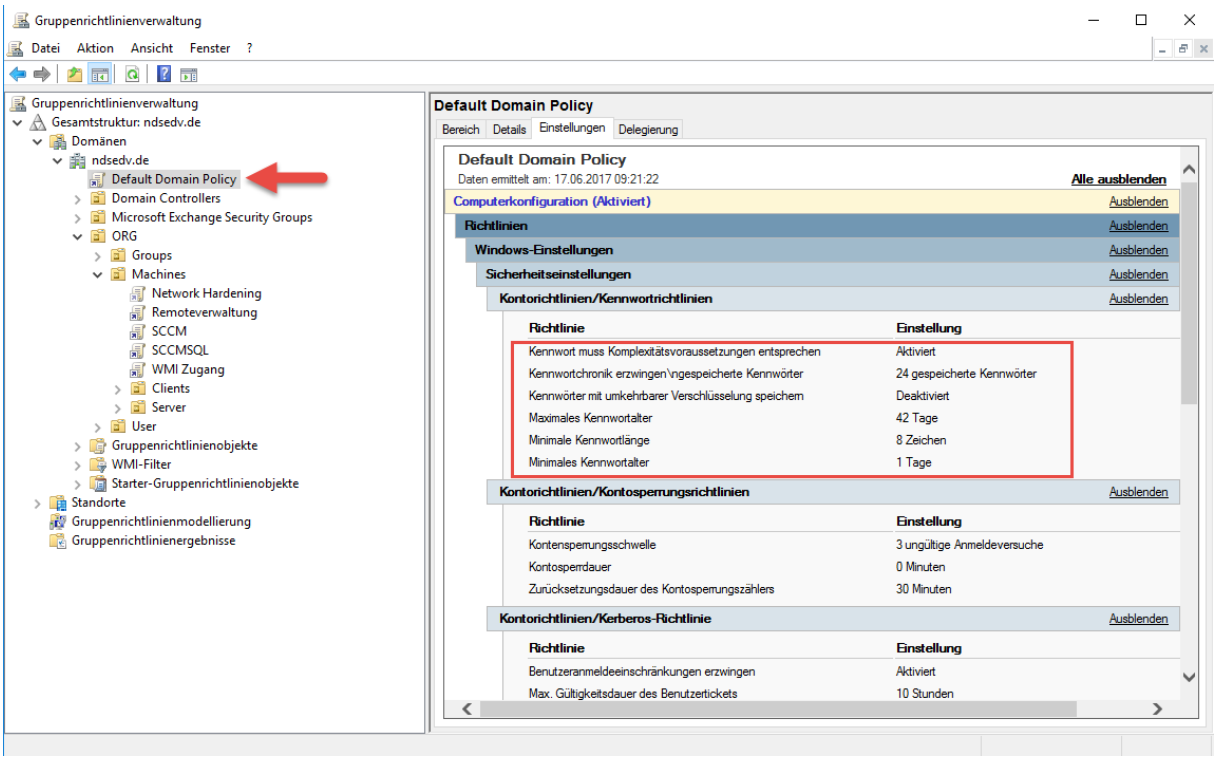
Die aktuellen Anforderungen an ein starkes Passwort kann über die Default Domain Policy nicht mehr erreicht werden.

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:

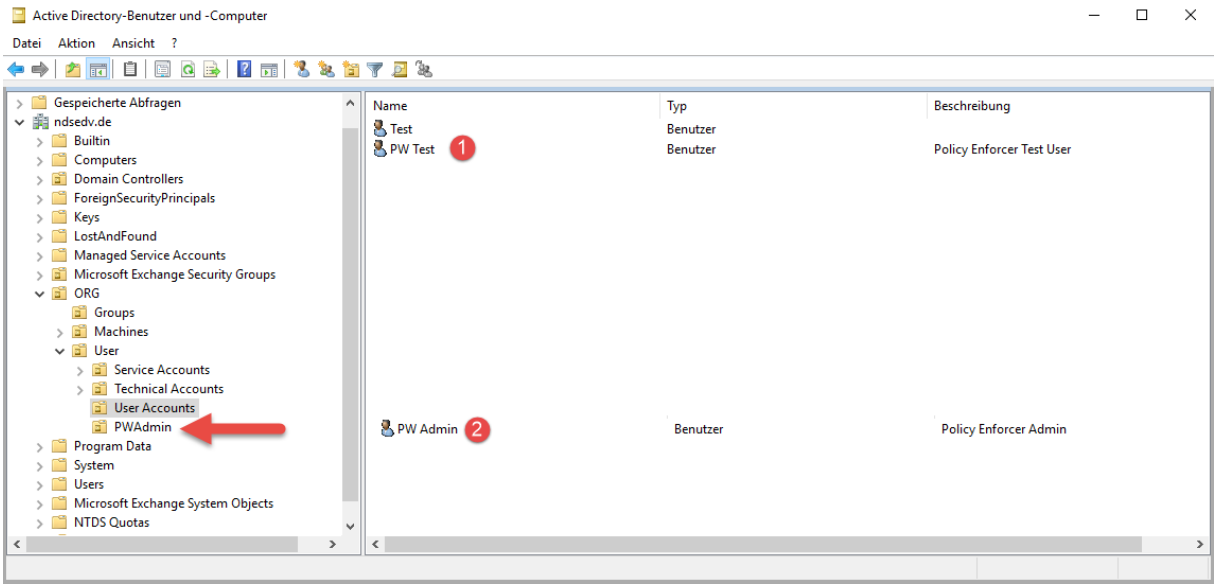


Der Grund liegt in der Erfüllung der Richtlinien. Wenn 2 Richtlinien aktiv sind, so muss das eingerichtete/geänderte Passwort einmal der Richtlinie der DDP entsprechen so wie der des Password Policy Enforcers. Wenn jedoch die Einstellungen der DDP in das PPE Regelwerk übernommen werden und diese sich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

Ein Hinweis am Rande:

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

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

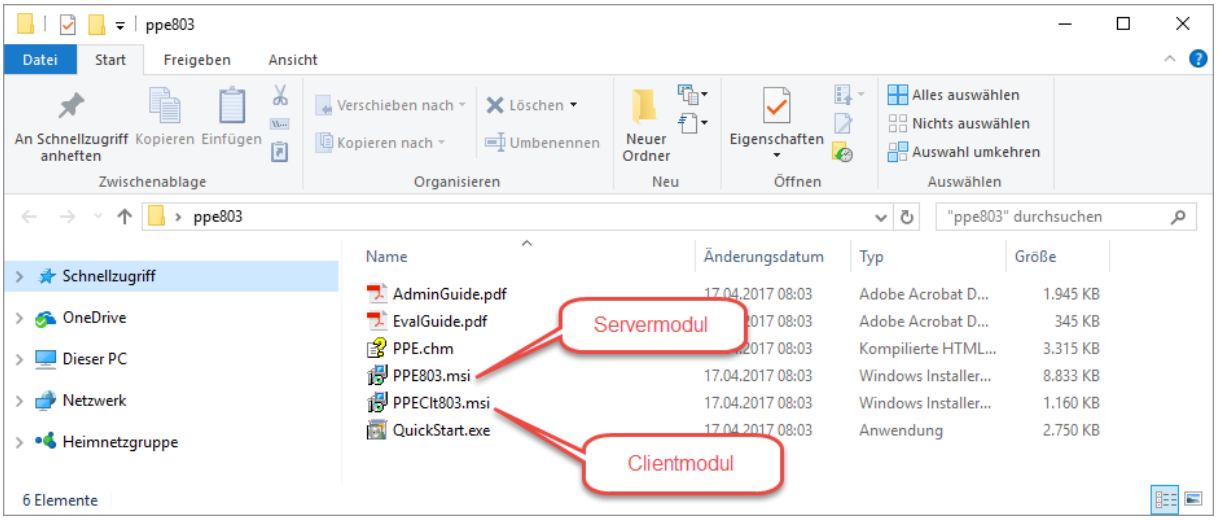
The Password Policy Server responds by sending a datagram with the following attributes back to the Password Policy Client:

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

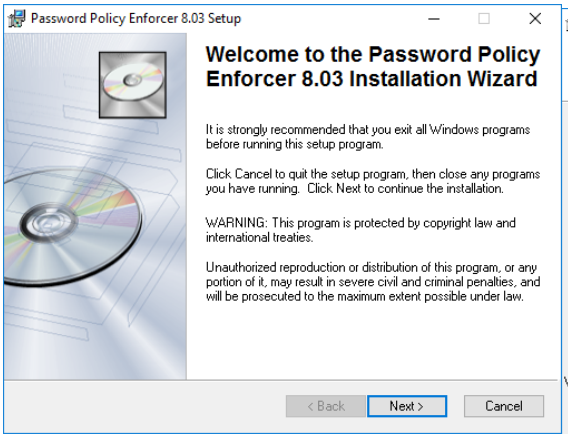
Ich habe das Installation Paket mal zur Veranschaulichung extrahiert um zu zeigen was alles enthalten ist.

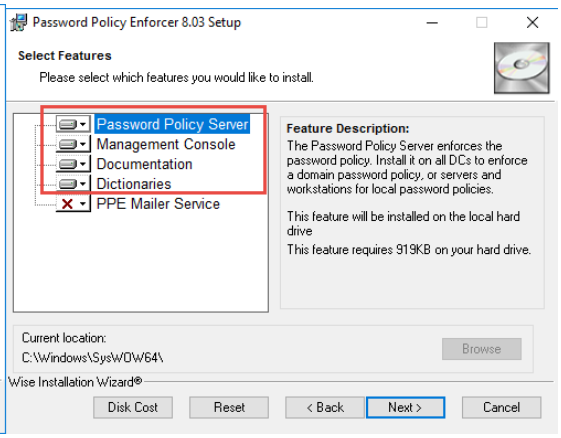


Systemanforderungen:

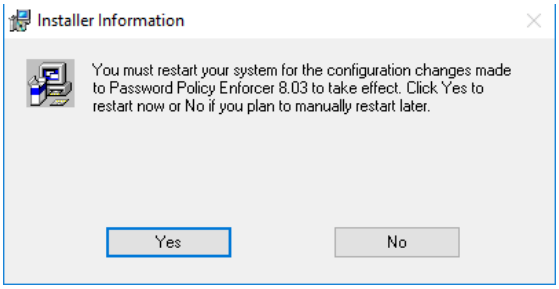
- Windows Server 2003 > Windows Server 2016
- Windows XP > Windows 10
- 15 MB Festplattenplatz
- 4 MB RAM

Als erstes installieren wir das Servermodul auf den Domain Controllern.





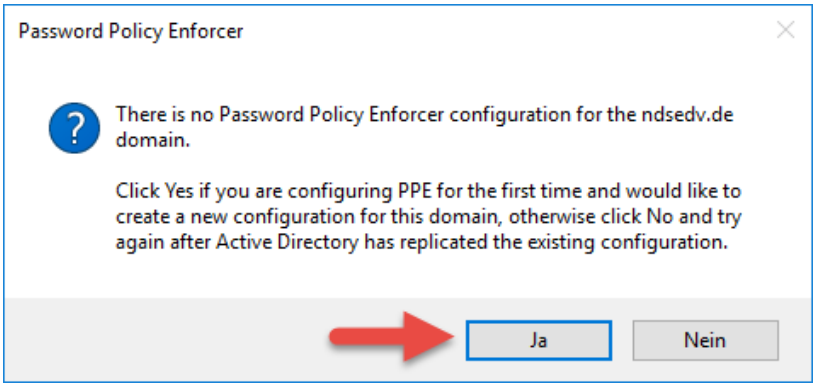
Der PPE Mailer ist ein Service um die User an die bevorstehende Passwortänderung zu informieren.



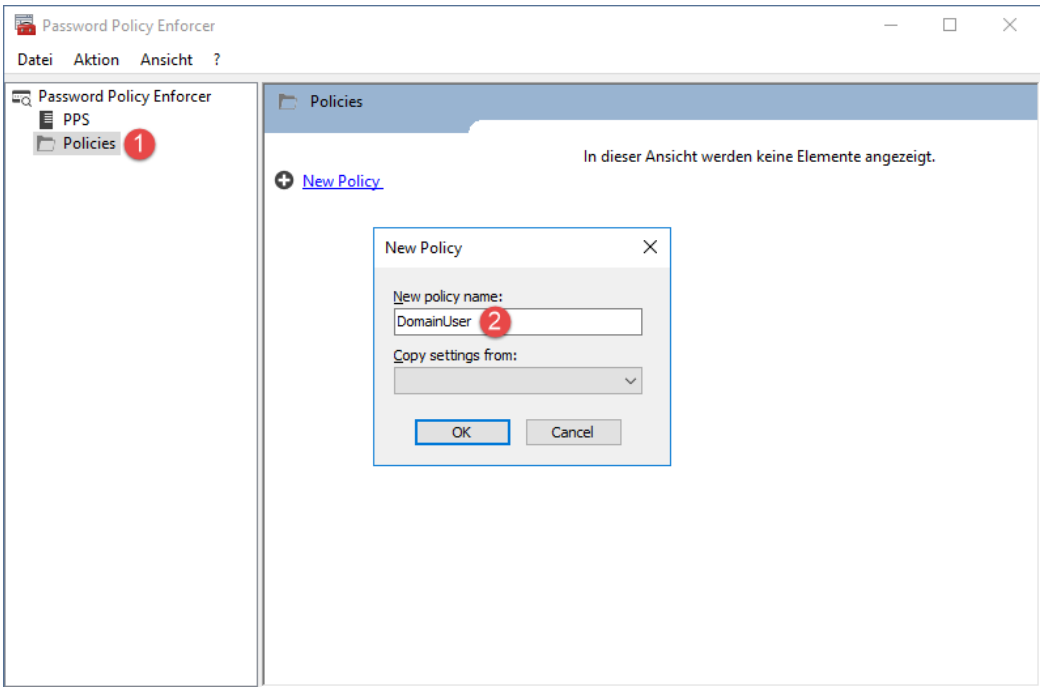
Der Neustart ist zwingend notwendig!

Anixis Password Policy Enforcer

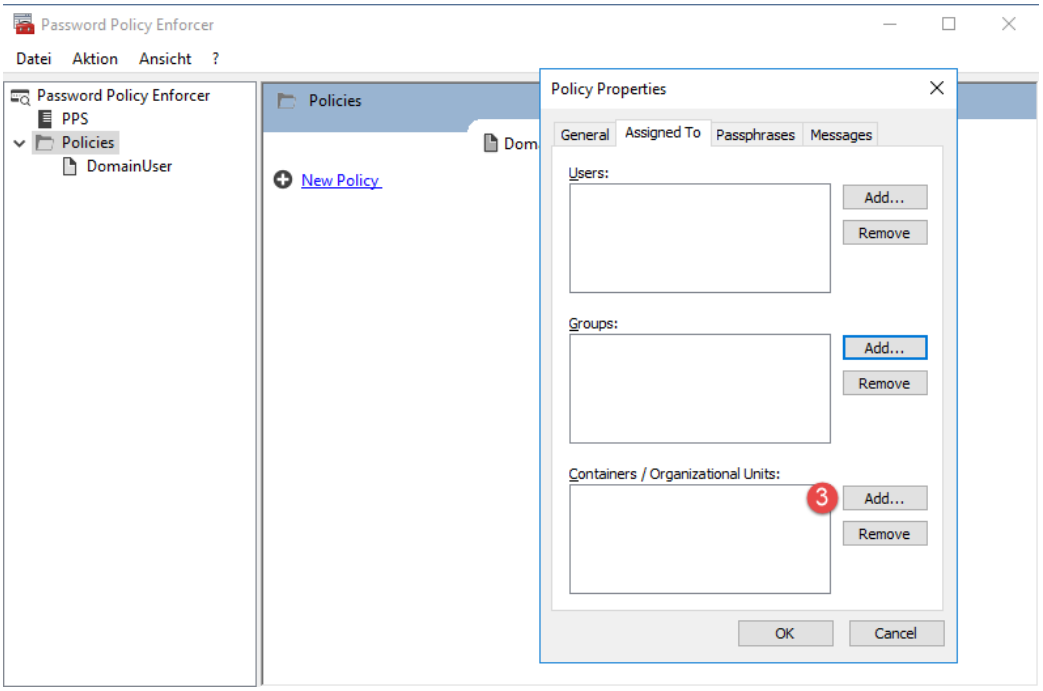
Nach dem Neustart starten wir den Password Policy Enforcer und erstellen als erstes eine neue Regel (Set).



