



Deine Guidelines zu Richtlinien

Über Richtlinien und Best Practice

Admincamp 2017

Innovative Software-Lösungen.

www.assono.de



Vorstellung - Ich

Manuel Nientit

Diplom Wirtschaftsinformatiker

Seit knapp 2004 mit IBM Notes und Domino

Seit 2008 IT-Consultant der Firma assono GmbH

Erst Entwickler dann Administrator





Agenda

Was? Warum?

Begriffe *yawn*

Richtlinien anwenden

Einstellungen (Best Practice)

Troubleshooting



Was? Warum?

Vorkonfiguration des Clients und Standardaufgaben

- Keine durch Nutzer *verfummelten* Clients
- Kein: „Habe ich bei der Konfiguration vergessen“
- Weniger Konfigurationsarbeit generell



Probleme

Vergleich der Policies mit effektiven Einstellungen
nur manuell möglich

Kann kaum *debugged* werden

Bei Tests ist *Geduld* erforderlich

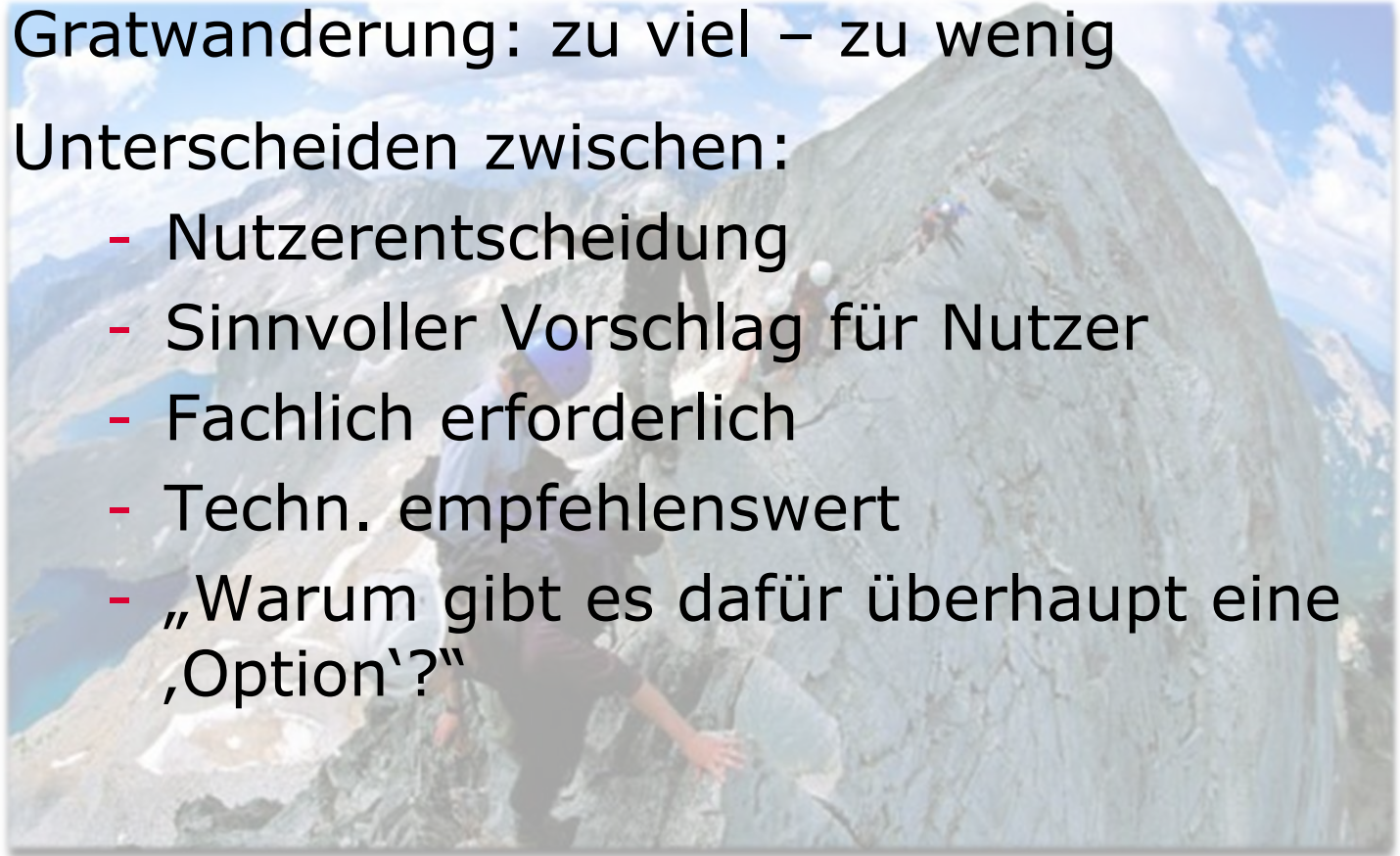
A decorative branch with small red berries is located in the top-left corner of the slide.

Herausforderungen

Gratwanderung: zu viel – zu wenig

Unterscheiden zwischen:

- Nutzerentscheidung
- Sinnvoller Vorschlag für Nutzer
- Fachlich erforderlich
- Techn. empfehlenswert
- „Warum gibt es dafür überhaupt eine ‚Option‘?“





Begriffsbestimmung

Richtlinie/Policy

vs.

Einstellung/Setting

vs.

Policysetting (Neologismus)

Policies

Was ist das?

