
# Comtarsia Logon Client 2008

## Handbuch

Version: 5.1.14.4, 20. July July 2011

# Inhaltsverzeichnis

# 1.Beschreibung

Comtarsia Logon Client 2008 für Windows Vista, Windows 7 und Server 2008.


Der Comtarsia Logon Client 2008 ermöglicht eine primäre LDAP Authentifizierung gegen ein beliebiges LDAP-Verzeichnis für Vista, Server 2008 und Windows7.

Die von Microsoft ab Windows Vista und Server 2008 eingeführte Credential Provider Schnittstelle wird vom Comtarsia Logon Client 2008 verwendet und erstsetzt den Microsoft Logon Kachel durch den LDAP Logon Kachel. Es besteht die Möglichkeit jederzeit auf  Microsoft Logon Kachel umzuschalten oder den Logon Client so zu konfiguieren, dass der Microsoft Crendential Provider ausgeblendet wird und für den Anwender nur die LDAP Anmeldung zur Verfügung steht.


Die User Account Control (UAC) ermöglicht eine gezielte Authorisierung zur Ausführung von Anwendungen, welche lokale Administratorrechte benötigen. Mit dem Comtarsia Logon Client ist es möglich, diese temporären lokalen Administratorberechtigungen über LDAP Bentuzer / Gruppenmitgliedschaften zur realisieren.

Weitere Informationen über die Comtarsia SignOn Solutions entnehmen Sie bitte unserer Web Site:

http://signon.comtarsia.com

# 2.Installation

## 2.1 Installation mit den Installationsprogramm

Die Installation, bzw. ein Update erfolgt mittels des Installationsprogrammes "SOS2008-5.0.X.4.exe". Bei einem Update bleibt die Konfiguration erhalten und der Lizenzschlüssel wird nur ersetzt wenn die Gültigkeitsdauer des bereits installierten Schlüssels kürzer ist als die des mitgelieferten. (Gekaufte Lizenzschlüssel werden in der Regel nie ersetzt.)

Das Installationsprogramm kopiert die erforderlichen Dateien und setzt die notwendigen Registry Werte damit der Comtarsia Logon Client Credential Provider aktiv wird. Ebenso werden für Konfigurationsparameter, welche sich nicht bereits in der Registry befinden (zb vorherige Konfiguration bei Update), die Default Werte in die Registry eingetragen.

Im Anschluss an die Installation wird das Konfigurationsprogramm „Comtarsia Management Console" gestartet. Siehe: Comtarsia Management Console (ComtMC)

# 3. Comtarsia Management Console (ComtMC)

Die Comtarsia Management Console (ComtMC) kann jederzeit über das Startmenü aufgerufen werden.

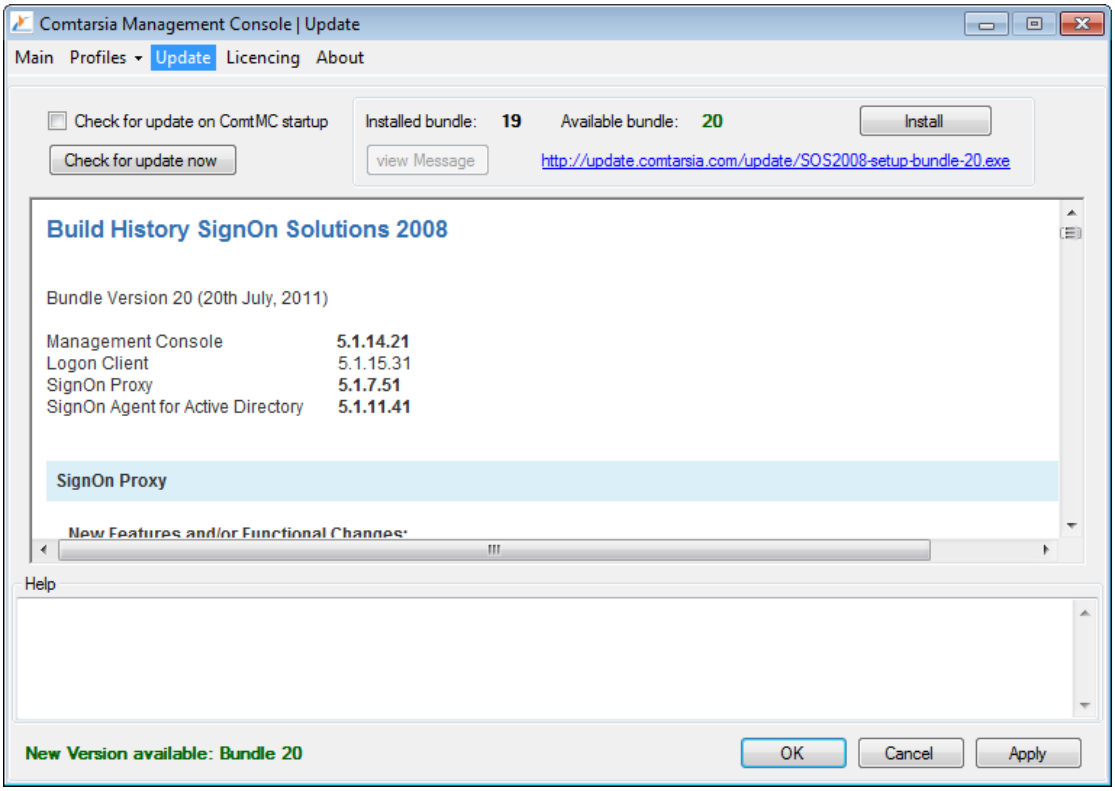
Beim ersten Aufruf der ComtMC wird man gefragt, ob man die automatische Update-Überprüfung aktivieren will. (Falls keine direkte Verbindung mit dem Internet besteht (Proxy Server benötigt) empfiehlt es sich das automatische Update vorerst zu deaktivieren). Diese Einstellung kann auch zu einem späteren Zeitpunkt angepasst werden. Siehe: Update Benachrichtigung

## 3.1 Update Benachrichtigung

Die Versionsüberprüfung und Benachrichtigung wird, insofern aktiviert, bei jedem Start der ComtMC durchgeführt.

Falls keine direkte Verbindung mit dem Internet besteht (Proxy Server benötigt um Webseiten aufzurufen) empfiehlt es sich das automatische Update vorerst zu deaktivieren. Die Update Überprüfung erfolgt ausschliesslich über http://update.comtarsia.com

Eine manuelle Überprüfung (Check for update now) kann über das „Update" Tab der ComtMC angestossen werden.



# 4. Basiskonfiguration

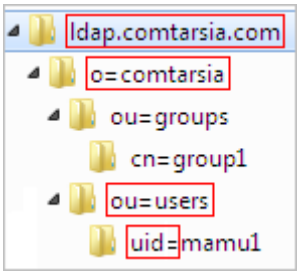
Am Grundlegendsten ist die LDAP-Benutzer Konfiguration, auf welche alle weiteren Szenarios und/oder Konfigurationsschritte aufbauen.

Folgende Informationen muss man zur Verfügung haben:
- LDAP-Server Adresse/Port Nicht-SSL oder SSL
- LDAP Servertyp (zB.: OpenLDAP, IBM Directory Server 6, etc)
- LDAP Verzeichnisstruktur
- 1 LDAP Benutzer mit Passwort (zum Testen)

LDAP Verzeichnisse folgen keinem starren Muster und sind üblicherweise immer auf Firmenszenarien und Anwendungen abgestimmt, wodurch die LDAP Konfiguration des Comtarsia Logon Client oftmals ebenso nicht mittels starrer Prozedurschritte bewerkstelligt werden kann.
Hier wird versucht mit möglichst einfachen Schritten eine grundlegende Konfiguration zu erstellen, welche eine Anmeldung gegenüber einem LDAP Server ermöglicht. Weitergehende Szenarien und/oder Konfigurationsschritte werden unter Usage Szenarios erläutert.

Um die Basiskonfiguration einfach zu halten, wird davon ausgegangen, dass sich alle LDAP-Benutzer in dem selben Container befinden.

In der Beispiel-Hirarchie des LDAP Servers „ldap.comtarsia.com", befindet sich der Benutzer „mamu1", in „ou=users", welche sich wiederum in „o=comtarsia" befindet. „o=comtarsia" ist gleichzeitig die BaseDN. Das Naming-Attribut des Beispiel-Benutzers ist „uid". (üblicherweise „uid" oder „cn")
Die volle DN (Distinquished Name) des Benutzers ist somit „uid=mamu1,ou=users,o=comtarsia".



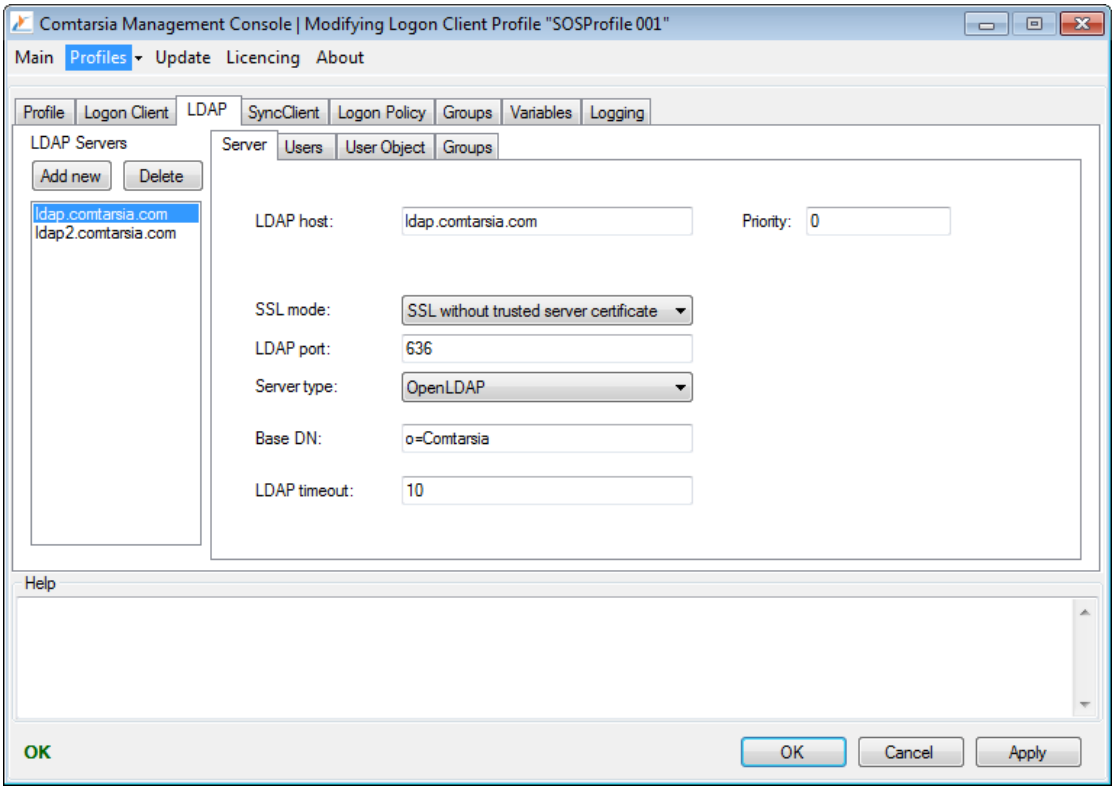

Die Schreibweise von vollen DNs ist immer von der untersten Ebene (leaf) bis zum Basis Objekt (Root oder „baseDN").

LDAP Server sind oft unverschlüsselt über den Port 389, als auch SSL-verschlüsselt über den Port 636 erreichbar. Für den Testbetrieb, mit Testbenutzern, ist eine unverschlüsselte Kommunikation ausreichend. Im Produktiveinsatz, sollte jedoch unbedingt SSL Verschlüsselung verwendet werden da ansonsten jegliche Kommunikation zum LDAP Server (inklusive Anmeldeinformationen) im Klartext stattfindet.

In der Comtarsia Management Console im Tab „[ LDAP ] -> [ Server ]", konfiguriert man zunächst den Hostnamen (oder IP-Adresse) des LDAP-Servers, den LDAP Port (und dazugehörigen SSL Modus).
Falls die Kommunikation zum Server mittels SSL-Verschlüsselung erfolgen soll, sollte vorerst einfachheitshalber der SSL-Modus „SSL without trusted server

certificate" gewählt werden. Für weitere Konfigurationshinweise zum SSL-Modus, siehe: LDAP über SSL

Ebenfalls wichtig ist die BaseDN (im Beispiel „o=Comtarsia"), welche den Basis-Eintrag für LDAP-Suchen bildet.




Im Tab „[ LDAP ] -> [ Users ]" wird konfiguriert, wo sich die Benutzer-Objekte im LDAP befinden, bzw. wie der Comtarsia Logon Client die Authentifizierung durchführt.

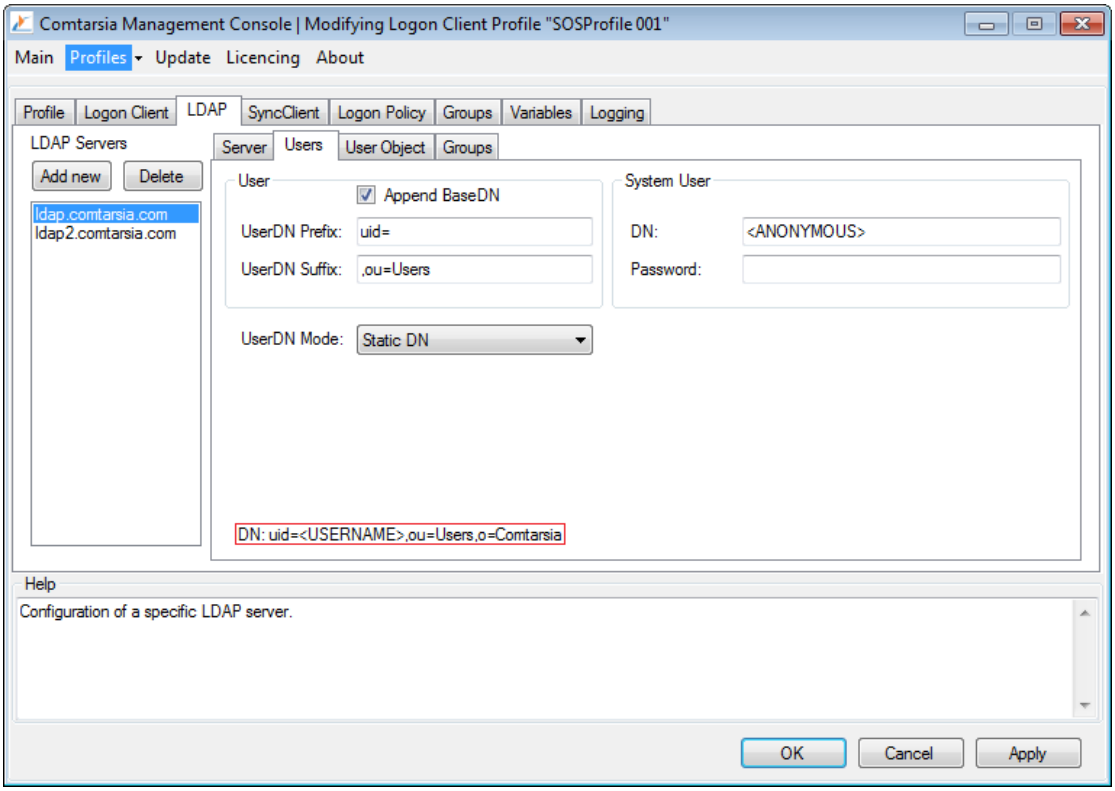
Die einfachste Konfiguration verwendet den „UserDN Mode": „Static DN". Bei diesem Modus nimmt der Comtarsia Logon Client den vom Benutzer angegebenen Logon-Namen und die konfigurierten „BaseDN, UserDN Suffix, UserDN Prefix" um eine gültige LDAP DN zu erlangen und führt anschliessend einen Bind-Request mit dieser DN und den vom Benutzer angegebenen Passwort durch. Gestattet der LDAP-Server diesen, wird der Benutzer als gülig erachtet.

Die BenutzerDN setzt sich folgendermassen zusammen:
UserDN Prefix + <Logon-Name> + UserDN Suffix + Base DN
Das Zusammenfügen dieser Teile muss eine gültige LDAP DN ergeben.

Im Beispiel resultiert dies in:
UserDN Prefix=„uid="
UserDN Suffix=„,ou=Users" (inklusive dem Komma)
BaseDN=„o=Comtarsia"

Die Comtarsia Management Console zeigt eine Vorschau der BenutzerDN an, damit man auf einen Blick sehen kann ob diese Werte richtig angegeben wurden

und der eigenen LDAP-Struktur entsprechen (In der nachstehenden Abbildung rot umrandet)



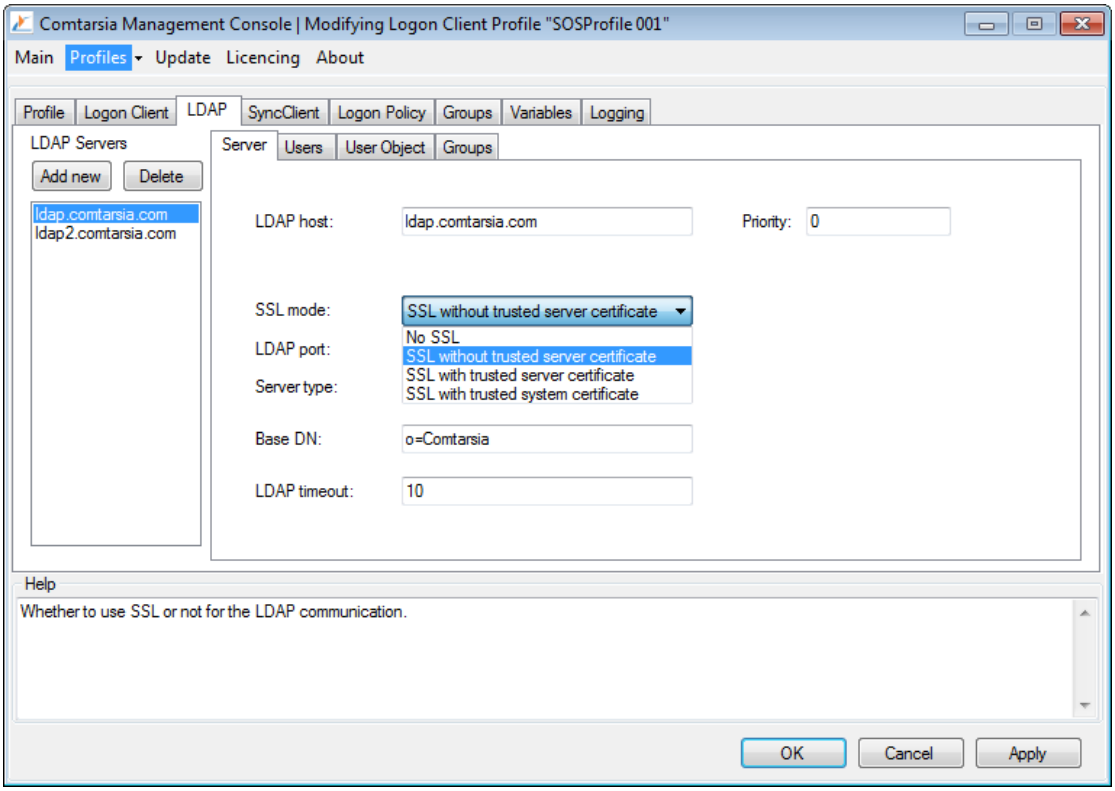
# 5. Usage Szenarios

## 5.1 LDAP über SSL

Es gibt verschiedene Modi für die Kommunikation zwischen Comtarsia Logon Client 2008 und dem LDAP Server.
Die Grundidee der SSL-Kommunikation ist ein Verschlüsseln der Klartext-Daten welche über das Netzwerk gesendet werden. (Modus 1).

Der Modus 1 ist am einfachsten zu konfigurieren.

Die Einstellung wird im Konfigurator unter [LDAP -> Server -> SSL mode] vorgenommen.




Beschreibung der Modi:

**Modus 1: SSL without "trusted server certificate"**
**Voraussetzungen:**

**Client:** Keine
**LDAP Server:** SSL Kommunikation (ldaps) muss aktiviert sein. Das Zertifikat muss nicht zwingend von einer CA ausgestellt sein. (kann auch self-signed sein)
**Vorteile:** Verschlüsselung der ansonsten im Klartext vorliegenden Kommunikation zwischen Comtarsia Logon Client 2008 und LDAP Server.