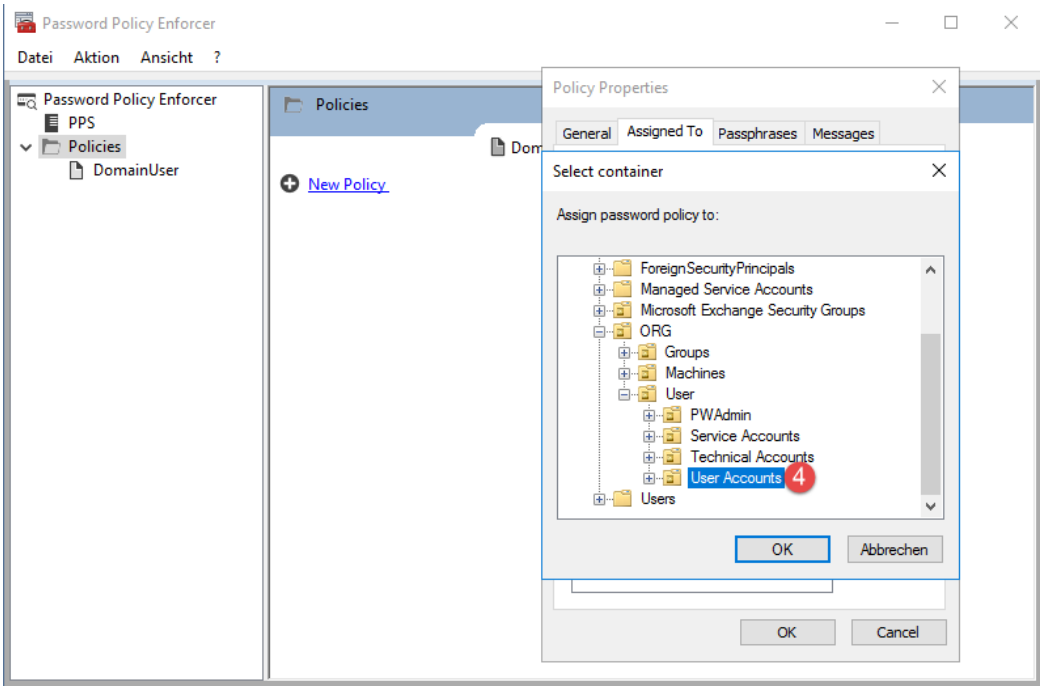
Eine erstellte Regel kann entweder auf einen User, einer Gruppe oder auf eine OU angewendet werden. Es können maximal 256 Regeln erstellet werden.



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

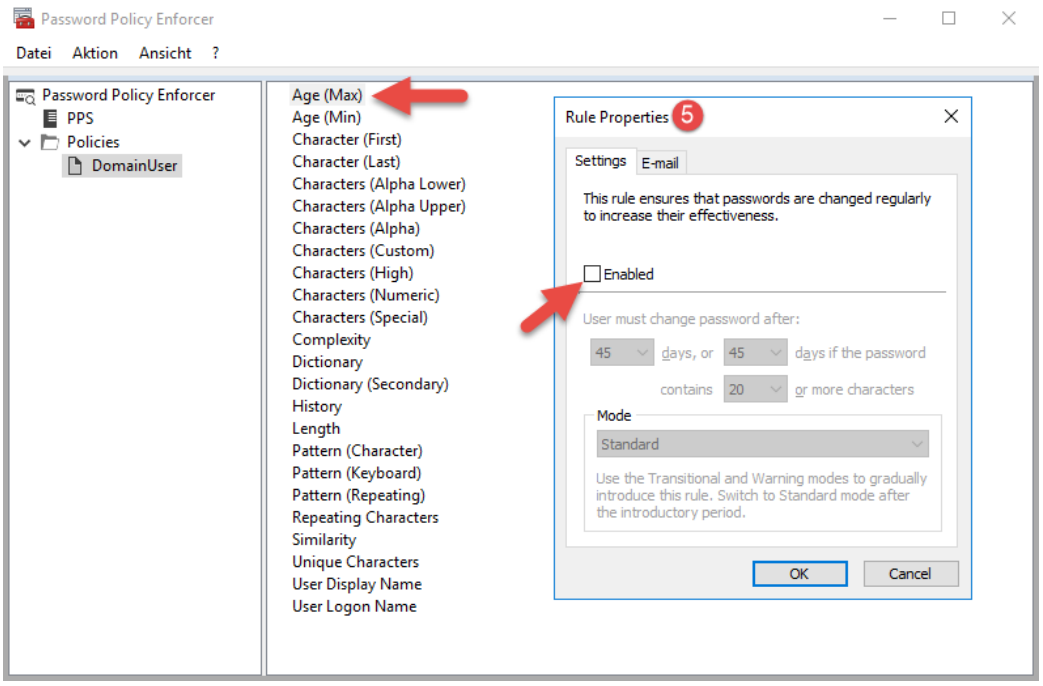


ADD > OU auswählen > OK

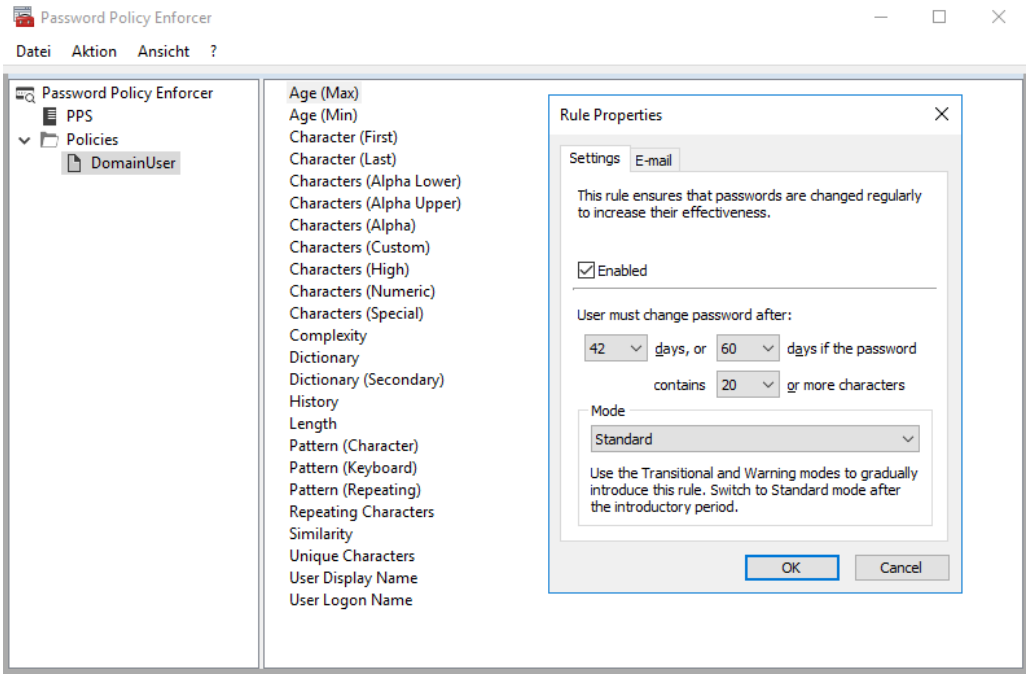


Anixis Password Policy Enforcer

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

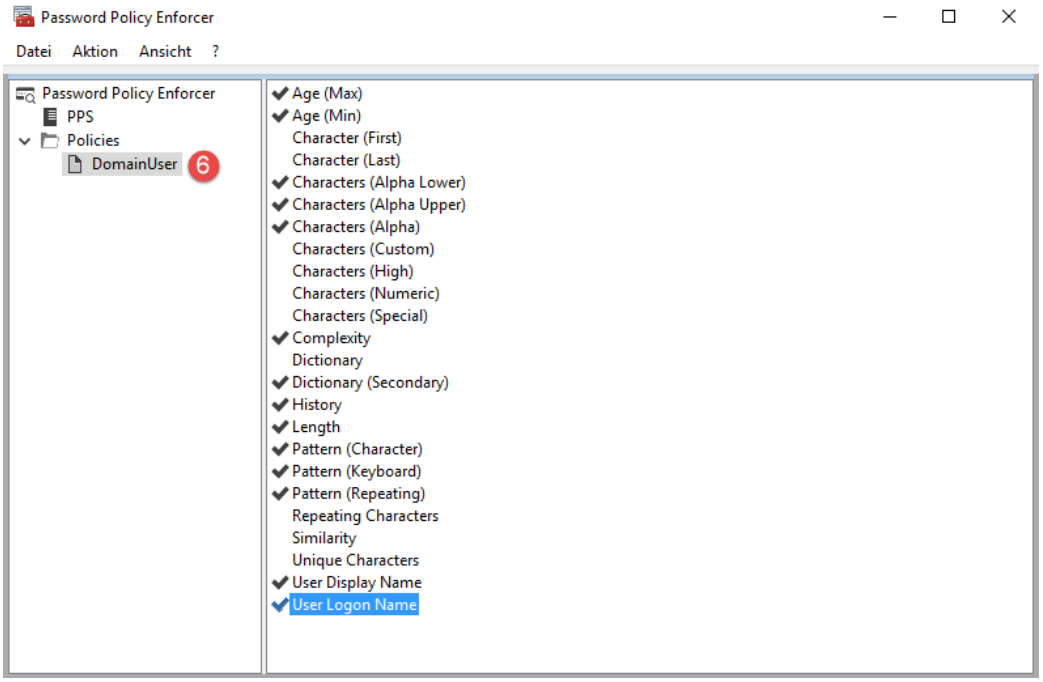


Es ist ganz klar zu erkennen, dass wir mit diesem Produkt wesentlich mehr Möglichkeiten haben als uns die Default Domain Policy anbietet.

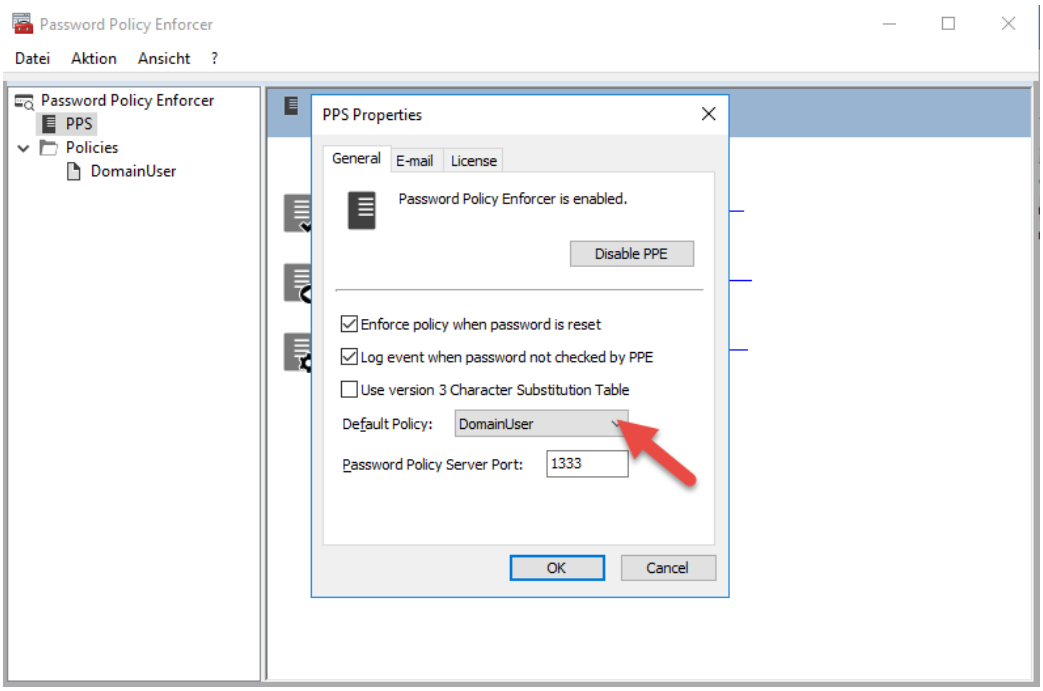


Anixis Password Policy Enforcer

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

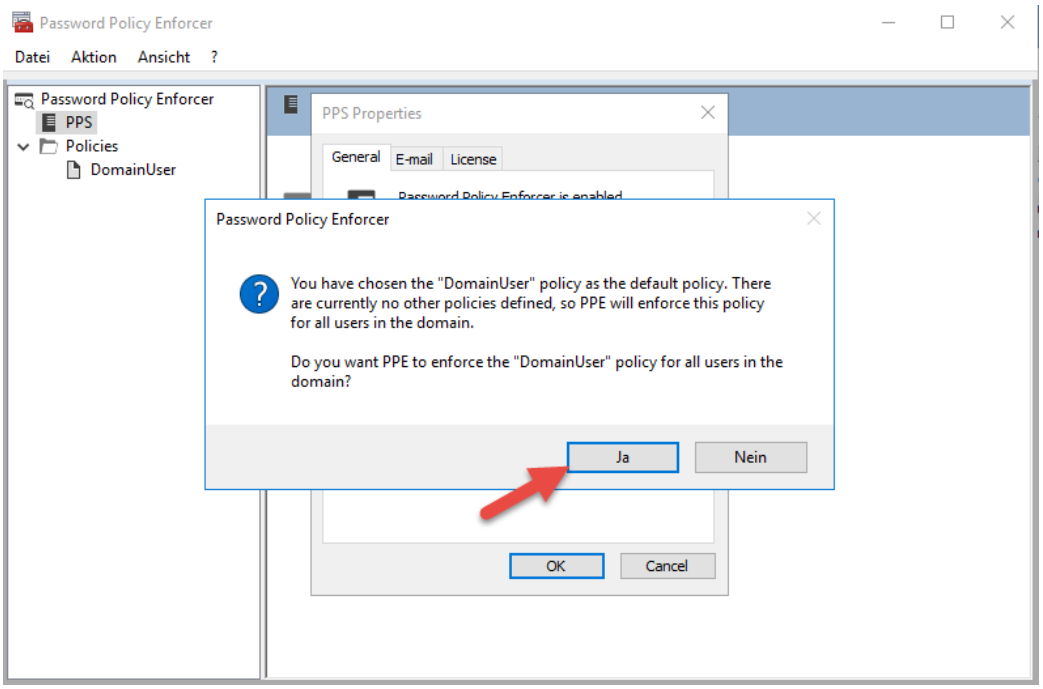


Wir könnten diese Richtlinie auch als Default Policy aktivieren und damit die alte Default Domain Policy ersetzen. Somit könnten z.B. auf Basis dieser Regel weitere folgen.

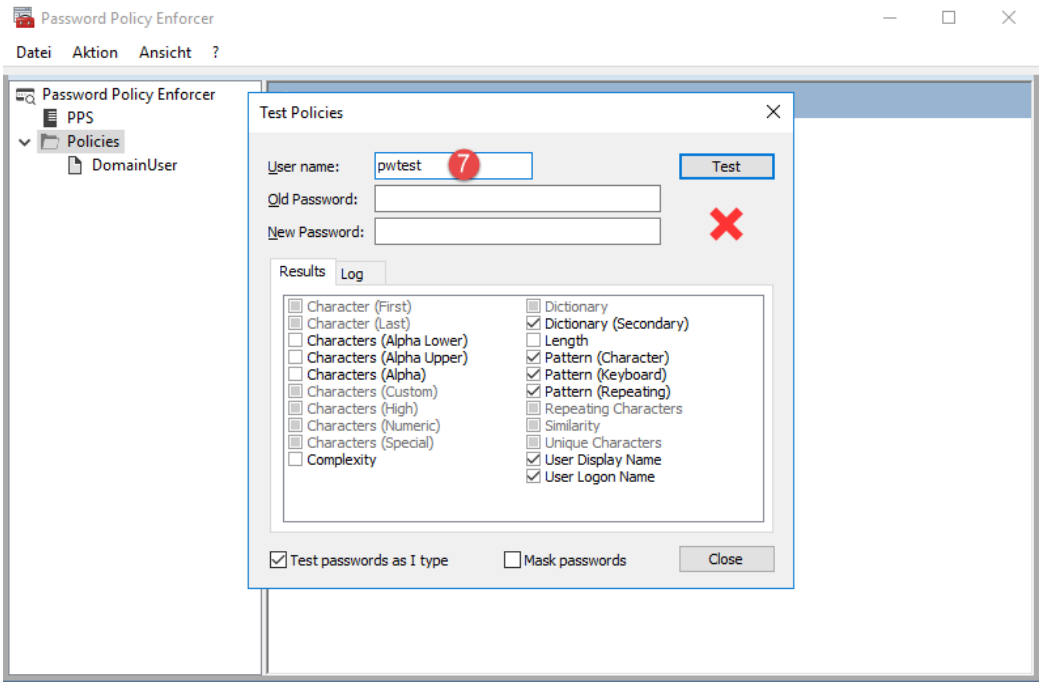


Anixis Password Policy Enforcer

Ein Konzept sollte vorher erarbeitet worden sein.