Zuordnungsregeln von Einstellungen zu Personen

Basics | Comments | Administration

Basics

Policy name: [Create Child](#)

Policy type:

Description:

Category:

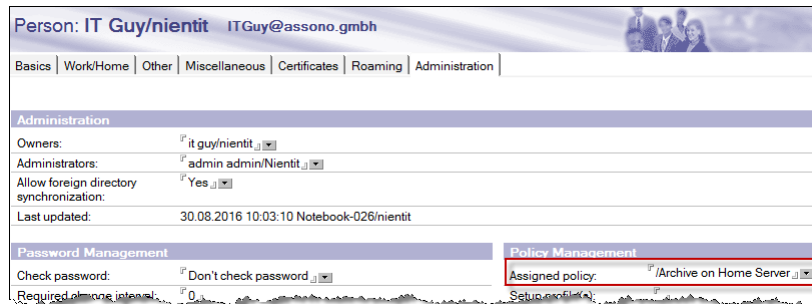
Setting Type	Setting Name	
Registration:	<input type="text"/>	New...
Setup:	<input type="text"/>	New...
Archiving:	<input type="text"/>	New...
Desktop:	<input type="text"/>	New...

Policies

Typen von Policies

3 Varianten:

- Organisatorisch (z.B: */assono)
- Explizit (im Personendokument)
- Dynamisch (im Policydocument)



Person: IT Guy/nientit ITGuy@assono.gmbh

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming | Administration

Administration

Owners: IT Guy/nientit

Administrators: admin admin/Nientit

Allow foreign directory synchronization: Yes

Last updated: 30.08.2016 10:03:10 Notebook-026/nientit

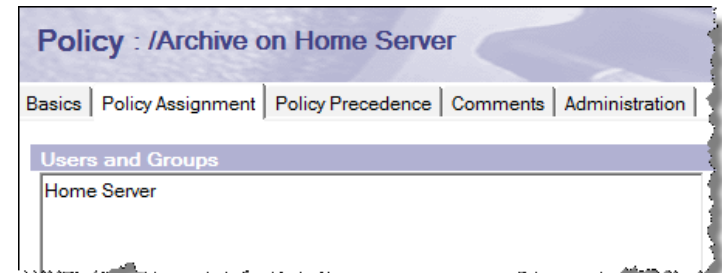
Password Management

Check password: Don't check password

Required among internal: 0

Policy Management

Assigned policy: /Archive on Home Server



Policy : /Archive on Home Server

Basics | Policy Assignment | Policy Precedence | Comments | Administration

Users and Groups

Home Server

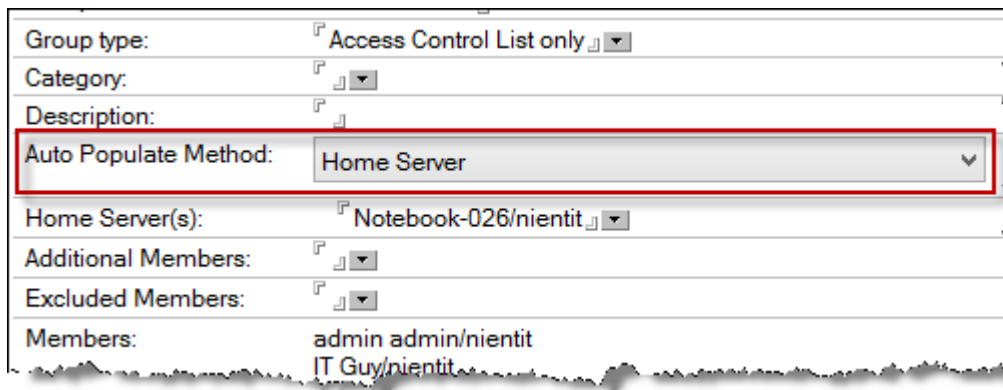
„Beliebig“ viele kombinierbar

Policies

Dynamische Richtlinie

Neu mit Domino 8.5.1

Gut zu kombinieren mit berechneten Gruppen

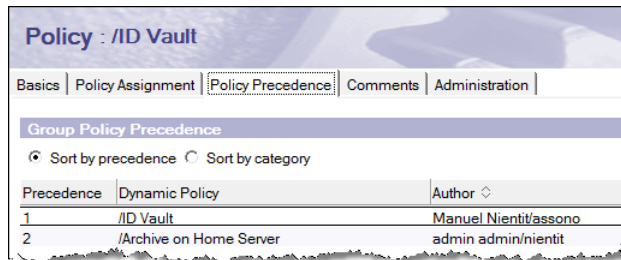


Group type:	Access Control List only
Category:	
Description:	
Auto Populate Method:	Home Server
Home Server(s):	Notebook-026/nientit
Additional Members:	
Excluded Members:	
Members:	admin admin/nientit IT Guy/nientit

Policies

Policy Precedence

- Es findet ein *Merge* auf Ebene der Polycysettings statt
- Die *expliziteste* zieht
 - Explizit vor dynamisch vor organisatorisch
- Auf Ebene der dynamischen Richtlinien kommt die Precedence ins Spiel