**Modus 2: SSL with "trusted server certificate"**
**Voraussetzungen:**

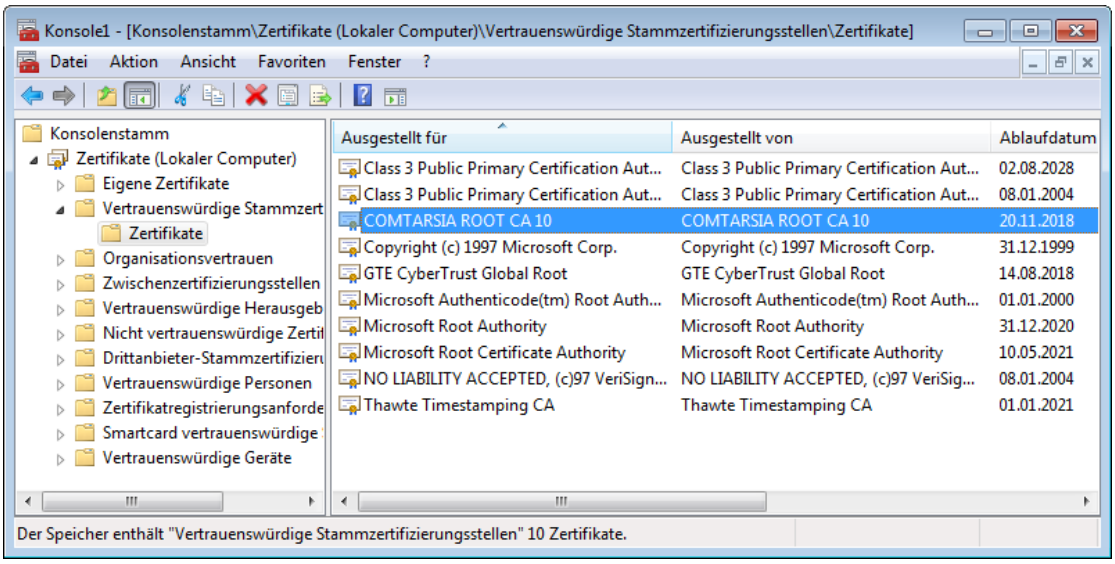
**Client:** Der Zertifizierungsstelle (Certificate Authority / CA), welche das LDAP Server Zertifikat ausgestellt hat, muss vertraut werden. Hierfür

müssen alle CA-Zertifikate in der Zertifizierungskette in den "Vertrauenswürdige Stammzertifizierungsstellen"-Zweig des Computer-Zertifikatsspeichers eingespielt sein. (siehe nachfolgende Abbildung)
**LDAP Server:** Das Zertifikat des LDAP Servers muss von einer Zertifizierungsstelle (CA) ausgestellt sein, welcher der Client vertraut.
**Vorteile:** Verschlüsselung. Der Comtarsia Logon Client stellt sicher dass dem Server vertraut wird indem er das Serverzertifikat überprüft. (Schliesst "Man in the middle"-Attacken aus)

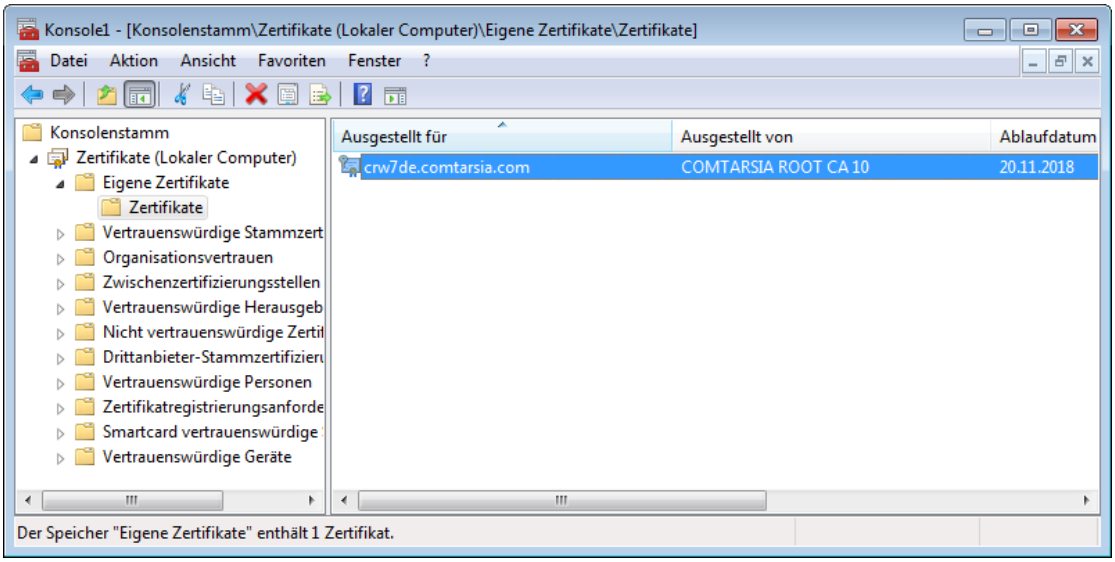
## Modus 3: SSL with "trusted client certificate"

**Voraussetzungen:**

**Client:** Wie Modus 2. Zusätzlich muss der Client ein "Clientzertifikat inklusive Schlüssel" im "Eigene Zertifikate" Zweig des Computer-Zertifikatspeichers vorliegen haben. Dieses Zertifikat muss den Hostnamen des jeweiligen Clients als Teil der Zertifikat-CN gesetzt haben. (siehe nachfolgende Abbildungen)
**LDAP Server:** Wie Modus 2. Zusätzlich muss der LDAP Server der CA welche das Client Zertifikat ausgestellt hat vertrauen.
**Vorteile:** Wie 2. Der LDAP Server kann so konfiguriert sein dass er nur "vertrauenswürdige Clients" zulässt.



[Abbildung: MMC: Vertrauenswürdige Stammzertifizierungsstellen des Computers]



[Abbildung: MMC: Eigene Zertifikate des Computers]

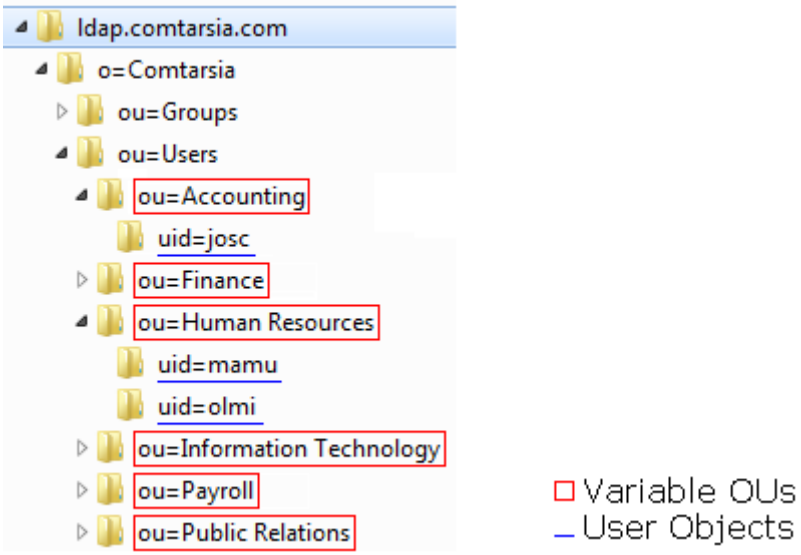
## 5.2 LDAP Benutzer aus mehreren OUs

Oftmals ist die vorhandene LDAP Hierarchie nicht flach und die Benutzer befinden sich in mehreren Organisazionseinheiten (OU).

In der Grundkonfiguration befinden sich alle Benutzer innerhalb der OU "ou=Users", welche sich wiederum innerhalb der Organisazion "o=Comtarsia" befinden, in den folgenden Beispielen wird jedoch davon ausgegangen dass es eine zusätzliche Hierarchieebene gibt.

```
uid=<Username>,ou=<Variable Einheit>,ou=Users,o=Comtarsia
```

zb:
```
uid=<Username>,ou=Human Resources,ou=Users,o=Comtarsia
uid=<Username>,ou=Public Relations,ou=Users,o=Comtarsia
```



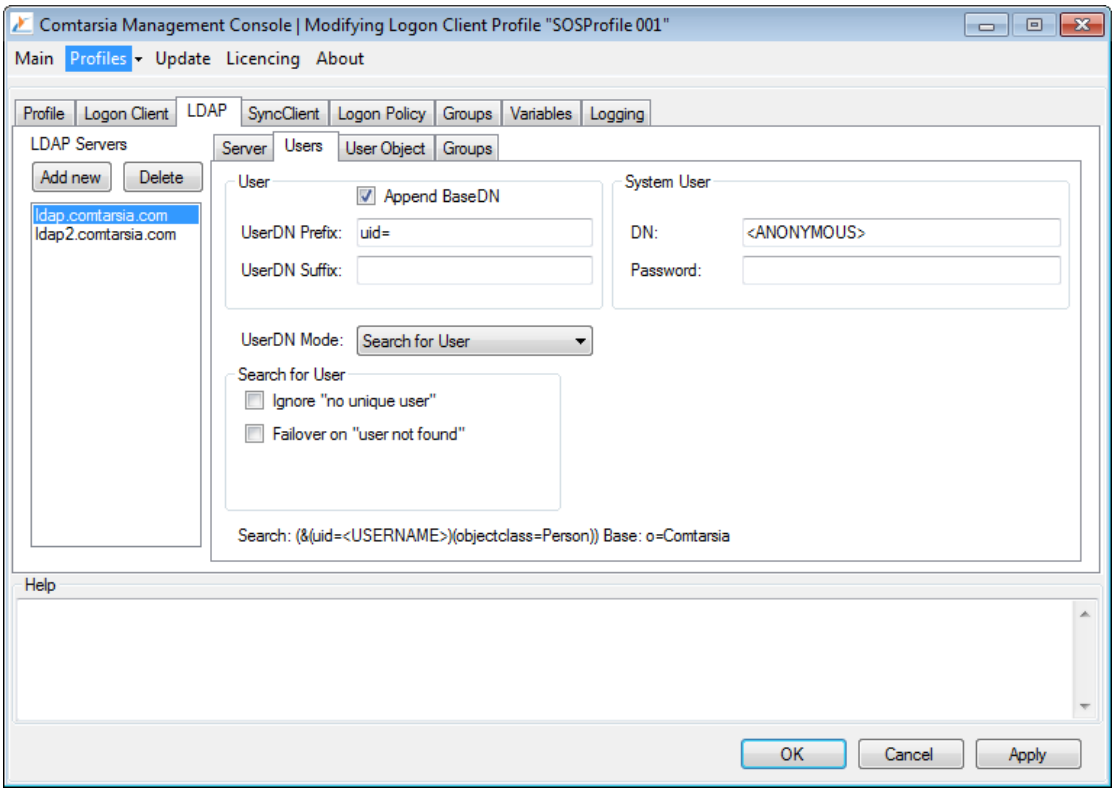
[Abbildung: LDAP Beispiel: Multiple OUs]

Es gibt unterschiedliche Möglichkeiten dies am Comtarsia Logon Client 2008 zu konfigurieren. Bei der ersten Möglichkeit (Search for User) wird einfach innerhalb eines LDAP-Zweiges (inklusive aller Unterzweige jeglicher Tiefe) nach dem Benutzer gesucht. Die zweite Möglichkeit (OU Searchlist) ist dass man eine Liste an erlaubten/möglichen OUs konfiguriert und der Comtarsia Logon Client 2008 sieht in jeder der resultierenden DNs nach ob der Benutzer sich darin befindet.

In beiden Fällen muss die LDAP-Suche innerhalb der Benutzerzweige entweder für Anonymous zugelassen sein, oder aber benötigt man einen fixen LDAP-Benutzer welchen der Comtarsia Logon Client für die Suche verwenden kann.

### 5.2.1 Search for User

Der Comtarsia Logon Client authentifiziert sich am LDAP server mittels des konfigurierten "System User" (LDAP > Users > System User).

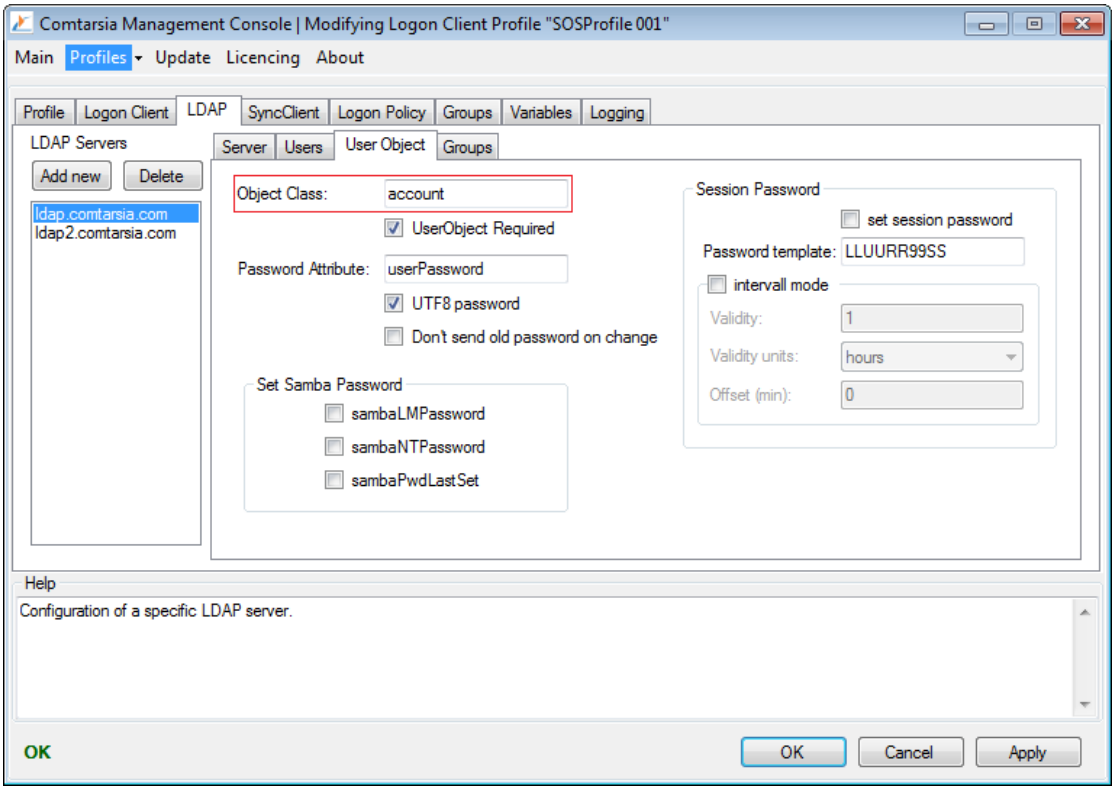


[Abbildung: ComtMC: LDAP > Users: UserDN Mode = Search for User]

Anschließend setzt der Logon Client eine LDAP Suche ab, welche sich folgendermassen zusammensetzt:

`(&(uid=<USERNAME>)(objectclass=person))` `baseDN: o=Comtarsia`

- "`<USERNAME>`": vom Benutzer angegebener Benutzername
- "`uid=`": das konfigurierte "UserDN Prefix"
- "`person`": die konfigurierte "User Object > Object Class" (siehe Abb.)
- "`o=Comtarsia`" ist die konfiguierte "baseDN"



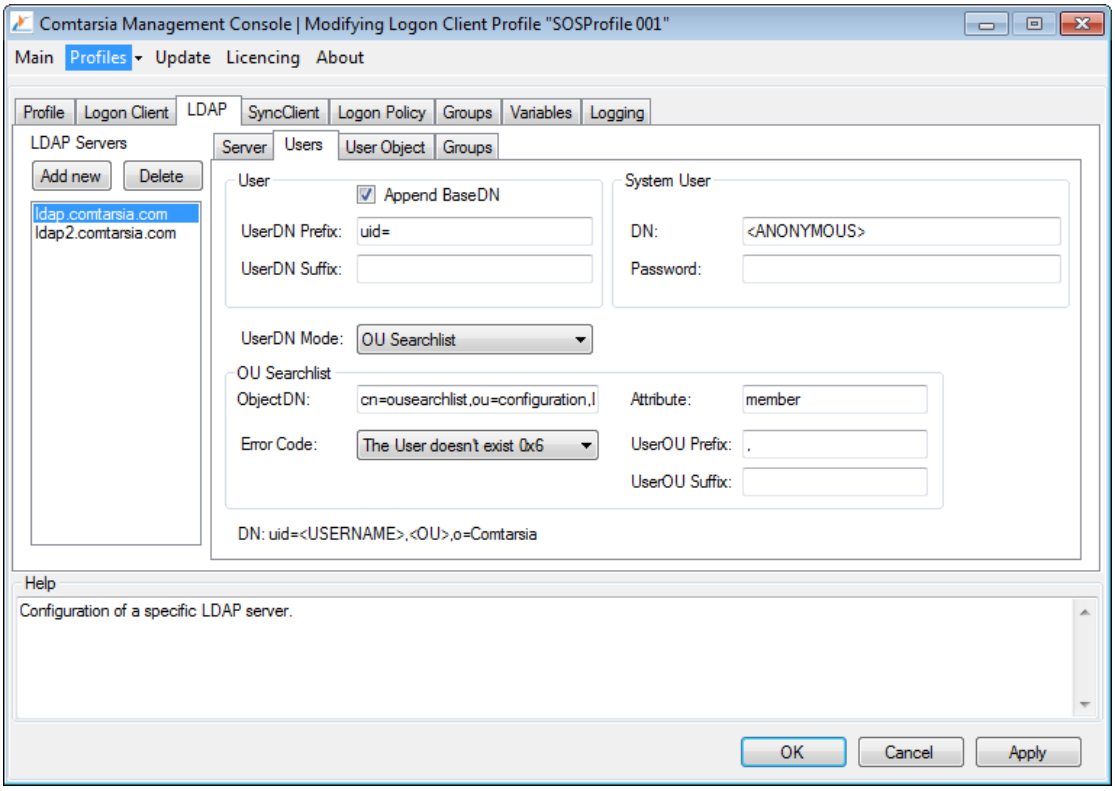
[Abbildung: ComtMC: LDAP > User Object > Object Class]

Wenn ein eindeutiger Benutzer gefunden wurde, wird die volle DN dieses Objektes genommen um eine LDAP Anmeldung mit dem vom Benutzer angegebenen Passwort durchzuführen. In allen weiteren Schritten (zb Gruppenermittlung) wird die ermittelte DN des Benutzers verwendet.
Falls der Benutzer nicht eindeutig bestimmt werden konnte (Benutzer mit der selben Kennung kommt mehrfach im Verzeichnis vor), wird mit einer Fehlermeldung abgebrochen.

### 5.2.2 OU Searchlist

Der Comtarsia Logon Client authentifiziert sich am LDAP Server mittels des konfigurierten "System User".

Anschließend liest der Logon Client die Attribute (Abb.) des LDAP Objektes mit der konfigurierten "OU Searchlist > ObjectDN" DN aus.
Dieses Objekt beinhaltet eine Liste von "<OU>"-Werten im konfigurierten Attribut.



[Abbildung: ComtMC: LDAP > Users > UserDN Mode = OU Searchlist mode]

In der Default-Konfiguration kann dieses Objekt eine LDAP-Gruppe sein, und die "<OU>"-Werte werden im Member-Attribut abgelegt.

Beispiel LDIF des OU Searchlist Objekt:

```
dn: cn=ousearchlist, ou=Groups, o=Comtarsia
objectClass: top
objectClass: groupOfNames
member: ou=Accounting
member: ou=Finance
member: ou=Human Resources
member: ou=Information Technology
member: ou=Payroll
member: ou=Public Relations
cn=ousearchlist
```

Mittels dieser Werte, setzt der Logon Client mögliche gültige BenutzerDNs in der folgenden Form zusammen:
`<UserDN Prefix><USERNAME><UserDN Suffix><UserOU Prefix><OU><UserOU Suffix>,<baseDN>`
In der Beispiel Konfiguration resultiert dies in:
`uid=<USERNAME>,<jeweilige OU>,o=Comtarsia`

- "`<UserDN Prefix>`": konfiguriert in "LDAP > Users > User > UserDN Prefix"
- "`<USERNAME>`": vom Benutzer angegebener Benutzername
- "`<UserDN Suffix>`": konfiguriert in "LDAP > Users > User > UserDN Suffix"
- "`<UserOU Prefix>`": konfiguriert in "LDAP > Users > OU Seachlist > UserOU Prefix"
- "`<OU>`": hier werden die jeweiligen ermittelten OUs eingesetzt
- "`<UserOU Suffix>`": konfiguriert in "LDAP > Users > OU Seachlist > UserOU Suffix"

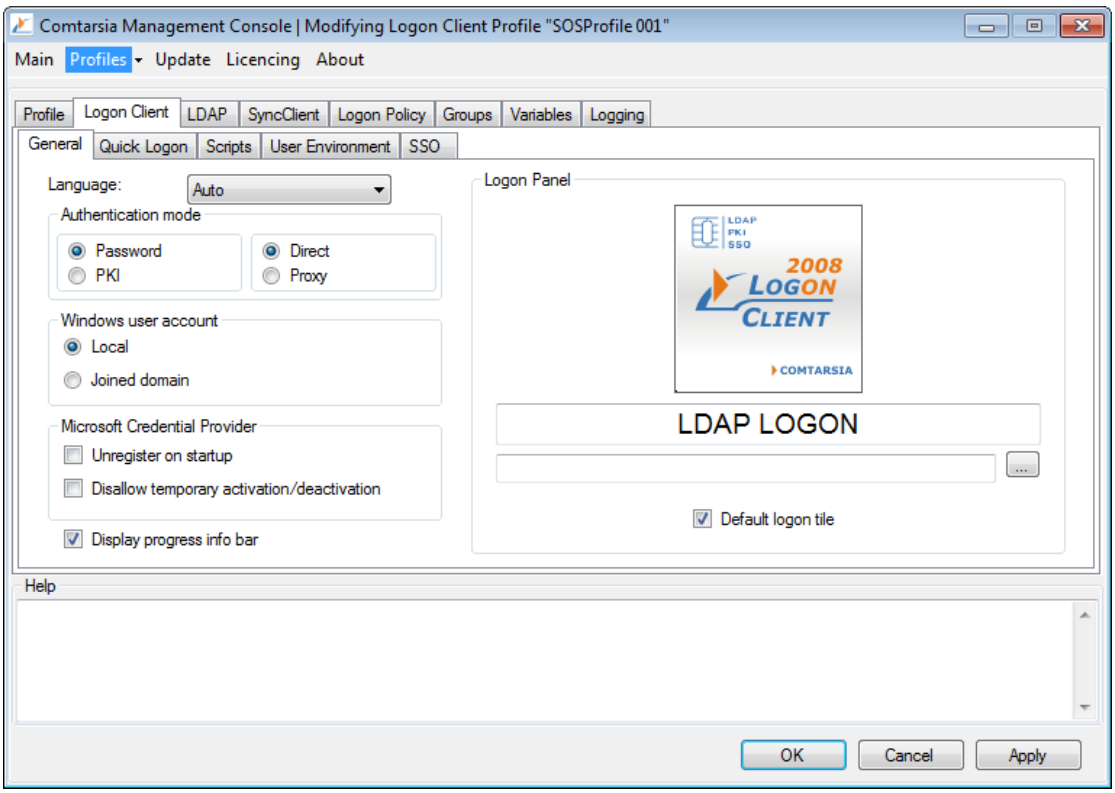
- "<baseDN>": konfiguriert in "LDAP > Server > baseDN"

Der Comtarsia Logon Client überprüft der Reihe nach ob es einen Benutzer mit einer der resultierenden Benutzer-DNs gibt.
Sobald ein Benutzer gefunden wurde wird die volle DN dessen für die LDAP-Authentifizierung und anschliessend für alle weiteren Schritten (zb Gruppenermittlung) verwendet.
Falls keine der ermittelten Benutzer-DNs gültig ist, wird der konfigurierte "Error Code" (LDAP > Users > OU Searchlist > Error Code) füd den Benutzer ausgegeben und die Anmeldung schlägt fehl.

# 6. Konfigurationsparameter

## 6.1 Logon Client

### 6.1.1 General




Language
Definiert die Benutzer-Interface-Sprache. Derzeit sind die Sparchen deutsch, englich und französisch verfügbar.

Authentication mode
enableSmartcard: Erlaubt die Anmeldung für dieses Profil zwischen "Benutzer Password" und "PKI" (Smartcard) umzustellen.
enableProxyLogon: Mittels "Direct" wird die Benutzerauthentifizierung direkt am den LDAP Server durchgeführt. Bei "Proxy" werden die Credentials (Benutzer Password oder Certificate Handshake) über den Comtarsia SignOn Proxy abgewickelt, welcher den Benutzer über LDAP authentifiziert.

Windows user account
Dieser Parameter aktiviert/deaktiviet Enable Domain Logon. Wenn der Wert "Local" ausgewählt ist, ist der „Local User Mode" aktiv, bei "Joined Domain" schaltet der Logon Client in den „Domain User Mode".

**Local User Mode:**
Nach erfolgreicher LDAP Anmeldung wird ein lokales Benutzerkonto für die Workstation Anmeldung verwendet. Die Verwaltung (Anlegen, aktivieren, Passwort-Synchronsiation, etc..) wird vom Logon Client durchgeführt.

