

# Policies richtig verwenden

Was geht und was nicht mit Standardmitteln

A solid blue horizontal bar.

# Agenda

1. Architektur
2. Einstellungen zuweisen
3. Vererbung von Policies: Inherit / Enforce
4. Mechanismen
5. Debugging

# Architektur: Woraus bestehen Policies

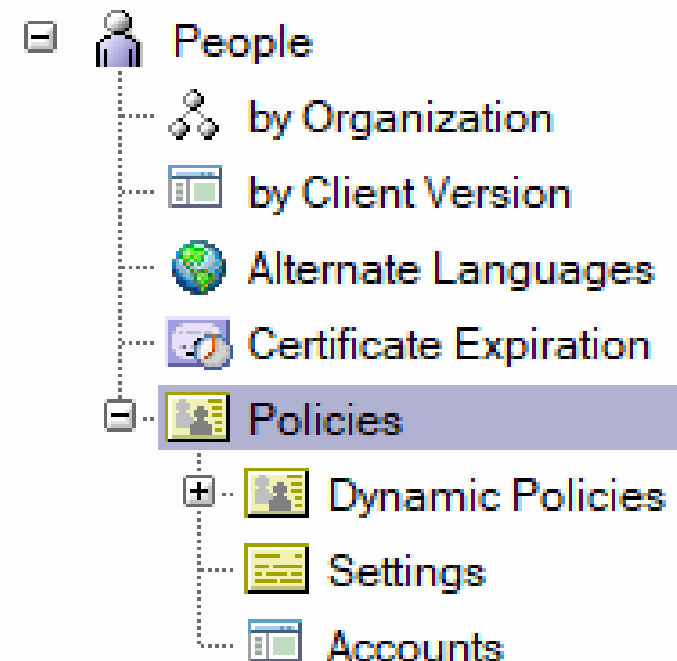
## 1. Settings

- Einstellungsdokumente für die verschiedenen Bereiche.
- n Einstellungsdokumente für jeden Typ.
- Alleine stehend keine Auswirkung auf Benutzer

## 2. Policies

- Weisen bestimmte Einstellungen bestimmten Personen zu
- Zuweisung der Settings passiert über die UNID des Dokuments:  
Cut & Paste von Settings- Dokumenten zerstört diese Zuweisung!

Setting Type	Setting Name
Registration:	
Setup:	
Archiving:	
Desktop:	
Security:	<Policy has been deleted>
Mail:	
Connections:	
Lotus Traveler:	
Roaming:	
Symphony:	