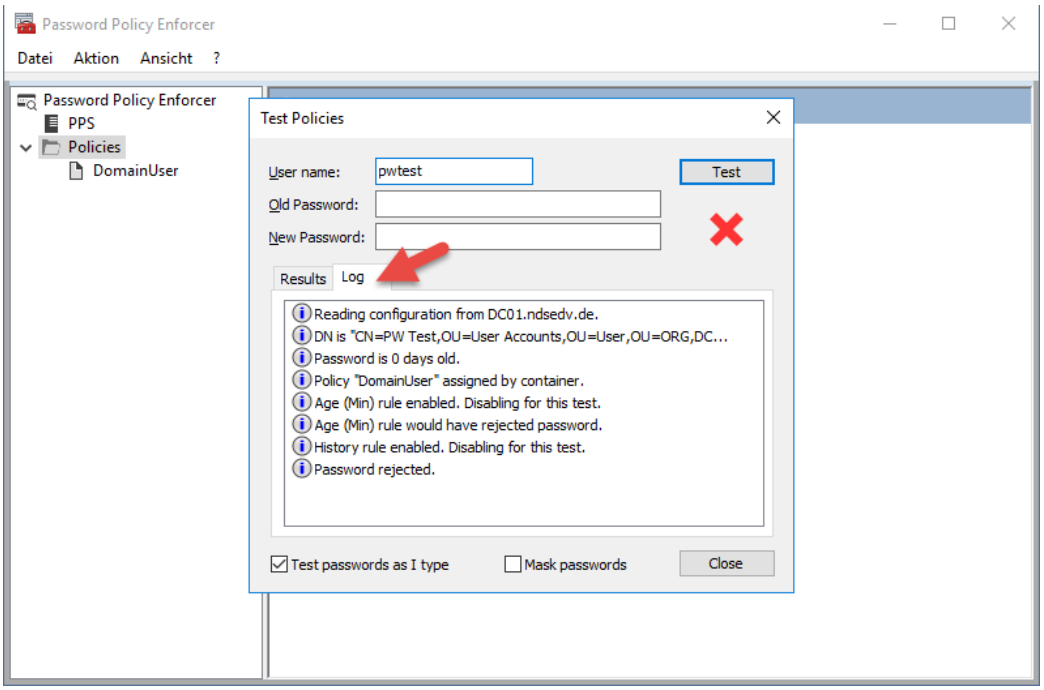


Die neue Richtlinie lässt sich nun auch live testen.



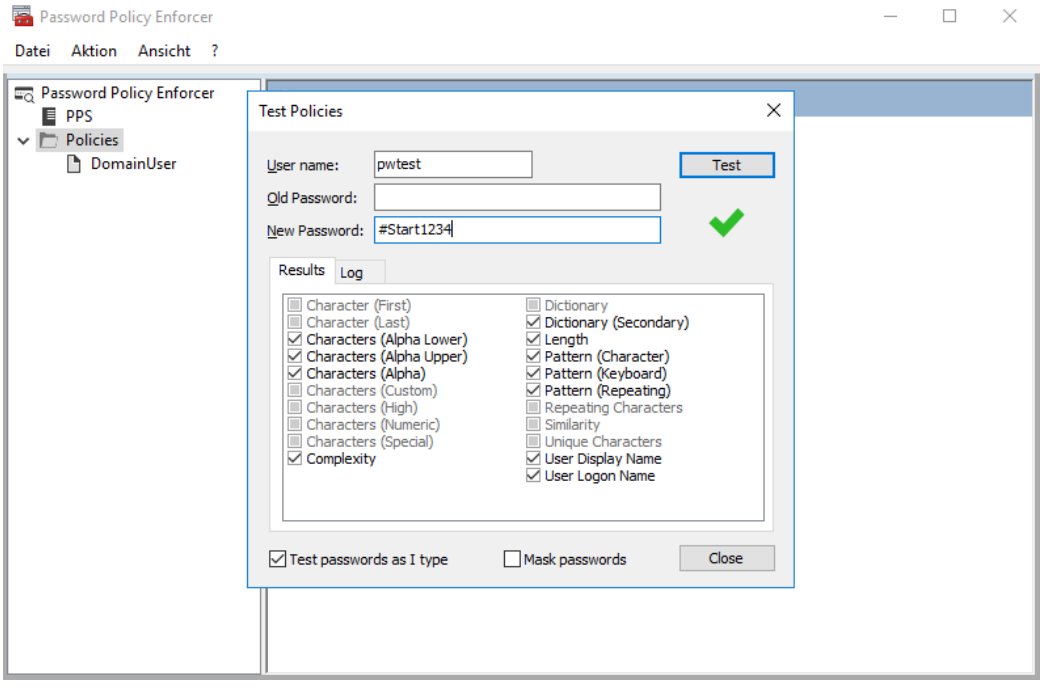
Anixis Password Policy Enforcer

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



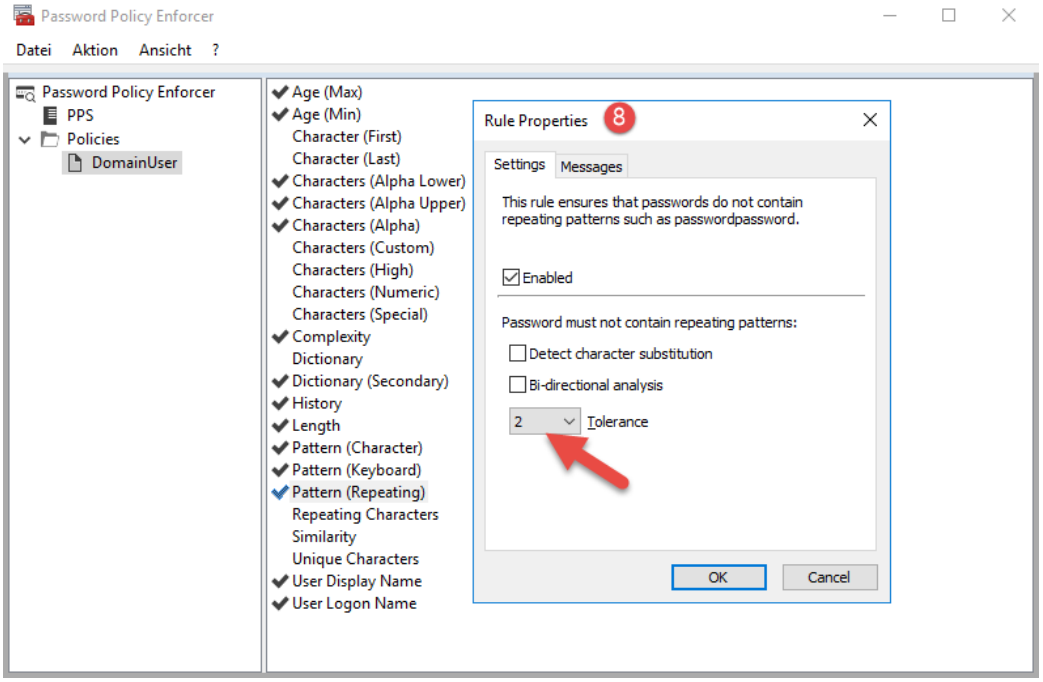
Starten wir einen Test. Das Passwort #Start1234 entspricht nun unserem Regelwerk. Es enthält das was wir konfiguriert und aktiviert haben.

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

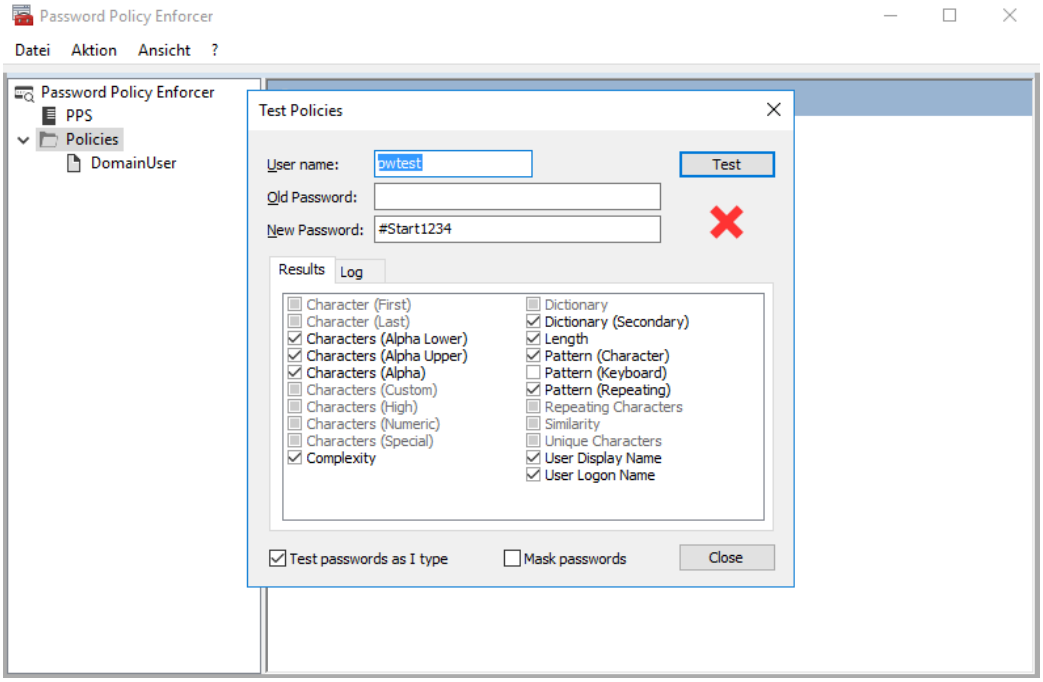


Anixis Password Policy Enforcer

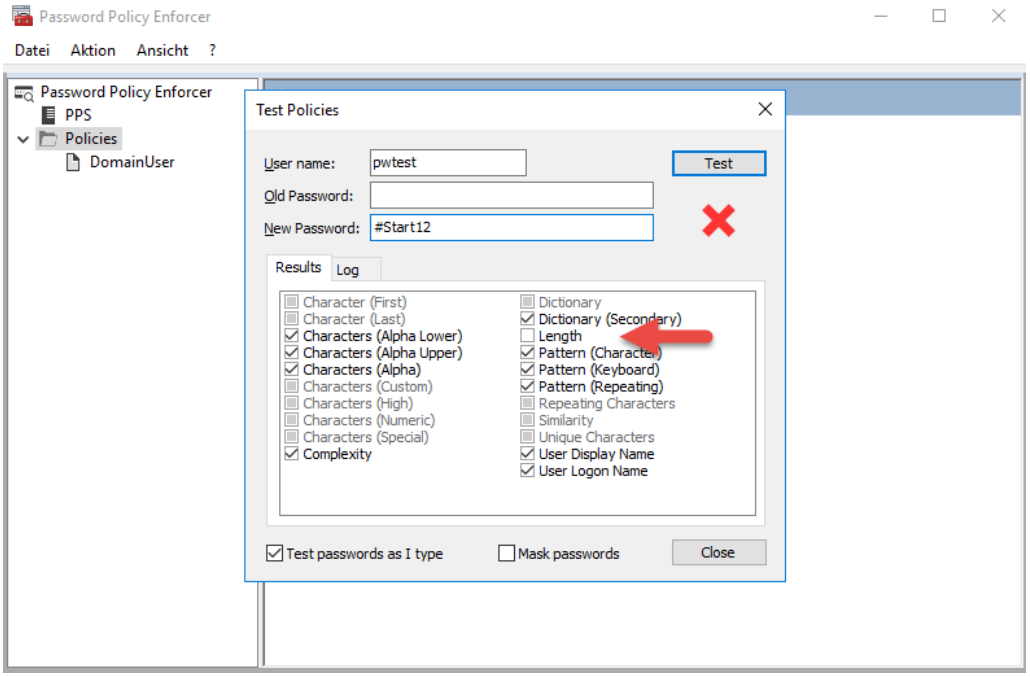
Ich ändere dafür die Pattern Toleranz von 4 auf 2.



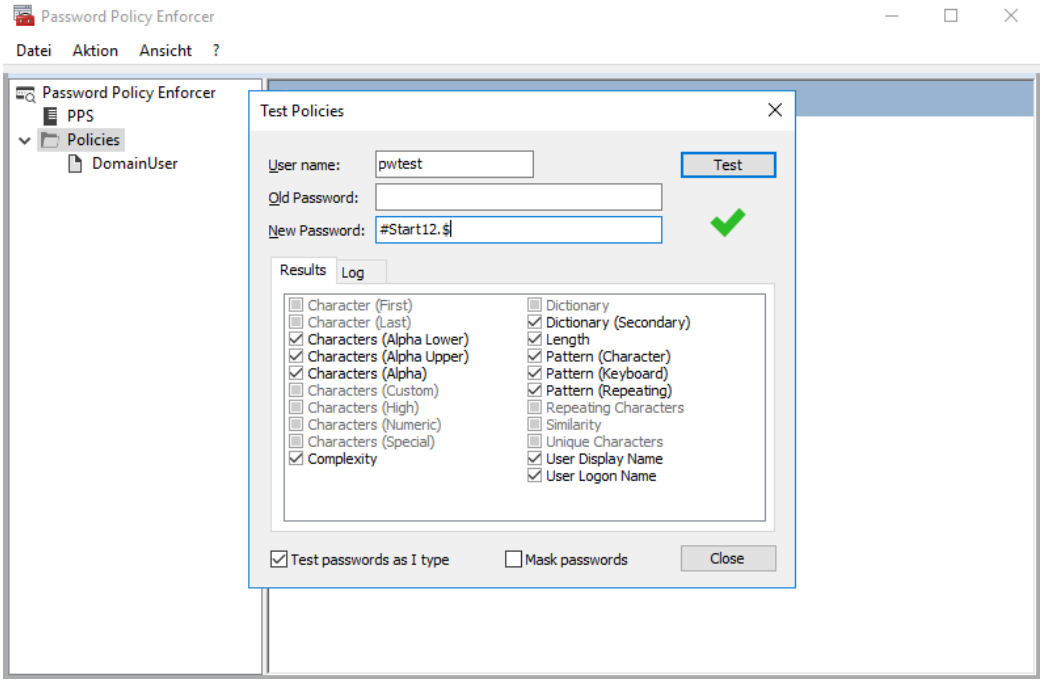
Das Passwort wird jetzt wegen der Toleranz nicht mehr akzeptiert, es sind zu viele Zahlen hintereinander, mehr als die Regel erlaubt.