**Domain User Mode:**

Nach erfolgreicher LDAP Anmeldung wird ein ein Domänen-Benutzerkonto für die Workstation Anmeldung verwendet. Damit eine Automatische Anmeldung an eine Domäne funktioniert, müssen zwei Voraussetzungen erfüllt sein:

- Die Workstation muss Mitglied dieser Domäne sein.
- Da die automatische Benutzerverwaltung nicht vom Logon Client übernommen werden kann, ist die SignOn Gate-Konfiguration erforderlich. Siehe SyncClient Konfiguration.

**Microsoft Credential Provider**

Der Logon Client ermöglicht es, den Standard Microsoft Credential Provider auszfiltern, d.h. am Anmelde- bzw. Workstation-Ensperren-Maske ist dann nur mehr der Comtarsia Logon Client Credential Provider verfügbar, der Button „anderer Benutzer" ist dann nicht vorhanden.

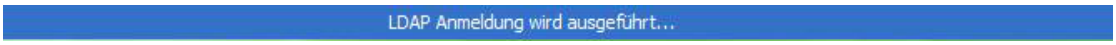
Unregister on Startup

Ist dieser Parameter aktiviert, wird bei jeden Systemstart der Microsoft Credential Provider ausgefiltert.

Disallow temprary activation/deactivation

Ist dieser Parameter nicht aktiv, ist über den Link „Microsoft Logon Ausschalten" bzw. „Microsoft Logon Einschalten" in der Anmelde-Maske das temporäre aktivieren bzw. deaktivieren
des Microsoft Credential Provider Filters möglich. Ist dieser Parameter aktiv, wird dieser Link nicht eingeblendet. Display progress info bar

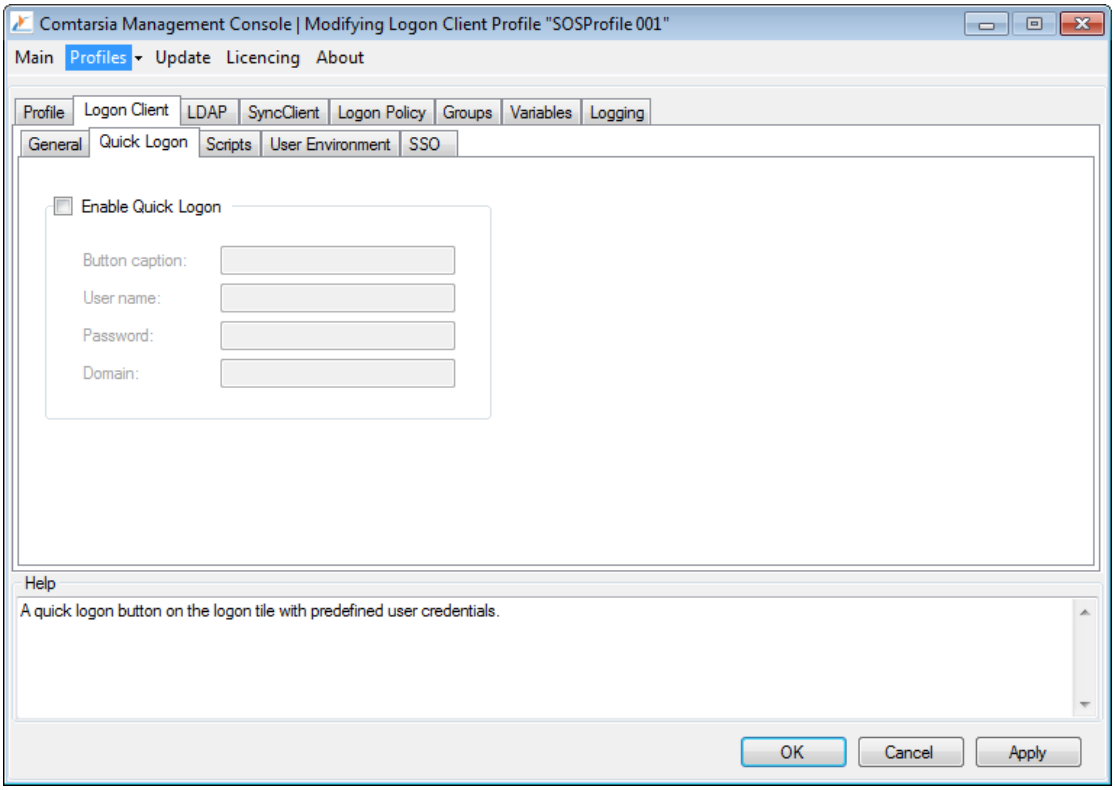
Wenn dieser Parameter aktiviert ist, wird während der Anmeldung am oberen Bildschirmrand eine Fortschrittsanzeige eingeblendet.




Logon Panel Bitmap

Mit diesen Paramenter kann ein alternatives Bitmap, z.b. eignes Firmen-Logo, im Credential Provider Kachel geladen werden. Das Bitmap mus eine Auflösung von 128 x 128 Pixel haben und während der Anmeldung für das System verfügbar sein.

### 6.1.2 Quick Logon




Enable Quick Logon
Aktiviert eine "Quick Logon" (schnell-Anmeldung) Schaltfläche auf der Anmeldemaske um sich mit einem vordefiniertem Benutzer anmelden zu können. (1-click Anmeldung)

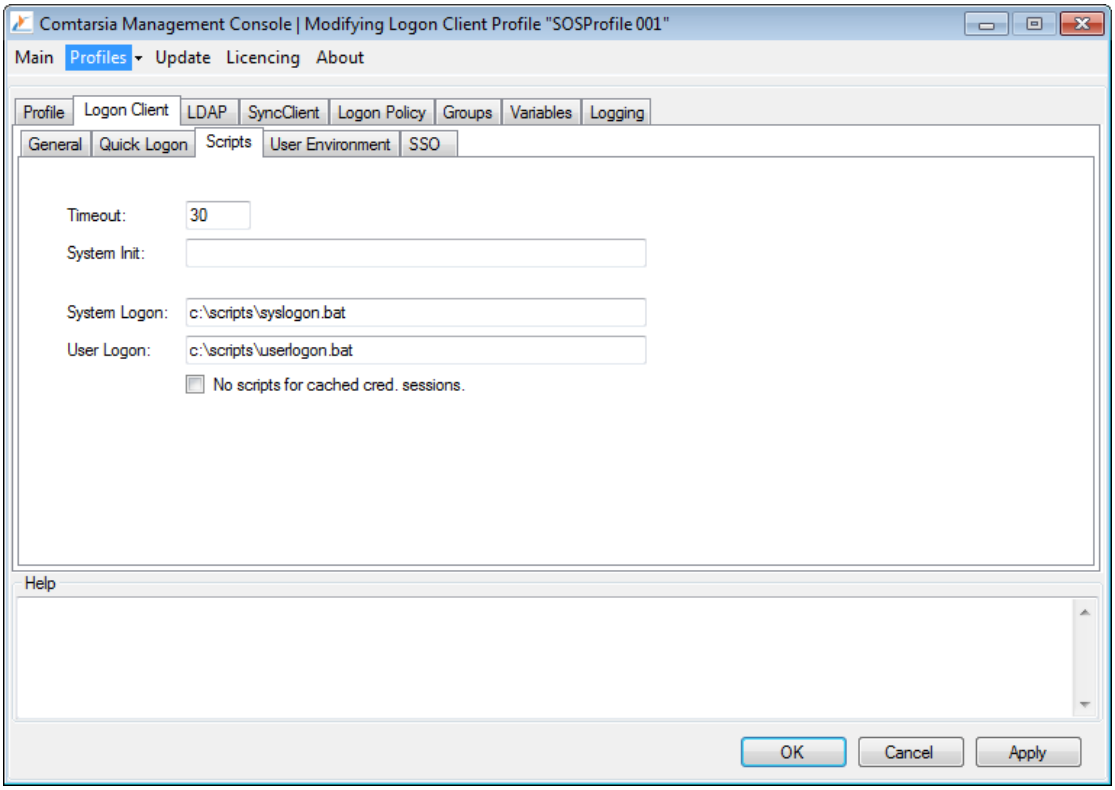
Button caption
Definiert den Text für die Quick-Logon-Schaltfläche.

User name
Definiert den Benutzername welcher für die Quick-Logon Anmeldung verwendet werden soll.

Password
Definiert das Passwort welcher für die Quick-Logon Anmeldung verwendet werden soll.

Domain
Definiert die Quick-Logon Domain. Um einen existierenden lokalen Benutzer zu verwenden kann "local" oder "%computername%" verwendet werden; anderenfalls wird eine LDAP-Anmeldung mit dem definierten Benutzer durchgeführt.

### 6.1.3 Scripts




Der Parameter Timeout definiert die Zeit in Sekunden, innerhalb welcher die Scripts beenden müssen, bevor der Prozess vom Logon Client beendet wird.

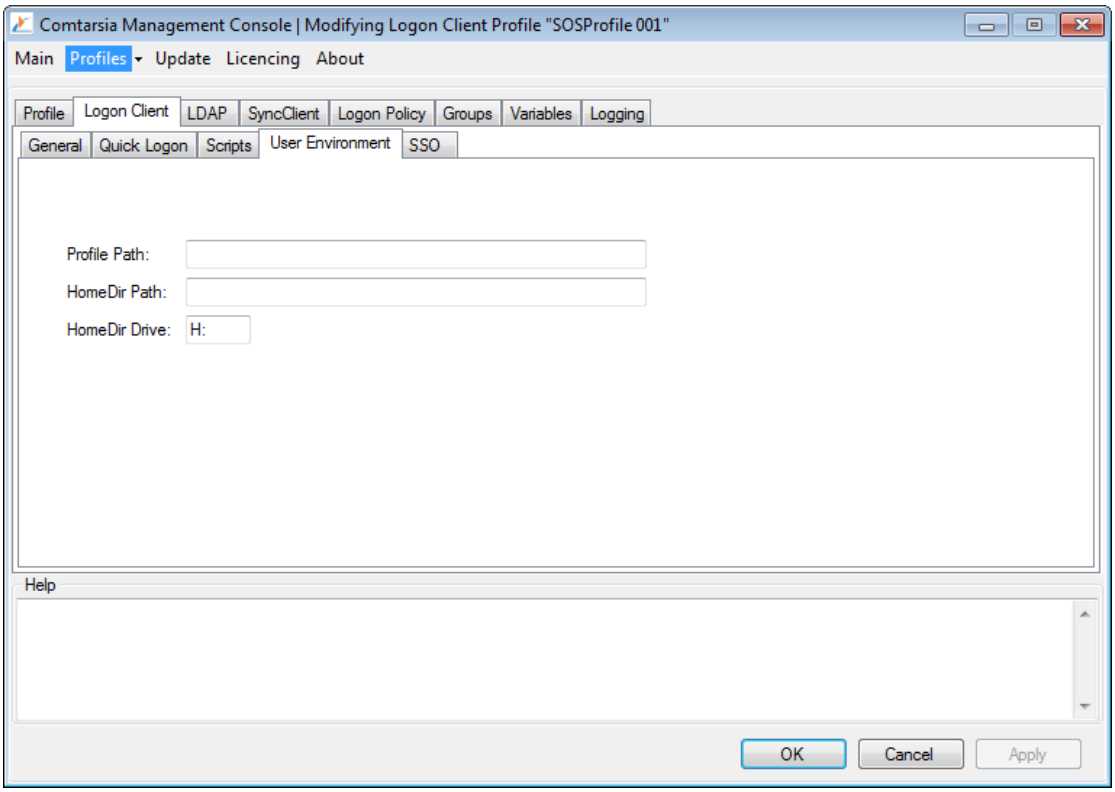
Das System Init Script wird beim Systemstart mit System-Rechten im System-Kontext ausgeführt.

Das System Logon Script wird bei der Anmeldung mit System-Rechten im System-Kontext ausgeführt.

Das User Logon Script wird bei der Anmeldung mit Benutzer-Rechten im Benutzer-Kontext ausgeführt.

Ist der Parameter No scripts for cached cred. sessions aktiviert, werden Anmelde-Scripts bei Offline- /Cached Credential-Anmeldungen nicht ausgeführt.

### 6.1.4 User Environment




Der Parameter Profile Path definiert den Pfad des Benutzer-Profiles welches dem lokalen Benutzer zugwiesen wird.
ZB.: \\SERVER1\profiles\%USERNAME%
Dieser Wert kann durch die Variable "profile_path" überschrieben werden.

Der Parameter HomeDir Path definiert den Pfad des Benutzer-Verzeichnisses welches dem lokalen Benutzer zugwiesen wird.
ZB.: \\SERVER1\homes\%USERNAME%
Dieser Wert kann durch die Variable "home_dir_path" überschrieben werden.

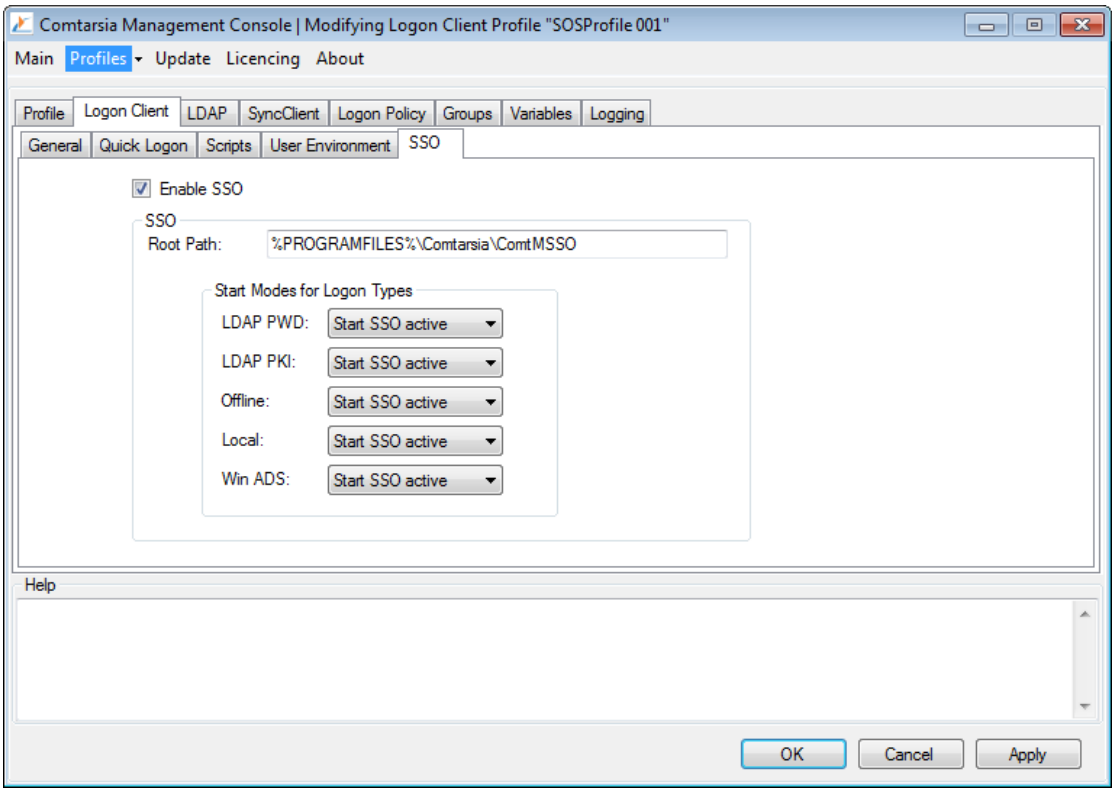
Der Parameter HomeDir Drive definiert den Laufwerksbuchstaben des Benutzer-Verzeichnisses welches dem lokalen Benutzer zugwiesen wird.
ZB.: H:
Dieser Wert kann durch die Variable "home_dir_drive" überschrieben werden.

Im „Domain User Mode", bei aktivierten Parameter Enable Domain Logon, kann der Logon Client diese Parameter für Domain Benutzer nicht zuweisen, diese Aufgabe kann das Comtarsia SignOn Gate (Agent Konfiguration) übernehmen.

Der Default Profile Pfad kann unter folgenden Windows System Regsitry Parameter definiert werdern: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\Default

Nützliche Hinweise zum Anpassen von Standardbenutzerprofilen unter Windows 7 und Windows Server 2008 bzw. das einrichten von verbindlichen Benutzerprofilen können diesen Microsoft Artikel entnommen werden:
http://support.microsoft.com/kb/973289/de

### 6.1.5 SSO




Enable SSO
Aktiviert das Comtarsia Managed Single SignOn (ComtMSSO) Modul. (Dieses muss separat installiert werden.)

Root Path
Definiert den Pfad zur ComtMSSO Installation.

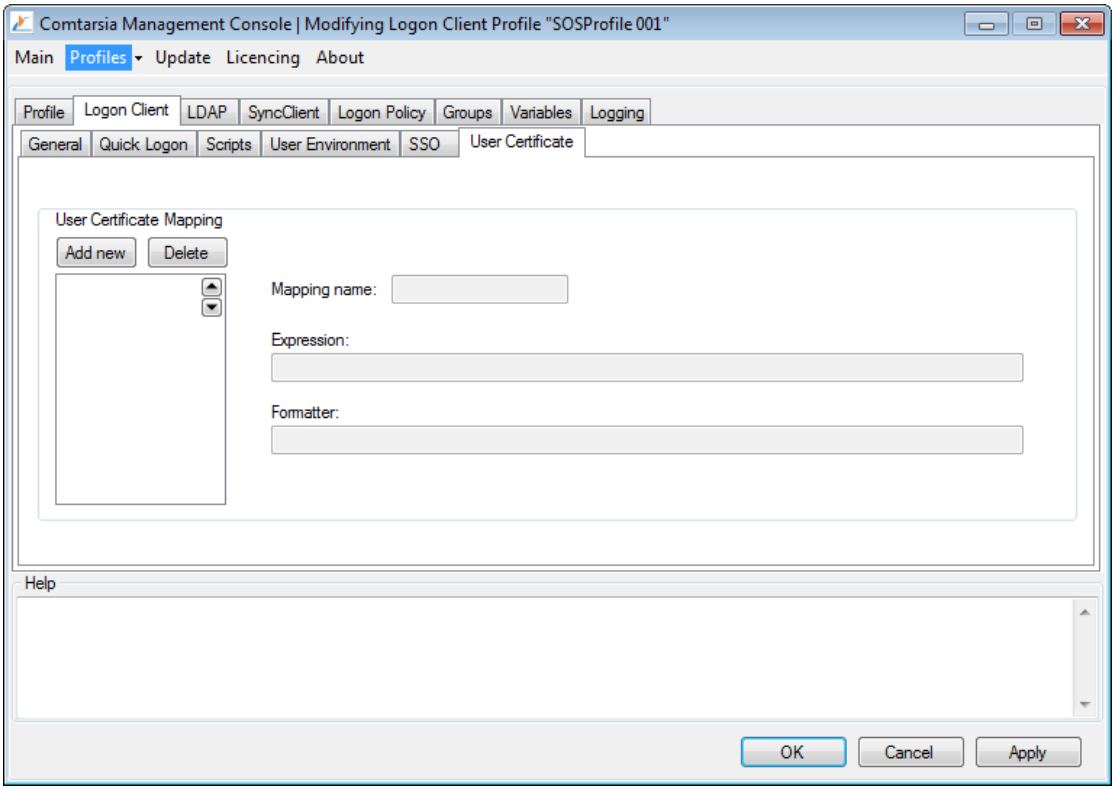
Start Modes for Logon Types
Die Start Modi geben an bei welcher Anmelde-Art (Logon Types), und in welchem Modus (Start Modes), das ComtMSSO-Modul gestartet werden soll.
Start Modes:

- Don't start SSO: Das ComtMSSO Modul wird nicht geladen.
- Start SSO inactive: Das Modul wird zwar gestartet, ist jedoch auf „inaktiv" gesetzt. (Der Benutzer kann es über das Tray Icon bei bedarf aktivieren)
- Start SSO active: Das Modul wird normal gestartet.

Logon Types: (alle über den Comtarsia Logon Kachel)

- LDAP PWD: LDAP-Anmeldung mittels Benutzer-Passwort Authentifizierung
- LDAP PKI: LDAP-Smartcard-Anmeldung
- Offline: Offline Anmeldung
- Local: Lokale Anmeldung
- Win ADS: Active Directory Anmeldung

### 6.1.6 User Certificate




Dieser Tab ist nur im PKI Modus verfügbar. (siehe: Logon Client - General - Authentication mode)

Ein User Certificate Mapping definiert einen regulären Ausdruck um die Zertifikat-DN des Benutzers einer LDAP-Benutzer-DN zuordnen zu können.
Es können mehrere User Certificate Mappings definiert werden welche vom Logon Client der Reihe nach durchgeführt werden (von oben nach unten). Der erste zutreffende Reguläre Ausdruck (Expression) wird verwendet.

Der Mapping name kann einen beliebigen Namen beinhalten und dient legitlich organisatorischen Zwecken.

Der Wert Expression definiert den zu verwendenten Regulären Ausdruck. Wenn die Zertifikats DN (Subject) mit diesem Ausdruck übereinstimmt, wird der Formatter verwendet um die resultierende LDAP Benutzer zu erhalten. (Der Resultierende String wird beim ermitteln des LDAP Benutzers als "USERNAME" verwendet und je nach LDAP Konfiguration für einen direkten Bind oder eine Suche verwendet)

Der Wert Formatter definiert wie das Resultat des übereinstimmenden Regulären Ausdruckes in Expression formatiert werden soll.

Beispiel:
Expression: ^[Cc][Nn]=([^,]*),.*
Formatter: uid=$1,ou=users,dc=company,dc=com

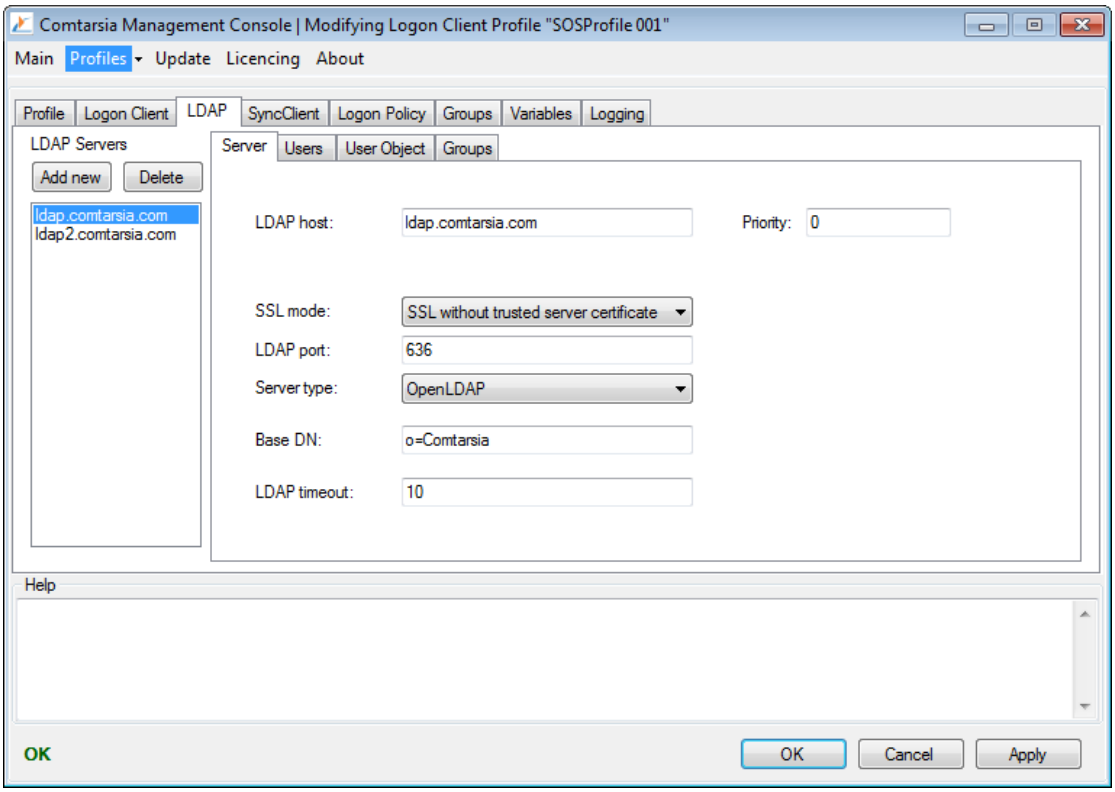
Zertifikats DN: cn=mustermann, ou=example, cn=controling
Resultierende LDAP DN: uid=musterman,ou=users,dc=company,dc=com

Zertifikats DN: cn=mustermann2, dc=company
Resultierende LDAP DN: uid=musterman2,ou=users,dc=company,dc=com

## 6.2 LDAP

### 6.2.1 Server

Hier wird der LDAP Server konfiguriert.