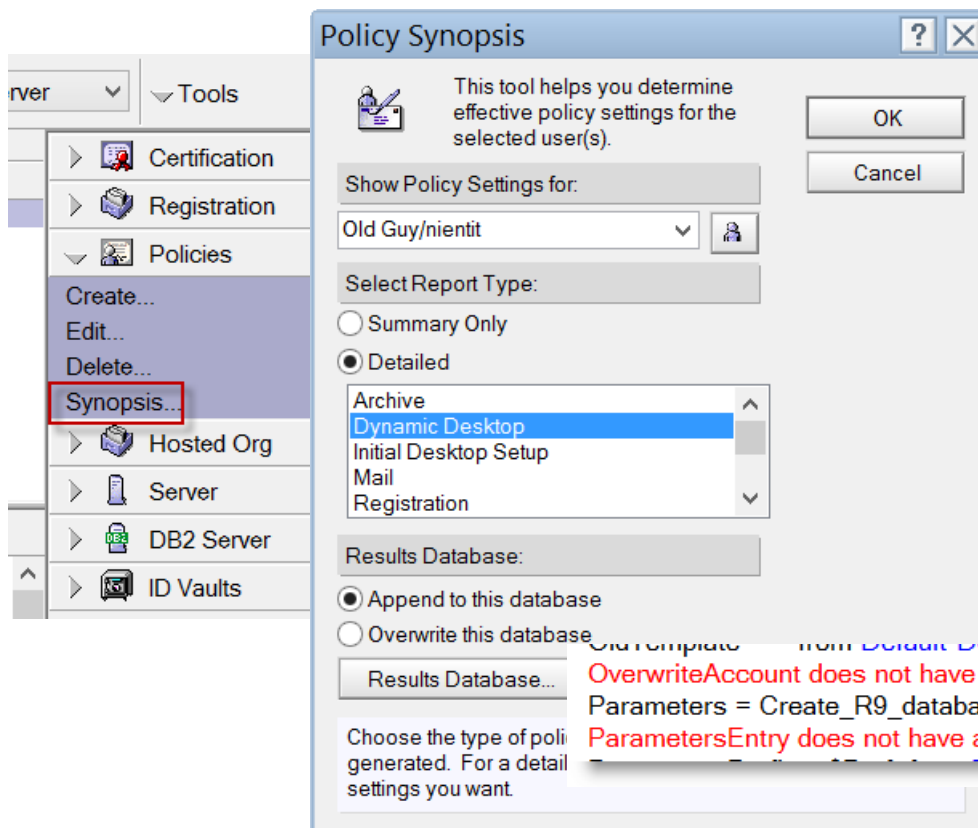


Policy : /ID Vault		
Basics Policy Assignment Policy Precedence Comments Administration		
Group Policy Precedence		
<input checked="" type="radio"/> Sort by precedence <input type="radio"/> Sort by category		
Precedence	Dynamic Policy	Author
1	/ID Vault	Manuel Nientit/assono
2	/Archive on Home Server	admin admin/nientit

Policies

Was gilt?

Policy Synopsis



Effective Policy for: Old Guy/nientit

Derived from the following policies:

*/nientit
*

Old Template from Default Desktop assigned in policy */nientit

OverwriteAccount does not have a value set

Parameters = Create_R9_databases=1, Enforce from Default-Desktop assigned in policy */nientit

ParametersEntry does not have a value set



Policies

Grundlegende Philosophie

Eine für Alle!