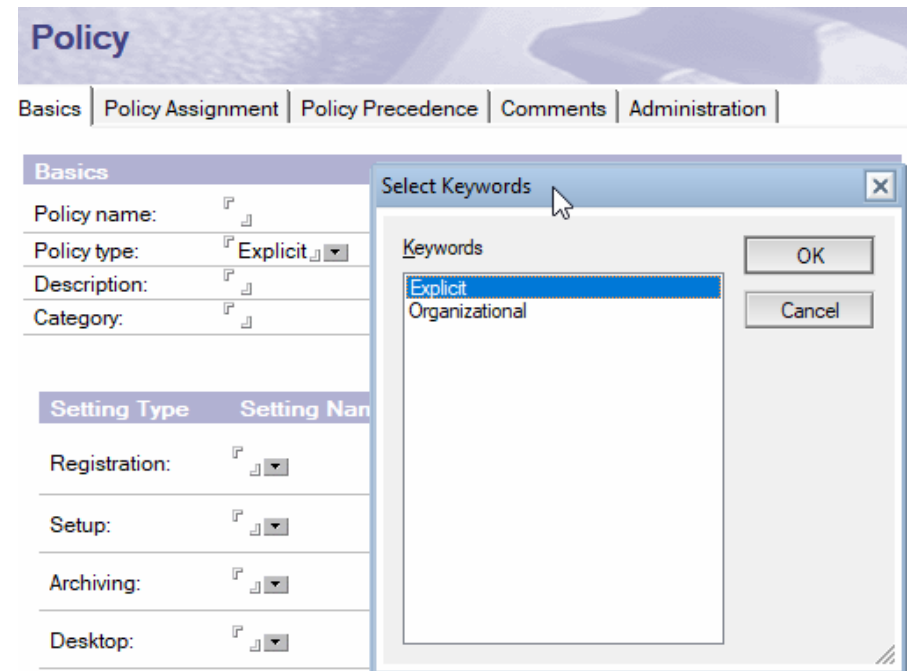
# Architektur: Policytypen

## 1. Hierarchisch (=Organizational)

- Zuweisung erfolgt über OUs, O, C
- Gilt automatisch für alle Benutzer mit passendem Certifier:  
Torsten Link/Freiburg/Bechtle-Gruppe/DE matcht auf:
  - \*/Freiburg/Bechtle-Gruppe/DE
  - \*/Bechtle-Gruppe/DE
  - \*/DE

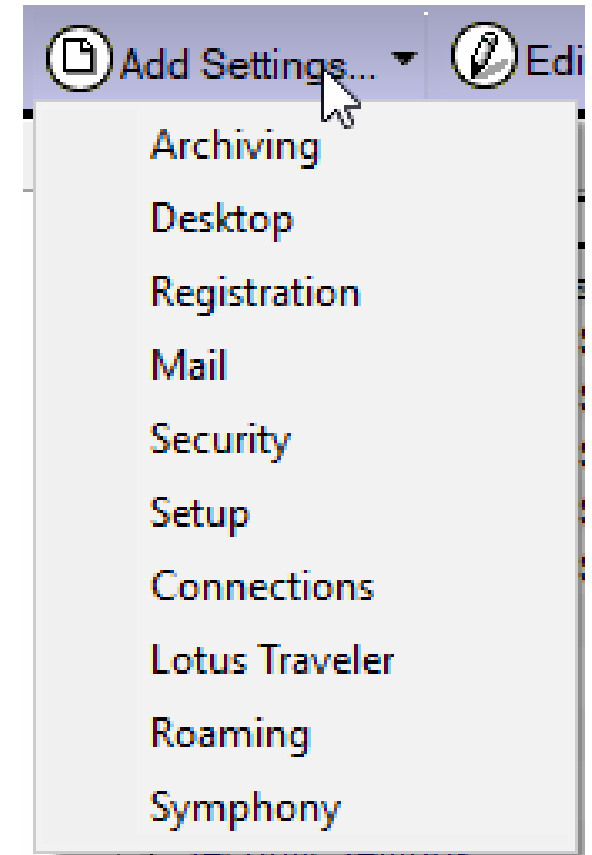
## 2. Explizit / Dynamisch (=Explicit)

- Zuweisung erfolgt Explizit über:
  - Direkte Zuweisung im Personendokument:  
Alte Methode → NICHT MEHR VERWENDEN
  - Zuweisung über „Policy Assignment“- Tab der Policy  
→ Policies, die so zugewiesen werden, heißen „Dynamisch“



# Architektur: Welche Settings

1. **Archiving** : Archivierungsvorgaben: Lokal oder Server, Kriterien vorgeben
2. **Desktop**: hunderte Einstellungen, um den Client einzurichten
3. **Registration**: Erleichtert Administration, vermeidet Fehleingaben (ClusterRepliken, Zugriff, etc)
4. **Mail**: Anpassungen des Kalenderprofils + Disclaimer
5. **Security**: Kennwortrichtlinien, ID Vault, Kennwortsynchronisierung
6. **Setup**: Subset der Desktop- Richtlinien, größtenteils verdrängt durch Desktop Settings
7. **Connections**
8. **Lotus Traveler**: Vorgaben für Traveler Devices, analog zu LotusTraveler.nsf
9. **Roaming**: File system Roaming
10. **Symphony**: Obsolet