LDAP host
Definiert den LDAP Server. Dies ist der primäre LDAP-Server.

Failover LDAP host
Definiert einen zweiten LDAP Server zur Ausfallsicherheit. Dieser wird nur kontaktiert, falls der primäre LDAP-Server nicht erreicht werden konnte.

SSL mode
Dieser Parameter definiert ob, und welche Art von SSL kommunikation mit dem LDAP-Server verwendet werden soll. (siehe: LDAP über SSL)

LDAP port
Der Port über welchem die LDAP Server erreichbar sind. Wenn die Kommunikation über SSL erfolgt, muss der SSL-Port angegeben werden.

Server type
Definiert welche LDAP-Serversoftware im Einsatz ist. Dies ist notwendig damit zb Passwort Policy Meldungen richtig ausgewertet werden.

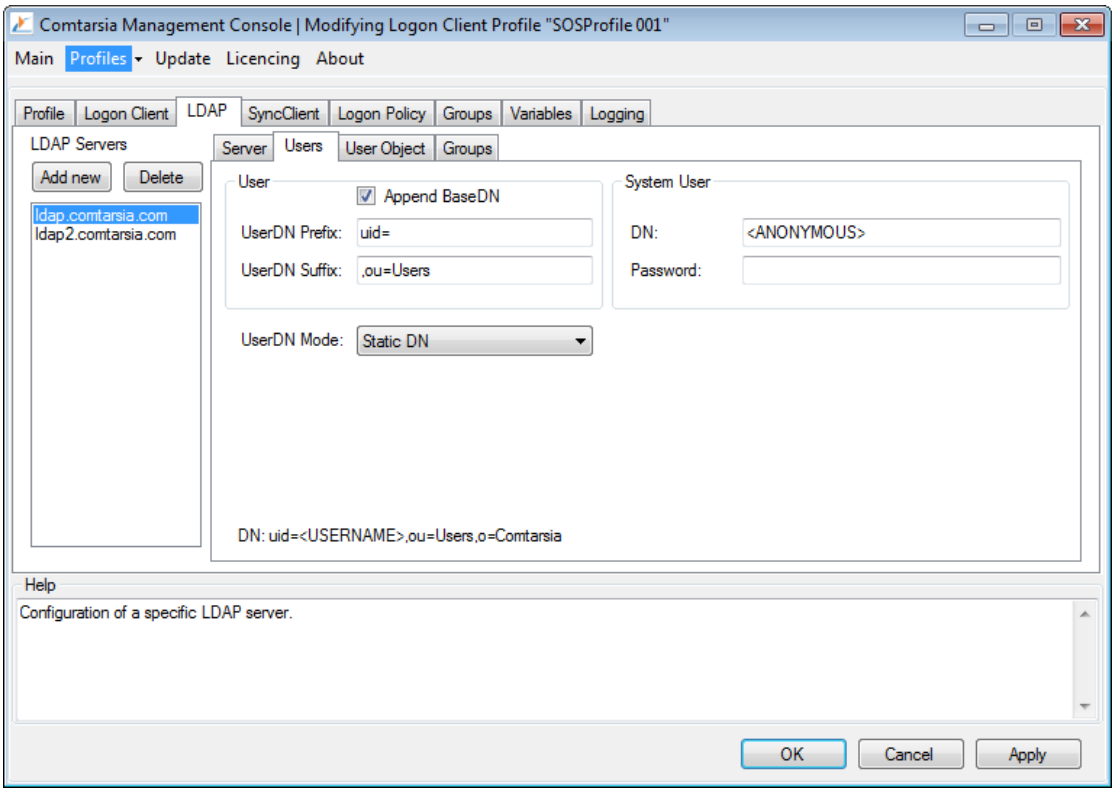
Base DN
Definiert die Basis-DN aller LDAP-Operationen.

LDAP timeout
Definiert ein Timeout innerhalb welchem die LDAP-Kommunikation abgeschlossen sein muss. Ansonsten bricht die Anmeldung ab.

### 6.2.2 Users

Hier wird konfiguriert wie der LDAP-Benutzer ermittelt wird.

### Static DN




Append BaseDN
Wenn dieser Parameter aktiviert ist, wird die BaseDN an die BenutzerDN angehängt. (Default und empfohlen)

UserDN Prefix
Definiert das Naming-Attribut des Benutzers. Der angegebene Wert wird beim „Bind als Benutzer" als auch für die Benutzersuche (wenn konfiguriert) verwendet.

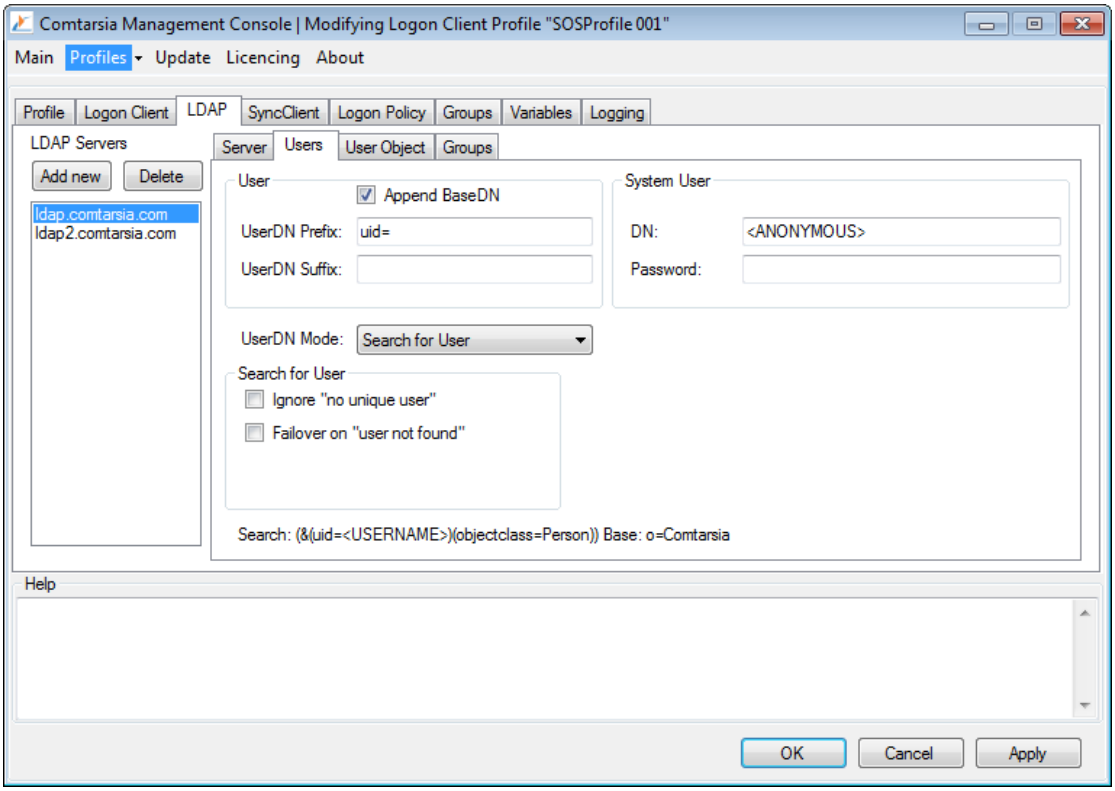
UserDN Suffix
Der hier konfigurierte Text wird bei, „Bind als Benutzer" hinter den Benutzernamen gehängt.

UserDN Mode (searchForUser, ouSearchListMode)

Definiert wie der Benutzer aufgefunden werden soll. „Static DN" definiert dass die BenutzerDN mit den angegebenen Werten konstruiert, und direkt mit dieser resultierenden DN gebinded wird. (siehe auch LDAP Benutzer aus mehreren OUs)

DN: zeigt die aus der Konfiguration resultierende User-BindDN  oder den entsprechenden Suchstring.

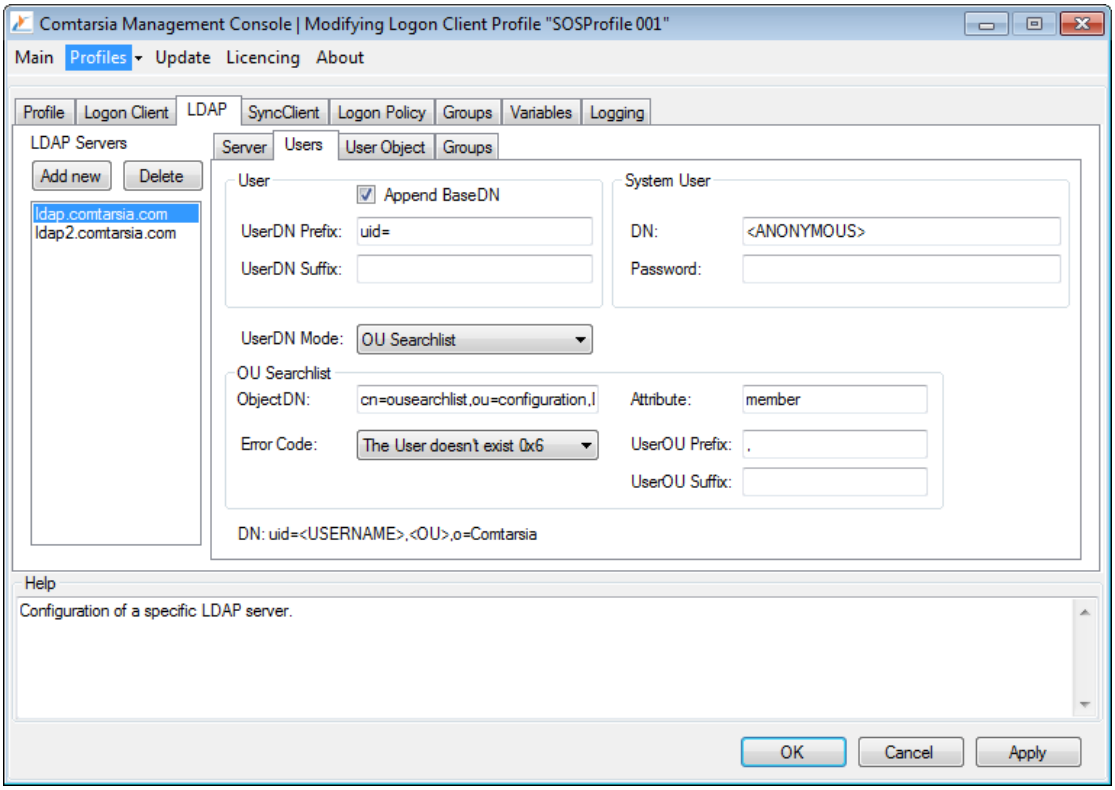
## Search for User




System User > DN
Definiert die volle DN eines LDAP-Systembenutzers welcher für die LDAP Suche (sowohl „UserDN Mode: Search for User", als auch „UserDN Mode: OU Searchlist) verwendet werden soll. Dies dient zum Auffinden des LDAP Benutzers, falls die Benutzer sich in mehreren LDAP OUs befinden. (siehe auch: LDAP Benutzer aus mehreren OUs, und Search for User)

System User > Password
Definiert das Passwort des LDAP-Systembenutzers. Das Passwort wird verschlüsselt hinterlegt.

## OU Searchlist




OU Searchlist
siehe auch: LDAP Benutzer aus mehreren OUs, und OU Searchlist

OU Searchlist > ObjectDN
Gibt an in welchem LDAP-Objekt die OU Searchlist hinterlegt ist.

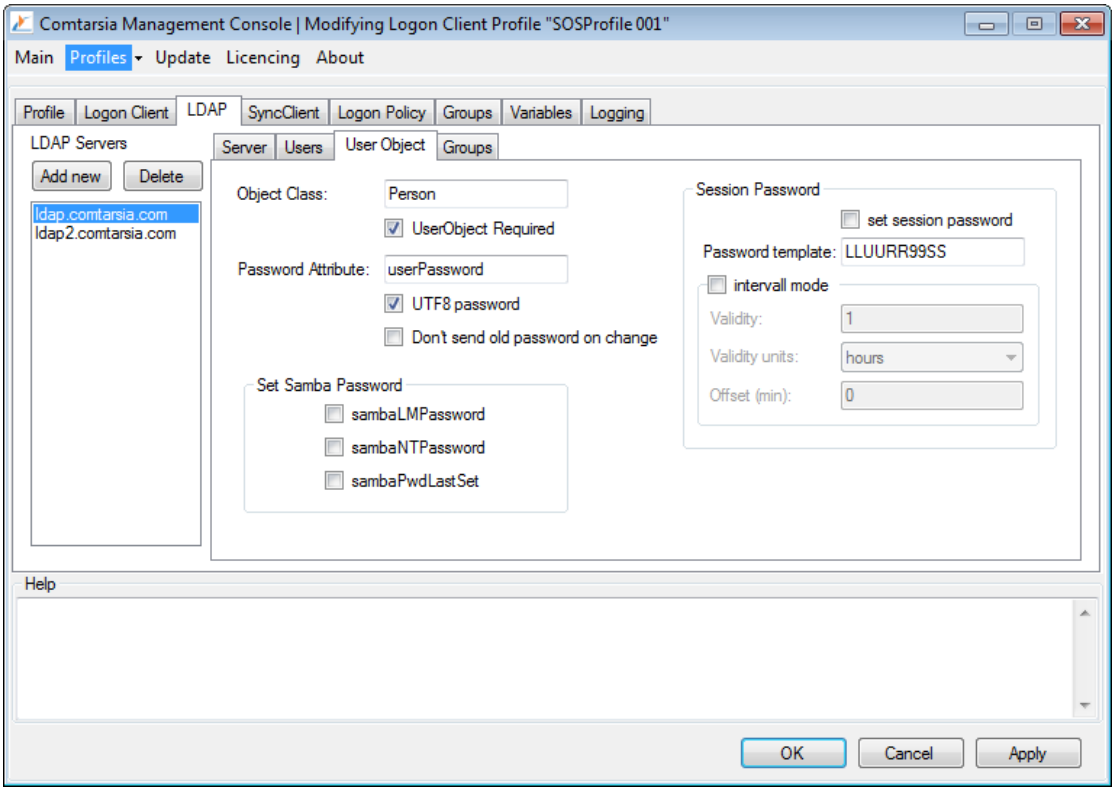
OU Searchlist > Attribute
Gibt an in welchem LDAP-Attribut des OU Searchlist-LDAP-Objekts die Liste der OUs hinterlegt ist.

OU Searchlist > Error Code
Gibt an welcher Fehler zurückgeliefert werden soll falls der Benutzer in keiner der angegebenen OUs gefunden wurde.

OU Searchlist > UserOU Prefix
Definiert ein Prefix welches beim konstruieren der vollen Benutzer-DN der jeweiligen OUs verwendet werden soll.
Die möglichen BenutzerDNs setzen sich zusammen aus:
`<UserDN Prefix><USERNAME><UserDN Suffix><UserOU Prefix><OU><UserOU Suffix>,<baseDN>`
(siehe auch: LDAP Benutzer aus mehreren OUs, und OU Searchlist)

OU Searchlist > UserOU Suffix
Definiert ein Prefix welches beim konstruieren der vollen Benutzer-DN der jeweiligen OUs verwendet werden soll.
Die möglichen BenutzerDNs setzen sich zusammen aus:
`<UserDN Prefix><USERNAME><UserDN Suffix><UserOU Prefix><OU><UserOU Suffix>,<baseDN>`
(siehe auch: LDAP Benutzer aus mehreren OUs, und OU Searchlist)

### 6.2.3 User Object




User Object
Object Class
Gibt an welche ObjectClass beim Ermitteln des LDAP-Benutzerobjekts verwendet werden soll.

UserObject Required
Wenn diese Option aktiviert ist, wird eine Anmeldung nur zugelassen wenn das LDAP-Benutzerobjekt tatsächlich ausgelesen werden konnte. In seltenen Fällen kann es vorkommen dass der LDAP Server so konfiguriert ist dass eine Anmeldung mit „falscher Benutzer-DN" zugelassen wird.

Password Attribute
Definiert in welchem Attribut des LDAP-Benutzers das Passwort hinterlegt ist.

UTF8-password
Wenn diese Option aktiviert ist, wird das Passwort sowohl bei der Anmeldung als auch beim Passwortwechsel UTF-8 encodiert.

Don't send old password on change
Bei einem Passwortwechsel wird das alte Passwort nicht mitgeschickt. (Default: Altes Passwort wird mitgeschickt: empfohlen).

Set Samba Password
Mit den folgenden Optionen kann das Samba Passwort des LDAP-Benutzerobjekts mit dem LDAP Passwort des Benutzers synchronisiert werden. Dies ist hilfreich wenn der LDAP-Benutzer gleichzeitig ein Samba Benutzer ist.

sambaLMPassword

Aktualisiert das LDAP-Benutzerattribut „sambaLMPassword" mit dem LM-Hash des Benuzter-Passworts.

sambaNTPassword
Aktualisiert das LDAP-Benutzerattribut „sambaNTPassword" mit dem NT-Hash des Benuzter-Passworts

sambaPwdLastSet
Setzt das LDAP-Benutzerattribut „sambaPwdLastSet" auf den momentanen Zeitstempel (bei jeder Anmeldung) um ein Ablaufen des Samba Passworts zu verhindern.

Session Password
Das Session Password wird bei einer Smartcard Anmeldung (abhängig vom Session Password Mode) unter der Verwendung des Private Keys des Benutzers generiert und als Windows Benutzerpassword verwendet. Wenn der Sync Client aktiv ist, wird das Session Password ebenfalls an diesen zur Synchronisation gesendet.

set session password
Das Session Password wird ins LDAP Benutzerobjekt in das konfigurierte "Password Attribute"-Feld zurückgeschrieben.
Achtung: da das Session Passwort dem Benutzer nicht bekannt ist, kann dieser anschliessend keine LDAP Benutzer-Passwort Anmeldung mehr durchführen.

password template
Dieser Wert definiert das Template zum generieren des Session Passworts. Dabei finden folgende Zeichen verwendung:

| | |
|---|---|
| L | lowercase character (a-z) |
| U | uppercase character (A-Z) |
| 9 | number (0-9) |
| S | special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{\|}~) |
| R | random (zufällig aus L, U, 9 oder S) |

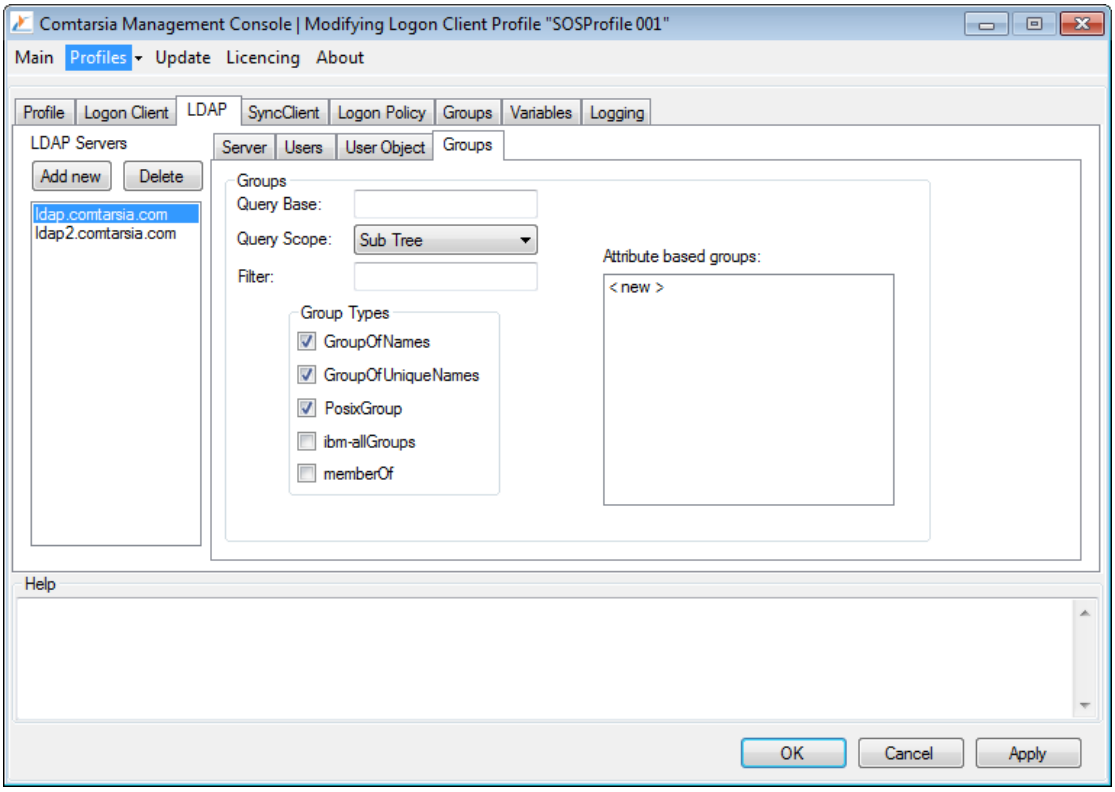
interval mode
Mit dieser Option wird der Wert smartCardSessionPasswordMode auf "1" (interval mode) gesetzt. Mit dem "interval mode" kann man sicherstellen dass das Passwort über definierte Zeiträume, und auch auf unterschiedlichen Arbeitsplätzen gleich bleibt. Damit wird verhindert dass, wenn sich der Benutzer auf mehr als 1 Arbeitsplatz anmeldet, unterschiedliche Passwörter verwendet werden.

validity
Definiert die Anzahl von 'validity units' die das Session Password gleich bleibt.

validity units
Definiert die Einheit des Gültigkeitswertes.

offset
Definiert ein Offset in Minuten.
ZB.: Ein "validity: 1, validity units: days" Passwort ändert sich immer um 0:00 jedes Tages. Mittels des Offsets kann dieser Zeitpunkt (in Minuten) verschoben werden.