Geht natürlich selten



- > So wenig Ausnahmen und so flach wie möglich



Policies

Überlegungen zur Struktur

Abhängigkeiten vom Home-Server

- Archivierung
- Repliken
- Roaming

Abhängigkeit vom Endpoint

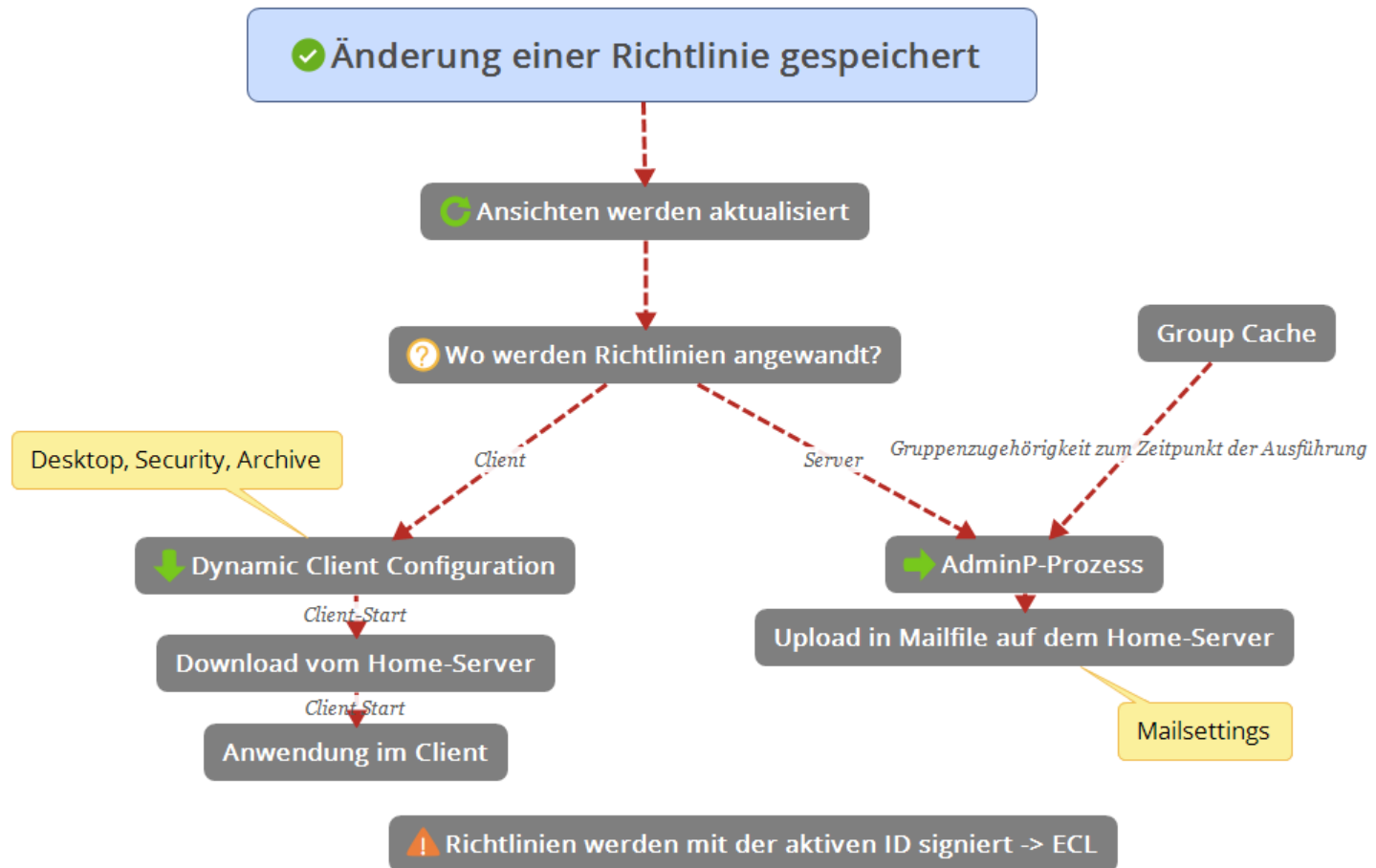
- Repliken
- Roaming

Abhängigkeit von Org-Einheit

- Repliken

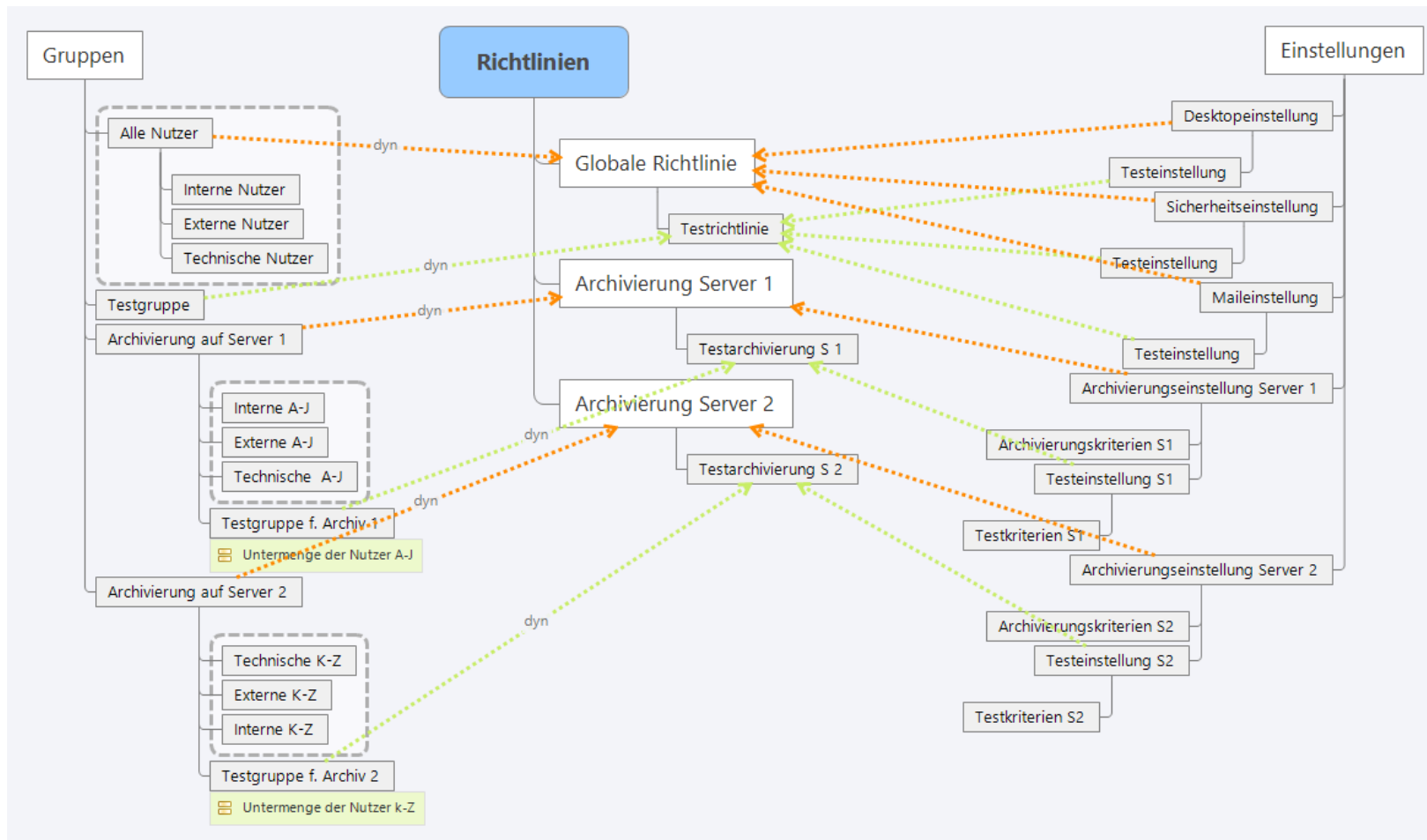
Policies

Wie werden Richtlinien angewandt?



Policies

Ein Fallbeispiel





Richtlinien

Zum Fallbeispiel

Eventuell wäre es sinnvoll, die dynamische Zuweisung zur Gruppe „Alle Nutzer“ durch eine organisatorische Richtlinie zu ersetzen?

Die manuell Erstellung der Gruppen „A-J“ und „K-Z“ kann durch eine berechnete Gruppe nach „Home-Server“ ersetzt werden.

Vorteil in beiden Fällen: die Gruppen müssen nicht manuell gepflegt werden, so dass es nicht zu Fehlern kommt, wenn die Pflege vernachlässigt wird.