# Einstellungen zuweisen

## 1. Es wird unterschieden zwischen „Admin“- Einstellungen und „Benutzer“- Einstellungen:

- Admin- Einstellungen sind die, für die es keine GUI- Einstellungen gibt. Für diese gibt es nur „Setzen“ oder „Nicht setzen“ (Don't set value)

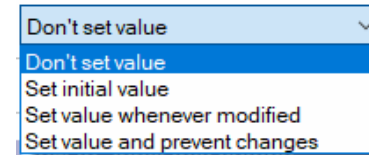
How to apply this setting:

☐ Don't set value

- Benutzer- Einstellungen sind die, die der Benutzer irgendwo in der GUI verändern kann, für diese gibt es vier Optionen:

- Don't set value: nicht setzen
- Set initial value: Wert initial EINMAL setzen  
**ACHTUNG:** Ist kein „Set Once“, wird also nicht „immer wieder mal“ gesetzt, wenn die Policy gespeichert wird.

How to apply this setting:








- Set value whenever modified: Wert wird jedesmal gesetzt, wenn die DCC läuft (ndyncfg.exe, bei jeder Authentifizierung am Server, typischerweise Client- Neustart)
- Set value and prevent changes: Veränderung der Einstellung durch den Benutzer verhindern.  
**ACHTUNG:** Ob Felder in Profilen bearbeitbar sind, bestimmt deren Design:  
→ Falsches Template → Keine Sperrung

# Vererbung

1. Für jede Einstellung gibt es für jeden Benutzer genau EINEN Wert. Der Wert wird nach „Spezifität“ folgendermassen bestimmt: Je spezifischer eine Einstellung, desto höher ihre Priorität:
1. Explizite Policy: Eine Policy, die dem Benutzer direkt zugewiesen ist, hat die höchste Priorität
2. Dynamische Policy: Hat der Benutzer mehrere Dynamische Policies, dann bestimmt die „Policy Precedence“.  
ACHTUNG: Umsortieren über „Increase Precedence“ und „Decrease Precedence“ signieren ALLE beteiligten Policies.

Anmerkung: Auch Dynamische Policies können „Pseudo“- Hierarchisch über „/“ im Namen organisiert werden. Vererbung funktioniert dann gemäß der Hierarchischen Vererbung.

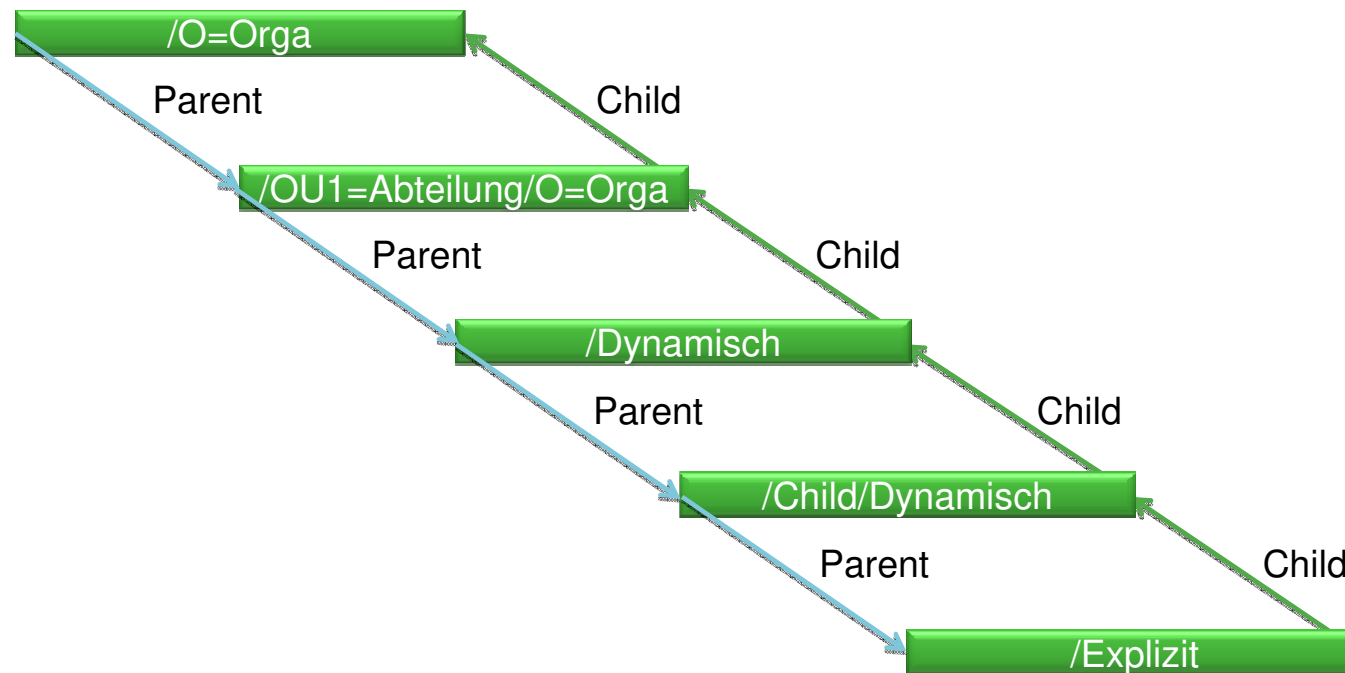
 Add Policy  Edit Policy  Delete Policy  Increase Precedence  Decrease Precedence		
Precedence	Dynamic Policy	Author
2	/Desktop Settings	
3	/MOBILE ACCESS DEL	
4	/MOBILE ACCESS VAR	