### 6.2.4 Groups




Query Base
Mit dieser Option kann eine andere, oder genauere Basis-DN, für die LDAP-Gruppensuche definiert werden. Wenn dieser Wert leer gelassen wird, wird die konfigurierte [LDAP > Server > Base DN] verwendet.

Query Scope
Definiert die „Reichweite" (Scope) der LDAP-Gruppensuche.
- Base: Nur die verwendete „Query Base" selber.
- One Level: Alle Einträge unmittelbar unterhalb der „Query Base".
- Sub Tree: Der komplette Baum unterhalb der „Query Base".

Filter
Definiert einen zusätzlichen LDAP-Suchfilter welcher in die LDAP-Gruppensuche mit einbezogen wird. Gruppen welche diesem Suchfilter nicht entsprechen werden ausgelassen.
Damit kann zum Beispiel:
- das Vorhandensein eines LDAP-Attributes erfordert werden: (description=*)
- ein Attribut mit einen bestimmten Wert verlangt werden: (GroupUsage=LogonGroup)
- Mehrere unterschiedliche Anforderungen an die LDAP-Gruppen gestellt werden um diese aufzunehmen: (|(GroupUsage=LogonGroup)(GroupUsage=WinGroup))

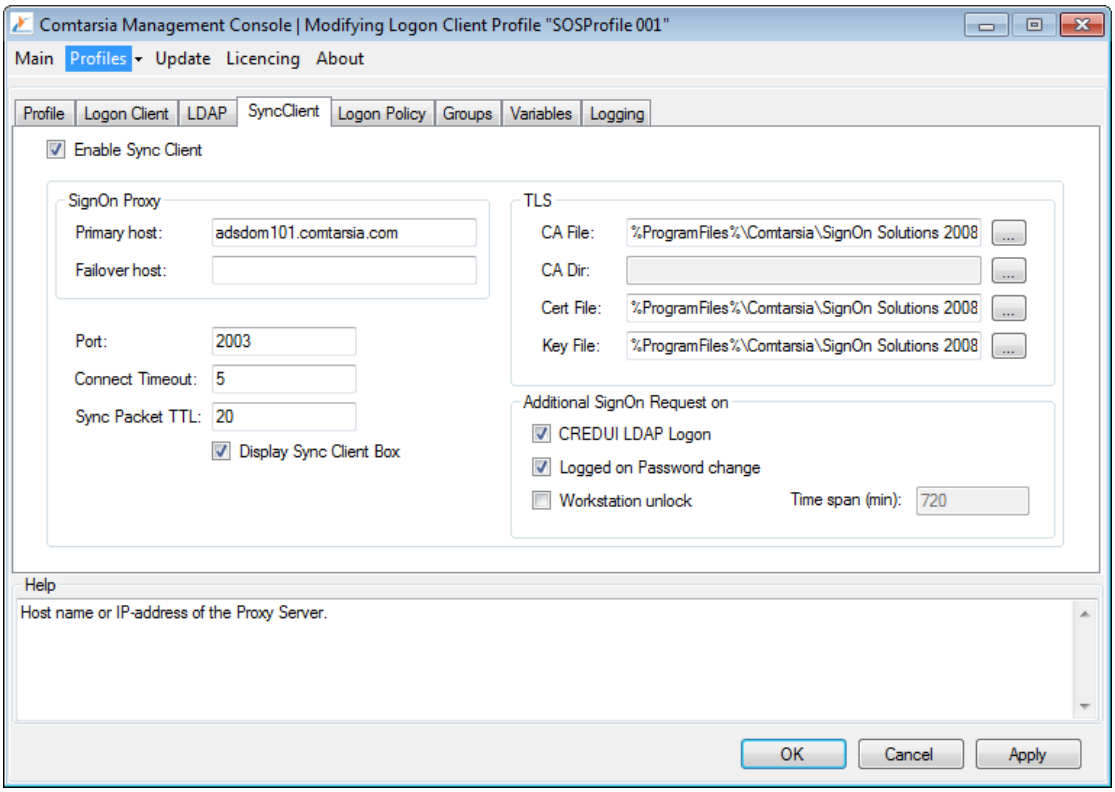
Group Types
Dieser Parameter gibt an nach welchen LDAP-Gruppentypen gesucht werden soll. Die zu verwendente Konfiguration dieses Parameters hängt von den im LDAP verwendeten Gruppen ab.

- GroupOfNames
- GroupOfUniqueNames
- PosixGroup
- ibm-AllGroups: Spezielles Benutzerattribut, welches nur vom IBM-Directory Server verwendet wird. (ignoriert Query Base und Filter)
- memberOf: Spezielles Benutzerattribut, welches nur vom Microsoft Active Directory Server verwendet wird. (ignoriert Query Base und Filter)

Attribute based groups

Mit „attribute based groups" können Attribute des LDAP-Benutzerobjektes als Gruppen verwendet werden.
Wenn zum Beispiel die LDAP-Benutzerobjekte ein LDAP-Attribut „department" haben, kann „department" als „Attribute based group" aufgenommen werden um die Werte des LDAP-Attributes „department" als zusätzliche Gruppe zu verwenden.

## 6.3 SyncClient




Enable Sync Client
Dieser Parameter aktiviert den Sync Client. Nach jeder erfolgreichen LDAP Anmeldung wird ein Sync-Request abgesetzt.

**SignOn Proxy**Primary host
Mit diesem Parameter wird die IP-Adresse bzw. der Hostname des SignOn Proxy Servers definiert.

Failover host
Mit diesem Parameter wird die IP-Adresse bzw. der Hostname des Failover SignOn Proxy Servers definiert.

Port
Dieser Parameter definiert den IP-Port für die Kommunikation mit dem ProxyServer.

Connect Timout
Dieser Parameter definiert den Timeout in Sekunden für den Verbindungsaufbau mit dem Proxy Server.

Sync Packet TTL
Dieser Parameter definiert den Timeout in Sekunden für die Bearbeitung der SyncPackets.

Display Sync Client Box

Ist dieser Parameter aktiv, wird im linken oberen Ecke des Anmeldefensters der Synchronisationsstatus eingeblendet.


**TLS**
CA File
Dieser Parameter definiert das CA-Zertifikat.
Cert File
Dieser Parameter definiert das Benutzer/Computer-Zertifikat.
Key File
Dieser Parameter definiert den Benutzer/Computer-Schlüssel.

Nähere Informationen über die Logon Client <-> SigOn Proxy Kommunikation entnehmen Sie bitte dem Manual Architekturübersicht-SSL-Zertifikate Kaptiel 2.1.

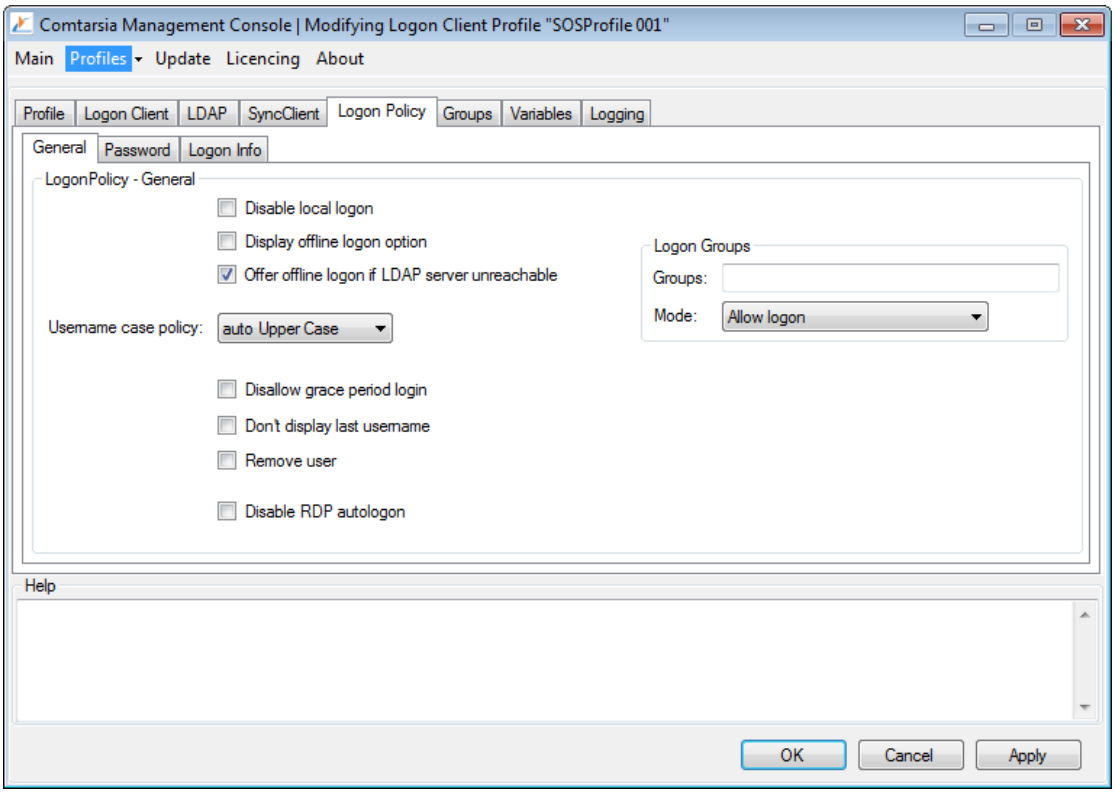
**Additional SignOn Request on**
Ist der Parameter CREDUI LDAP Logon aktiviert, wird ein Sync-Request nach jeder erfolgreicher CREDUI LDAP Anmeldung abgesetzt.
(Z.b. Bei der Windows UAC)


Ist der Parameter Logged on Password change aktiviert, wird ein Sync-Request nach jeder erfolgreicher LDAP-Passwortänderung in einer angemeldeten Benutzersitzung abgesetzt.

Ist der Parameter Workstation Unlock aktiviert, wird ein Sync-Request vor dem entsperren der Arbeitstation abgesetzt. Mit dem Parameter Time span (min) kann die Zeitspanne seit der letzten erfolgreichen Synchronisation eingestellt warden. Diese Funktion ist notwendig, wenn Arbeitstationen länger gesperrt sein können als die Zeitspanne am SignOn Gate TTL definiert ist.

## 6.4 Logon

### 6.4.1 Logon Policy




Ist der Parameter Disable local logon aktiviert, steht die Option, „LOKALE ANMELDUNG" in der Anmeldemaske nicht zur Verfügung.

Display offline logon option

Offer offline logon if LDAP server unreachable

Der Parameter Username case policy definiert die mögliche Groß- und Kleinschreibung bei der Eingabe des Benutzernamens in der Anmeldemaske.

No Case Policy: Gross und Kleinschreibung wird verwendet.
Auto Upper Case: Sämtliche Zeichen warden in Grossbuchstaben konvertiert.
Auto Lower Case: Sämtliche Zeichen warden in Kleinbuchstaben konvertiert.

**Achtung!**

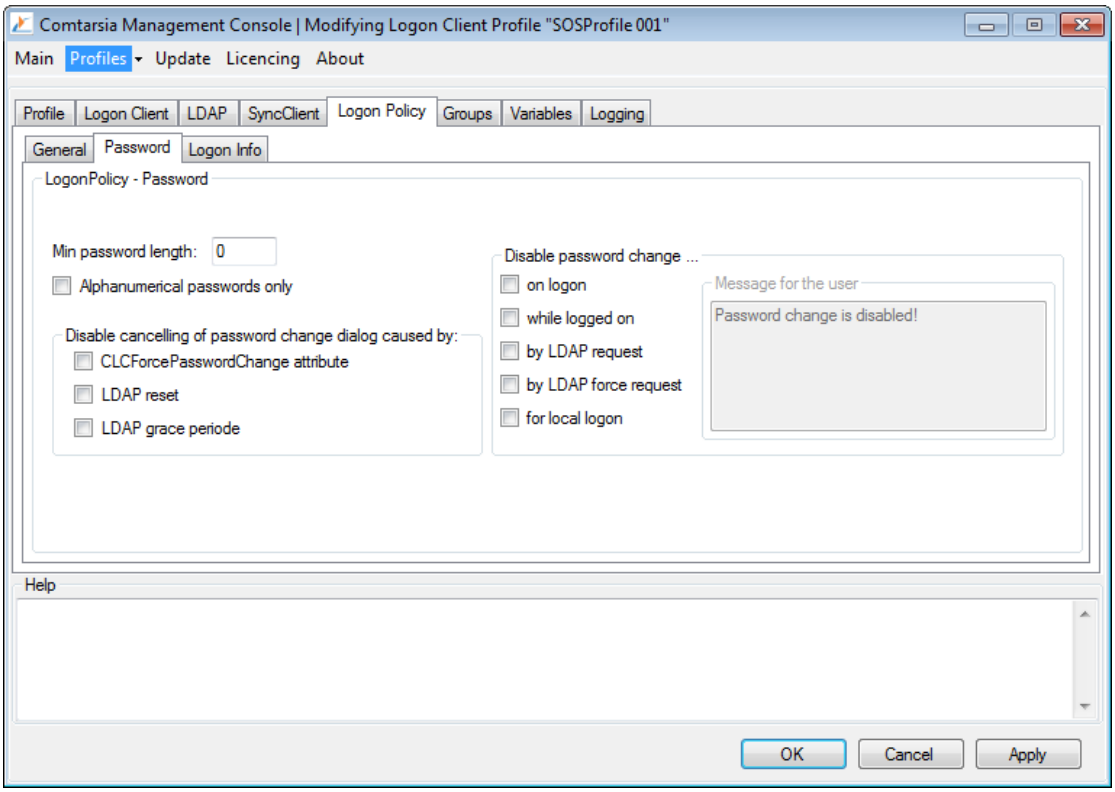
Die Einstellung „No Case Policy" ist nur empfehlenswert, wenn die primäre Anmeldedomäne bzw. der LDAP-Server, Groß-/Kleinschreibung unterscheidet!

z.B. akzeptiert der LDAP-Server für den Benutzer „USER1", die Eingabe „user1" oder „User1", ist nicht sichergestellt, dass womöglich auf nicht Case Sensitive Ressourcesysteme, welche über das Modul Comtarsia SignOn Gate synchronisiert werden, der Benutzer richtig und einheitlich übertragen wird.

Ist der Paramete Remove user aktiviert, wird bei Abmeldung einer LDAP-Logonsitzung mit lokalen Benutzermodus das Benutzerkonto und das Benutzerpofil automatisch gelöscht. Diese Funktion wird nur auf Benutzerkonten angewandt welche vom Logon Client im Zuge einer LDAP-Anmeldung selber erstellt wurden.
(gekennzeichnet durch die Benutzerbezeichnung „SERV_TEMP_USER").
Im Domain-Modus, d.h. bei Verwendung von Domain Usern, ist dies Funktionalität nicht aktiv. Hier kommt folgende Windows Policy zur Anwendung:
REG_DWORD:HKLM\Software\Policies\Microsoft\Windows\System\DeleteRoaming Cache = 1

Disable RDP autologon

**Logon Groups**
Mit dem Parameter Groups kann eine Beistrich-separierte Liste von LDAP-Gruppennamen definiert werden, von welcher eine LDAP-Anmeldung abhängig gemacht werden kann. Ob diese Liste die Gruppen definiert, für welche die Anmeldung erlaubt bzw. verboten ist, kann über den Parameter Mode eingestellt werden. Ist die Liste leer, ist eine LDAP Anmeldung unabhängig von Gruppenmitgliedschaften möglich.
Über die Funktion „Attribute based groups" (siehe: Konfiguration LDAP-groups und Parameter Attribute based groups) können Werte von LDAP-Benutzer-Attributen als zusätzliche Gruppen verwendet werden.




**Password**

Mit den Parameter Min password length kann die Mindestlänge des Passwortes defniert werden, welches für die LDAP-Anmeldung bzw. für den LDAP-Passwordwechsel akzeptiert werden.

Ist der Parameter Alphanumerical passwords only aktiviert, werden beim LDAP-Passwortwechsel nur Alphanumerische Zeichen erlaubt.

Das Abbrechen vom Passwortwechseldialog kann ich folgenden Fällen unterbunden werden:

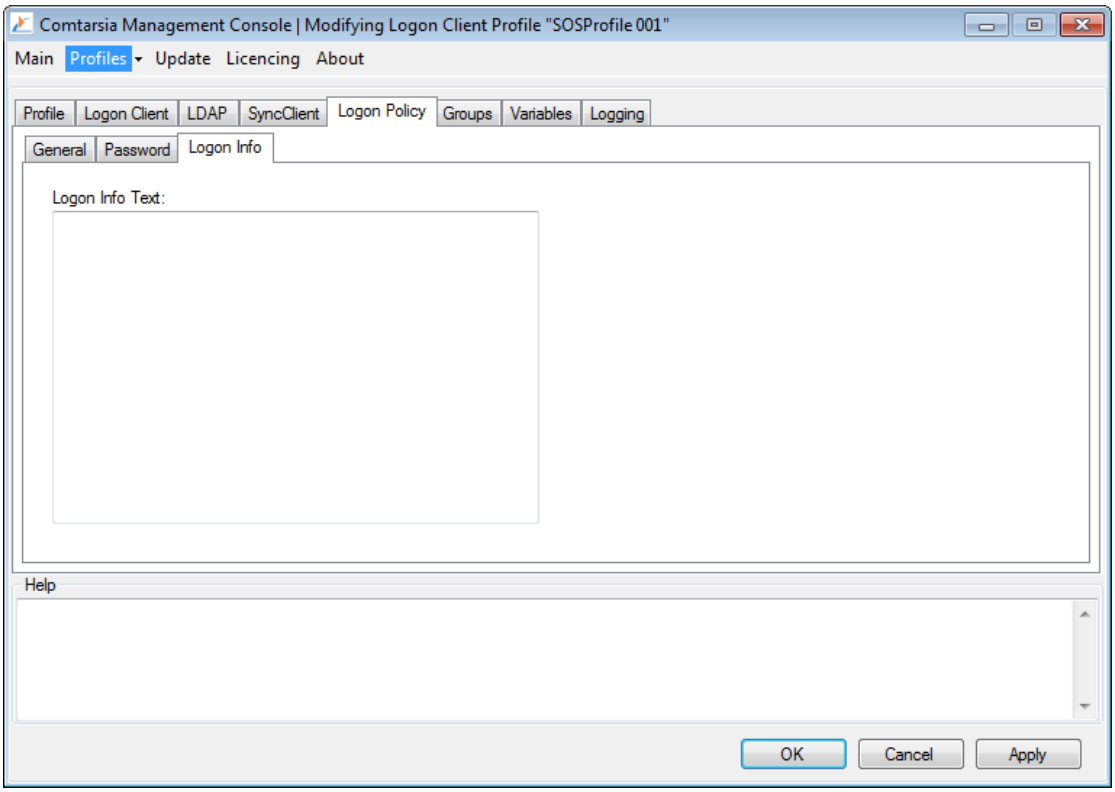
- Bei aktivierten Parameter CLCForcePasswordChange attribute wenn durch das gleichnamige LDAP-Attribute des LDAP-Benutzerobjekts der Passwortwechsel angestossen wurde.
- Bei aktivierten Parameter LDAP reset wenn der LDAP-Server über die Password-Policy „must change on reset" einen Passwortwechsel verlangt.
- Bei aktivierten Paramenter LDAP grace periode wenn auf Grund einer grace-Periode ein Passwortwechsel angestossen wurde.

Das Passwortwechseln kann in folgenden Fällen unterbunden werden:

- Bei aktivierten Parameter on logon über die Check-Box „Passwort Wechseln" in der Anmelde Maske.
- Bei aktivierten Parameter while logged on im angemeldeten Zustand.
- Bei aktivierten Parameter by LDAP request der LDAP-Server (zb mittels „warn expire") ein Passwort Wechsel verlangt.
- Bei aktivierten Parameter by LDAP force request wenn das CLCForcePWDchange Attribute des LDAP-Benutzerobjekts, oder der LDAP-Server mittels „must change Password" (zb über die LDAP Policy „must change on reset") einen Passwortwechsel anstossen.
- Bei aktivierten Parameter for local logon bei lokaler Anmeldung.

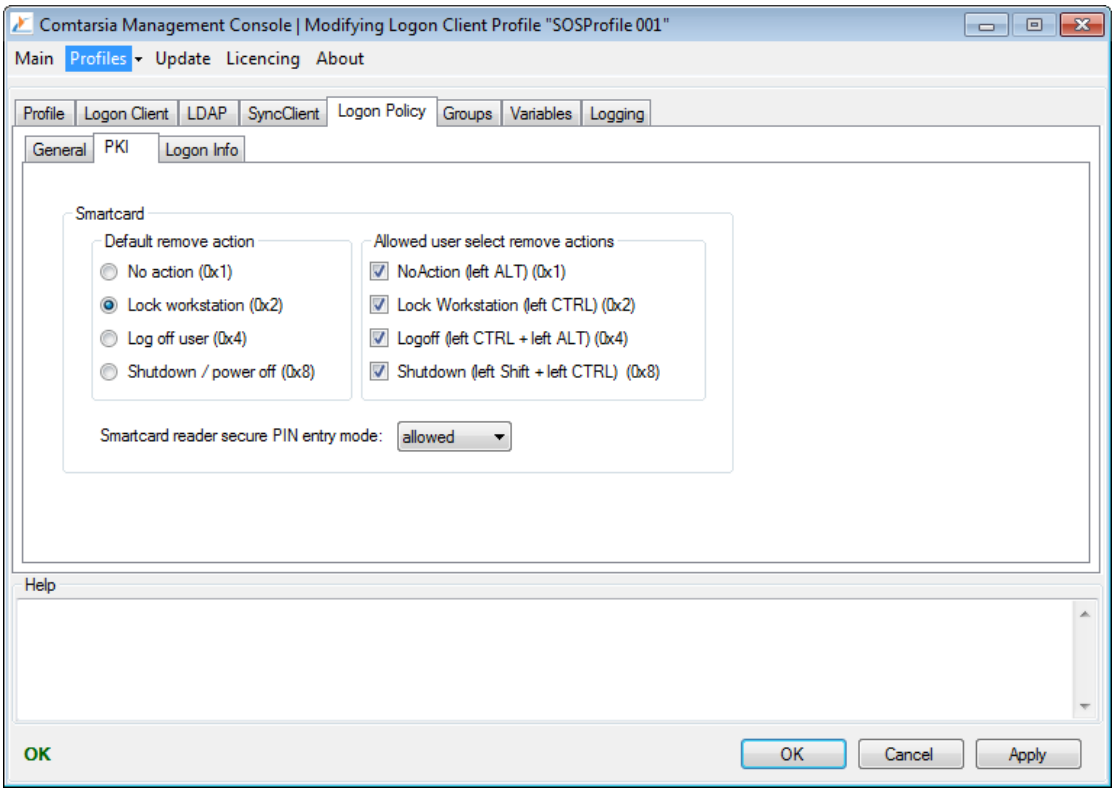
Wird ein Passwortwechsel auf Grund dieser Policies unterbunden, kann dem Anwender über den Parameter Message for the user eine Nachricht angezeigt werden. Z.b. mit den Hinweis dass er sein Passwort über folgende Webseite welchsen kann etc...