Einstellungen

- Enthalten die tatsächlichen Einstellungs-Items
- 10 verschiedene Einstellungstypen
- Maximal ein Einstellungsdocument pro Typ und Richtlinie
- Mehrfachverwendung von Settings möglich



Einstellungen

Typen 1/3

Archive-Settings

- E-Mail Archivierung
- Server und/oder lokal
- Regeln und Ziele

Dynamic Desktop

- IBM Notes-Client Einstellungen
- Lücke: Connections und Locations
- Keine Fernanalyse möglich



Einstellungen

Typen 2/3

Initial Desktop Setup

- (fast) redundant zu dynamic Desktop

Mail-Settings

- Entspricht ca. den Mailvorgaben
- Nicht zu viel einstellen

Registration Settings

- Vorgaben für die Registrierung

Traveler Settings

- Wenn keine eingestellt, dann Default Settings



Einstellungen

Typen 3/3

Security

- Passwort
- Netzwerk
- ECL
- ID Vault

Connections und
Symphony(Produktivitätswerkzeuge) sind
obsolet

Roaming Settings

- Was und wo?

Einstellungen

Vererbung/Durchsetzung

- Inherit from parent policy (fast alle)
- Enforce in Child Policy (nur die wichtigsten)



All users

Corporate Home Pages database: ☐ Don't set value

Default Home Page:

Home page selection: ☒ Do not allow

[Discover Page](#)

- Kein Anwendungsfall für „Set value whenever modified“ bekannt -> nicht einsetzen



Einstellungen

Desktop - steuerbar

Steuerung der Clienteeinstellungen

- Notes.ini
- Repliken/Lesezeichen
- Mailreplika (Managed)
- Proxy
- Diagnostic
- Eclipse-Settings nur mit fortgeschrittener Kenntnis



Einstellungen

Desktop – nicht steuerbar

- Arbeitsumgebungen (nur eingeschränkt)
- Verbindungen
- Replication-Page
- Vorhandene Repliken nicht identifizier-/löschar



Einstellungen

Desktop – Vorschläge (1/6)

- Private Arbeitsumgebungsdokumente nicht zulassen
- Beim Klicken auf einen Hyperlink im Standard-Client folgenden Browser verwenden: OS-Browser
- Open List/Launcher -> Lesezeichenleiste (Vorschlag)
- Enable Synchronize Contacts (!)



Einstellungen

Desktop – Vorschläge (2/6)

- “Do not automatically add names to recent contacts” (?)
 - DPABRemoveRule
 - DisableDPABCCandToprocessing
 - DisableDPABCCprocessing
 - DisableDPABReceivedprocessing
- Mail-File Replik – Managed Replica (?)
- Enable silent failover when server goes down



Einstellungen

Desktop – Vorschläge (3/6)

- Empty Trash Folder (?)
- Save state on exit (Vorschlag)
- Enable Auto Save
- Make Internet URLs into Hotspot
- Drag and Drop save as eml file
- Require My Permission to show remote images (Schutz gegen Trackermails)



Einstellungen

Desktop – Vorschläge (4/6)

- Save sent mail (Standard – sollte nicht deaktiviert werden können)
- When mail arrives slide in Summary (Vorschlag – kennen viele nicht)
- Replication schedule gilt für ALLE Arbeitsumgebungen (außer „no connection“)



Einstellungen

Desktop – Vorschläge (5/6)

- Disabled Ports=LAN0 (BSI Empfehlung)
- AttachmentActionDefault=1 (2/3/4)
 - Öffnet Anhänge immer in einem bestimmten Modus – ohne Dialog (Öffnen/Bearbeiten/Ansicht/Speichern)
- **Achtung: Notes.ini Parameter entfernen nicht direkt möglich**
 - Ungültigen Wert übergeben: z.B. „“



Einstellungen

Desktop – Vorschläge (6/6): Diagnostic Collection Options

- Bei jedem Absturz läuft nsd
- Nsd-logs können an den Server zu Auswertung gesendet werden
- Sollte nicht optional sein -> „Prompt user to send diagnostic reports: No“
- Standardeinstellungen sonst OK



Einstellungen

Mail – (nicht) steuerbar

Entspricht ~ Mailvorgaben

- Keine Mail-Regeln einstellbar
- Von persönlichen Vorlieben abhängig, daher nur wenig vorgeben



Einstellungen

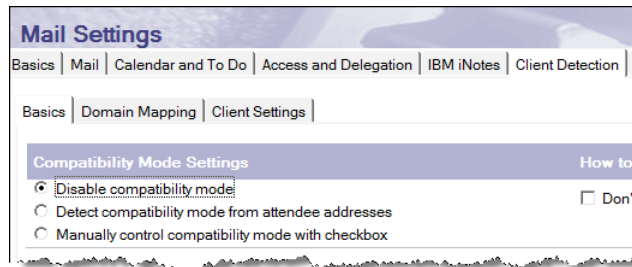
Mail – Vorschläge (1/2)

- Allow users to change mail file ownership: No (sicherheitsrelevant)
- Enable mailbox maintenance: No
 - Besser: Quota und Archivierung
- Message recall (?)
- Terminkonflikte prüfen

Einstellungen

Mail – Vorschläge (2/2)

Kompatibilitätsmodus



Mail Settings

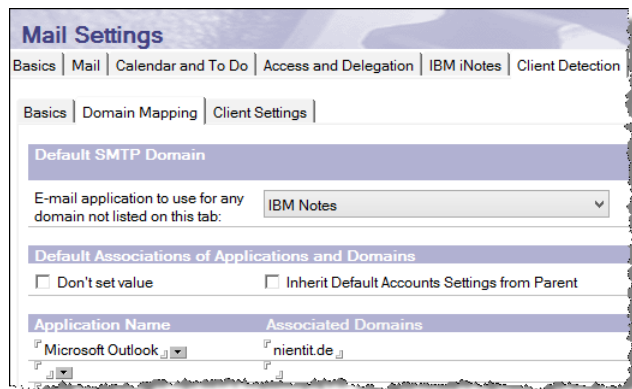
Basics | Mail | Calendar and To Do | Access and Delegation | IBM iNotes | Client Detection

Basics | Domain Mapping | Client Settings

Compatibility Mode Settings How to...