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



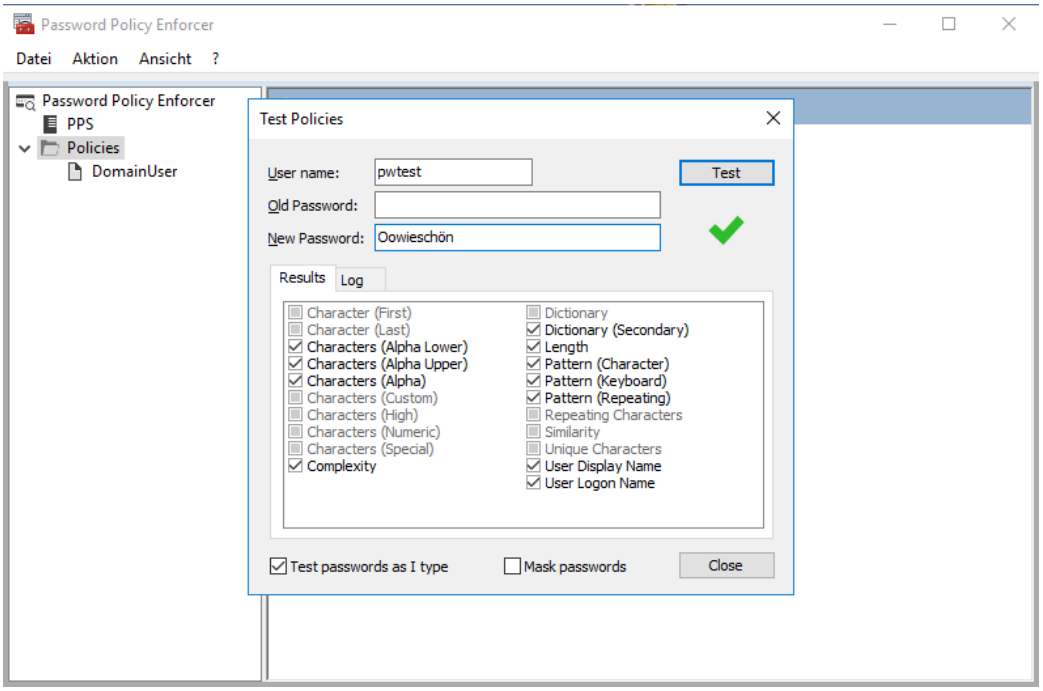
Wir fügen dem Passwort 2 weitere Sonderzeichen hinzu und es entspricht nun wieder dem Gesamtregelwerk.



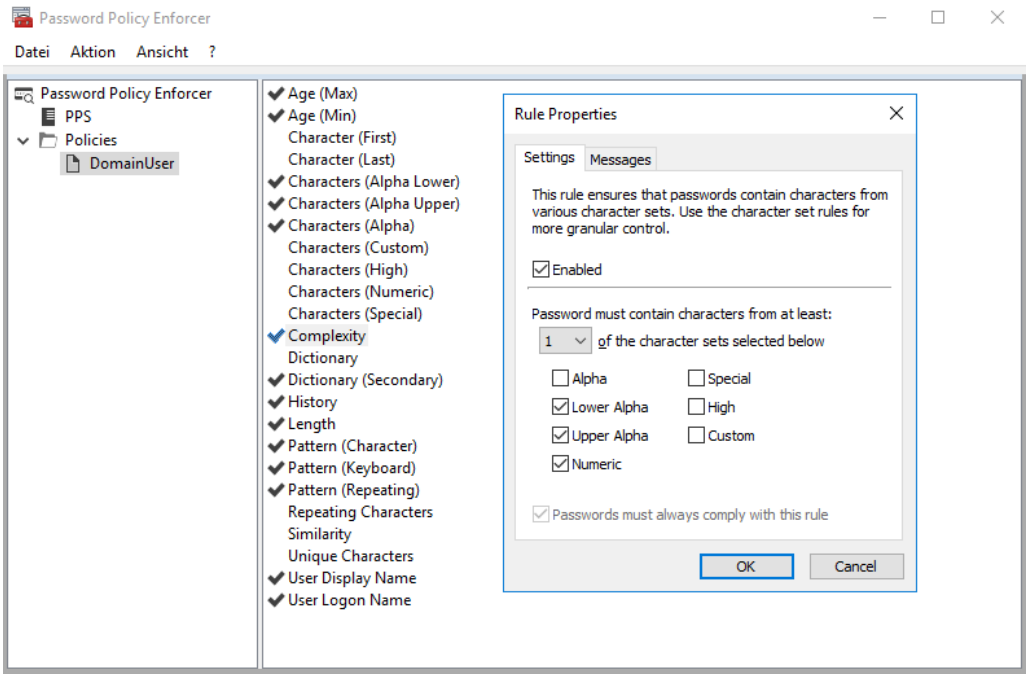
Anixis Password Policy Enforcer

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.

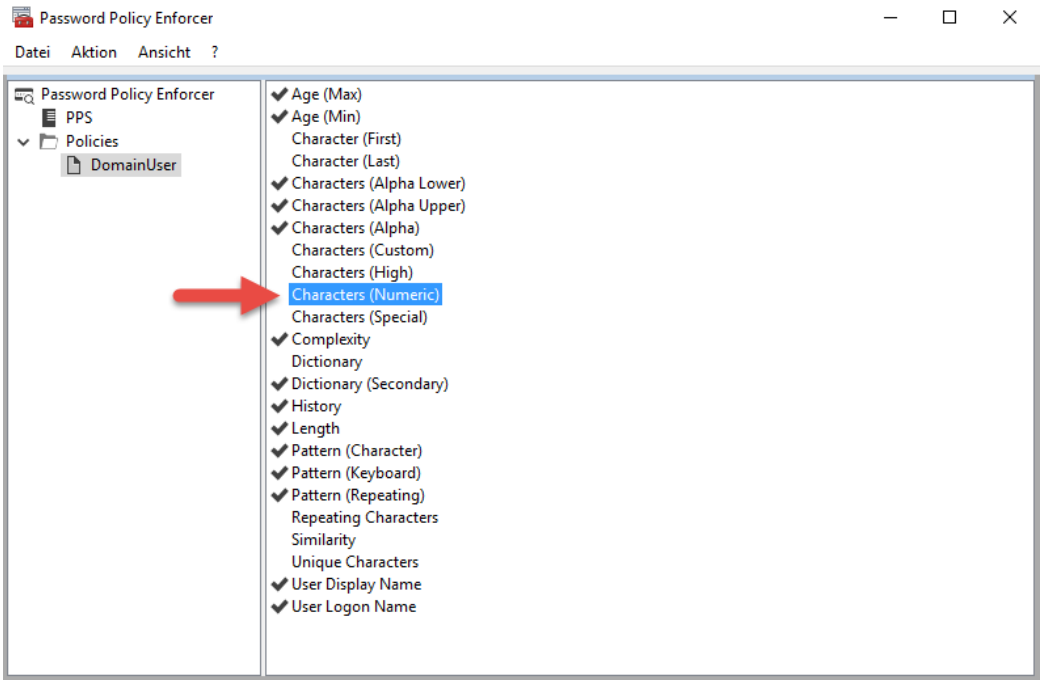


Es liegt nicht an der Complexity, die ist korrekt eingestellt. Do you remember?

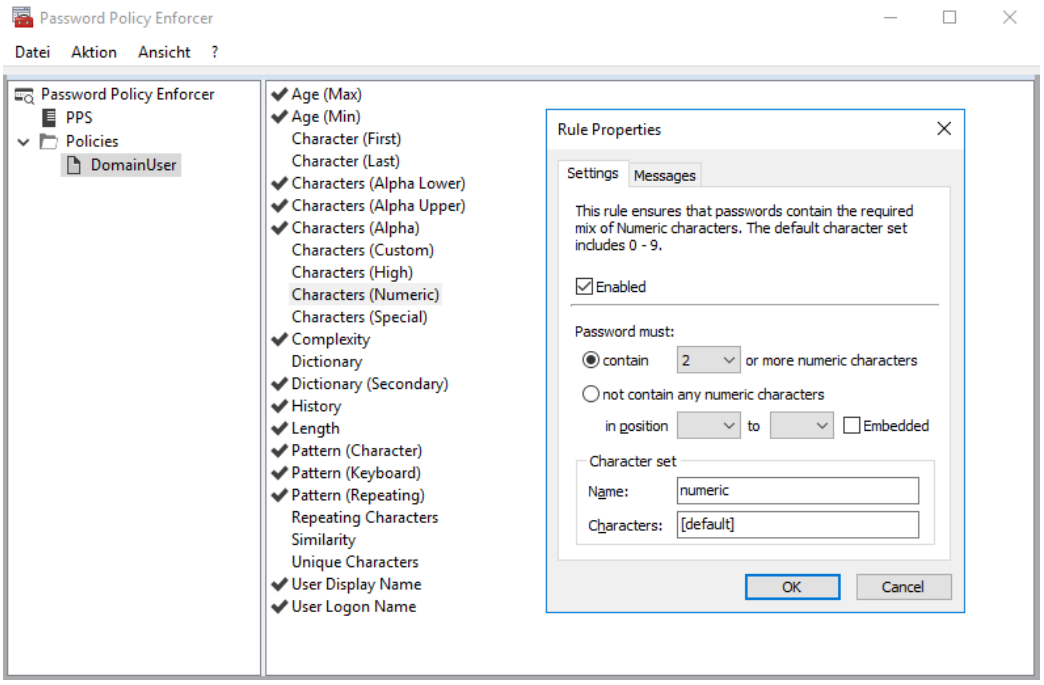


Ich hatte doch die Regel Numeric nicht aktiviert und somit werden auch keine Zahlen erwartet. ;-)

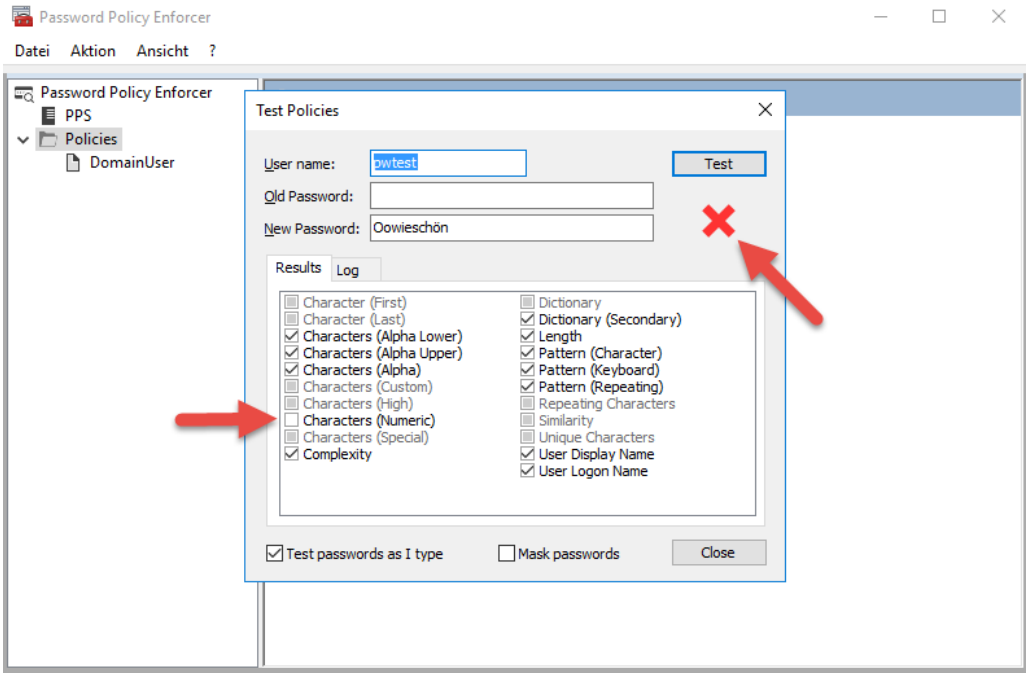
Das holen wir jetzt nach.



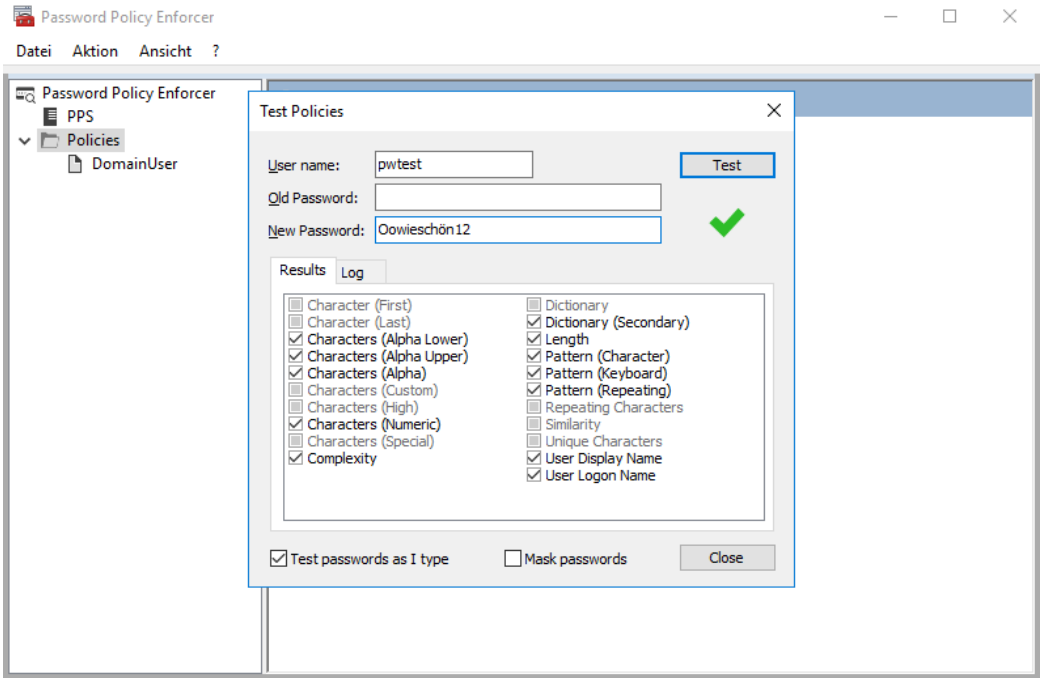
Info: Die Komplexitätsregel ist eine untergeordnete Funktion die nur dann richtig funktioniert wenn auch alle Abhängigkeiten aktiviert sind.



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.

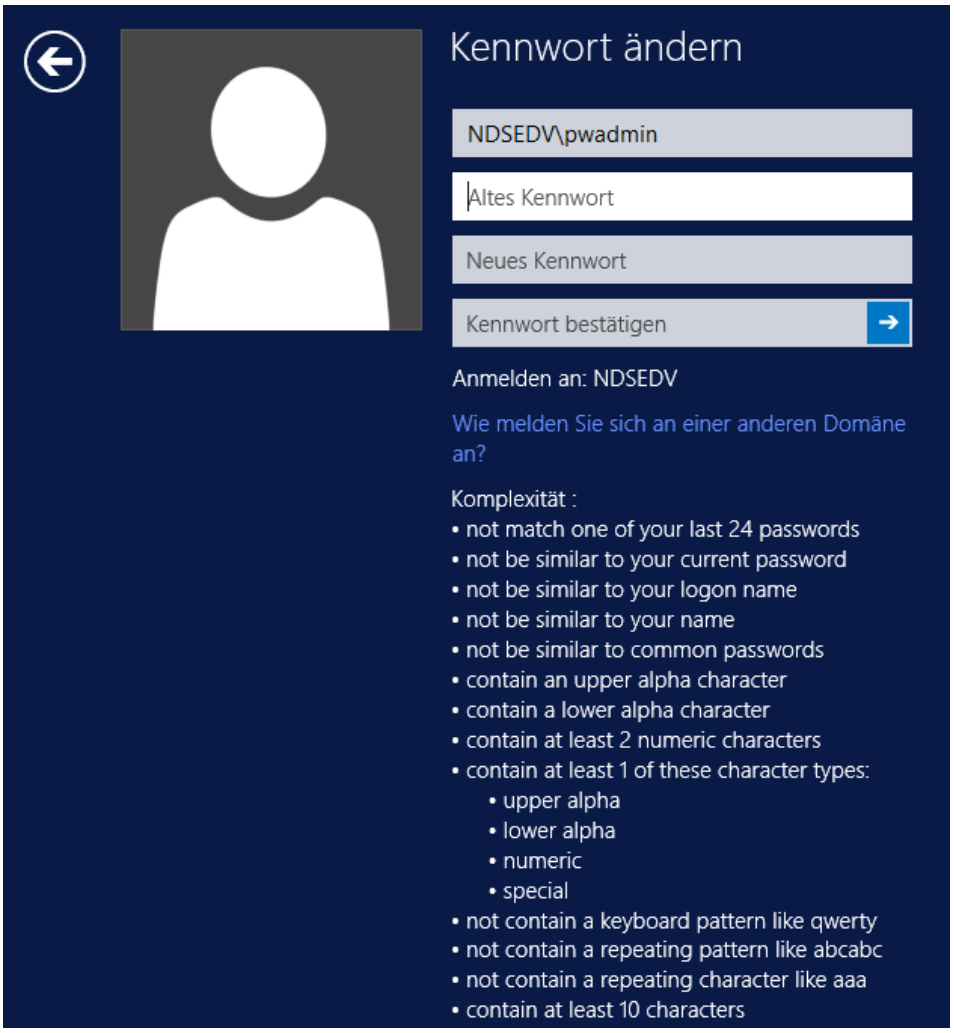
So sieht das Kennwort ändern Feld aus, wie wir es von Server 2016 oder Windows 10 kennen. Das Passwort muss ab sofort der neuen Richtlinie entsprechen, aber wie sieht diese aus eigentlich?!