### 6.4.2 Logon Info

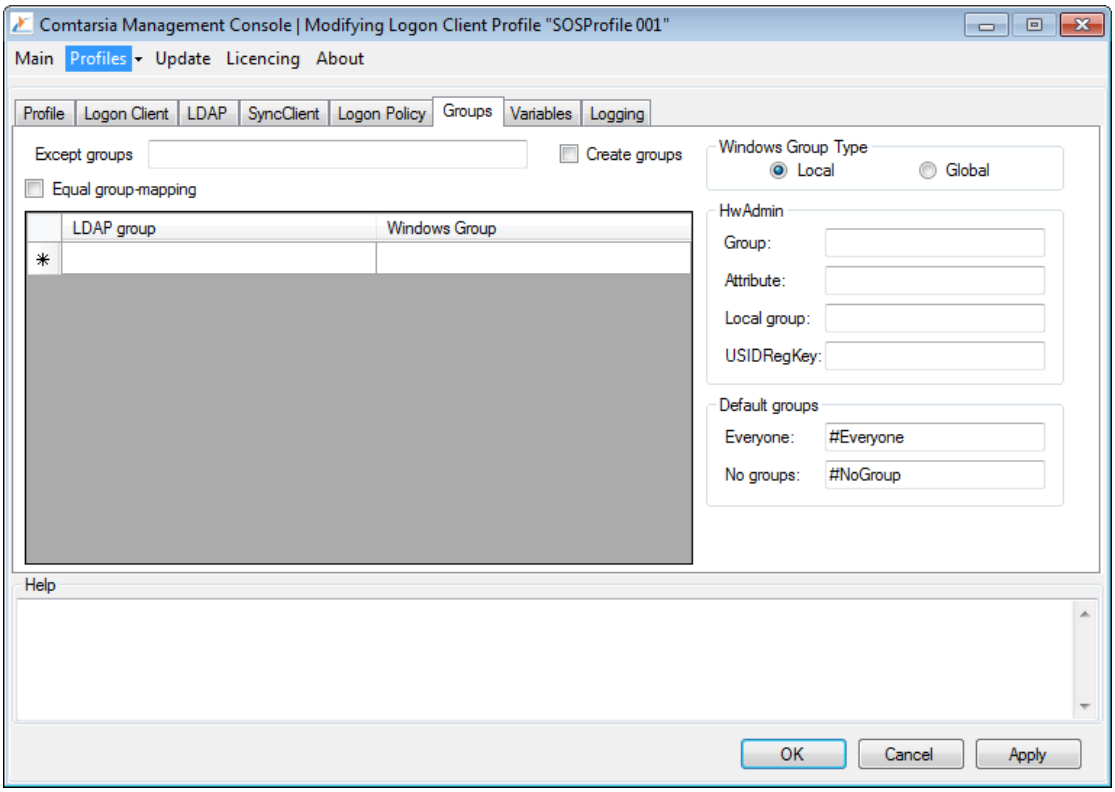



Über den Parameter Logon Info Text kann ein alternativer Informationstext definiert werden, welcher dem Benutzer über den Link „Information" in der Anmeldemaske angezeigt wird.

### 6.4.3 PKI


Comtarsia Management Console | Modifying Logon Client Profile "SOSProfile 001"
Main
Profiles
Update
Licencing
About
Profile
Logon Client
LDAP
SyncClient
Logon Policy
Groups
Variables
Logging
General
PKI
Logon Info
Smartcard
Default remove action
No action (0x1)
Lock workstation (0x2)
Log off user (0x4)
Shutdown / power off (0x8)
Allowed user select remove actions
NoAction (left ALT) (0x1)
Lock Workstation (left CTRL) (0x2)
Logoff (left CTRL + left ALT) (0x4)
Shutdown (left Shift + left CTRL) (0x8)
Smartcard reader secure PIN entry mode:
allowed
Help
OK
OK
Cancel
Apply

## 6.5 Groups




Mit den Parameter Except groups können lokale Gruppen definiert werden, welche in der Groupmapping-Funktion ausgenommen werden sollen.

Mit aktivierten Create groups Parameter werden Gruppen am System während der Anmeldung automatisch erstellt, wenn die Gruppe nicht existiert auf welche eine „Group-mapping"-Aktion durchgeführt werden soll.

Mit dem Parameter Windows Group Type kann der Typ der Systemgruppen umgestellt werden. Auf Workstation bzw. auf Server ohne Domain Controller Funktion muss der Typ auf „local Groups" gestellt werden. Auf Domain Controller kann das „Group-mapping" auf Globale Gruppen gestellt werden.

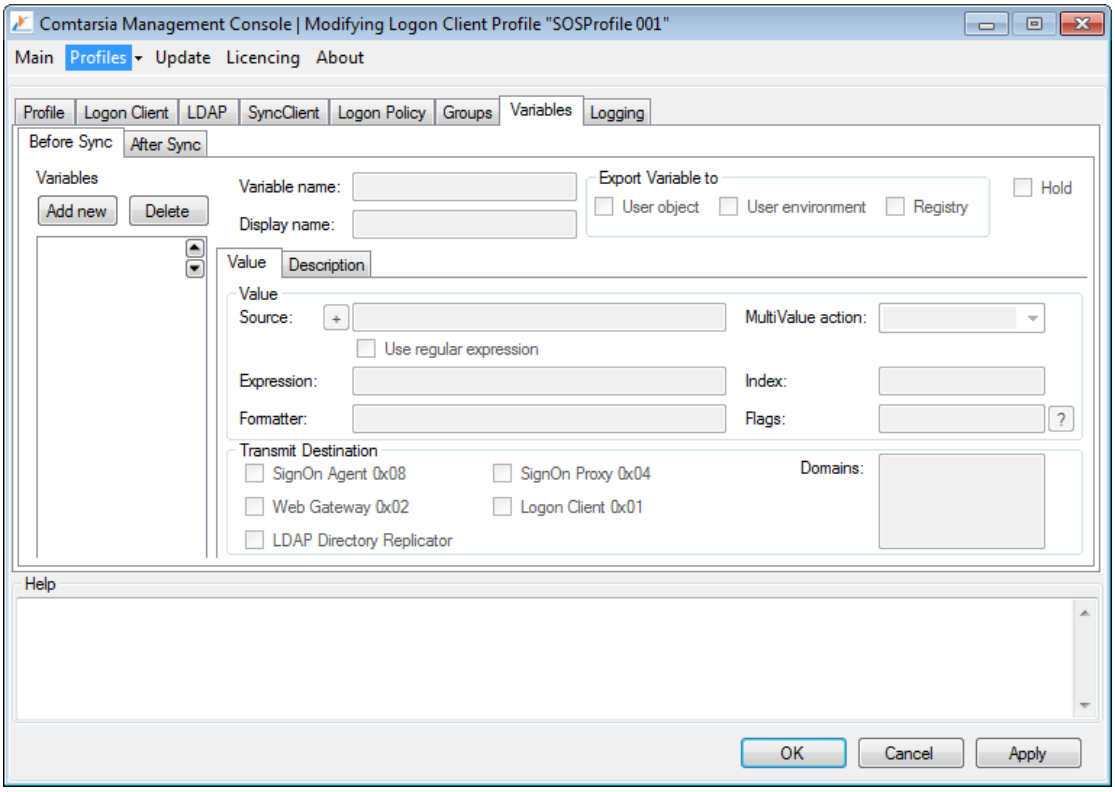
Ist der Parameter Equal group-mapping aktiviert, werden automatisch sämtliche LDAP Gruppen auf System Gruppen zugewiesen.
Ist dieser Parameter nicht aktiviert, kann eine manuelle „Group-mapping"-Tabelle definiert werden.
In der Spalte „LDAP group" kann eine LDAP Gruppe auf lokale System Gruppen (mit Beistich getrennt) In der Spalte „Windows group" gemapped werden. D.h. ist der LDAP-Bentuzer in dieser LDAP-Gruppe oder auf Grund von AttributeBasedGroups wird der System-Benutzer in die Windows-Gruppen als Mitglied hinzugefügt.

**HwAdmin**Der Parameter HwAdmin Group gibt an, in welcher LDAP-Gruppe der Benutzer Mitglied sein muss, damit HWAdmin Rechte ermöglicht werden.

Der Parameter HwAdmin Attribute gibt an, welches Attribut des LDAP-Benutzersobjektes eine Liste mit Rechnernamen enthält, für welche dieser Benutzer HWAdmin werden darf
Sind beite Kretierien erfüllt, wird der Windows Benutzer Mitglied der lokalen Administratoren Gruppe. Der Name der lokalen Administratoren Gruppe muss über den LocalAdminGroup Parameter definiert werden

**Default groups**
Der Parameter Everyone definiert einen virtuellen LDAP-Gruppennamen um alle Benutzer, unabhängig von einer LDAP-Gruppenmitgliedschaft, Windows-Gruppen zuzuweisen.
Der Parameter No groups definiert einen virtuellen LDAP-Gruppennamen um Benutzer welche nicht Mitglied einer LDAP-Gruppe sind (inkl. AttributeBasedGroups) Windows-Gruppen zuzuweisen.

## 6.6 Variables




Variablen sind Platzhalter für veränderbare Werte welche in der Comtarsia Produktfamilie von verschiedenen Quellen bezogen, weiterverarbeitet und zwischen den Produkten ausgetauscht werden können. Mittels der Variablen kann sowohl das Verhalten der jeweiligen Produkte beeinflusst, als auch können die Werte in das jeweilige Zielsystem exportiert werden.

Beispiele für mögliche Quellen: LDAP Benutzerobjekt; Registry; Computer Environment, intern zur Verfügung gestellte Werte.
Beispiele für mögliche Export ziele: Attribute des Windows Benutzerobjekts (zb Kommentar, Home/Profil Pfade, 'Full Name'); Benutzer Environment.

Die Variablen können zu zwei unterschiedlichen Zeitpunkten angewandt werden was durch die Tabs "Before Sync" und "After Sync" definiert wird.
Before Sync: Variablen werden vor der Synchronisation des Benutzers andewendet (können somit auch zum SignOn Proxy/SignOn Agent übertragen werden)
After Sync: Variablen werden nach der Synchronisation angewendet. Somit kann der SignOn Agent/SignOn Proxy Werte an den Client zurücksenden.
Ebenso werden die Variablen der Reihe nach abgearbeitet (von Oben nach Unten) weswegen mittels der Pfeil-Schaltflächen die Reihenfolge verändert werden kann.

Der Variable name definiert den Namen der Variable. Falls die Variable exportiert wird, muss dieser Name mit dem Namen der Zielvariable/des Zielattributes übereinstimmen.

Mit den Display name kann eine beliebige Bezeichnung/Beschreibung definiert werden welche in der Variablen Liste angezeigt wird. Technisch hat dieser Wert keine Auswirkung und dient legitlich der Organisation.

Über "Export Variable to" kann die Variable exportiert werden.
User object: Der Wert des Benutzerobjekts (mit dem Namen der Variable) wird auf den Wert der Variable gesetzt.
User environment: Die Variable wird in das Benutzer Environment (als Umgebungsvariable) exportiert.

Mittels Hold kann dieser Variablen Eintrag temporär deaktiviert werden.

**Value**
Der Source definiert die Quelle bzw den Wert der Variable. Dieses Feld kann neben Text auch andere Variablen (zwischen zwei '%') beinhalten. Um '%' als Text zu verwenden muss man '%%' angeben. Die "+" Schaltfläche kann zum einfügen von Variablen-Templates verwendet werden.

Mittels MultiValue action wird definiert was mit MultiValue Variablen (Variablen welche ein Array darstellen) passieren soll.
Overwrite: Eine eventuell bereits existierende Variable wird überschrieben.
Delete: Die Variable wird gelöscht.
DeleteValue: Der resultierende Wert wird aus der vorhandenen Variable gelöscht.
AddValue: Der resultierende Wert wird zum Array hinzugefügt. (um zum Beispiel eine Gruppe zur vorhandenen Gruppen Liste hinzuzufügen)

Mittels Use regular expression kann man die Verwendung Regulärer Ausdrücke aktivieren.

Der Wert Expression definiert einen Regulären ausdruck welcher auf den aufgelösten Inhalt von Source angewendet wird. Wenn also Source auch Variablen beinhaltet, werden diese ersetzt bevor der Reguläre Ausdruck angewendet wird.

Der Formatter definiert wie der resultierende Wert aus Wert und Regulärem Ausdruck zusammengesetzt werden soll.

Mittels des Index kann auf eine bestimmte Übereinstimmung verwiesen werden falls die Reguläre Ausdruck mehr als eine Übereinstimmung liefert. Üblicherweise ist der Index immer 0.

Die Flags definieren eine Bitmaske durch welche die Funktionsweise der Regulären Ausdrücke beeinflusst werden kann.

Gültige Flags:

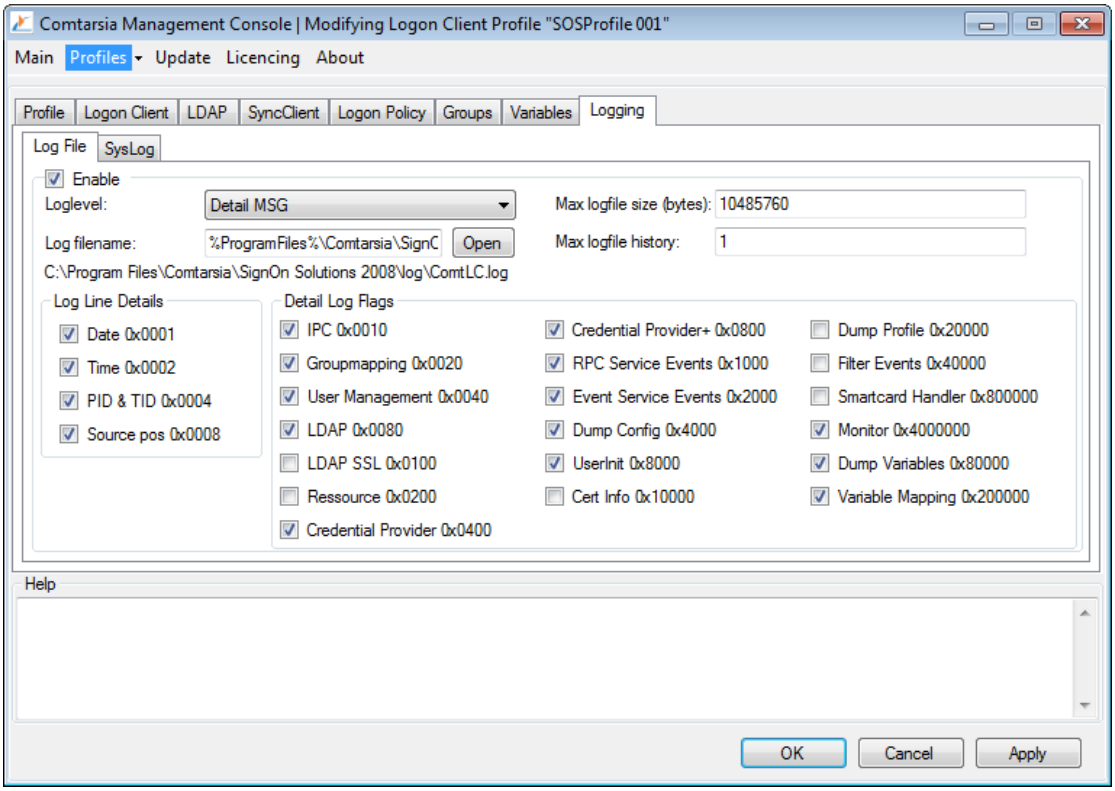
```
match_default           0,
match_not_bol           0x00000001, /* first is not start of line */
match_not_eol           0x00000002, /* last is not end of line */
match_not_bob           0x00000004, /* first is not start of buffer
*/
match_not_eob           0x00000008, /* last is not end of buffer */
match_not_bow           0x00000010, /* first is not start of word */
match_not_eow           0x00000020, /* last is not end of word */
match_not_dot_newline   0x00000040, /* \n is not matched by '.' */
match_not_dot_null      0x00000080, /* '\0' is not matched by '.' */
match_prev_avail        0x00000100, /* *--first is a valid expression
*/
match_init              0x00000200, /* internal use */
match_any               0x00000400, /* don't care what we match */
match_not_null          0x00000800, /* string can't be null */
match_continuous        0x00001000, /* each grep match must continue
*/
                                    /* uninterupted from the previous
one */
match_partial           0x00002000, /* find partial matches */

match_stop              0x00004000, /* stop after first match (grep)
V3 only */
match_not_initial_null  0x00004000, /* don't match initial null, V4
only */
match_all               0x00008000, /* must find the whole of input
even if match_any is set */
match_perl              0x00010000, /* Use perl matching rules */
match_posix             0x00020000, /* Use POSIX matching rules */
match_nosubs            0x00040000, /* don't trap marked subs */
match_extra             0x00080000, /* include full capture
information for repeated captures */
match_single_line       0x00100000, /* treat text as single line and
ignor any \n's when matching ^ and $. */
match_unused1           0x00200000, /* unused */
match_unused2           0x00400000, /* unused */
match_unused3           0x00800000, /* unused */
match_max               0x00800000,

format_perl             0,          /* perl style replacement */
format_default          0,          /* ditto. */
format_sed              0x01000000, /* sed style replacement. */
format_all              0x02000000, /* enable all extentions to
sytax. */
format_no_copy          0x04000000, /* don't copy non-matching
segments. */
format_first_only       0x08000000, /* Only replace first occurance.
*/
format_is_if            0x10000000, /* internal use only. */
format_literal          0x20000000, /* treat string as a literal */
```

**Transmit Destination**

Die Transmit Destination bestimmt an welche anderen Comtarsia Systeme die momentane Variable weitergeleitet werden soll. (Ungültige Zielsysteme sind ausgegraut)

Falls die Transmit Destination 'SignOn Agent 0x8' ausgewählt ist (nur am SignOn Proxy möglich) kann man mittels der Domains definieren an welche SignOn Agent Domänen die momentane Variable übermittelt werden soll. Wenn dieses Feld leer ist, wird die Variable an alle Agents übermittelt.

## 6.7 Logging




Log File
Enable
Aktiviert/deaktiviert das Schreiben des Logs in eine Datei.

Loglevel
Definiert welche Art von Meldungen in die Log-Datei geschrieben werden sollen. Die „Detail Log Flags" werden unabhängig vom Loglevel behandelt. zB Kann „Loglevel"=None, und „Detail Log Flags"=Monitor definiert werden um nur „Überwachungs-ausgaben" zu erhalten.

- None: Keine
- Error: Nur Fehler
- Exception: Fehler und Ausnahmen
- Warn: Fehler, Ausnahmen und Warnungen
- Info: Fehler, Ausnahmen, Warnungen und zusätzliche Informationen
- Detail MSG: Alle Ausgaben (ausser Detail Log Flags)

Log filename
Definiert den Pfad zur Datei in welche die Logausgaben geschrieben werden sollen.

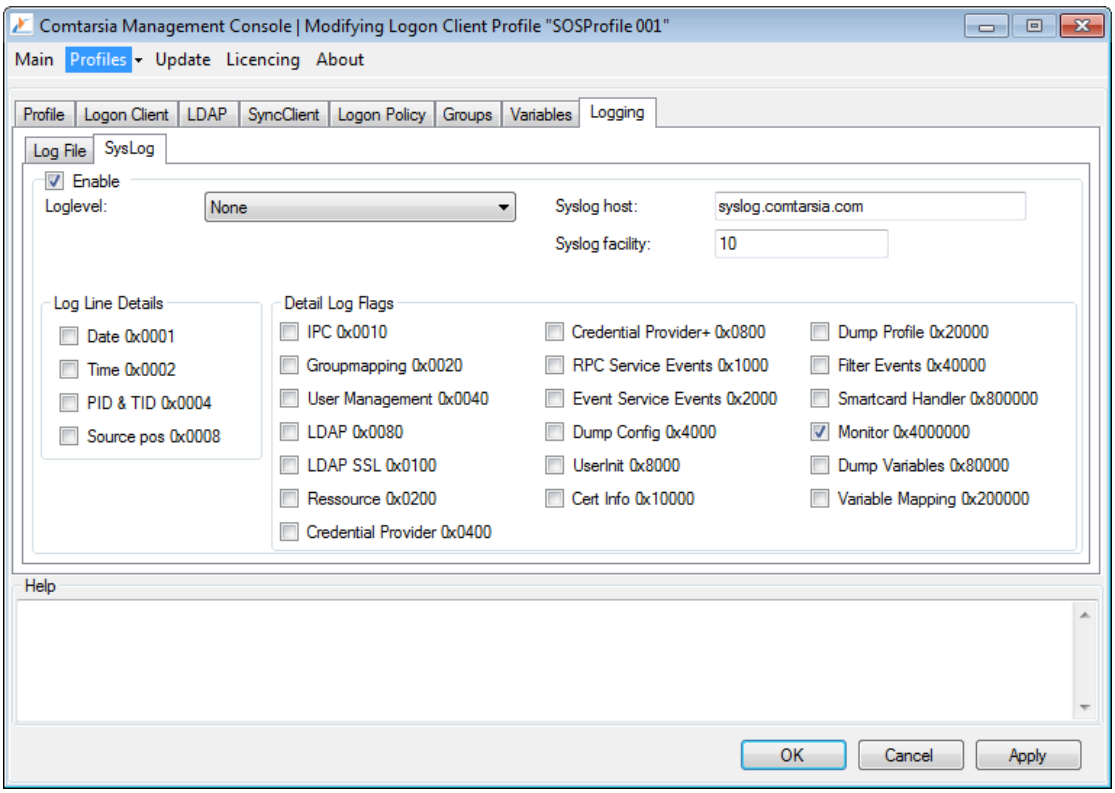
Max logfile size
Wenn die Grösse der Logdatei die hier definierte Grösse (in Bytes) überschreitet, wird die Logdatei rotiert. (abhängig von „Max logfile history")

Max logfile history
Die Anzahl der Logdateien welche rotiert werden sollen.

Detail Log Flags
Definiert welche spezifischen Informationen geloggt werden sollen. Die „Detail Log Flags" fungieren unabhängig vom Loglevel.

Log Line Details
Welche Informationen pro Logzeile ausgegeben werden sollen.

- Date: Datum
- Time: Uhrzeit
- PID & TID: Prozess- und Thread-ID
- Source pos: Die momentane Position im Quellcode




SysLog
Enable
Aktiviert/deaktiviert die Logübermittlung an einen SysLog Server

Loglevel
Definiert welche Art von Meldungen geloggt werden sollen.
Die „Detail Log Flags" werden unabhängig vom Loglevel behandelt. zB Kann „Loglevel"=None, und „Detail Log Flags"=Monitor definiert werden um nur „Überwachungs-ausgaben" zu erhalten.