3. Hierarchische Policy: /OU1/OU2/O vor /OU2/O vor /O

➔ Diese feste Reihenfolge kann durch „Enforce“ und „Inherit“ verändert werden.

# Vererbung: Parent / Child

1. Aus der vorhergehenden Folie ergibt sich der folgende „Parent / Child“- Baum.
2. Die Parent / Child- Beziehung geht dabei über die verschiedenen Policy- Typen hinweg!





# Vererbung: INHERIT / ENFORCE

1. Gemäß vorheriger Folie sind die organisatorischen Policies die „schwächsten“. Policies. Gleichzeitig sind sie die „weitreichendsten“
2. Es kann Einstellungen geben, die man „für alle“ setzen möchte, diese aber nicht in jeder einzelnen Policy eintragen möchte: Für diese Einstellungen setzt man das „Enforce“- Flag in der übergeordneten Policy: Die Einstellungen werden in allen Child- Policies forciert, die Einstellungen in den Childs werden ignoriert. Es gibt keine Ausnahme vom „Enforce“ \*
3. Umgekehrt kann man Policies definieren, die als „Ausnahmepolicies“ definiert sind. Dann setzt man Enforce NICHT, dafür in der Child- Policy überall „Inherit“: Die Child- Policy ignoriert dann ihre eigene Einstellung und übernimmt diese Einstellung aus dem Parent. Bei den einzelnen Settings, die man ändern möchte, lässt man dann das Flag weg.

Inherit from parent policy:	Enforce in child policies:

\* Außer Exemption Policy – siehe nächste Seite

☐ Inherit

☐ Enforce

# Vererbung: INHERIT / ENFORCE

## 1. Ausnahme: Exemption Policy

Auf dem Administrations- Tab kann man ein Häkchen setzen bei “Ignore settings from ancestor policies”.

## 2. Damit wird diese Policy aus der Hierarchie “herausgelöst”: Parent- Policies gelten für diese Art der Policy gar nicht.