- ☒ Disable compatibility mode
- ☐ Detect compatibility mode from attendee addresses
- ☐ Manually control compatibility mode with checkbox

☐ Don't



Mail Settings

Basics | Mail | Calendar and To Do | Access and Delegation | IBM iNotes | Client Detection

Basics | Domain Mapping | Client Settings

Default SMTP Domain

E-mail application to use for any domain not listed on this tab: IBM Notes

Default Associations of Applications and Domains

☐ Don't set value ☐ Inherit Default Accounts Settings from Parent

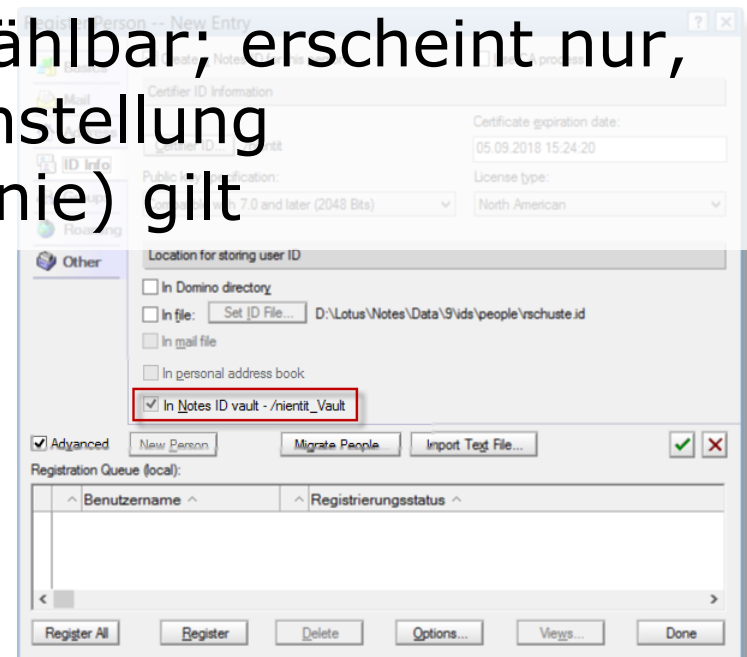
Application Name	Associated Domains
Microsoft Outlook	nientit.de
	

Einstellungen

Registrierung

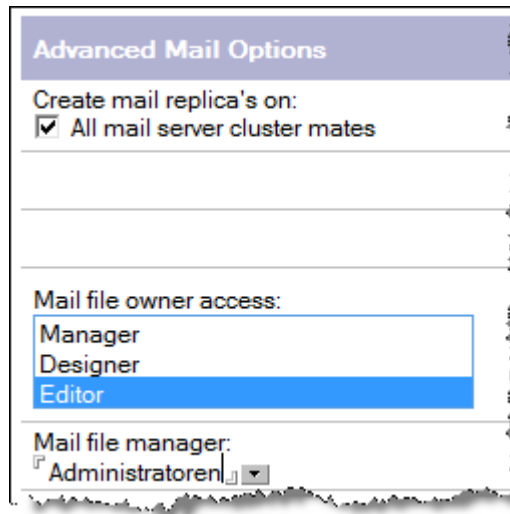
Steuert den Registrierungsprozess so weit, dass ggf. nur noch Benutzername und Kennwort eingegeben werden muss

Achtung: ID-Vault nicht wählbar; erscheint nur, wenn eine Sicherheitseinstellung (organisatorische Richtlinie) gilt



Einstellung Registrierung

Vorschläge

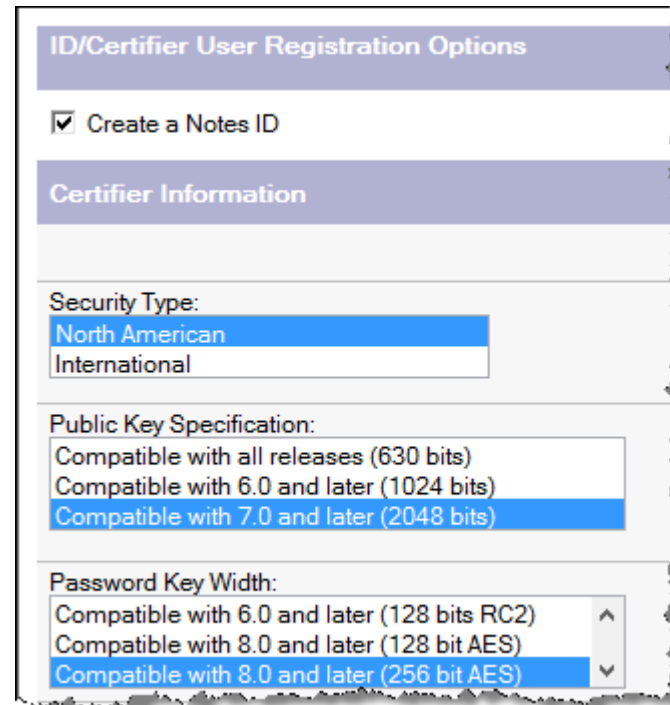


Advanced Mail Options

Create mail replica's on:
☒ All mail server cluster mates

Mail file owner access:
Manager
Designer
Editor

Mail file manager:
Administratoren



ID/Certifier User Registration Options

☒ Create a Notes ID

Certifier Information

Security Type:
North American
International

Public Key Specification:
Compatible with all releases (630 bits)
Compatible with 6.0 and later (1024 bits)
Compatible with 7.0 and later (2048 bits)

Password Key Width:
Compatible with 6.0 and later (128 bits RC2)
Compatible with 8.0 and later (128 bit AES)
Compatible with 8.0 and later (256 bit AES)

Group assignments beachten



Einstellungen

Sicherheit – (nicht) steuerbar

- Passwortsicherheit (SSO, NSL, NFL)
- Plugins
- Schlüsselstärke
- ID-Vault
- ECL(!)