- None: Keine
- Error: Nur Fehler
- Exception: Fehler und Ausnahmen

- Warn: Fehler, Ausnahmen und Warnungen
- Info: Fehler, Ausnahmen, Warnungen und zusätzliche Informationen
- Detail MSG: Alle Ausgaben (ausser Detail Log Flags)

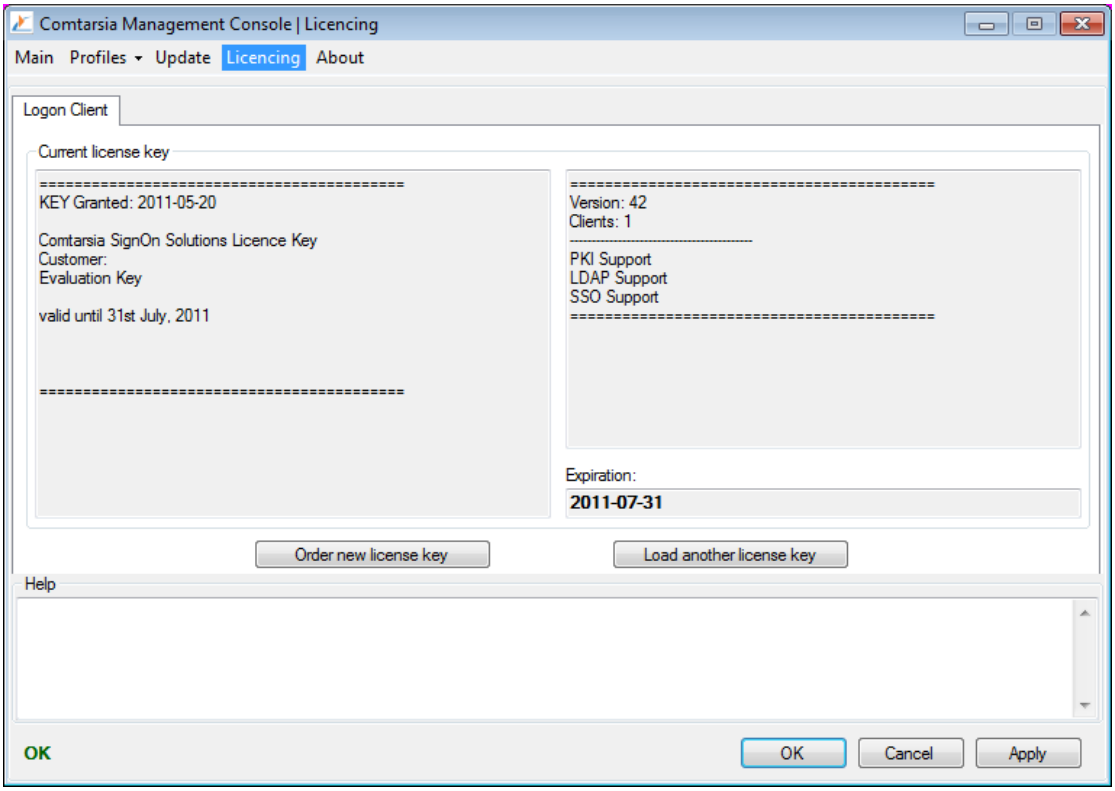
Syslog host
Definiert den zentralen SysLog-Logging-Server an welchen die Logausgabe übermittelt werden soll

Syslog facility
Definiert die SysLog facility. Der SysLog Server kann die Zugehörigkeit der Nachrichten anhand dieser Facility bestimmen.

Detail Log Flags
Definiert welche spezifischen Informationen geloggt werden sollen. Die „Detail Log Flags" fungieren unabhängig vom Loglevel.

Log Line Details
Welche Informationen pro Logzeile ausgegeben werden sollen.
- Date: Datum
- Time: Uhrzeit
- PID & TID: Prozess- und Thread-ID
- Source pos: Die momentane Position im Quellcode

## 6.8 Licensing




Mit dem Button „Load another license key" wird der Lizenzschlüssel mit den Namen „key042" in das Verzeichniss %ProgramFiles%\Comtarsia\SignOn Solutiions 2008\Key kopiert.

# 7.Registry Gegenüberstelltung mit Comtarsia Logon Client 2006

**Erklärung der Farben:**

CLC 2006 Konfiguration
CLC 2008 Konfguration

**Umschalten Vista Credential Provider?**
"DisableMsGina"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonClient]
"UnregisterMsCredProvider"=dword:00000001
"DisableMsCredProviderToggle"=dword:00000001

**Groupmapping**
"GroupAdministrator"="0xWS"
"GroupPowerUser"="0xPU"

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\GroupMapping]
@=""
"0xWS "="Administrators"
"0xPU "="PowerUser"
"0xWS "="Administratoren"
"0xPU "="Hauptbenutzer"

**Mode**
"EnableDomainLogon"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonClient]
"EnableDomainLogon"=dword:00000001
"WinDomain"="ADSDOM146"

"EnableSyncClient"=dword:0000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonClient]
"EnableSyncClient"=dword:00000001

"DisableLocalLogon"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
"DisableLocalLogon"=dword:00000000

**HomeDir**
"HomeDirDrive"="Z:"
"HomeDirPath"="\\\\QA%physicaldeliveryofficename%A01\\users$\\%USERNAM
E%"

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile
001\UserEnvironment]
"HomeDirDrive"="Z"
"HomeDirPath""="\\\\QA%physicaldeliveryofficename%A01\\users$\\%USERNAM
E%"

**PWD**
"MinPwdLen"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
"MinPwdLen"=dword:00000001

**USER**
"UserNameCasePolicy"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
" UserNameCasePolicy "=dword:00000001

**LDAP**
"LDAPEnableSSL"=dword:00000002

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile
001\LDAP\Servers\lind.comtarsia.com]
"sslMode"=dword:00000002

"EnableLDAP"=dword:00000001
Dieser Parameter ist nicht mehr mehr notwendig

**GPUpdate**
"GPUpdate_CMD"="gpupdate.cmd"
"GPUpdate_Mask"=dword:00000102

Noch nicht implementiert, (kann derzeit mit Scripts gelöst warden)->
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\Script]
"UserLogon"=" gpupdate.cmd "
"SystemLogon"=" gpupdate.cmd "

**SSO:**
"EnableSSOExec"=dword:00000002
"MSSORootPath"="C:\\Programme\\Comtarsia\\ComtMSSO"
"EnableSSO"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\SSO]
"EnableSSO"=dword:000000000
"RootPath"=""

**OUT-Parameter**
"USID"="S-1-5-21-1630323187-507556056-2246393201-1296"
"CSID"=

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\temp]
"USID"="S-1-5-21-157906255-4040051303-1972554199-500"
"CSID"= "S-1-5-21-157906255-4040051303-1972554199"

**Disabled**
"DontDisplayLastUserName"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
"DontDisplayLastUserName"=dword:00000000

"ProfilePath"=""

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\UserEnvironment]
"ProfilePath"=""

"DenyCancleForcePWDChangeDlg"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
"DenyCancleForcePWDChangeDlg"=dword:00000001

**Scripts:**
"DisplayScriptError"=dword:00000001
"ScriptTimeout"=dword:000000b4
"NoScriptsByCachedCredLogon"=dword:00000001
"UserLogoffScript"="\\\\%INSTSRV%\\netlogon\\UserLogoff.cmd"
"UserLogonScript"="\\\\%INSTSRV%\\netlogon\\UserLogon.cmd"
"DisableEqualGroupMapping"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\Script]
"Timeout"=dword:000000b4
"UserLogon"=""
"UserLogoff"=""
"SystemLogon"=""
"SystemLogoff"=""
"SystemInit"=""

**Groupmapping**
"HwAdminAttribute"="uniqauapname"
"HwAdminGroup"="APP-UAP-HWAdmin"

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\Group]
@=""
"HwAdminGroup"="localhwadmin"
"HwAdminAtrribute”=""

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\GroupMapping]
@=""
"GROUP1"="Administrators"
"GROUP3"="lg1"

**WkstLogonPolicy**
"EnableWkstLogonPolicy"=dword:00000001
"WkstLogonPolicyRootOUGroups"=hex(7):4f,00,55,00,3d,00,55,00,41, ….

[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\LogonPolicy]
"AlphaNumPwd"=dword:00000000
"DisablePasswordChange"=dword:00000000
"DisallowGraceLogin"==dword:00000000

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\Log]
"logLevel"=dword:00000005
"logMask"=dword:00001400
```

# 8.Parameterbeschreibung

## [HKLM\SOFTWARE\Comtarsia]

## [.\SignOn Solutions 2008]

### path
**path**=REG_SZ:"C:\\Program Files\\Comtarsia\\SignOn Solutions 2008"
Product installation directory.

## [.\SignOn Solutions 2008\Components]

## [.\SignOn Solutions 2008\DefaultProfiles]

### LogonClient
**LogonClient**=REG_SZ:"SOSProfile 001"

## [.\SignOn Solutions 2008\LogonClient]

### userInit
**userInit**=REG_SZ:"%SYSTEMROOT%\\system32\\userinit.exe"

### credProvMode
**credProvMode**=REG_DWORD:0

### detectedCredProvMode
**detectedCredProvMode**=REG_DWORD:0

### displayCredProvConfig
**displayCredProvConfig**=REG_DWORD:0

## [.\SOSProfile *]

### language
**language**=REG_SZ:"Auto"
Language of the user interface. (Logon screen, messages)

### profileName
**profileName**=REG_SZ:""

### profileComment
**profileComment**=REG_SZ:""

### profileConfigVersion
**profileConfigVersion**=REG_SZ:""

## [.\SOSProfile *\Group]
Configuration of the system specific groups.

### equalGroupMapping
**equalGroupMapping**=REG_DWORD:0
0: use the groupmapping list to map LDAP groups to system groups
1: use the LDAP groups 1:1 without mapping

### exceptGroups
**exceptGroups**=REG_SZ:""
A comma seperated list of group names which should be ignored.

### globalGroups
**globalGroups**=REG_DWORD:0
0: use local system groups
1: Use global groups (only valid on domain controllers)

### HwAdminGroup
**HwAdminGroup**=REG_SZ:""

### HwAdminAttribute
**HwAdminAttribute**=REG_SZ:""

### HwAdminUSIDRegKey
**HwAdminUSIDRegKey**=REG_SZ:""

### HwAdminSubOU
**HwAdminSubOU**=REG_SZ:""

### localAdminGroup
**localAdminGroup**=REG_SZ:""

### createGroups
**createGroups**=REG_DWORD:0
Create non-existing groups.

### defaultEveryoneGroup
**defaultEveryoneGroup**=REG_SZ:"#Everyone"
A default group every LDAP user will be a member of. It can also be used with group mapping.

### defaultNoGroup
**defaultNoGroup**=REG_SZ:"#NoGroup"
A default group every LDAP user who doesn't have any LDAP groups will be a member of.

## [.\SOSProfile *\GroupMapping]

## [.\SOSProfile *\LDAP]

# [.\SOSProfile *\LDAP\Servers]

# [.\SOSProfile *\LDAP\Servers\<LDAP-Server>]

The name of this key (<LDAP-Server>) is also the hostname of the LDAP server

## priority

**priority**=REG_DWORD:0

**failoverHost**

**failoverHost**=REG_SZ:""

**baseDN**

**baseDN**=REG_SZ:"o=comtarsia"

The LDAP baseDN

**userDNPrefix**

**userDNPrefix**=REG_SZ:"uid="

**userDNSuffix**

**userDNSuffix**=REG_SZ:",ou=sd"

**userOUPrefix**

**userOUPrefix**=REG_SZ:""

**userOUSuffix**

**userOUSuffix**=REG_SZ:""

**userObjectClass**

**userObjectClass**=REG_SZ:"Person"

**userObjectRequired**

**userObjectRequired**=REG_DWORD:1

**userQueryScope**

**userQueryScope**=REG_DWORD:2

**groupTypes**

**groupTypes**=REG_DWORD:7

**groupQueryBase**

**groupQueryBase**=REG_SZ:""

**groupQueryScope**

**groupQueryScope**=REG_DWORD:2

**attributeBasedGroups**

**attributeBasedGroups**=REG_MULTI_SZ:"System.String[]"

**userPasswordAttribute**

**userPasswordAttribute**=REG_SZ:"userPassword"

**timeout**

**timeout**=REG_DWORD:0xA

**port**
**port**=REG_DWORD:0x185

**sslMode**
**sslMode**=REG_DWORD:0

**serverType**
**serverType**=REG_DWORD:0x0

**useUTF8Password**
**useUTF8Password**=REG_DWORD:0

**dontSendOldPasswordOnChange**
**dontSendOldPasswordOnChange**=REG_DWORD:0

**systemUserDN**
**systemUserDN**=REG_SZ:""

**systemUserPassword**
**systemUserPassword**=REG_SZ:""

**OUSearchListMode**
**OUSearchListMode**=REG_DWORD:0

**OUSearchListErrorCode**
**OUSearchListErrorCode**=REG_DWORD:6

**OUSearchListObjectDN**
**OUSearchListObjectDN**=REG_SZ:""

**OUSearchListAttribute**
**OUSearchListAttribute**=REG_SZ:""

**appendBaseDN**
**appendBaseDN**=REG_DWORD:1

**searchForUser**
**searchForUser**=REG_DWORD:0

**groupFilter**
**groupFilter**=REG_SZ:""

**ignoreNoUniqueUser**
**ignoreNoUniqueUser**=REG_DWORD:0

**failoverOnUserNotFound**
**failoverOnUserNotFound**=REG_DWORD:0

## setSessionPasswordasUserPassword
**setSessionPasswordasUserPassword**=REG_DWORD:0

## followReferrals
**followReferrals**=REG_DWORD:1

# [.\SOSProfile *\Log]

**enable**
**enable**=REG_DWORD:1
With this parameter, this logging-method can be enabled/disabled.
**logFileName**
**logFileName**=REG_SZ:"%ProgramFiles%\\Comtarsia\\SignOn Solutions 2008\\log\\ComtRPCSrv.log"

**logLevel**
**logLevel**=REG_DWORD:4
Specifies the log level.
URGENCY_ERROR = 1,
URGENCY_EXCEPTION = 2,
URGENCY_WARN = 3,
URGENCY_INFO = 4,
URGENCY_MSG = 5,
**logMask**
**logMask**=REG_DWORD:0

**logDetails**
**logDetails**=REG_DWORD:0xFFFFFFFF
pecifies the log details.
logDetails = 0x0 = No log details
logDetails = 0x1 = Date
logDetails = 0x2 = Time
logDetails = 0x4 = Process and thread ids.
logDetails = 0x8 = Source postion
logDetails = 0xFFFFFFFF = All details
**enableLogTransactions**
**enableLogTransactions**=REG_DWORD:0

**maxLogFileSize**
**maxLogFileSize**=REG_DWORD:0xA00000

**maxLogFileHistory**
**maxLogFileHistory**=REG_DWORD:1

## [.\SOSProfile *\Log\SysLog]

**enable**
**enable**=REG_DWORD:0
With this parameter, this logging-method can be enabled/disabled.

**host**
**host**=REG_SZ:""
Specifies the SysLog server.

**facility**
**facility**=REG_DWORD:10
Specifies the SysLog facility.

**logLevel**
**logLevel**=REG_DWORD:0
Specifies the log level.
URGENCY_ERROR = 1,
URGENCY_EXCEPTION = 2,
URGENCY_WARN = 3,

```
URGENCY_INFO = 4,
URGENCY_MSG = 5,
```

**logMask**
**logMask**=REG_DWORD:0

**logDetails**
**logDetails**=REG_DWORD:0x0
```
Specifies the log details.
logDetails = 0x0 = No log details
logDetails = 0x1 = Date
logDetails = 0x2 = Time
logDetails = 0x4 = Process and thread ids.
logDetails = 0x8 = Source postion
logDetails = 0xFFFFFFFF = All details
```

# [.\SOSProfile *\SyncClient]

**connectTimeout**
**connectTimeout**=REG_DWORD:5

**proxyPort**
**proxyPort**=REG_DWORD:0x7D3

**syncPacketTTL**
**syncPacketTTL**=REG_DWORD:0x14

**syncProxy1**
**syncProxy1**=REG_SZ:""

**syncProxy2**
**syncProxy2**=REG_SZ:""

**tlsCAFile**
**tlsCAFile**=REG_SZ:"%ProgramFiles%\\Comtarsia\\SignOn Solutions 2008\\cert\\ca.pem"

**tlsCADir**
**vn**=REG_SZ:""
**tlsCertFile**
**tlsCertFile**=REG_SZ:"%ProgramFiles%\\Comtarsia\\SignOn Solutions 2008\\cert\\client.pem"

**tlsKeyFile**
**tlsKeyFile**=REG_SZ:"%ProgramFiles%\\Comtarsia\\SignOn Solutions 2008\\cert\\client.key"

# [.\SOSProfile *\UserCertificateMapping]

# [.\SOSProfile *\UserCertificateMapping\<UserCertificateMapping Name>]

The name of this key (<UserCertificateMappingName>) is in the form NNN_MappingName, where 'N' are numbers and define the order of the mapping rules. The first matching rule will be applied.

### expression
**expression**=REG_SZ:""

### formatter
**formatter**=REG_SZ:""

## [.\SOSProfile *\Variables]

## [.\SOSProfile *\Variables\BeforeSync]

## [.\SOSProfile *\Variables\AfterSync]

## [.\SOSProfile *\Variables\<VariableEffectivePoint>]
The name of this key can be "BeforeSync" or "AfterSync" and defines when the variables under this key should be mapped.

## [.\SOSProfile *\Variables\<VariableEffectivePoint>\<VariableName>]
The name of this key (<VariableName>) is in the form NNN_Name, where 'N' are numbers and define the order of the mapping rules. The 'Name' is the resulting name of the variable.

### displayName
**displayName**=REG_SZ:""

### variableComment
**variableComment**=REG_SZ:""

### source
**source**=REG_SZ:""

### transmitDestination
**transmitDestination**=REG_DWORD:0x0

### exportDestination
**exportDestination**=REG_DWORD:0x0

### transmitDestinationDomains
**transmitDestinationDomains**=REG_MULTI_SZ:"System.String[]"

### mappingType
**mappingType**=REG_DWORD:0

**expression**
**expression**=REG_SZ:""

**formatter**
**formatter**=REG_SZ:""

**index**
**index**=REG_DWORD:0

**flags**
**flags**=REG_DWORD:0x2000000

**multivalueAction**
**multivalueAction**=REG_DWORD:0
0:Override
1:Delete
2:DeleteValue
3:AddValue

**hold**
**hold**=REG_DWORD:0
This option can be used to temporarily disable a variable mapping.

## [.\SOSProfile *\UserEnvironment]

**defaultUserProfile**
**defaultUserProfile**=REG_SZ:""

**profilePath**
**profilePath**=REG_SZ:""

**homeDirDrive**
**homeDirDrive**=REG_SZ:"H:"

**homeDirPath**
**homeDirPath**=REG_SZ:""

## [.\SOSProfile *\LogonClient]

**displayProgressBox**
**displayProgressBox**=REG_DWORD:1

**enableSyncClient**
**enableSyncClient**=REG_DWORD:0

**displaySyncBox**
**displaySyncBox**=REG_DWORD:1

**WTSMode**
**WTSMode**=REG_DWORD:0

**ADSLogonMode**
**ADSLogonMode**=REG_DWORD:0

**winDomain**
**winDomain**=REG_SZ:""

**enableDomainLogon**
**enableDomainLogon**=REG_DWORD:0

**userinit**
**userinit**=REG_SZ:"%SYSTEMROOT%\\system32\\userinit.exe"

**GPUpdate_Mask**
**GPUpdate_Mask**=REG_DWORD:0

**GPUpdate_CMD**
**GPUpdate_CMD**=REG_SZ:""

**disableMsCredProviderToggle**
**disableMsCredProviderToggle**=REG_DWORD:0

**unregisterMsCredProvider**
**unregisterMsCredProvider**=REG_DWORD:0

**panelBitmap**
**panelBitmap**=REG_SZ:""

**refreshUnlockTimer**
**refreshUnlockTimer**=REG_DWORD:720

**removeUser**
**removeUser**=REG_DWORD:0