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

Anixis Password Policy Enforcer

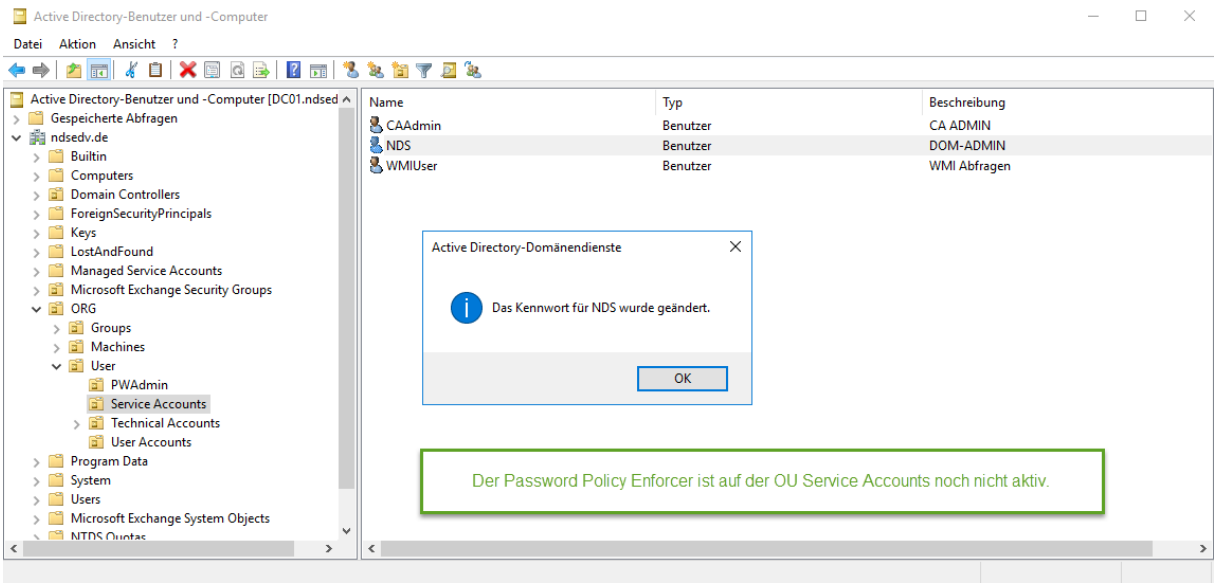
Die Ansicht bei einem Server 2012 R2 ohne Client Modul.

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

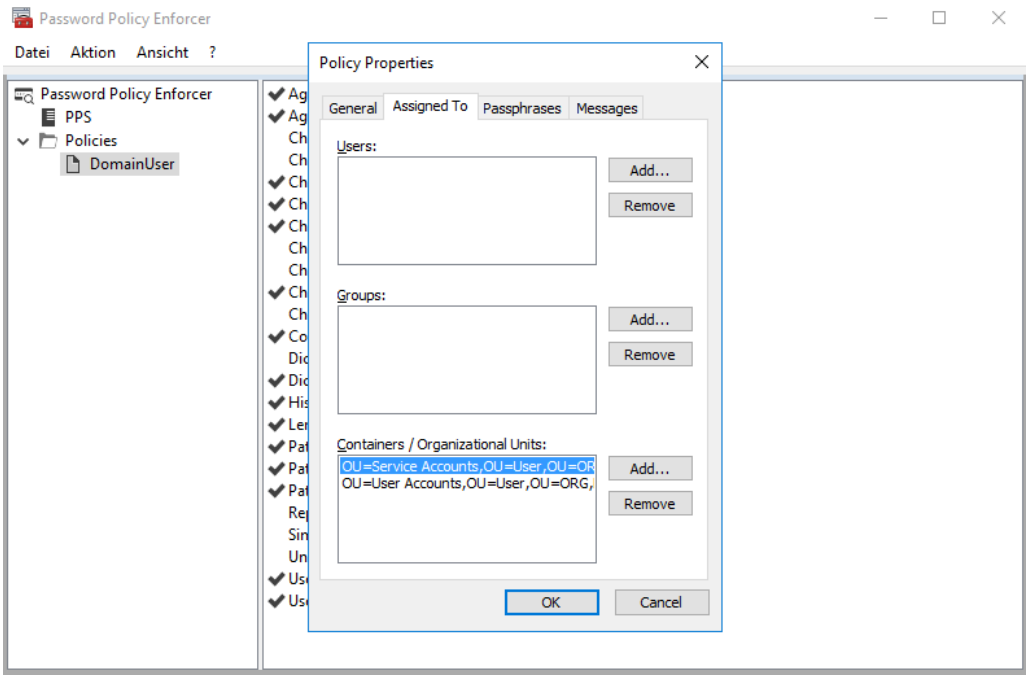


Anixis Password Policy Enforcer

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.



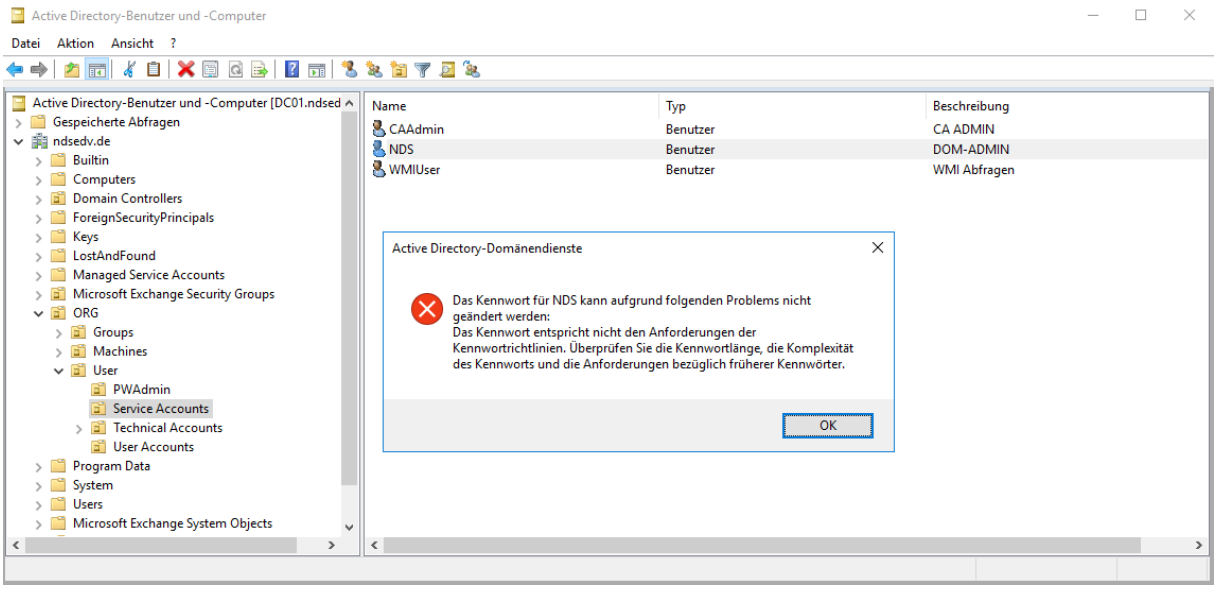
Verknüpfe die Richtlinie nun auf die **OU = Service Accounts** und werde als Domänen-Admin versuchen das Passwort erneut zu ändern.



Anixis Password Policy Enforcer

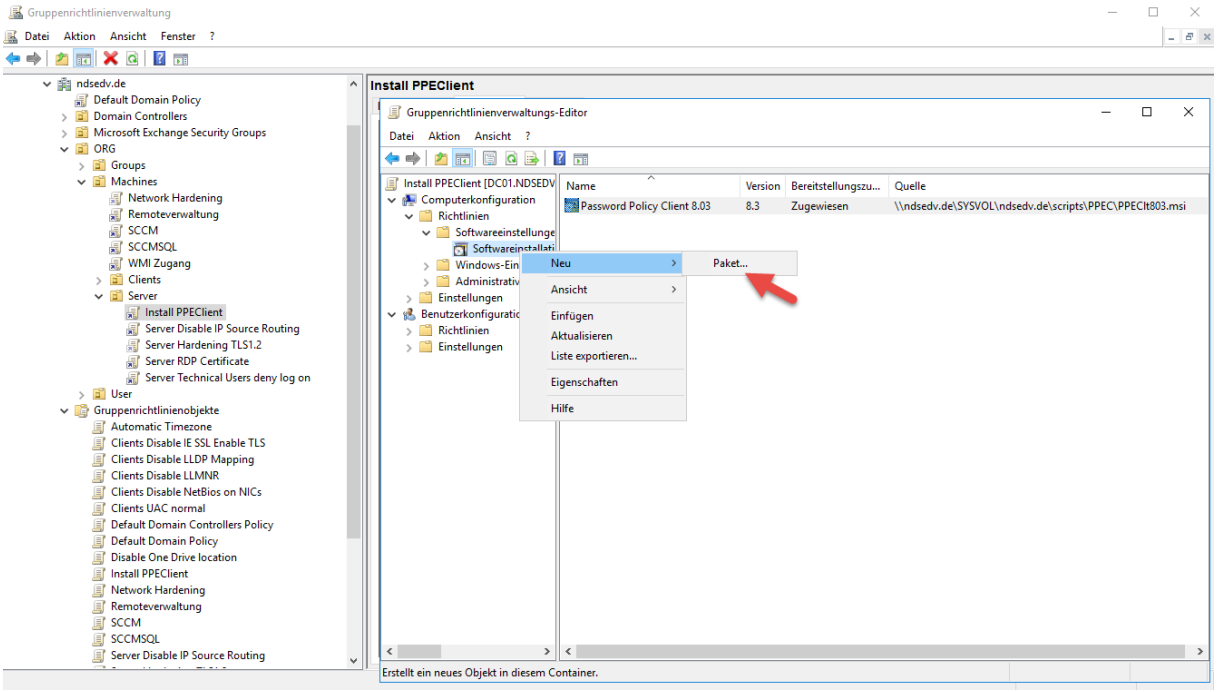
Erstaunlich. Auch der Admin hat sich an die gültige Richtlinie zu halten. TOP!

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

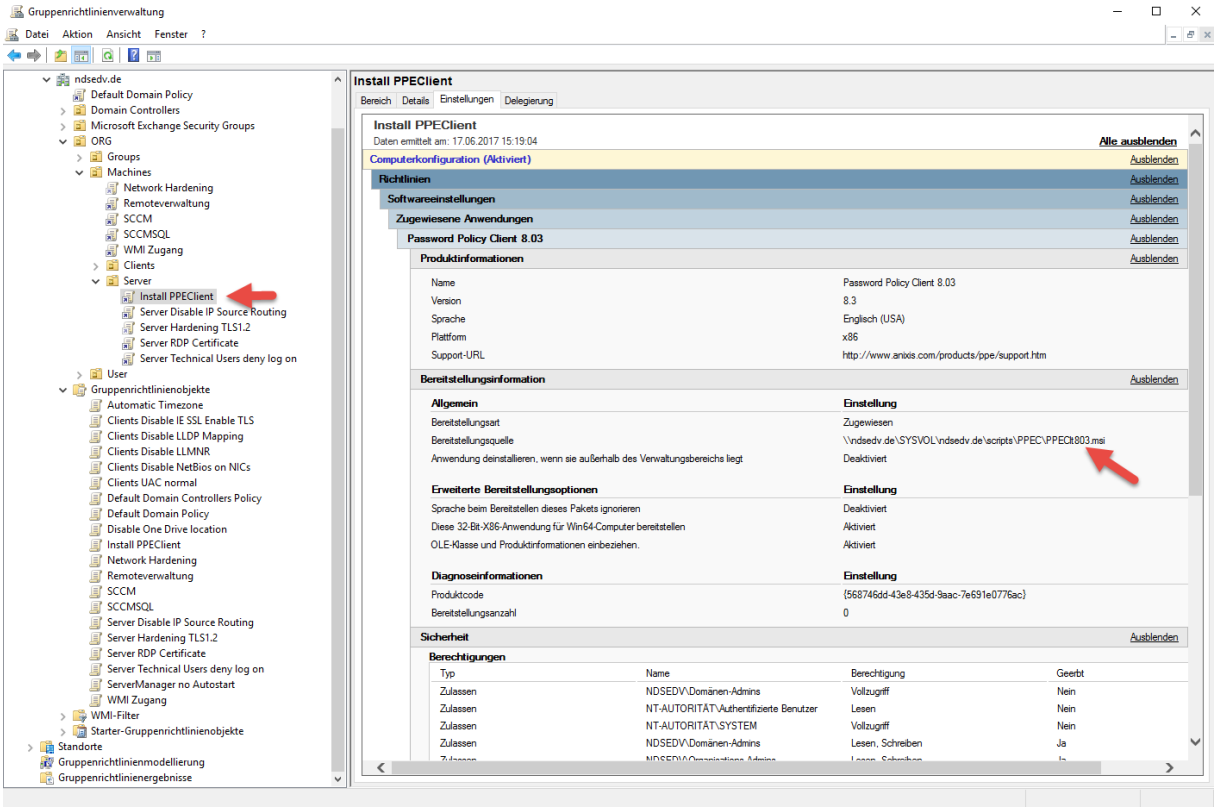


Automatische Verteilung des Client Moduls über eine Gruppenrichtlinie.
Neue GPO erstellen und das Paket per UNC Pfad einbinden.

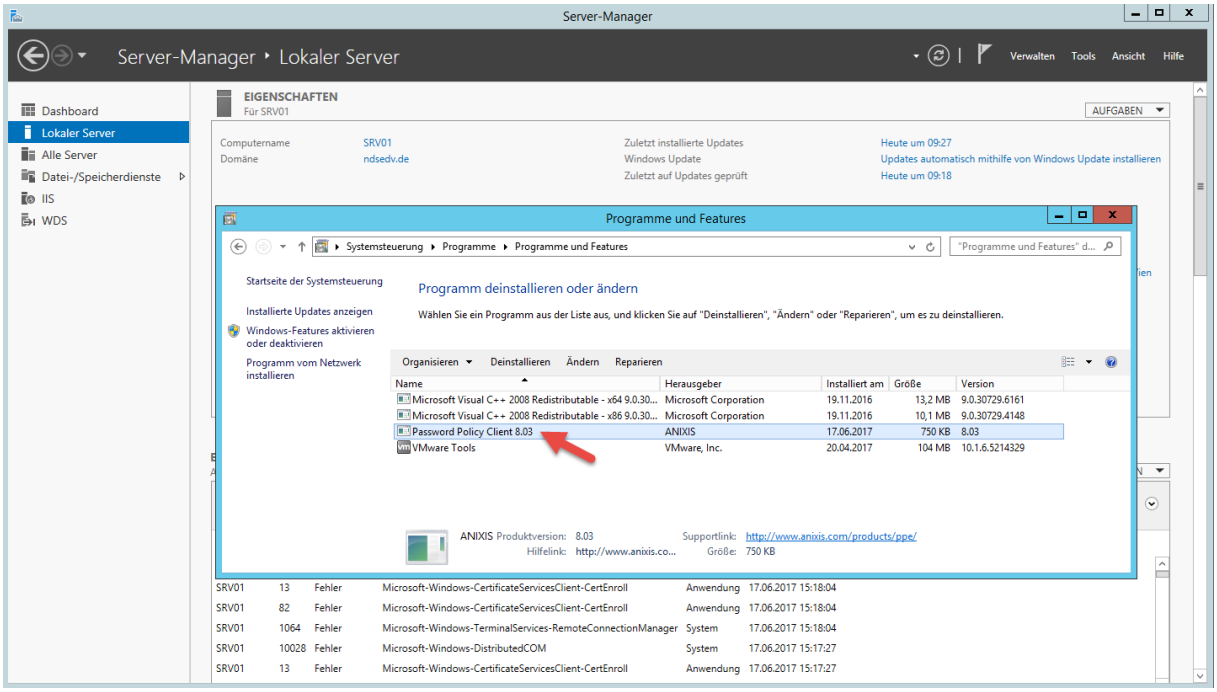
C:\Windows\SYSVOL\sysvol\ndsedv.de\scripts\PPEC\PPEClt803.msi



Anixis Password Policy Enforcer



Nach einem Neustart erhalten die Clientsysteme das Paket automatisch.