Nicht steuerbar:

- Verschlüsselung (DB, Mail...)



Einstellungen

Sicherheit – Vorschläge

- "Update Internet Password When Notes Client Password Changes = No" – BSI
- Passwortstärke (Achtung bei SSO)
- PW-Gültigkeit (Achtung bei SSO)
- SSO-Einstellung (?)
- Signed Plugins – Nutzer fragen (außer IBM)
- Schlüsselstärke (Rollover möglich)



Einstellungen

Sicherheit – ID Vault

- Kennwort muss nach Zurücksetzung geändert werden = Ja
- Notes-basierte Programme dürfen ID Vault verwenden = Nein
- Automatische ID Downloads zulassen = ? – normalerweise nicht, aber bei Roaming?



Einstellungen

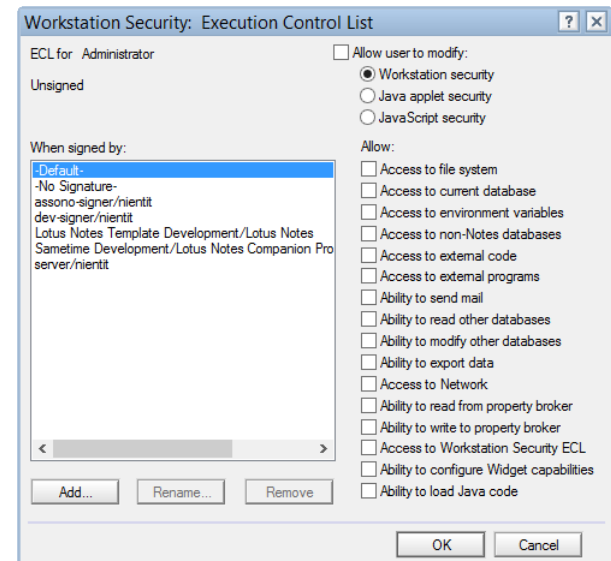
Sicherheit – ECL (1/2)

- Kann die Ausführung ungeprüfter Fremdanwendungen verhindern
- Unterbindet unerwünschte Funktionen
- Funktioniert nur ideal mit einem differenzierten Signaturkonzept
 - Für jeden Fremdanbieter eine eigene Signatur
 - Interne Entwickler eine eigene Dev-ID

Einstellungen

Sicherheit – ECL (2/2)

- Default und Anonymous = Kein Zugriff
- Eigentümer/Nutzer keine Rechte zur Änderung der ECL
- IBM Signaturen = Volle Rechte
- Dev-ID minimale Rechte
- KEINE Wildcard-Rechte





Einstellungen

Archivierung – (nicht) steuerbar

- Wer archiviert?
- Welche Kriterien?
- Wohin?

Nicht einstellbar:

- Wann wird archiviert bzw. was ist Auslöser?
 - Entweder manuell durch Nutzer oder
 - Programmdokument: compact -a



Einstellungen

Archivierung – Besonderes

In den Archivierungskriterien können Zielserver angegeben werden

-> ggf. mehrere Zielserver, so dass pro Archivserver eine eigene Richtlinie mit eigener Einstellung erstellt werden muss: 1:1:1



Einstellungen

Archivierung – Vorschläge

- Private Archivierung nicht zulassen = ja
- Archivierung erfolgt auf Server = ja
- Dokument nur löschen, wenn die Kriterien auch alle Antworten löschen = Ja



Einstellungen

Archivierung – Vorschläge: Kriterien

- Alte Dokument in Archivdatenbank kopieren; dann Datenbank bereinigen
- Ältere Dokumente aus Datenbank löschen
- Dokumente die nicht geändert wurden mehr als x (~365) Tage



Einstellungen

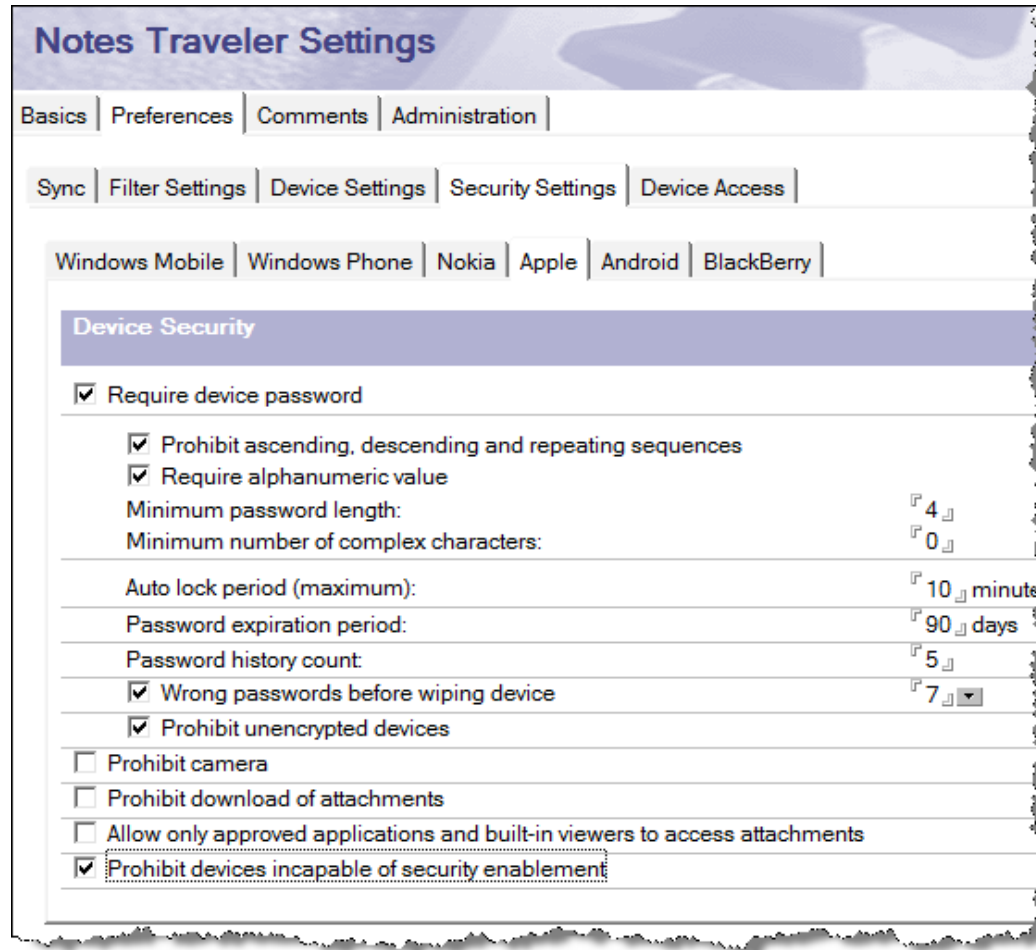
Traveler

Wenn keine Traveler Richtlinie vorhanden gelten die Default-Einstellungen aus der lotustraveler.nsf

- Sicherheitseinstellungen
- Sync-Einstellungen (Roaming)
- Größenfilter

Einstellungen

Traveler – Vorschläge (1/2)



Notes Traveler Settings

Basics | Preferences | Comments | Administration

Sync | Filter Settings | Device Settings | Security Settings | Device Access

Windows Mobile | Windows Phone | Nokia | Apple | Android | BlackBerry

Device Security

- ☒ Require device password
 - ☒ Prohibit ascending, descending and repeating sequences
 - ☒ Require alphanumeric value
 - Minimum password length: 4
 - Minimum number of complex characters: 0
 - Auto lock period (maximum): 10 minutes
 - Password expiration period: 90 days
 - Password history count: 5
 - ☒ Wrong passwords before wiping device: 7
 - ☒ Prohibit unencrypted devices
 - ☐ Prohibit camera
 - ☐ Prohibit download of attachments
 - ☐ Allow only approved applications and built-in viewers to access attachments
 - ☒ Prohibit devices incapable of security enablement

Einstellungen

Traveler – Vorschläge (2/2)

Notes Traveler Settings

Basics | Preferences | Comments | Administration |

Sync | Filter Settings | Device Settings | Security Settings | Device Access

Restrict Device Access

☒ Require approval for device access

Number of devices to allow per user before approval is required:

Optional: Addresses to notify when approval action is pending:

Configuration Settings : Notebook-026/nientit

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings

Internet Lockout

Enforce Internet Password Lockout:

Log Settings: ☒ Lockouts ☐ Failures

Default Maximum Tries Allowed:

Default Lockout Expiration:

Default Maximum Tries Interval:



Troubleshooting

Wie bemerke ich überhaupt Fehler?

Im Regelfall erst, wenn sie sichtbare Symptome haben -> Zu spät

Kein SOLL-IST-Abgleich möglich



Tests entdecken zumindest teilweise konzeptionelle Fehler



Troubleshooting

Geduld!

Ist ausreichend Zeit seit Änderung der Richtlinie vergangen?

- Ansichtenaktualisierung
- Aktualisierung Group Cache
- Replikation auf Homeserver
- Ausführung von AdminP (alle 12h)
 - Tell adminp process mail policy
- Clientneustart ($\geq 2x$)





Troubleshooting

Wer?

- Viele:
 - Zuordnung der Einstellung zur Richtlinie korrekt?
 - Richtlinie korrekt zugeordnet?
 - Signatur der Richtlinie berechtigt?
- Einer:
 - Policy-Synopsis



Troubleshooting

Client

- Log.nsf
 - <date> <time> Dynamic Client Configuration started
 - <date> <time> Initializing Dynamic Client Configuration
 - <date> <time> Dynamic Client Configuration updating location information
 - <date> <time> Dynamic Client Configuration shutdown
 - Debug_Policy=1 - for general policy troubleshooting
 - Debug_Dynconfig=1 - for dynamic client configuration checking
- > Zeigt leider nur eingeschränkt, was geladen wird



Troubleshooting

Client

- Versteckte Ansicht „(\$Policies)“ in names.nsf
 - Masken nicht vorhanden (ggf. aus pubnames.ntf kopieren)
 - Felder nicht sprechend benannt (im Design prüfen)
- Lokale Dokumente löschen
- Richtlinien auf Server erneut speichern
- Client mehrfach ($\geq 2x$) neu starten



Troubleshooting

Client

Calendarprofil untersuchen (Zusatztool erforderlich)

iNotes-Profil untersuchen (Zusatztool erforderlich)

-> Ultimativ: PMR erzeugen



Fragen?

Jetzt stellen oder später...



Heiße Quellen

Dynamic Policies: <https://www-10.lotus.com/ldd/dominowiki.nsf/dx/domino-policies-an-example-using-the-new-8.5-features>

How do policy changes get applied?: <https://www-10.lotus.com/ldd/dominowiki.nsf/dx/when-will-a-domino-policy-change-take-effect>

How the new Dynamic Group Policies can reduce your administration workload: <https://www-10.lotus.com/ldd/dominowiki.nsf/dx/how-the-new-dynamic-group-policies-can-reduce-your-administration-overhead>

Troubleshooting Policies on a Domino Server: <http://www-01.ibm.com/support/docview.wss?uid=swg27036076>

Domino Policy Precedence Explained: <https://www-10.lotus.com/ldd/dominowiki.nsf/dx/domino-policy-precedence-explained>

Notes / Domino Policy Troubleshooting Flow Chart: https://www-10.lotus.com/ldd/dominowiki.nsf/dx/Notes_Domino_Policy_Flow_Chart