## 3. Trotzdem vererbt eine Exemption Policy ihre Einstellungen an Ihre Children weiter.

Policy : /Test Dynamic

Basics | Policy Assignment | Policy Precedence | Comments | Administration

**Administration**

Owners:	Torsten Link/Link
Administrators:	Torsten Link/Link
Exception Policy:	<input checked="" type="checkbox"/> Ignore settings from ancestor policies
Last updated:	15.09.2018 11:53:55 Torsten Link/Link

# Mechanismen

## Wo werden Policies verarbeitet

Client	Server
Archive	Archive (lo compact –A)
Desktop	Mail (tell adminp process mail)
Registration	IBM Traveler (tell adminp process traveler)
Security	
Setup	
Connections	
Roaming	
Symphony	

# Mechanismen

1. Server ermittelt vs. (\$Policies)- View die korrekte Einstellung für den User
  - Der Zeitstempel des Ansichts- Index der Ansicht bestimmt, ob sich was geändert hat.
2. Serverbasierte Policies werden durch den AdminP assigned.
  - Standardmäßig alle 12 Stunden, kann gesteuert werden über ini- Parameter **ADMINP\_POLL\_INTERVAL** bzw.  
manuell über **tell adminp process mail** oder **tell adminp process traveler**
3. Clientbasierte Policies werden bei jeder Serverauthentifizierung durch die Dynamische Client Configuration DCC angewendet (ndyncfg.exe)

# Mechanismen - DCC

1. Der Client sendet während der Authentifizierung einen Hash der aktuellen Policies an den Mail- / Homeserver
2. Der Server berechnet ebenfalls einen Hash dessen, was der Client haben sollte
3. Der Server vergleicht die beiden Hashes
4. Stimmen die Werte nicht überein, sagt der Server dem Client, dass er die Policies neu ziehen soll.

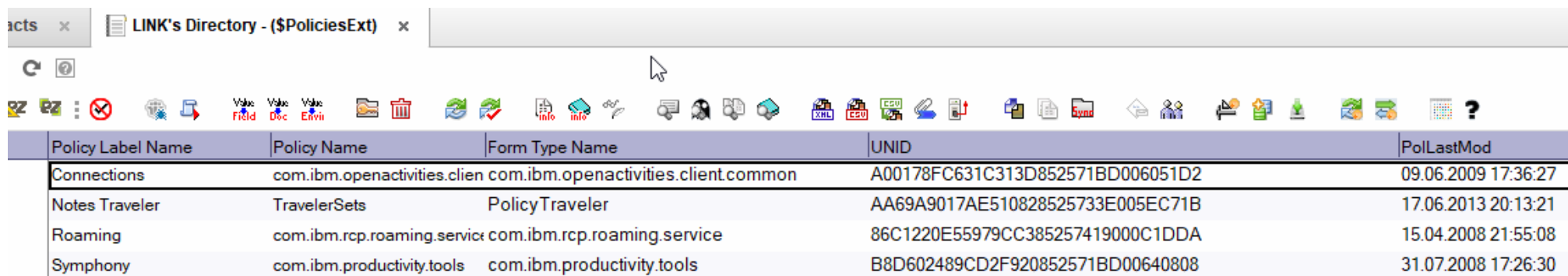
# Mechanismen - DCC

1. DCC speichert gecachte Policies in (\$Policies)- Ansicht in lokaler names.nsf
  - Können nicht „angeschaut“ werden, weil Masken und Script- Libraries fehlen → Troubleshooting
2. DCC speichert außerdem Informationen über zugewiesene / Effektive Policies im DirectoryProfile der lokalen names.nsf
  - Informationen können falsch sein → Troubleshooting

# Troubleshooting

1. Scope: Betrifft das Problem EINEN Benutzer oder alle?
2. Gibt es Fehlermeldungen zu den Policies am Server (DDM):
  - Typischerweise Probleme mit Signatur (vielleicht hat ein Admin das Unternehmen verlassen?)
  - Policies abspeichern signiert sie NICHT zwingendermassen neu.
  - Die Signatur lässt sich nicht einfach ablesen, die Spalte im Directory ist NICHT aussagekräftig (obwohl da „Signed By“ steht).
  - Aktionen – Resign Policy auf gewählte Dokumente. Gilt für Policies UND Settings.
  - Manchmal sind aber die „Default“- Policies der IBM betroffen, die sieht man nicht in den normalen Ansichten. Diese sieht man nur in der Ansicht (\$PoliciesExt)