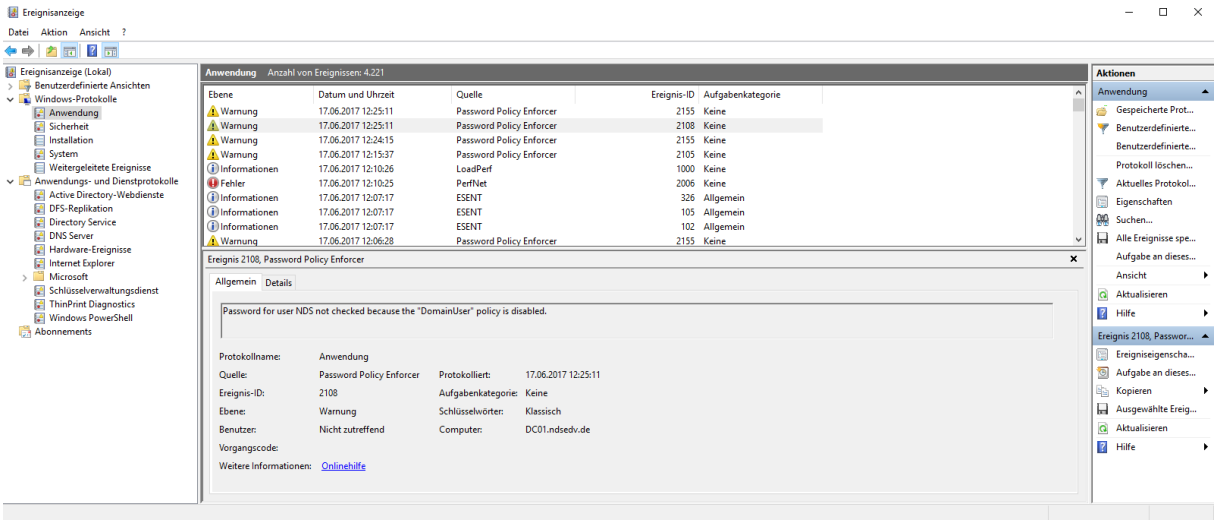


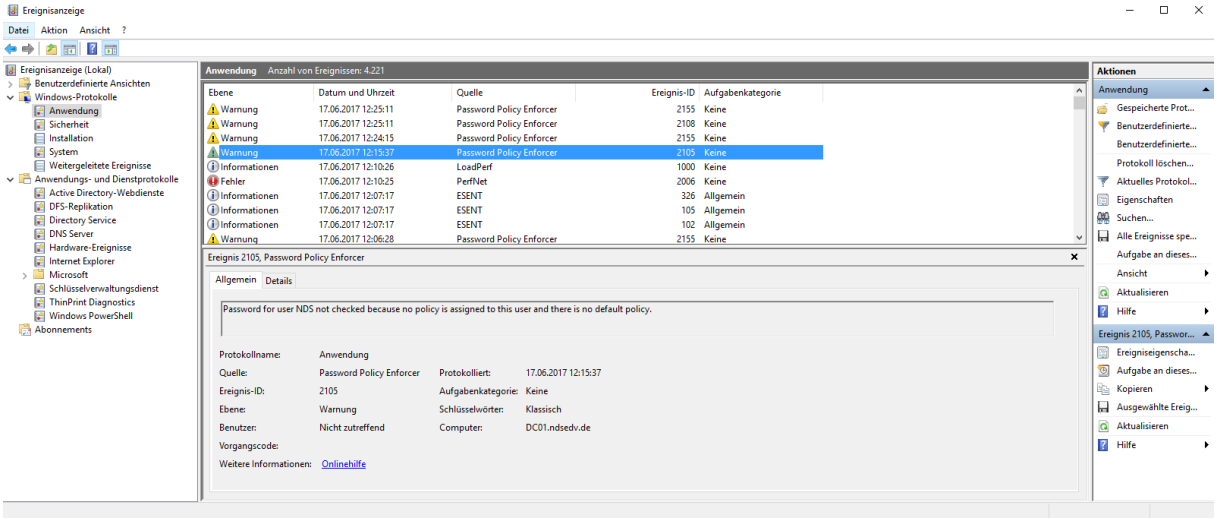
Erstellt von Jörn Walter **17.06.2017**

Anixis Password Policy Enforcer

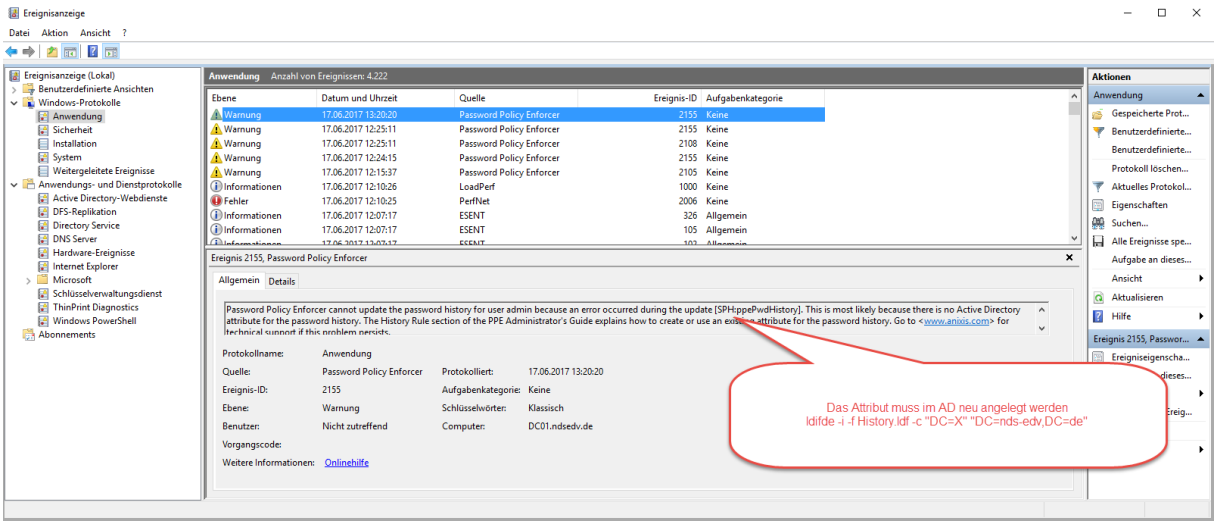
Troubleshooting:

Das Ereignisprotokoll ist sehr aussagekräftig und gibt Hinweise auf Lösungen.





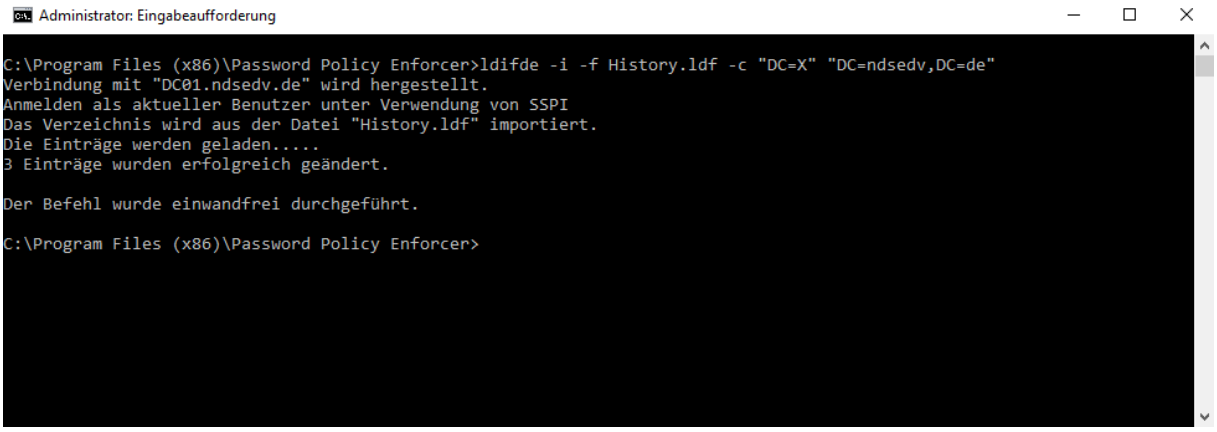
Fehlendes Attribut setzen: ldifde -i -f History.ldf -c "DC=X" "DC=nds-edv,DC=de"



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

Erstellt von Jörn Walter **17.06.2017**

Anixis Password Policy Enforcer

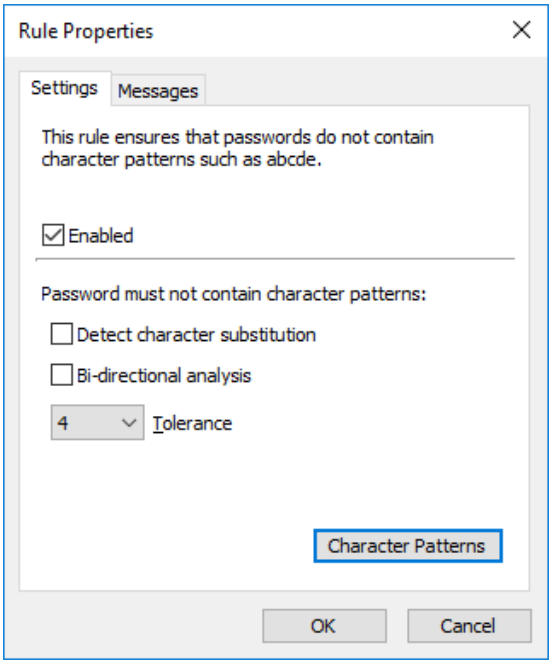


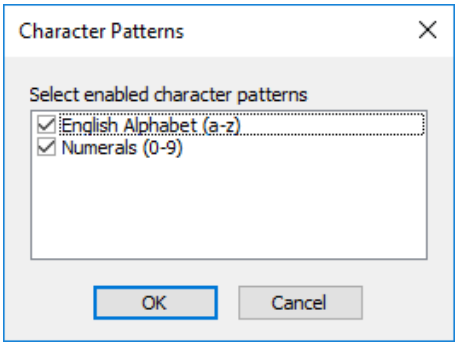
Anixis Password Policy Enforcer

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.

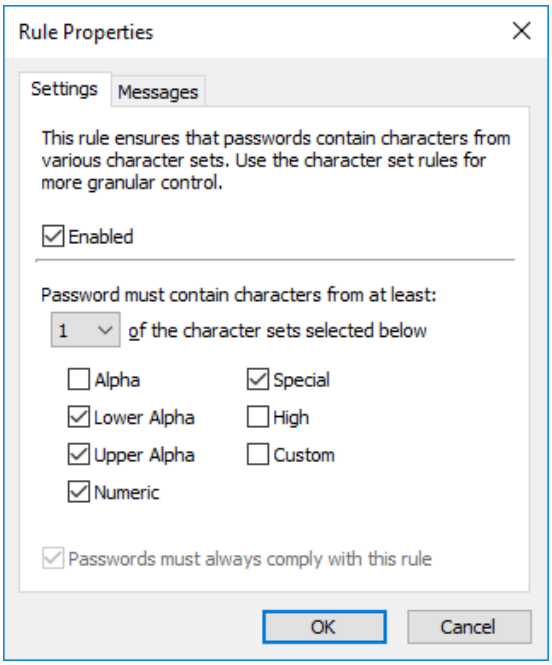




Anixis Password Policy Enforcer

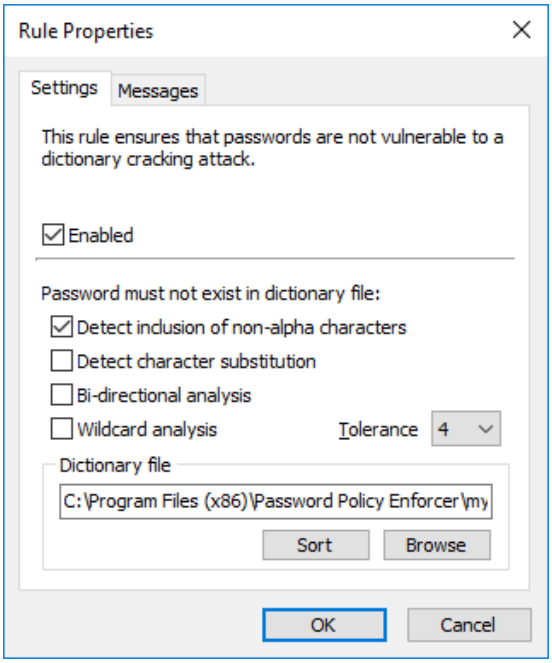
Complexity:

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



Dictionary:

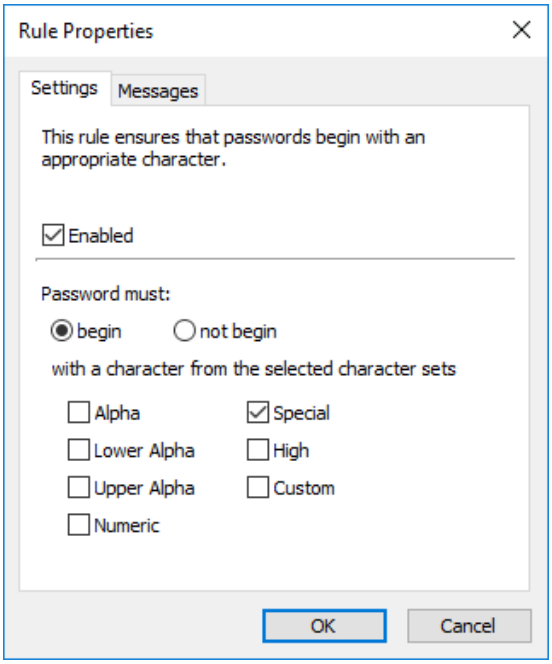
Die Wörterbuchregel lehnt Passwörter ab, die anfällig für Hackerangriffe sind. Hierbei wird ein lokales Wörterbuch verwendet, indem der PPE dieses einliest und mit den Passwörtern vergleicht. Diese Regel erkennt partielle Übereinstimmungen mit einem Passwort und kann Zeichensubstitutionen (ersetzen von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



Anixis Password Policy Enforcer

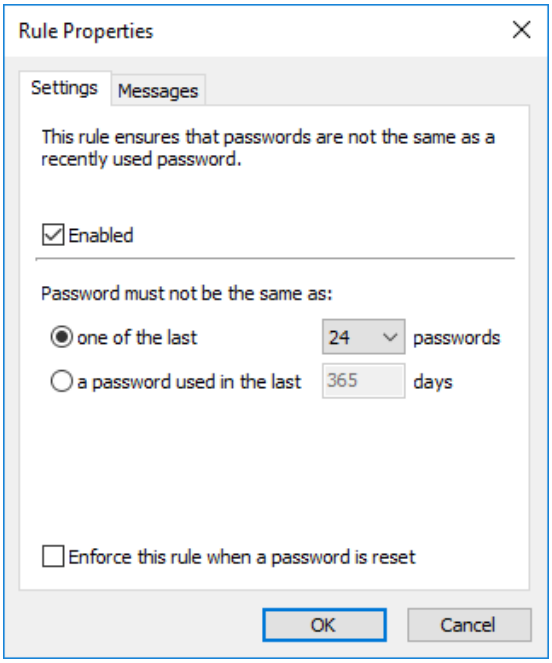
First Character:

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



History:

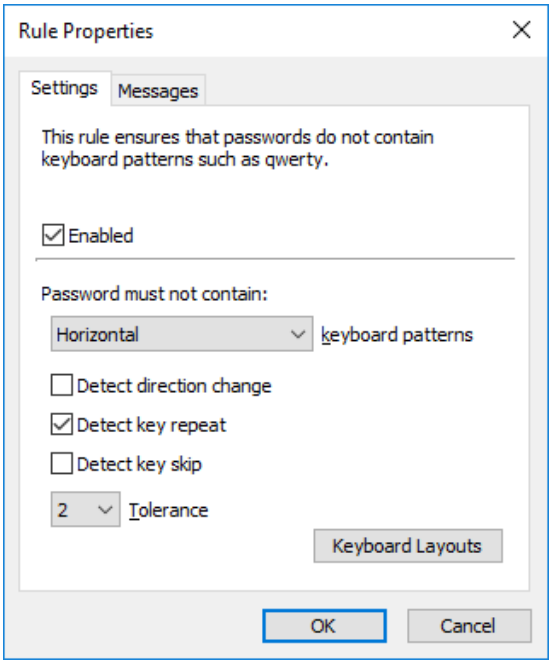
Die Historienregel lehnt Passwörter ab, die kürzlich bereits verwendet wurden.