```
bitmask: (only for local mode)
0x1 User Account
0x2 Profile // (0x1 User Account, 0x2 Profile), only local mode.
```

**LDAPSetPasswordAsSambaPassword**
**LDAPSetPasswordAsSambaPassword**=REG_DWORD:0

## enableSmartCard
**enableSmartCard**=REG_DWORD:0

## smartCardDefaultRemoveAction
**smartCardDefaultRemoveAction**=REG_DWORD:2

## smartCardRemoveActionUserSelectMask
**smartCardRemoveActionUserSelectMask**=REG_DWORD:0xF

## logonPanelTileDisplayName
**logonPanelTileDisplayName**=REG_SZ:""

## enableProxyLogon
**enableProxyLogon**=REG_DWORD:0

## sessionPasswordTemplate
**sessionPasswordTemplate**=REG_SZ:"LLUURR99SS"

## smartCardSessionPasswordMode

**smartCardSessionPasswordMode**=REG_DWORD:0

### smartCardSessionPasswordValidity
**smartCardSessionPasswordValidity**=REG_DWORD:1

### smartCardSessionPasswordValidityUnits
**smartCardSessionPasswordValidityUnits**=REG_DWORD:0

### smartCardSessionPasswordValidityOffset
**smartCardSessionPasswordValidityOffset**=REG_DWORD:0

### smartCardSecurePINEntryMode
**smartCardSecurePINEntryMode**=REG_DWORD:1

### displayMsgStrID
**displayMsgStrID**=REG_DWORD:0

## [.\SOSProfile *\LogonPolicy]

**minPwdLen**
**minPwdLen**=REG_DWORD:0

**alphaNumPwd**
**alphaNumPwd**=REG_DWORD:0

**userNameCasePolicy**
**userNameCasePolicy**=REG_DWORD:1

**disablePasswordChange**
**disablePasswordChange**=REG_DWORD:0

**disableLocalLogon**
**disableLocalLogon**=REG_DWORD:0

**changePasswordInfo**
**changePasswordInfo**=REG_SZ:"Password change is disabled!"

**denyCancelForcePWDChangeDlg**
**denyCancelForcePWDChangeDlg**=REG_DWORD:0

**disallowGraceLogin**
**disallowGraceLogin**=REG_DWORD:0

**dontDisplayLastUserName**
**dontDisplayLastUserName**=REG_DWORD:0

**logonAllowGroups**
**logonAllowGroups**=REG_SZ:""

**negateLogonAllowGroups**
**negateLogonAllowGroups**=REG_DWORD:1

### enableWkstLogonPolicy
**enableWkstLogonPolicy**=REG_DWORD:0

### wkstLogonPolicyRetryTimer
**wkstLogonPolicyRetryTimer**=REG_DWORD:60

### wkstLogonPolicyRootOUGroups
**wkstLogonPolicyRootOUGroups**=REG_MULTI_SZ:"System.String[]"
**logonInformationText**
**logonInformationText**=REG_SZ:""

### offerOfflineLogonByUnreachableLDAP
**offerOfflineLogonByUnreachableLDAP**=REG_DWORD:1

### offerOfflineLogonAsLogonOption
**offerOfflineLogonAsLogonOption**=REG_DWORD:0

### enableQuickLogon
**enableQuickLogon**=REG_DWORD:0

### quickLogonButtonCaption
**quickLogonButtonCaption**=REG_SZ:""

### quickLogonUser
**quickLogonUser**=REG_SZ:""

### quickLogonPassword
**quickLogonPassword**=REG_SZ:""

### quickLogonDomain
**quickLogonDomain**=REG_SZ:""

### disableRdpAutoLogon
**disableRdpAutoLogon**=REG_DWORD:0

### setAsDefaultLogonTile
**setAsDefaultLogonTile**=REG_DWORD:1

## [.\SOSProfile *\Script]

**userLogon**
**userLogon**=REG_SZ:""

**userLogoff**
**userLogoff**=REG_SZ:""

**systemLogon**
**systemLogon**=REG_SZ:""

**systemLogoff**
**systemLogoff**=REG_SZ:""

**systemInit**
**systemInit**=REG_SZ:""

**timeout**
**timeout**=REG_DWORD:0x1E

**noScriptByCachedCredLogon**
**noScriptByCachedCredLogon**=REG_DWORD:0

## [.\SOSProfile *\SSO]

**rootPath**
**rootPath**=REG_SZ:"%PROGRAMFILES%\\Comtarsia\\ComtMSSO"

**enableSSO**
**enableSSO**=REG_DWORD:0

**LDAP_PWD_MODE**
**LDAP_PWD_MODE**=REG_DWORD:2

**LDAP_PKI_MODE**
**LDAP_PKI_MODE**=REG_DWORD:2

**OFFLINE_MODE**
**OFFLINE_MODE**=REG_DWORD:2

**LOCAL_LOGON_MODE**
**LOCAL_LOGON_MODE**=REG_DWORD:2

**WIN_ADS_MODE**
**WIN_ADS_MODE**=REG_DWORD:2

# 9.Scripts für SW-Verteilung

## 9.1 Software Installation

Das angeführte Software-Verteil Script führt folgende Operationen durch:
.) Entpacken des SOS2008-setup-bundle-*.exe Installationspacketes
.) Ermitteln der SOS2008 Versionsnummer
.) Entpacken der platformspezifischen Dateien von LC2008-5.1.*.31.exe (32/64bit)
.) Ermitteln der LC2008 Versionsnummer
.) Entpacken der Management Console aus MC2008-5.1.*.21.exe
.) Services werden insofern vorhanden gestoppt
.) Dateien werden ins Zielverzeichnis kopiert
.) Credential Provider wird registriert
.) Registry Datei wird importiert und sichergestellt dass keine eventuell vorher vorhandenen LDAP-Server übrig bleiben
.) SOS2008 und LC2008 Versionsnummern werden in Registry gesetzt
.) "ComtMC.exe applyDefault" wird gestartet (eventuell notwendige migration der Konfiguration wird von der Management Console durchgeführt)
.) UserInit wird bei bedarf auf Comtarsia Userinit geändert und vorhandene Userinit in Comtarsia Config abgelegt
.) Services werden bei bedarf installiert
.) Services werden gestartet

Um das Software Verteil Script zu verwenden müssen folgende Schritte durchgeführt werden:
Das Script muss gemeinsam mit folgenden Dateien in ein lokales Verzeichnis abgelegt werden:

SOS2008-setup-bundle-*.exe
LC2008.reg
key042

**SOS2008-setup-bundle-*.exe**
Das zu installierende Comtarsia Softwarepacket.

**LC2008.reg**
Die zu importierende Konfiguration (exportiert von einem fertig konfiguriertem Referenzsystem: HKEY_LOCAL_MACHINE\Software\Comtarsia )

**key042**
Der Kundenspezifische Lizenz-Schlüssel (Nur falls vorhanden).

Anschliessend muss das Script mit Administrationsrechten ausgeführt werden.

### 9.1.1 install.cmd

```
@echo off
:: ############################################################
:: instructions: place this script into a local directory
:: together with:
::      .)  SOS2008-setup-bundle-*.exe
::      .)  LC2008.reg
::      .)  key042 (Customer license key, if available)
:: LC2008.reg has to contain the TESTED Logon Client settings
:: (exportet HKEY_LOCAL_MACHINE\Software\Comtarsia key)
```

```
:: ############################################################
SETLOCAL
:: ###### Configuration
:: regfile has to point to a registry file which contains the desired
configuration.
set regfile=%CD%\LC2008.reg

:: installation directory
set COMT_INSTALL_PATH=C:\Program Files\Comtarsia\SignOn Solutions 2008


:: ############################################################
:: ############ Don't change code below this line ############

:: set "DBE" to echo, to enable debug echo, otherwise set it to "::"
set DBE=echo
:: xcp is used for xcopy and specifies whether it should ask about overwriting
files or not. set to "xcopy /Y" for overwriting without asking
set xcp=xcopy /Y
:: regparam specifies an additional parameter for the "reg" command. set to  "/f"
to ommit prompts
set regparam=/f
set cnt=0
set SOSInstallerFile=""
set SOSInstallerDir=""
set SOSVersion=""
set LCInstallerFile=""
set LCInstallerDir=""
set LCVersion=""
set MCInstallerFile=""
set MCInstallerDir=""
set MCInstallerVersion=""

set initialDir=%CD%
set SOSInstallerWildcard=SOS2008-setup-bundle-*.exe
set LCInstallerWildcard=LC2008-5.1.*.31.exe
set MCInstallerWildcard=MC2008-5.1.*.21.exe

:: ## check if reg file exists
IF EXIST "%regfile%" GOTO :regFileExists
set ERRORSTR=Registry File "%regfile%" does not exist. This file is required for
the unattended installation and has to contain the desired configuration.
goto :ERROR
:regFileExists

:: ################## extracting SOS Installer
:: ## get SOSInstallerFile
for %%a in ("%SOSInstallerWildcard%") do set SOSInstallerFile=%%a&& set /A
cnt=(cnt+1) && echo %%a

:: ## check if 1 (and only 1) SOS installer file found
IF NOT "%cnt%"=="0" GOTO :cntSOSNotNull
set ERRORSTR=%SOSInstallerWildcard% not found.
goto :ERROR

:cntSOSNotNull
IF "%cnt%"=="1" GOTO :cntSOSFoundOne
set ERRORSTR=more than one file matching %SOSInstallerWildcard% found (%cnt%)
goto :ERROR

:cntSOSFoundOne

:: ## extract the bundle number and set SOSInstallerDir
set BundleNumber=%SOSInstallerFile:~21,-4%
set SOSVersion=5.1.%BundleNumber%.11
```

```
set SOSInstallerDir=SOS2008-%SOSVersion%

:: ## extracting SOSInstaller and changing to SOSInstallerDir
echo found SOSInstaller: "%SOSInstallerFile%"
echo extracting to "%SOSInstallerDir%" ...
%SOSInstallerFile% /unpack
cd %SOSInstallerDir%


:: ################## extracting LC Installer
:: ## get LCInstallerFile
set cnt=0
for %%a in ("%LCInstallerWildcard%") do set LCInstallerFile=%%a&& set /A
cnt=(cnt+1) && echo %%a

:: ## check if 1 (and only 1) LC installer file found
IF NOT "%cnt%"=="0" GOTO :cntLCNotNull
set ERRORSTR=%LCInstallerWildcard% not found.
goto :ERROR

:cntLCNotNull
IF "%cnt%"=="1" GOTO :cntLCFoundOne
set ERRORSTR=more than one file matching %LCInstallerWildcard% found (%cnt%)
goto :ERROR

:cntLCFoundOne

:: ## extract the LCInstallerDir from LCInstallerFile
set LCVersion=%LCInstallerFile:~7,-4%
set LCInstallerDir=%LCInstallerFile:~0,-4%

echo LCInstallerFile: %LCInstallerFile%
echo LCInstallerDir: %LCInstallerDir%

:: ## Unpack command for LCInstaller depends on Processor architecture
set UNPACKCommand=""
IF "%PROCESSOR_ARCHITECTURE%"=="x86" set UNPACKCommand=/unpack
IF "%PROCESSOR_ARCHITECTURE%"=="AMD64" set UNPACKCommand=/unpack64
IF NOT "%UNPACKCommand%"=="" GOTO :archOK
set ERRORSTR=Unknown processor archictecture: %PROCESSOR_ARCHITECTURE% Expected:
x86 or AMD64
goto :ERROR

:archOK
%DBE% using unpack command %UNPACKCommand% for processor architecture
%PROCESSOR_ARCHITECTURE%
:: ## extracting LCInstaller
%LCInstallerFile% %UNPACKCommand%


:: ################## extracting MC Installer (needed for "ComtMC applydefault")
:: ## get MCInstallerFile
set cnt=0
for %%a in ("%MCInstallerWildcard%") do set MCInstallerFile=%%a&& set /A
cnt=(cnt+1) && echo %%a

:: ## check if 1 (and only 1) MC installer file found
IF NOT "%cnt%"=="0" GOTO :cntMCNotNull
set ERRORSTR=%MCInstallerWildcard% not found.
goto :ERROR

:cntMCNotNull
IF "%cnt%"=="1" GOTO :cntMCFoundOne
set ERRORSTR=more than one file matching %MCInstallerWildcard% found (%cnt%)
goto :ERROR
```

```
:cntMCFoundOne

:: ## extract the MCInstallerDir from MCInstallerFile
set MCVersion=%MCInstallerFile:~7,-4%
set MCInstallerDir=%MCInstallerFile:~0,-4%

echo MCInstallerFile: %MCInstallerFile%
echo MCInstallerDir: %MCInstallerDir%

:: ## extracting MCInstaller
%MCInstallerFile% /unpack

:: ########################################################################

:: ## changing to LCInstallerDir
cd %LCInstallerDir%

:: #### actual installer

call :stopServices
call :copyFilesToInstallDir
call :registerCredProv
call :applySettingsAndUserInit
call :installAndStartServices

%DBE% done
:: ################## after extracting LC Installer
:: ################## after extracting SOS Installer
GOTO :END



:: ################## Functions #################
GOTO :END

:: ######################################
:: ######## stop Services so that Files aren't in use:
:stopServices
%DBE% %0
call :stopServiceIfExists ComtEventSrv
call :stopServiceIfExists ComtRPCSrv
goto :eof

:: ######################################
:: ######## stop Services so that Files aren't in use:
:stopServiceIfExists
%DBE% %0 %*
sc query %1 2>&1 >NUL
if "%ERRORLEVEL%"=="1060" GOTO :ServiceDoesntExist
net stop %1
:ServiceDoesntExist
goto :eof

:: ######################################
:: ######## copy all files to bin directory
:copyFileSToInstallDir
%DBE% %0
%xcp% bin "%COMT_INSTALL_PATH%\bin\"
%xcp% cert "%COMT_INSTALL_PATH%\cert\"
%xcp% doc "%COMT_INSTALL_PATH%\doc\"
%xcp% key "%COMT_INSTALL_PATH%\key\"
IF NOT EXIST "%initialDir%\key042" GOTO :LicKeyNotExist
echo copying license Key: "%initialDir%\key042"
%xcp% "%initialDir%\key042" "%COMT_INSTALL_PATH%\key\"
```

```
:LicKeyNotExist
goto :eof

:: ########################################
:: ######### regiser comtarsia credential provider
:registerCredProv
%DBE% %0
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{EE234E82-AC01-4e9f-9174-E19375BED421}" /ve /t REG_SZ /d
"ComtCredentialProvider" %regparam%
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}" /ve  /t REG_SZ /d
"ComtCredentialProvider" %regparam%
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}\InprocServer32" /ve /t
REG_SZ /d "%COMT_INSTALL_PATH%\bin\ComtCredentialProvider.dll" %regparam%
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}\InprocServer32" /v
"ThreadingModel" /t REG_SZ /d "Apartment" %regparam%
goto :eof

:: ########################################
:: ######### apply Settings
:applySettingsAndUserInit
%DBE% %0

:: ## applydefault Regsettings
call :setPathAndVersions
%DBE% applying Defaults
"%initialDir%\%SOSInstallerDir%\%MCInstallerDir%\bin\ComtMC.exe"
"%initialDir%\%SOSInstallerDir%\%MCInstallerDir%\bin\ComtMC.exe" applydefault

:: ## remove entries that have to come from %regfile%
reg delete "HKLM\SOFTWARE\Comtarsia\SOSProfile 001\LDAP\Servers" %regparam%
reg delete "HKLM\SOFTWARE\Comtarsia\SOSProfile 001\Variables" %regparam%

call :installUserInit

REM REG IMPORT "%regfile%" %regparam%
REG IMPORT "%regfile%"
:: ## overwrite install path and versions to maks sure they're correct
call :setPathAndVersions

goto :eof

:: ########################################
:: ########## set install path and installed versions
:setPathAndVersions
%DBE% %0
reg add "HKLM\SOFTWARE\Comtarsia\SignOn Solutions 2008" /v "Path" /t REG_SZ /d
"%COMT_INSTALL_PATH%" %regparam%
reg add "HKLM\SOFTWARE\Comtarsia\SignOn Solutions 2008\Components" /v "Comtarsia
SignOn Solutions 2008" /t REG_SZ /d "%SOSVersion%" %regparam%
reg add "HKLM\SOFTWARE\Comtarsia\SignOn Solutions 2008\Components" /v "Comtarsia
Logon Client 2008" /t REG_SZ /d "%LCVersion%" %regparam%
goto :eof

:: ########################################
:: ########## copies winlogon userinit to comtarsia reg-settings and registers
comtarsia userinit as winlogon userinit
:: ##################### zieht HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile
001\LogonClient userinit VOR HKLM\SOFTWARE\Comtarsia\SignOn Solutions
2008\LogonClient  ??????
:installUserInit
%DBE% %0
:: ## copy winlogon userinit to comtarsia key
set ComtUserInitKey=HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile
001\LogonClient
```

```
set ComtUserInitPath=%COMT_INSTALL_PATH%\bin\comtuserinit.exe

FOR /F "skip=2 tokens=2*" %%i IN ('reg query "%ComtUserInitKey%" /V "userinit"') do
set "COMT_USERINIT=%%j"
:: ## if comtUserInit is already set, assume LC has been installed already
IF "%%SYSTEMROOT%%\system32\userinit.exe,"=="%COMT_USERINIT%" goto
:userinitAlreadySet
set COMT_USERINIT=

FOR /F "skip=2 tokens=2*" %%i IN ('reg query "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" /V "userinit"') do set "COMT_USERINIT=%%j"
:: ## if Winlogon Userinit is already set to "%ComtUserInitPath%", assume LC has
been installed already
IF "%ComtUserInitPath%"=="%COMT_USERINIT%" goto :userinitAlreadySet
set COMT_USERINIT=

:: ## retrieve originial winlogon userinit and set it as "userinit" for LC
FOR /F "skip=2 tokens=2*" %%i IN ('reg query "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" /V "userinit"') do set "COMT_USERINIT=%%j"
reg add "%ComtUserInitKey%" /v "userinit" /t REG_SZ /d %COMT_USERINIT% %regparam%
set COMT_USERINIT=

:: ## register Comtarsia Userinit as winlogon userinit (required for SSO and
Scripts)
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Userinit"
/t REG_SZ /d "%ComtUserInitPath%" %regparam%

GOTO :setUserInit

:userinitAlreadySet
%DBE% userinit was already set
:setUserInit
goto :eof

:: ########################################
:: ########## Install and start services
:installAndStartServices
%DBE% %0
:: ## install ComtRPC Service
sc create ComtRPCSrv binpath= "%COMT_INSTALL_PATH%\bin\ComtRPCSrv.exe" displayname=
"Comtarsia RPC Service"

:: ## install ComtEvent Service
"%COMT_INSTALL_PATH%\bin\ComtEventSrv.exe" -Service

:: ## start services
sc start ComtRPCSrv
sc start ComtEventSrv
goto :eof


:ERROR
echo ERROR: %ERRORSTR%
:END
cd %initialDir%

echo END
ENDLOCAL
pause
```

## 9.2 Anpassen des (De-)Installations-Scriptes

Die Datei install.cmd muss in das Verzeichnis „SOS2008-5.0.x.4" kopiert und angepasst werden.

**Der Installationspfad muss angepasst werden:**

```
set COMT_INSTALL_PATH=C:\Program Files\Comtarsia\SignOn Solutions 2008
```

**Der Installationspfad für das ComtMSSO-Modul muss angepasst werden (optional):**

```
set COMT_INSTALL_PATH_MSSO=C:\Program Files\Comtarsia\ComtMSSO\

REM ######## copy all files to bin directory
xcopy bin "%COMT_INSTALL_PATH%\bin\"
xcopy cert "%COMT_INSTALL_PATH%\cert\"
xcopy doc "%COMT_INSTALL_PATH%\doc\"
xcopy key "%COMT_INSTALL_PATH%\key\"
mkdir "%COMT_INSTALL_PATH%\log"

REM ######### register comtarsia credential provider

reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{EE234E82-AC01-4e9f-9174-E19375BED421}" /ve /t REG_SZ /d
"ComtCredentialProvider" /f
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}" /ve  /t REG_SZ
/d "ComtCredentialProvider" /f
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}\InprocServer32"
/ve /t REG_SZ /d "%COMT_INSTALL_PATH%\bin\ComtCredentialProvider.dll" /f
reg add "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}\InprocServer32"
/v "ThreadingModel" /t REG_SZ /d "Apartment" /f
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Provider Filters\{EE234E82-AC01-4e9f-9174-E19375BED421}" /ve /t REG_SZ /d
"ComtCredentialProvider" /f

REM ######### create SOSProfile key
reg add "HKLM\SOFTWARE\Comtarsia\SOSProfile 001" /v "Path" /t REG_SZ /d
"%COMT_INSTALL_PATH%" /f


REM ######### applydefault Regsettings
bin\ComtMC applydefault

REM ##########  copy winlogon userinit to comtarsia key
FOR /F "skip=2 tokens=2*" %%i IN ('reg query
"HKLM\SOFTWARE\Comtarsia\SOSProfile 001\LogonClient" /V "userinit"') do set
"COMT_USERINIT=%%j"
if NOT "%%SYSTEMROOT%%\system32\userinit.exe"=="%COMT_USERINIT%" goto
install_services
set COMT_USERINIT=
FOR /F "skip=2 tokens=2*" %%i IN ('reg query
"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /V "userinit"')
do set "COMT_USERINIT=%%j"
if "%COMT_INSTALL_PATH%\bin\comtuserinit.exe"=="%COMT_USERINIT%" goto
install_services
FOR /F "skip=2 tokens=2*" %%i IN ('reg query
"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /V "userinit"')
do set "COMT_USERINIT=%%j"
```

```
reg add "HKLM\SOFTWARE\COMTARSIA\SOSProfile 001\LogonClient" /v "Userinit"
/t REG_SZ /d %COMT_USERINIT% /f
set COMT_USERINIT=

reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
"Userinit" /t REG_SZ /d "%COMT_INSTALL_PATH%\bin\comtuserinit.exe" /f


:install_services
reg import my-SOSProfile001.reg


REM ######### install ComtRPC Service
sc create ComtRPCSrv binpath= "%COMT_INSTALL_PATH%\bin\ComtRPCSrv.exe"
displayname= "Comtarsia RPC Service"

REM ######### install ComtEvent Service
"%COMT_INSTALL_PATH%\bin\ComtEventSrv.exe" -Service

REM ######### start ComtRPC Service
sc start ComtRPCSrv

REM ######### start ComtRPC Service
sc start ComtEventSrv
```

**Installation des ComtMSSO Modules (optional)**

```
REM ######## ComtMSSO
vs_piaredist.exe /q
xcopy ComtMSSO "%COMT_INSTALL_PATH_MSSO%" /s /e /y
```

**Das perönliche PanelBitmap muss angegeben werden:**

```
REM ######## PanelBitmap
xcopy myPanelBitmap.bmp "%COMT_INSTALL_PATH%\bin\"
```

Die Datei uninstall.cmd muss in das Verzeichnis „SOS2008-5.0.x.4" kopiert und angepasst werden.

**Der Installationspfad muss angepasst werden:**

```
set COMT_INSTALL_PATH=C:\Program Files\Comtarsia\SignOn Solutions 2008
set COMT_INSTALL_PATH2=C:\Program Files\Comtarsia

REM ##########  copy winlogon userinit to comtarsia key
FOR /F "skip=2 tokens=2*" %%i IN ('reg query
"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /V "userinit"')
do set "COMT_USERINIT=%%j"
if NOT "%COMT_INSTALL_PATH%\bin\comtuserinit.exe"=="%COMT_USERINIT%" goto
uninstall_services

FOR /F "skip=2 tokens=2*" %%i IN ('reg query
"HKLM\SOFTWARE\Comtarsia\SOSProfile 001\LogonClient" /V "userinit"') do set
"COMT_USERINIT=%%j"
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
"Userinit" /t REG_SZ /d "%COMT_USERINIT%" /f
set COMT_USERINIT=

:uninstall_services

REM ######### start ComtRPC Service
sc stop ComtRPCSrv

REM ######### start ComtRPC Service
sc stop ComtEventSrv


REM ######### install ComtRPC Service
```

```
sc delete ComtRPCSrv

REM ######### install ComtEvent Service
sc delete ComtEventSrv

REM ######## Unregister Comtarsia Credential Provider
reg delete "HKLM\SOFTWARE\Comtarsia"
reg delete "HKCR\CLSID\{EE234E82-AC01-4e9f-9174-E19375BED421}"
reg delete
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{EE234E82-AC01-4e9f-9174-E19375BED421}"

REM ######## Register Microsoft Credential Provider
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}" /ve /t REG_SZ /d
"PasswordProvider" /f
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}\LogonPasswordReset" /ve  /t
REG_SZ /d "{8841d728-1a76-4682-bb6f-a9ea53b4b3ba}" /f

rmdir /S /Q "%COMT_INSTALL_PATH2%"
```



# 10. Disclaimer

Alle Seiten unterliegen dem Urheberschutz und dürfen nur mit schriftlicher Genehmigung von Comtarsia IT Services GmbH kopiert oder in eigene Angebote integriert werden.

Alle Rechte vorbehalten.

Irrtümer und Änderungen vorbehalten!

Die Comtarsia IT Services gibt keinerlei Zusicherungen oder Gewährleistungen für andere Websites, auf welche in diesen Handbuch verwiesen wird. Wenn Sie auf eine Nicht-Comtarsia IT Services Website zugreifen, ist das eine unabhängige Site, über deren Inhalt wir keine Kontrolle haben.
Dies gilt auch dann, wenn diese Site möglicherweise das Comtarsia IT Services Logo enthält.

Darüber hinaus bedeutet ein Link aus unserer Site heraus auf eine andere nicht, daß wir uns mit deren Inhalt identifizieren oder deren Nutzung unterstützen.