acts x LINK's Directory - (\$PoliciesExt) x

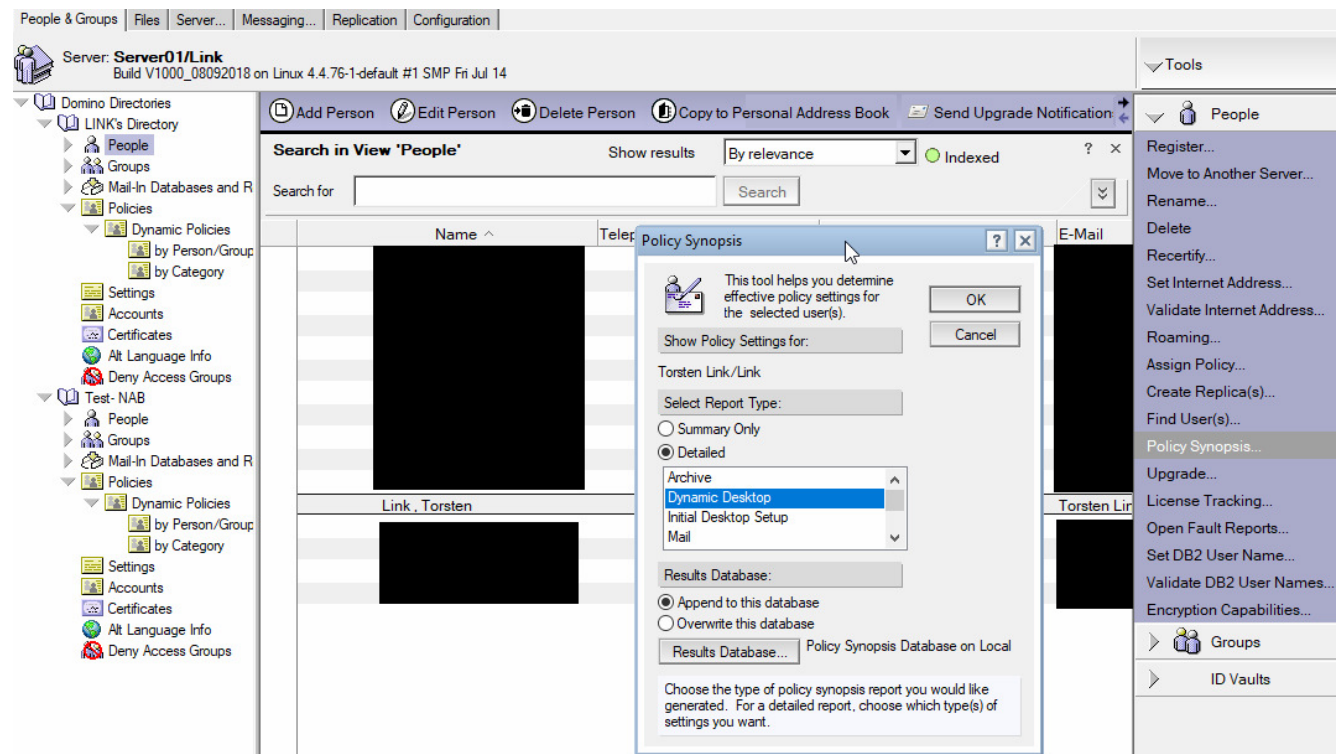


Policy Label Name	Policy Name	Form Type Name	UNID	PolLastMod
Connections	com.ibm.openactivities.client	com.ibm.openactivities.client.common	A00178FC631C313D852571BD006051D2	09.06.2009 17:36:27
Notes Traveler	TravelerSets	PolicyTraveler	AA69A9017AE510828525733E005EC71B	17.06.2013 20:13:21
Roaming	com.ibm.rcp.roaming.service	com.ibm.rcp.roaming.service	86C1220E55979CC385257419000C1DDA	15.04.2008 21:55:08
Symphony	com.ibm.productivity.tools	com.ibm.productivity.tools	B8D602489CD2F920852571BD00640808	31.07.2008 17:26:30