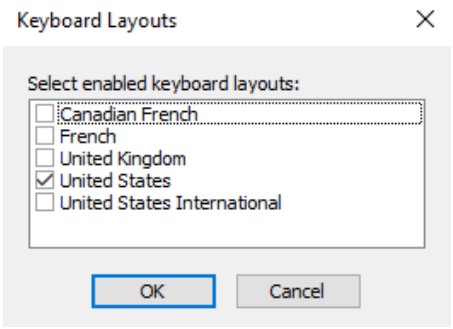


Anixis Password Policy Enforcer

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!

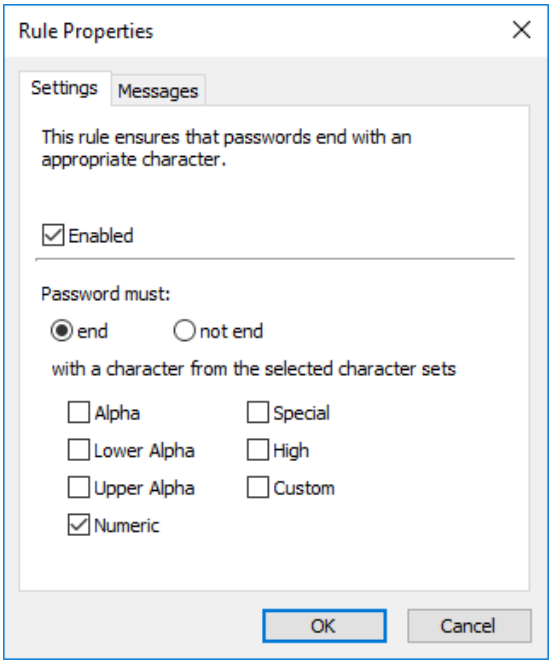




Anixis Password Policy Enforcer

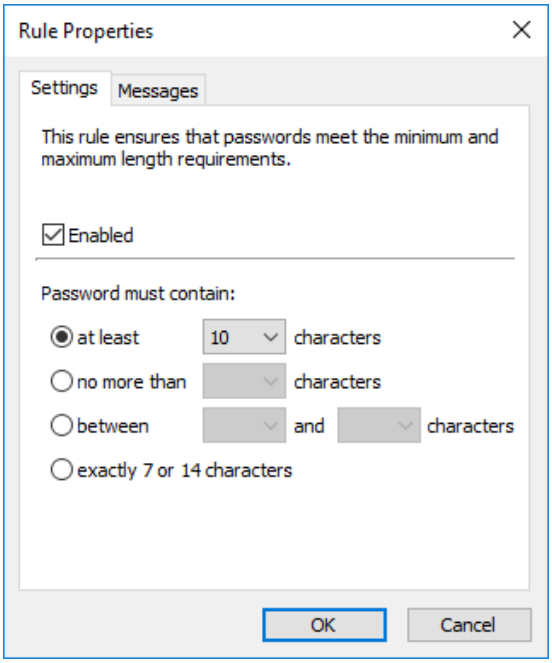
Last Character:

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



Length:

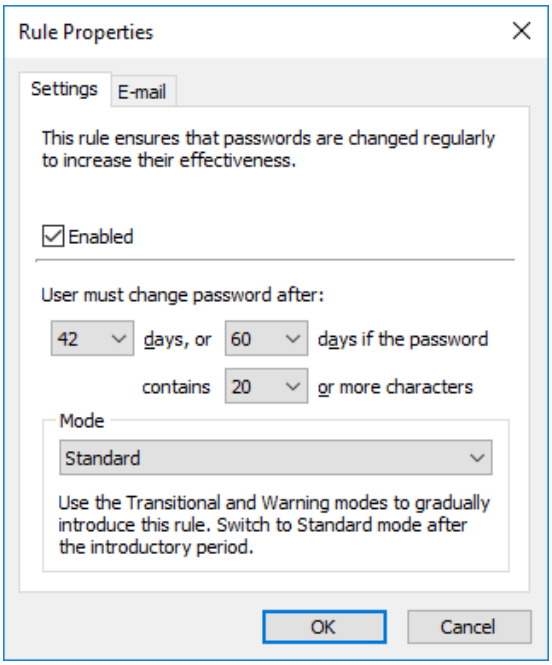
Die Längenregel lehnt Passwörter an die zu wenig oder zu viele Zeichen enthält.



Anixis Password Policy Enforcer

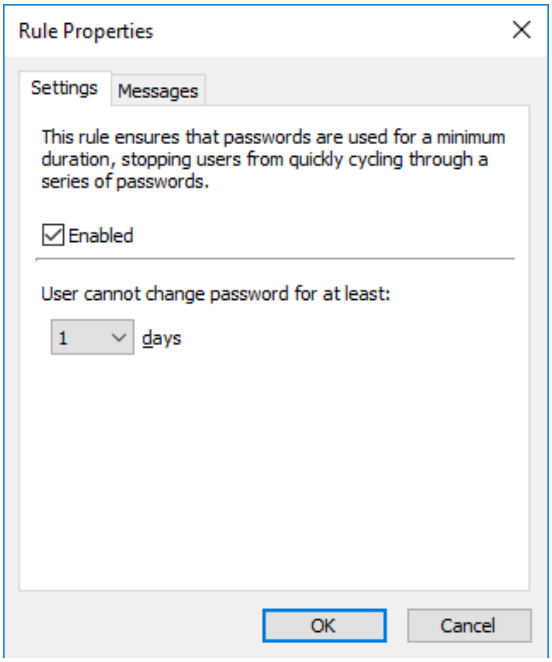
Maximum Age:

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.



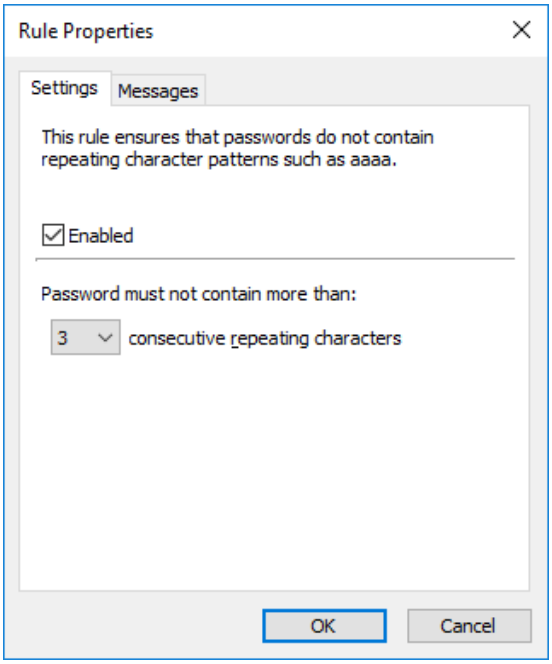
Minimum Age:

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



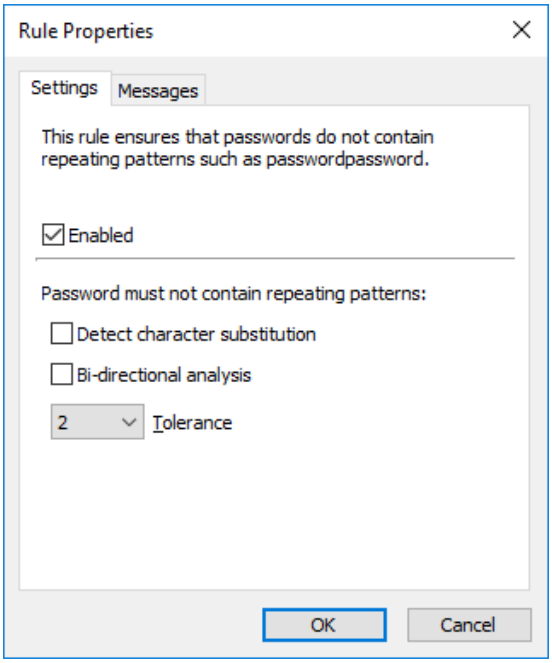
Repeating Characters:

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



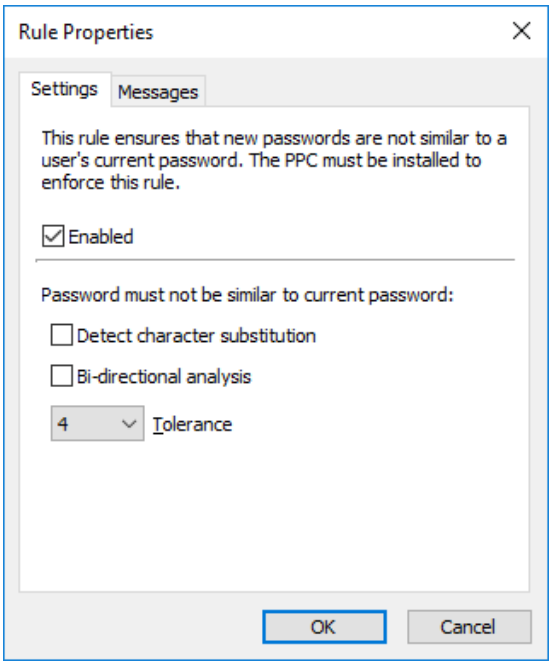
Repeating Pattern:

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).



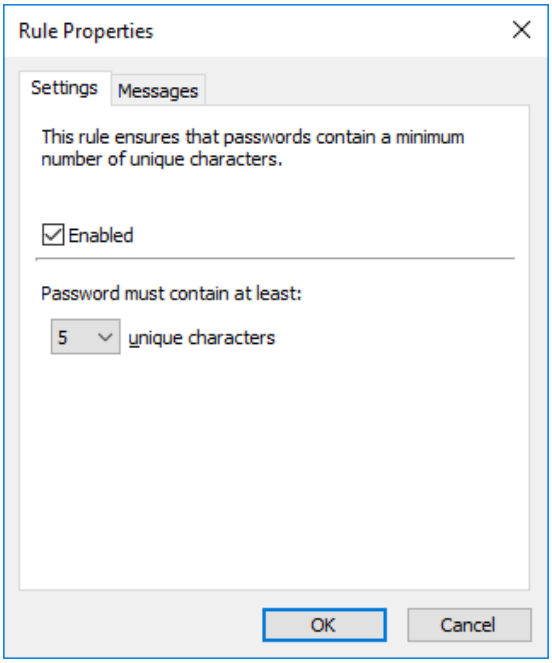
Similarity:

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:

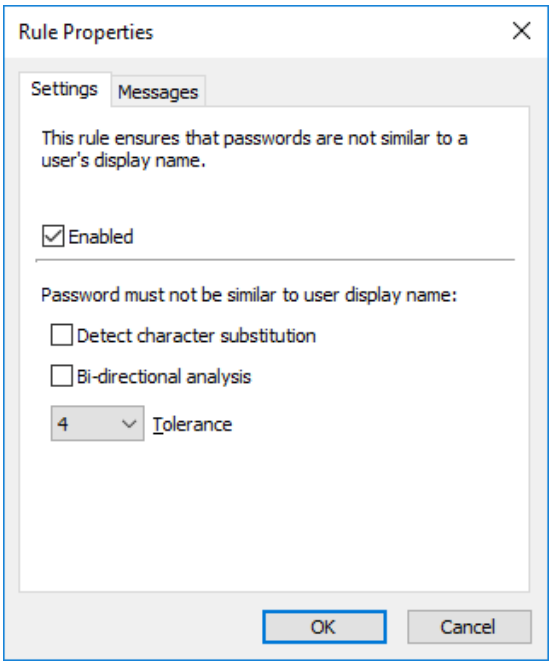
Diese Regel lehnt Passwörter ab, die keine minimale Anzahl von eindeutigen Zeichen enthält.



Anixis Password Policy Enforcer

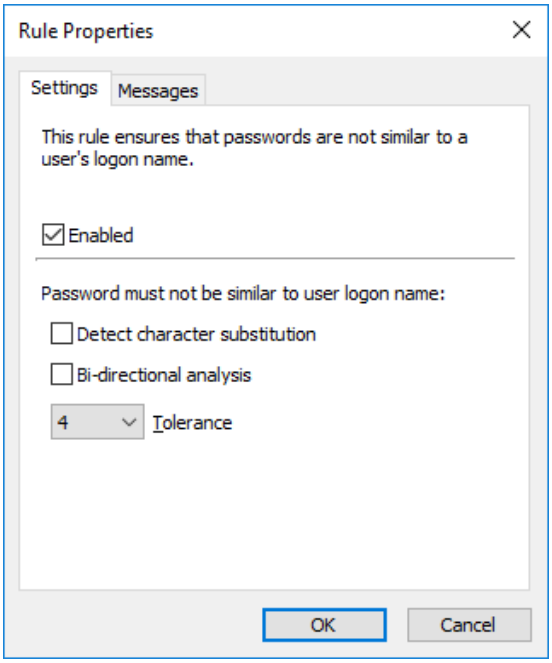
User Display Name:

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.

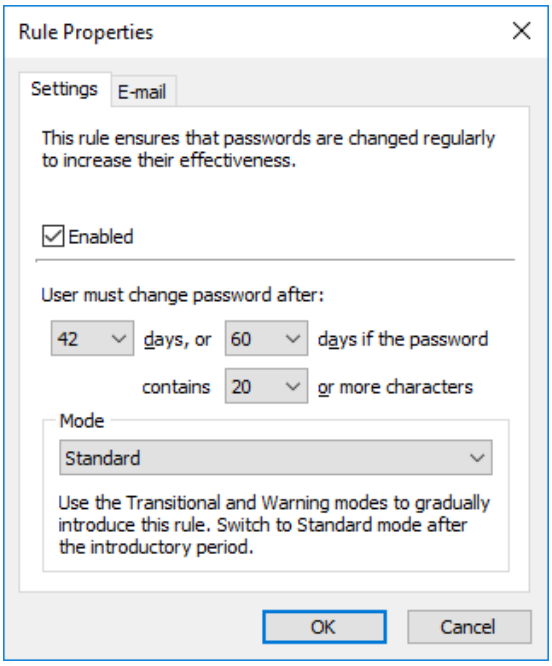
Die Regel Benutzer Anmeldename lehnt Passwörter ab, die sich mit dem Anmeldenamen im Active Directory ähneln. Zu den Optionen gehören auch hier die Match-Toleranz, Zeichensatzerkennung und die bidirektionale Analyse.