# Troubleshooting

## 1. Welche Policy hat der Benutzer laut Server – Stichwort Policy Synopsis

- Admin Client öffnen
- Benutzer in People & Groups wählen
- People – Policy Synopsis...
- „Detailed“
- Policy auswählen
- OK
- ACHTUNG: Der Dialog behält die Auswahl, man muss also die “Vorauswahl” vorher abwählen
- Dann aus Ansicht (ggf. Mit F9 aktualisieren) das letzte Dokument per Doppelklick öffnen





# Troubleshooting

## 2. Die Funktion berechnet die „Effektive Policy“

- Dummerweise werden die Werte in Form von Feldnamen + Feldwerte angezeigt → Wenn man die Feldnamen nicht kennt, muss man den Designer befragen

Contacts		How to apply this setting:
Enable "Synchronize Contacts" on the Replicator:	<input type="checkbox"/> Yes	Don't set value
Mark new contacts as private by default:	<input type="checkbox"/> Yes	Don't set value
Do not automatically add names to the Recent Contacts view:	Yes	Set value whenever modified

- Maske im Designer öffnen und Feld suchen:

Do not automatically add names to the Recent Contacts view:	\$PrefDisableDPABprocessing
---	-----------------------------

- \$Pref und \$Loc entfernen und dann in der Synopse suchen


Effective Policy for: [Torsten Link/Link](#)

Derived from the following policies:

[\\*/Link](#)

\*

[/Test Dynamic](#) (via dynamic assignment: [Torsten Link/Link](#))

 = Value was enforced in the specified settings document.

# Troubleshooting

## 1. Ist die Policy auf dem Client angekommen?

- names.nsf auf dem Client öffnen
- Shift + Strg + Menu „Ansicht – Gehe zu“
- (\$Policies) auswählen und prüfen, ob die Policy aktuell ist (Modified Datum, Feldwerte über Property Box).
- Leider sind die Masken der Settings- Dokumente nicht in der pernames.ntf vorhanden: Man kann die Dokumente nicht öffnen.
- Für erweitertes Troubleshooting kann man aber die Elemente der pubnames.ntf in die names.nsf per Designer kopieren, dann kann man die Dokumente auch anschauen:

### Masken

Policy Settings\Archive Settings	PolicyArchive	1
Policy Settings\Connections Settings	PolicyActivities	1
Policy Settings\Desktop Settings	PolicyDesktop	1
Policy Settings\Extended Settings	PolicyExt	1
Policy Settings\Lotus Traveler Settings	PolicyTraveler	1
Policy Settings\Mail Settings	PolicyMail	1
Policy Settings\Registration Settings	PolicyRegistration	1
Policy Settings\Roaming Settings	PolicyRoaming	1
Policy Settings\Security Settings	PolicySecurity	1
Policy Settings\Setup Settings	PolicySetup	1
Policy Settings\Symphony Settings	PolicyProdTools	1
Policy\Archive Criteria	PolicyArchiveCriteria	1

### Script- Libraries

Common	LotusScript
PolicyManagement	LotusScript
Isconst	LotusScript

### Gemeinsame Felder

\$HTMLAttributes
\$PolMdTm
\$PolRdrs
\$PolicyIFPIItems
\$PolicyPOLItems
LastMod
hbLoad
strMsg
vwCnt

# Troubleshooting – Policy nicht auf Client angekommen

## 1. Policy am Server erneut „verteilen“

- a. Betrifft das Problem nur einen Benutzer: Personendokument im Domino- Directory speichern: Eine Änderung am Personendokument triggert den Policy- Prozess
- b. Bei mehreren Benutzern: Policy- Dokument speichern und damit einen View- Rebuild der (\$Policies)- Ansicht auf dem Server triggern: Der Timestamp der Ansicht wird bei der Berechnung des Hashes für den Vergleich mit berücksichtigt.  
Alternativ:
  - Shift + Strg + Menu „Ansicht – Gehe zu“ im Domino Directory
  - (\$Policies) öffnen
  - Shift + F9, um einen Ansichts- rebuild zu triggern
  - ODER: lo updall -r names.nsf -t (\$Policies)

# Troubleshooting – Policy nicht auf Client angekommen

## 2. Policy am Client neu ziehen

- Client neustarten, triggert die DCC (ndyncfg), Policies sollten erneut gezogen werden.
- Manueller Aufruf ndyncfg: Einfach per Kommandozeile aus dem Programmverzeichnis „**ndyncfg xxx**“ eingeben.  
Es gibt keine dokumentierten Parameter für ndyncfg, aber in älteren Versionen erwartet sie „irgendeinen“. In früheren Dokumenten sah man hier oftmals „ndyncfg 20“ oder „ndyncfg 99“, aber auch ein „ndyncfg /?“ funktioniert...
- Wenn das nicht hilft: (\$Policies) in der Client names.nsf öffnen und alle Policies markieren und löschen, danach Neustart

# Troubleshooting – Policy nicht auf Client angekommen

## 2. Policy am Client neu ziehen

- Wenn alles nicht hilft: Holzhammermethode... Dann kann man das Directory- Profile in der lokalen names.nsf löschen, denn das enthält den Policy- Hash.

**ACHTUNG:** Enthält einige Benutzervorgaben

```

#include "lsconst.lss"
Dim db as NotesDatabase
Dim doc as NotesDocument
Dim ok as Variant
Set db = New NotesDatabase( "", "names.nsf" )
Set doc = db.GetProfileDocument( "DirectoryProfile" )
If not doc is Nothing then
    ok = MessageBox( "Wollen Sie wirklich die Kontaktvorgaben löschen", MB_OK +
    MB_YESNO + MB_ICONQUESTION , "ACHTUNG" )
    If ok = IDYES then
        Call doc.Remove( True )
        MessageBox "Profil wurde erfolgreich gelöscht", MB_OK +
        MB_ICONINFORMATION
    End If
Else
    MessageBox "Profil wurde bereits gelöscht", MB_OK + MB_ICONINFORMATION
End If

```

# Troubleshooting – Policy nicht auf Client angekommen

## 3. Debugging

- `DEBUG_DYNCONFIG=1`
- `DEBUG_POLICY=1`
- `CONSOLE_LOG_ENABLED=1`
  - Used for general troubleshooting
  - Enable the debug and force the policy to be updated
  - Contact support and provide console.log for review
  - You can also set this debug with value 2 or 4 for verbose
  - logging Can be enabled on client as well as on server
- `DEBUG_DUMP_POLICY=1`
- `DEBUG_POLICY_SIGNBIT=1`

# Allgemeines

1. Policies sind „Push only“: Das Löschen einer Policy hat KEINE Auswirkung auf die Clients. Sie Settings werden dadurch nicht zurückgesetzt.
2. Es gibt keine „Remove value“- Option. Einmal durch Policies gesetzt ist ein Wert so lange gültig, bis er wieder anders gesetzt wird. Es gibt keine „reset to default“ Option.
3. Set Initial ist trügerisch. Es ist KEIN Set Once: Wenn ein Wert irgendwie schon gesetzt ist, dann hat ein „Set Initial“ keine Auswirkung mehr.
4. Für ECHTE Client- Verwaltung gibt es Werkzeuge, die alle die Nachteile der Policies aufwiegen und vielen Zusatznutzen bieten. Christoph Adler erzählt Euch da sicher gerne etwas drüber.

# Zeit für Eure Fragen.

Weitere Infos:  
[bechtle.com](https://bechtle.com)