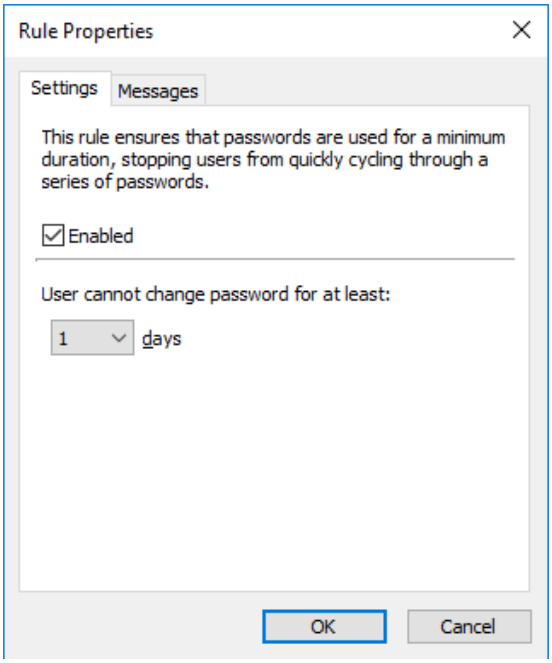
Anixis Password Policy Enforcer

Meine empfohlenen Einstellungen:

Age Max:

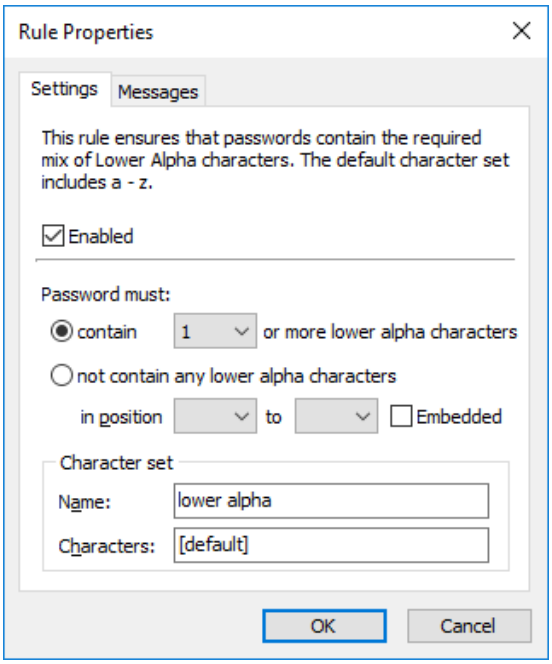


Age Min:

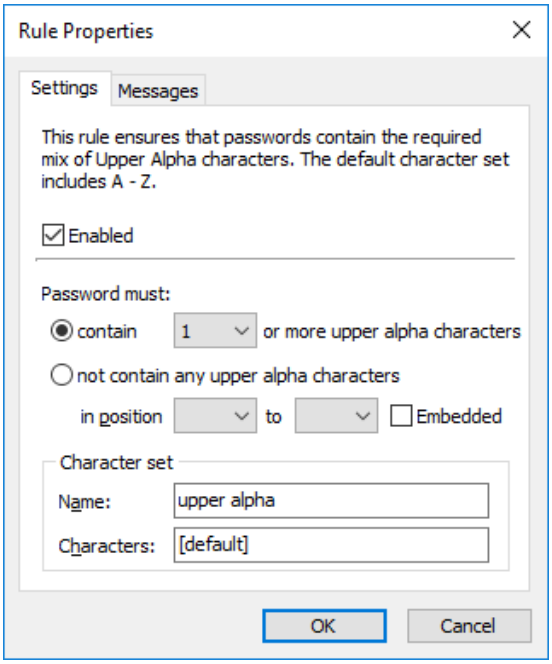


Anixis Password Policy Enforcer

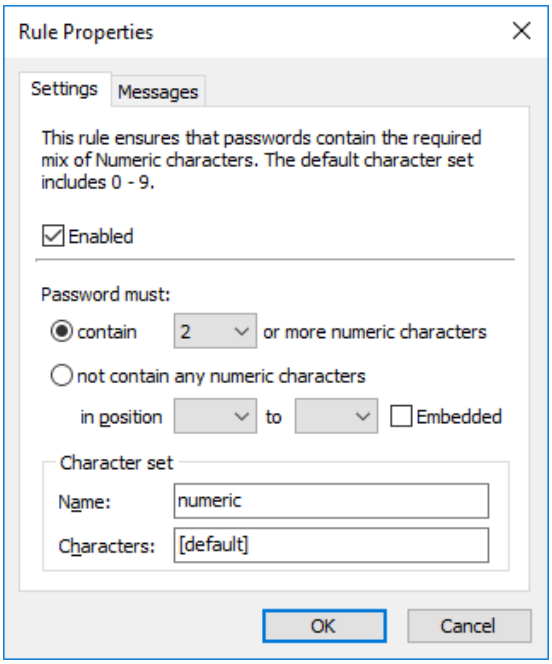
Character (Alpha Lower):



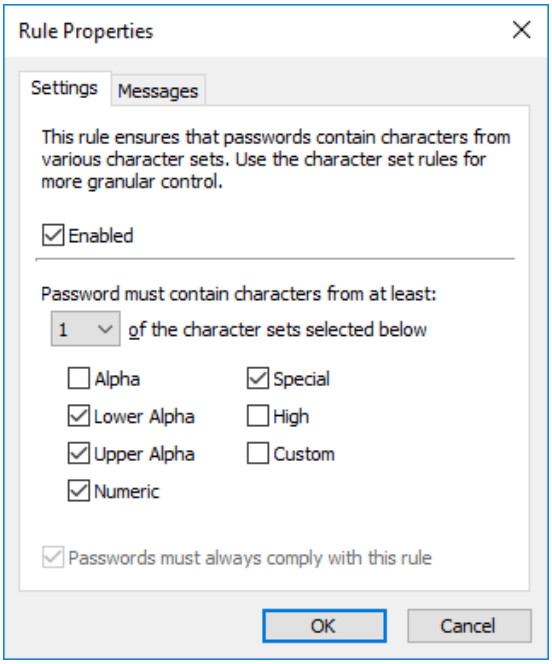
Character (Alpha Upper):



Character (Numeric):

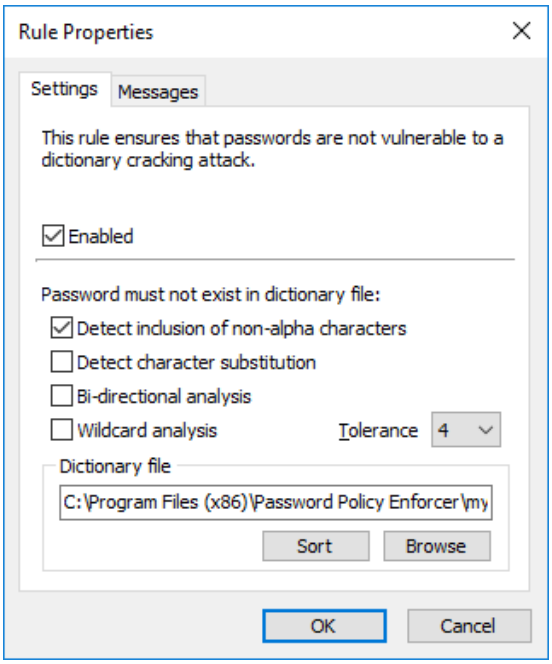


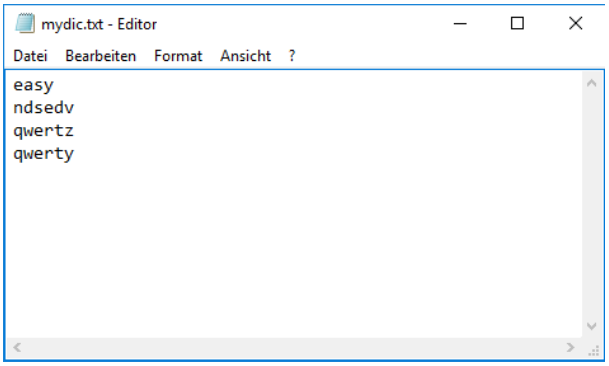
Complexity:



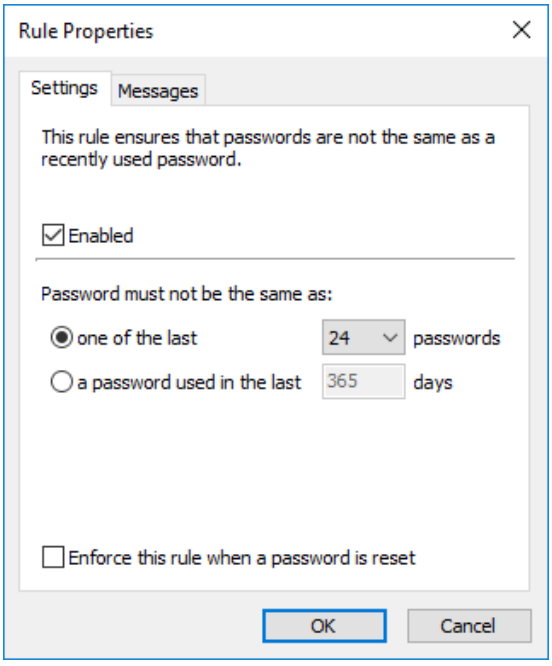
Anixis Password Policy Enforcer

Dictionary:



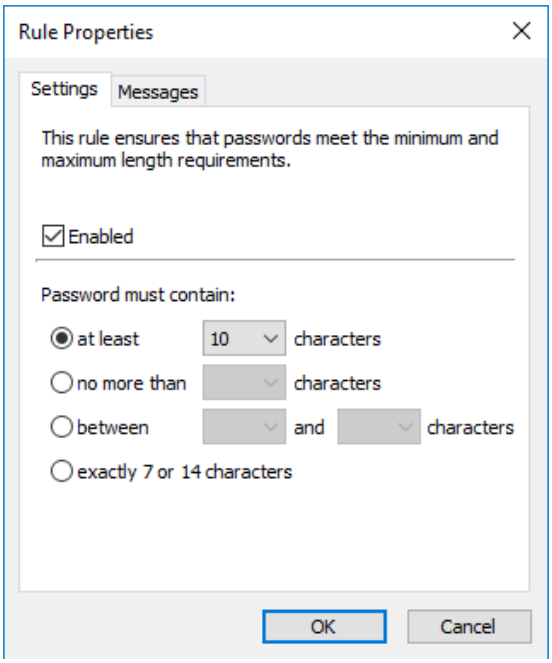


History:

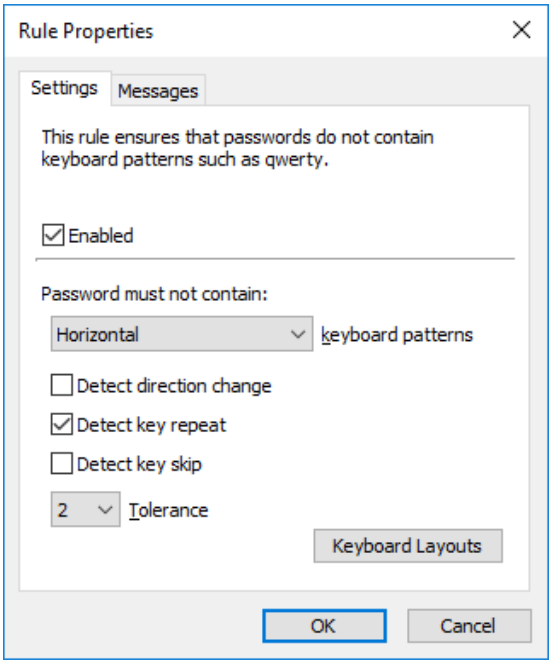


Anixis Password Policy Enforcer

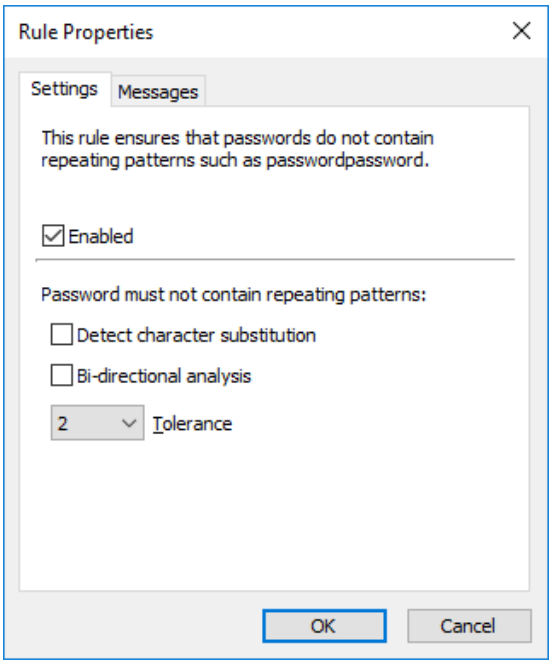
Length:



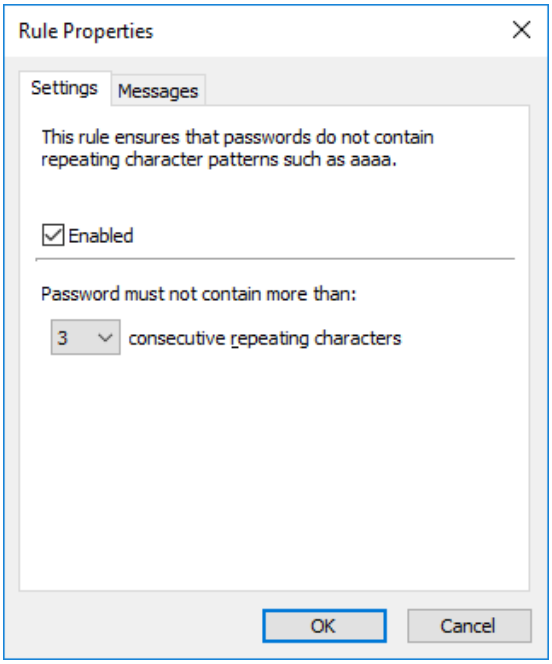
Pattern (Keyboard):



Pattern (Repeating):

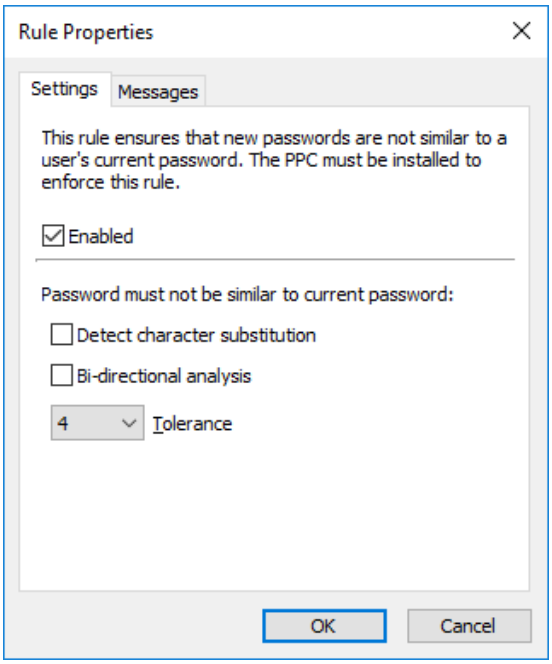


Repeating Characters:

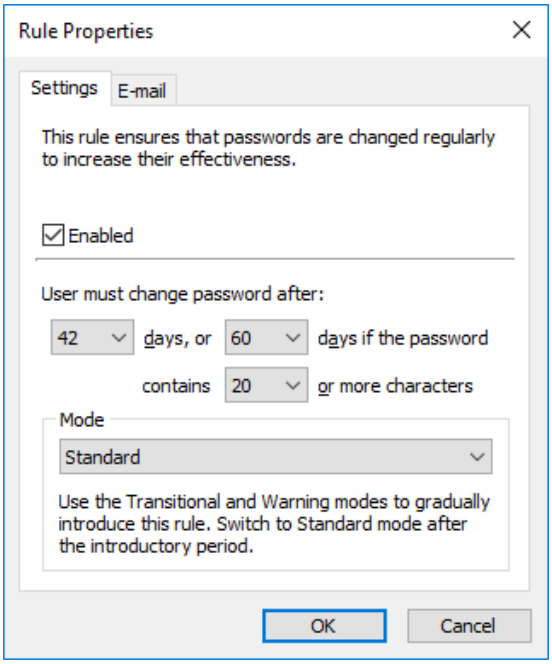


Anixis Password Policy Enforcer

Similarity:



Age Max:



Anixis Password Policy Enforcer

Age Min: