Comtarsia Logon Client 2006

Technische Beschreibung

Version: 4.1.13.4, 04-Jul-2006

Inhaltsverzeichnis

1. Beschreibung

Comtarsia Logon Client 2006, LDAP Logon Client Modul für Windows 2000 and Windows XP, Build 4.1.13.4
(Deutsch und Englisch)

Der Comtarsia Logon Client 2006 für Windows ermöglicht es für Windows 2000 und Windows XP Workstations, sowie an Terminal Service/Citrix Sitzungen eine primäre Authentifizierung an ein LDAP Directory.

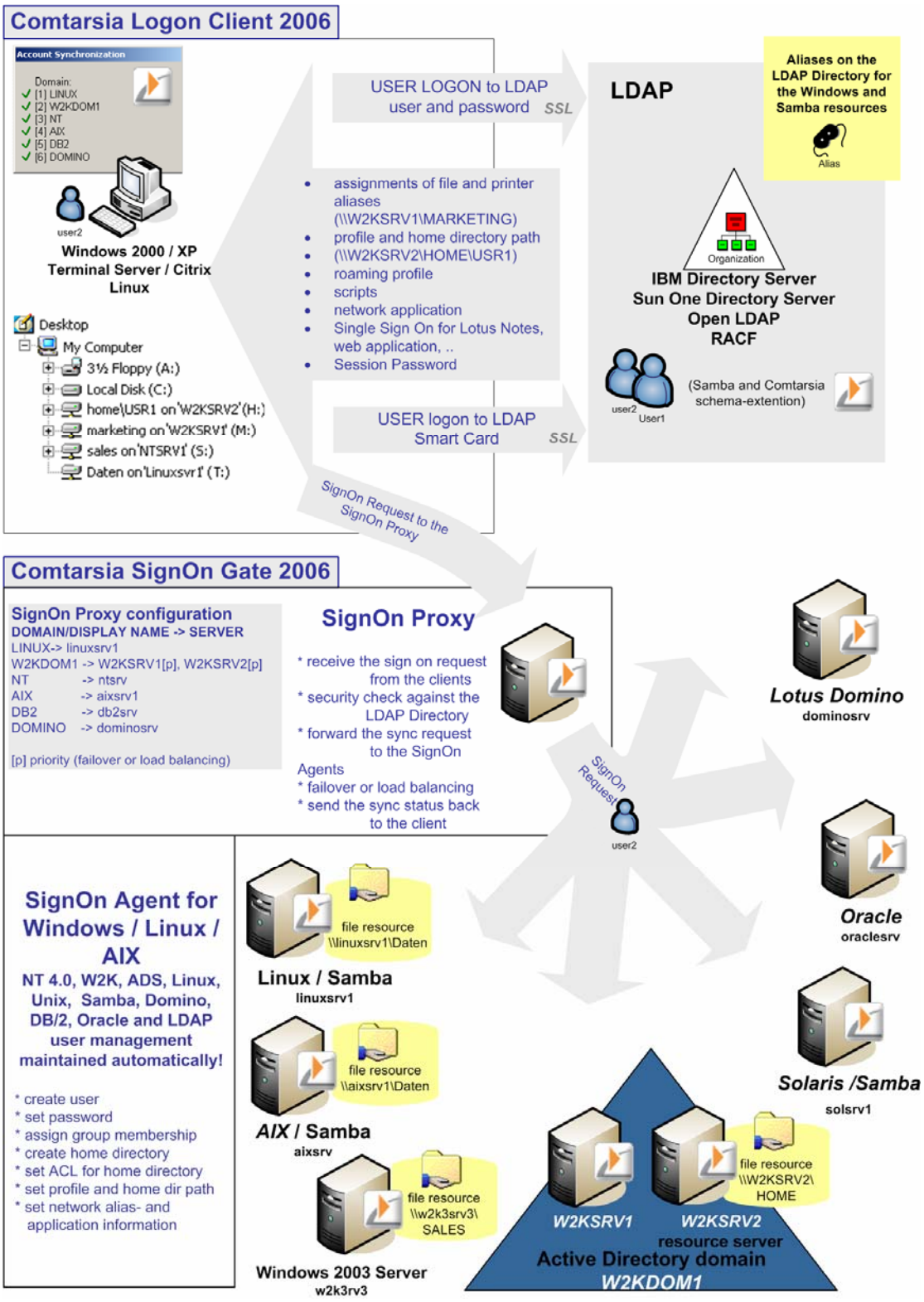
Mit dem Zusatzprodukt „Comtarsia Sign On Gate 2006“ besteht die Möglichkeit, Benutzerkonten auf Windows Servern, Windows Domänen (NT 4.0, W2K, W2K3/ ADS) und UNIX Servern automatisch verwalten zu lassen und als Ressourcen in der zentralen LDAP Benutzerverwaltung zu integrieren.

Die Produkte Comtarsia Logon Client und Comtarsia Sign On Gate sind optimale LDAP Integrationswerkzeuge und ermöglichen die Benutzerverwaltung von der Ressourcenverwaltung losgelöst zu betreiben. Dies bedeutet eine sehr entscheidende Unabhängigkeit gegenüber hersteller-propräterer Lösungen. Somit steht Comtarsia auch für Single Sign On, Centralized User Management und Security Management.

Weitere Informationen über die Comtarsia SignOn Solutions entnehmen Sie bitte unseren Web Sites.

http://signon.comtarsia.com

1.1 Comtarsia Sign On Produkt Übersicht



1.2 Voraussetzungen am Server:

LDAP:
Siehe Handbuch Comtarsia Logon Client 2006 und LDAP
http://signon.comtarsia.com/main/de/Manuals

1.3 Voraussetzungen am Client:

W2K Professional oder Windows XP Professional, Windows Terminal Server 2003 (Deutsch oder Englisch)
.

1.4 Installation:

1.4.1 Installation mittels Installer:

Die Datei **CLC_2006-4.1.X.4.exe** ausführen und die Anweisungen befolgen.
Die Einstellungen sämtlicher Parameter können nach der Installation über den Konfigurator durchgeführt werden.
(Siehe Handbuch Comtarsia Logon Client LDAP, Kapitel 2)

Das Handbuch orientiert sich auf die Registry Parameter, und ist für die Installation in großen Netzwerken via SW-Verteilung vorgesehen.

1.4.2 Installation mittels Software-Verteilung:

Den Logon Client Installer mit den Parameter “MODE=UNPACK” aufrufen.
Dies erzeugt ein Verzeichnis mit dem Namen „CLC_2006-VERSION“, in welchem sich nun alle für eine Softwareverteilungsinstallation benötigten Dateien befinden.

Die Installation besteht aus zwei Schritten, das Kopieren der Dateien und das Setzen der Registry-Keys.

Folgende Dateien werden im Verzeichnis „%SYSTEMROOT%“ auf dem Zielsystem benötigt:

- ComtSyncClient.exe
- comt_ldap.exe
- ComtSSOExec.exe

Folgende Dateien werden im Verzeichnis „%SYSTEMROOT%\SYSTEM32“ auf dem Zielsystem benötigt:

- comt_rsa.dll
- comt_sso.dll
- pcs_gina.dll
- key041

Die Datei CLCConfigurator.exe, sowie die Logon Client Handbücher werden auf dem Zielsystem nicht benötigt.

Die Dateien für die SSL Kommunikation (Zertifikat, Private Key, ein oder mehrere CA-Zertifikate) mit dem SignOn Proxy können in einen beliebigen Ordner kopiert werden, die Pfade müssen in der Registry (“HKEY_LOCAL_MACHINE \Software\PCS\GINA\ComtSyncClient” [tlsCAFile/tlsCertFile/tlsKeyFile]) entsprechend gesetzt werden. Der Default-Pfad ist „%PROGRAMFILES%\Comtarsia\Logon Client 2006“.

Zum Erzeugen einer Registry-Konfiguration wird empfohlen, den Logon Client Konfigurator zu verwenden und anschließend den Registry-Zweig unter “HKEY_LOCAL_MACHINE \Software\PCS\GINA” zu exportieren und diesen auf den Arbeitsstationen zu importieren.

Zusätzlich muss der Registry-Key “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL” auf “pcs_gina.dll” gesetzt werden.

1.5 Deinstallation:

Das Entfernen des Logon Clients ist über die Systemsteuerung / Software Entfernen möglich.

SW-Verteilung:

Die Datei ***uninstall.cmd*** ausführen.
Für die Deinstallation sind lokale Administrator-Rechte notwendig!

1.6 Parameter Beschreibung – Allgemeine Einstellungen:

**KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA **

1.6.1 EnableSyncClient

„EnableSyncClient“=DWORD:1
Mit diesem Schalter wird der Comtarsia SignOn Gate Unterstützung aktiviert.
(siehe SignOn Gate Unterstützung)
Default: 0

1.6.2 PolicyPath

Definiert den vollen Pfad des Policy-Files.
z.B.: "PolicyPath"="%LOGONSERVER%\\netlogon\\ntconfig.pol"
(siehe Windows Policy)

1.6.3 DefaultUserProfile

Damit wird der Pfad für das Default Profile festgelegt. Kann das angegebene Verzeichnis nicht gefunden werden, wird das lokale Default Profile verwendet.
z.B.:"DefaultUserProfile"="%LOGONSERVER%\\netlogon\\default profile"

1.6.4 ProfilePath

Damit wird der Pfad für das Profile festgelegt.
z.B.:"ProfilePath"=\\SERVER1\profiles\%USERNAME%
Siehe auch Punkt RoamingUserGroup

1.6.5 HomeDirDrive

"HomeDirDrive"="H:"
Sollte in der LAN Server Domäne kein Laufwerksbuchstabe definiert sein, wird dieser Laufwerksbuchstabe verwendet.

Achtung: Der Parameter "HomeDirPath" muß definiert sein!
(siehe Bild 8)

1.6.6 HomeDirPath

Sollte in der LS Domäne kein Home Directory definiert sein, wird versucht, diesen Netzwerkpfad als Home Directory zu verbinden.
z.B.: "HomeDirPath"="%LOGONSERVER%\\%USERNAME%"

Achtung: Der Parameter "HomeDirDrive" muß definiert sein!
(siehe Bild 8)

1.6.7 InitScript

Dieses Script wird beim Initialisieren von Windows mit System-Privilegs ausgeführt
Z.B.:“InitScript"="c:\cmd\init.cmd"

1.6.8 PreSystemLogonScript

Dieses Script wird beim Logon mit System-Privilegs ausgeführt.
Der lokale Benutzer Logon wurde noch nicht durchgeführt.
z.B.: "PreSystemLogonScript"="c:\cmd\cleanup.cmd"

1.6.9 SystemLogonScript

Dieses Script wird beim Logon mit System-Privilegs ausgeführt.
z.B.:"SystemLogonScript” = “c:\cmd\system.cmd"

1.6.10 SysUsrLogonScript

Dieses Script wird beim Logon im User Environment mit System-Privilegs ausgeführt.
z.B.:"SysUsrLogonScript“=“c:\system.cmd"

1.6.11 UserLogonScript

Dieses Script wird beim Logon im User Environment mit User-Privilegs ausgeführt.
z.B.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.12 LocalUserLogonScript

Dieses Script wird bei einem Lokalen Logon im User Environment mit User-Privilegs ausgeführt.
z.B.:"LocalUserLogonScript"="c:\scripts\localLogon.cmd"

1.6.13 AdminUsrLogonScript

Dieses Script wird beim Logon im User Environment mit Admin-Privilegs ausgeführt.
z.B.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"
(Achtung! Dieses Script wird nur bei einer Domänen bzw. LDAP Anmeldung ausgeführt!)

1.6.14 LocalAdminUsrLogonScript

Dieses Script wird bei einer lokalen Anmeldung im User Environment mit Admin-Privilegs ausgeführt.
z.B.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.15 UserLogoffScript

Dieses Script wird beim Logoff im User Environment mit User-Privilegs ausgeführt.
z.B.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.16 UserLogoffScriptErrorlevel

"UserLogoffScriptErrorlevel"=DWORD:0
Ist dieser Wert „1“, wird der Errorlevel des UserLogoffScripts abgefragt, und bei ungleich „0“ wird der Logoff abgebrochen.

1.6.17 SystemLogoffScript

Dieses Script wird beim Logoff (das User Environment ist nicht mehr vorhanden) mit System-Privilegs ausgeführt.
z.B.: "systemLogoffScript"="c:\cmd\cleanup.cmd"

1.6.18 Script Übersicht:

	Init Script	Pre System Logon Script	System Logon Script	Admin Usr Logon Script	Local Admin User Logon Script	SysUsr Logon Script	User Logon Script	Local User Logon Script	User Logoff Script	System Logoff Script
Ausführung bei										
Lokaler Logon	●	●	●		●	●		●	●	●
LDAP Logon	●	●	●	●		●	●		●	●
WTS / CITRIX Logon	●	●	●			●	●		●	●
WTS / Citrix Passthrough Logon	●	●	●			●	●		●	●
Citrix Anonymous Logon	●	●	●			●	●		●	●
Zeitpunkt der Ausführung (vor ➔● nach ●➔)										
SystemBoot	●➔									
WTS/Citrix Sitzungsaufbau	●➔									
Der Logon Dialog erscheint	➔●									
Erfolgreiche lokale Benutzer Passwort Verfikation (Local Logon)	➔●	●➔								
Erfolgreiche LDAP Benutzer Passwort Verfikation		●➔								
Vorbereitung der Benutzerumgebung		➔●								
Laden der Benutzerumgebung			●➔	●➔	●➔	●➔				
Laden des Benutzerprofiles			●➔	●➔	●➔	●➔				
Zuordnung der Netzwerk Aliases			➔●	●➔		●➔	●➔			
Zuordnung der Netzwerk Applikationen			➔●	●➔		●➔	●➔	●➔		
Freigeben des Benutzer Desktops				➔●	➔●	➔●	➔●	➔●		
Abmelde- oder Herunterfahr-Vorgang wird vom Benutzer gestartet									●➔	●➔
Schließen des Benutzer Desktops									➔●	●➔
Beenden der WTS/Citrix Sitzung									➔●	➔●
Zulassungen										
Lokale Systemrechte	●	●	●			●				
Lokale Benutzerrechte							●	●		
Lokale Administratorrechte				●	●					
Systemumgebung	●	●	●			●			●	●
Benutzerumgebung				●	●		●	●		
Netzwerkzugriff				●	●		●	●		
Zugriff auf HKEY_CURRENT_USER				R/W	R/W		R/W	R/W	R/W	
Zugriff auf HKEY_LOCAL_MASCHINE	R/W	R/W	R/W	R/W	R/W	R/W	R/W*	R/W	R/W*	R/W
Zugriff auf SYSTEMROOT	R/W	R/W	R/W	R/W	R/W	R**	R**	R**	R**	R/W

* abhängig von den aktuellen Benutzerrichtlinien
** abhängig von den aktuellen Benutzerdateizugriffsrechte

1.6.19 ScriptTimeout

"ScriptTimeout"=19
Dieser Wert definiert die Sekunden, die auf die Scripts gewartet wird.

1.6.20 DisplayScriptError

„DisplayScriptError“=DWORD:1
Ist dieser Parameter definiert, wird ein Pop-Up ausgegeben, wenn ein Script nicht innerhalb der definierten Zeit antwortet. Siehe auch Parameter ScriptTimeout und Scriptübersicht.

1.6.21 DisablePasswordChange

"DisablePasswordChange"=1
„0“ = Paßwort ändern ist erlaubt (Das LAN Server Paßwort und das lokale Paßwort werden geändert)
„1“ = Paßwort ändern ist nicht erlaubt, der User bekommt eine POP-UP Message, welche im Value "ChangePasswordInfo" definiert ist.
z.B:
„ChangePasswordInfo“ = Paßwort ändern ist unter Windows nicht erlaubt, nur über Web-Interface!“

1.6.22 ForceUnlockTime

"ForceUnlockTime"= 258
Damit wird die Zeit in Sekunden definiert, in welcher ein “Abmelden erzwingen” im gesperrten Zustand möglich ist.
Ist dieser Wert „0“, ist diese Funktion deaktiviert.
(siehe Bild 3 und Bild 4)

1.6.23 DisplayWError

"DisplayWError"=1
Ist dieser Wert „1“, werden interne Fehler über ein POP-UP ausgegeben, ist dieser Wert „0“, werden die Fehler nur in das File %systemroot%\gina.log geschrieben.
Diese Funktion kann auch im Logon Dialog mit gleichzeitigem Drücken der Taste „L-SHIFT“ und Klicken mit der linken Maustaste in den Dialog ein- oder ausgeschaltet werden.

1.6.24 DisplayProgressBox

"DisplayProgressBox"=DWORD:1
Damit kann die ProgressBox ein- bzw. ausgeschaltet werden.

1.6.25 RoamingUserGroup

"RoamingUserGroup"="USERS"
Über eine Gruppenmitgliedschaft am LAN Server kann gesteuert werden, ob der User ein Roaming Profile verwendet oder nicht.
Mit diesem Wert kann die jeweilige Gruppe definiert werden.
Z.B. am LAN Server wird eine Gruppe mit dem Namen ROAMINGP definiert, und nur die User, die ein Roaming Profile im Home Directory bekommen sollen, werden Mitglied dieser Gruppe. "RoamingUserGroup"="ROAMING"
Ist dieser Wert auf die Gruppe “USERS” gesetzt, werden alle User, die als User am LAN Server definiert sind, als RoamingUser behandelt.
(siehe Bild 5.)

1.6.26 AdminLogonGroup

"AdminLogonGroup"="ADMIN"
default=""
Über eine Gruppenmitgliedschaft am LDAP Directory kann gesteuert werden, welcher Benutzer für den Admin Logon berechtigt ist.
Z.B. am LDAP Directory wird eine Gruppe mit dem Namen ADMIN definiert, und nur die User, die den Administrator Logon ausführen dürfen, werden Mitglied dieser Gruppe.
Siehe AdminLogon.
Ist dieser Parameter nicht definiert, ist die Funktion AdminLogon deaktiviert.

1.6.27 Language

"Language"="german"
Damit wird die Dialog-Message definiert.
Es kann zwischen „english“ und „german“ gewählt werden.

1.6.28 PanelBitmap

“PanelBitmap” = “c:\logo.bmp”
Dieser Parameter definiert das Bitmap, welches anstelle des Comtarsia Logos im Logon Panel angezeigt wird. Siehe Bild 1.
Format: Bitmap 450x120 RGB

1.6.29 AlphaNumPwd

"AlphaNumPwd"=DWORD:1
Ist dieser Parameter definiert, akzeptiert der Logon Client im Passwort nur alphanumerische Zeichen.
(a-z u. 0-9)

1.6.30 DontDisplayLastUserName

„DontDisplayLastUserName“=DWORD:1
Mit diesem Parameter kann die Anzeige des letzten Benutzernamens im Logon Dialog abgeschaltet werden.

1.6.31 DisableMsGina

„DisableMsGina“=DWORD:1
Mit diesem Parameter kann die Möglichkeit, auf den Microsoft Logon Dialog umzuschalten, abgeschaltet werden. Siehe Microsoft GINA.

1.6.32 DisableEqualGroupMapping

„DisableEqualGroupMapping“=DWORD:1
Mit diesem Parameter wird die Gruppenzuordnung nach gleichen Namen abgeschaltet und die manuelle Gruppenzuordnung eingeschaltet. Siehe Funktion GroupMapping.

1.6.33 GroupAdministrator

"GroupAdministrator"="ADMIN"
Dieser Parameter definiert die LDAP Gruppe, in welcher der Benutzer Mitglied sein muß, damit er das lokale Administrator Privileg bekommt. Der Parameter DisableEqualGroupMapping“=dwor:1 muß ebenfalls definiert sein.

1.6.34 GroupPowerUser

"GroupPowerUser"="PUSER"
Dieser Parameter definiert die LDAP Gruppe, in welcher der Benutzer Mitglied sein muß, damit er das lokale Hauptbenutzer Privileg bekommt. Der Parameter DisableEqualGroupMapping“=DWORD:1 muß ebenfalls definiert sein.

1.6.35 NWAFolderActive

„NWAFolderActive“=DWORD:1
Dieser Schalter aktiviert die Unterstützung für LDAP Netzwerkapplikationen.
Siehe Kapitel Netzwerkapplikationen

1.6.36 NWAFolderNamePath

„NWAFolderNamePath“=“%USERPROFILE%\Desktop“,“%ALLUSERSPROFILE%\Desktop“
Definiert die Verzeichnisse, in denen ein Folder mit dem unter „NWAFolderName“ definierten Namen erzeugt wird.
Wird dieser Parameter nicht angegeben, wird standardmäßig der User-Desktop verwendet.

1.6.37 NWAFolderName

„NWAFolderName“=“LDAP-Anwendungen“
In diesem Folder werden die Shortcuts für die Netzwerkapplikationen erzeugt.
Wird dieser Parameter nicht angegeben, werden die Shortcuts direkt in den unter NWAFolderNamePath angegebenen Folder erstellt.

1.6.38 NWAAppFilter

„NWAAppFilter“=“*W2K*“
Definiert einen Applikationsfilter; nur Applikationen mit passender Applikations-ID werden erstellt.
Filter passende IDs
„XP“ XP
„XP*“ XP, XPAA, XPBBB
„*XP“ XP, AAXP, BBBXP
„*XP*“XP, XPAA, AAXP, XPBBB, BBBXP

1.6.39 NWADefaultIconPath

„NWADefaultIconPath“=“\\SERVER1\daten\icons“
Optional ein UNC-Pfad, in dem alternativ nach dem Programmicon gesucht wird, wenn dieses in der Programmposition nicht gefunden wird.

1.6.40 NWADefaultIcon

„NWADefaultIcon“= “default.ico“
Optional ein Dateiname einer Icon-Datei, die für Shortcuts verwendet wird, die kein eigenes Icon besitzen.
Es wird nur im Programmverzeichnis der jeweiligen Netzwerkapplikation nach dieser Icon-Datei gesucht.

1.6.41 NWAIconPath

„NWAIconPath“=“c:\temp“
Definiert ein lokales Verzeichnis, in dem temporäre Icon-Dateien gespeichert werden.
Default: c:\

1.6.42 NWATimeout

„NWATimeout“=DWORD:60
Definiert ein Timeout für die Abfrage und Erstellung der Netzwerkapplikationen in Sekunden.
Default: 60

1.6.43 MinPwdLen

„MinPwdLen“=DWORD:8
Definiert die minimale Anzahl an Zeichen, welche beim LDAP-Passwortwechsel für das neue Passwort gegeben sein muss.
Default:0

1.6.44 EnableDomainLogon

„EnableDomainLogon“=DWORD:1

default = 0

Mit diesem Schalter kann definiert werden, ob der Logon Client für die Windows Benutzer-Sitzung einen lokalen Benutzer, oder einen Windows Domänenbenutzer verwendet. Ist der Wert auf „1“ gestellt, versucht der Logon Client nach jeder erfolgreichen LDAP Anmeldung einen Windows Logon mit der im Parameter „strLocalDomain“ definierten Domäne durchzuführen. Damit anstelle eines lokalen Benutzers ein Domänenbenutzer verwendet werden kann, muss die Workstation bereits Mitglied dieser Domäne sein und der Benutzer mit dem selben Passwort muss in der Windows Domäne existieren. Dieser Modus ist daher nur im gemeinsamen Betrieb mit dem Produkt, Comtarsia SignOnGate, mit welchen die automatische Benutzerverwaltung in der Windows Domäne automatisiert werden kann.
Ist dieser Parameter auf „0“ gestellt, verwendet der Logon Client lokale Benutzer.

1.6.45 strLocalDomain

„strLocalDomain“=“W2KDOM“
default = “ “
Dieser Parameter definiert die lokale Domäne für die Windows Logon Sitzung im DomainLogon- bzw im Terminal Server Modus.

1.6.46 WTSMode

„WTSMode“=DWORD:1
default= DWORD:0
Wird der Logon Client auf einem Terminal Server installiert, muss dieser Wert auf „1“ gestellt werden.
Im Terminal Server Modus muss das Zusatzprodukt „Comtarsia SignOn Gate“ für die automatische Benutzerverwaltung am WTS Standalone Server oder am Domain Controller für die automatische Benutzerverwaltung installiert sein!
Der Domänenname muss im Parameter „strLocalDomain“ definiert sein.

1.6.47 ExpireTime

„ExpireTime“=DWORD:3600
Über diesen Parameter kann in Sekunden angegeben werden, wann der lokale, durch den Logon Client erstellte Benutzer durch das Betriebsystem abläuft und für die lokale Anmeldung nicht zur Verfügung steht. Bei jeder erfolgreichen LDAP Anmeldung über Logon Client wird die Ablaufzeit aktualisiert. Bei ExpireTime = 0 ist diese Funktion deaktiviert, alle Benutzer werden ohne Ablaufzeit erstellt.

1.6.48 RemoveUser

„RemoveUser“= DWORD:2

Über diesen Parameter kann angeben werden, dass ein durch den Logon Client lokal erstellter Benutzer nach dem Abmelden entfernt wird. Mit RemoveUser = 1 wird nur der Benutzer gelöscht, mit RemoveUser = 2 wird auch das lokal zwischengespeicherte Profil gelöscht. Mit RemoveUser = 0 wird diese Funktion deaktiviert.
Benutzer wie Administratoren, oder Benutzer, welche nicht durch den Logon Client erstellt wurden, werden nicht entfernt.

1.6.49 AutoLogonUserName

„AutoLogonUserName“=“U00101“
Über diesen Parameter kann ein Benutzername definiert werden, mit welchen der LogonClient eine automatische Anmeldung durchführt. Ist dieser Parameter nicht definiert oder blank ist die Funktion „Autologon“ nicht aktiviert.

1.6.50 AutoLogonPassword

„AutoLogonPassword“=“mypassword“ oder
„AutoLogonPassword“=“ {CLCALP}AVt9WrpakRg57q2RlUNB5Fh3ZcfDtwypXvcH5fZCcOOrJoq1“

Wenn über den Parameter „AutoLogonUserName“ die Funktion „Autologon“ aktiviert wurde, kann über diesen Parameter das Autologon Passwort definiert werden.
Das Passwort kann in Klartext oder über das Tool „SetAutPwd.exe“ (syntax: SetautoPwd mypassword) verschlüsselt abgelegt warden.

1.6.51 AutoLogonDomain

„AutoLogonDomain“=“DOM01“
Wenn über den Parameter „AutoLogonUserName“ die Funktion „Autologon“ aktiviert wurde kann über diesen Parameter die Autologon Domäne angegeben werden.
Für eine LDAP Anmeldung muss der String „LDAP LOGON“ und für eine lokale Anmeldung der String „LOCAL WORKSTATION“ definiert werden.

1.6.52 UserNameCasePolicy

„UserNameCasePolicy“=DWORD:1
Dieser Parameter definiert die mögliche Groß- und Kleinschreibung bei der Eingabe des Benutzernamens im Logon Dialog.

0 = Groß- und Kleinschreibung erlaubt
1 = Nur Großbuchstaben erlaubt
2 = Nur Kleinbuchstaben erlaubt

Achtung!

Die Einstellung „Groß- und Kleinschreibung erlaubt“ 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.

1.7 LDAP – Logon Client Einstellungen

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP

1.7.1 LDAPVersion

„LDAPVersion“ = DWORD:3
Version des LDAP-Protokolls, welche verwendet werden soll.
Der Logon Client unterstützt LDAP Version 2 (siehe http://www.ietf.org/rfc/rfc1777.txt) sowie LDAP Version 3 (siehe http://www.ietf.org/rfc/rfc2251.txt).
Alle derzeit am Markt erhältlichen Server unterstützen bereits LDAP Version 3, welches auch die automatische Erkennung der LDAPBaseDN ermöglicht (siehe LDAPBaseDN).

1.7.2 LDAPBaseDN

“LDAPBaseDN” = ""
Die LDAP Base DN z.B.: „dc=comtarsia,dc=com“

Ermittlung der LDAPBaseDN durch den Logon Client:
Wenn in der Registry ein Wert unter LDAPBaseDB eingetragen ist, wird dieser verwendet.
Wenn der LDAP Server LDAP Version 3 unterstützt und die LDAP Version in der Registry auf „3“ gesetzt ist, wird der Logon Client versuchen, die BaseDN über eine LDAP-Query zu ermitteln.
Achtung: Die meisten LDAP Server unterstützen mehr als eine BaseDN. Es muss unbedingt sichergestellt sein, dass die für den Client gewünschte BaseDN als erster Eintrag geliefert wird. Überprüfen läßt sich das z.B. mit einem LDAP-Browser
(http://www-unix.mcs.anl.gov/~gawor/ldap/)
Falls bis jetzt noch immer keine BaseDN ermittelt werden konnte, wird versucht, die BaseDN aus dem Domain-Namen des lokalen Rechners zu ermitteln.
z.B.: Domain = „comtarsia.com“
BaseDN = „dc = comtarsia, dc= com“

1.7.3 LDAPUserDNPrefix

“LDAPUserDNPrefix “= "uid="
Die UserDN wird aus mehreren Teilen zusammengebaut:
LDAPUserDNPrefix + USERNAME + LDAPUserDNSuffix + „,“ + LDAPBaseDN

LDAPBaseDN wird nur an die UserDN angehängt, wenn LDAPAppendBaseDN aktiviert ist.

Für die User-DN “cn=User1,ou=People,dc=comtarsia,dc=com” müssen folgende Einträge vorgenommen werden:
LDAPUserDNPrefix=’’cn=“
LDAPUserDNSuffix=“,ou=People“
LDAPBaseDN=’dc=comtarsia,dc=com“

1.7.4 LDAPUserDNSuffix

“LDAPUserDNSuffix” = ""
siehe LDAPUserDNPrefix

1.7.5 LDAPAppendBaseDN

“LDAPAppendBaseDN” = DWORD:1
Ist diese Einstellung aktiviert (1), wird die LDAPBaseDN an die User-DN angehängt.
Default: 1

1.7.6 LDAPEnableSSL

“LDAPEnableSSL” = DWORD:1

0 = kein SSL
Die gesamte Kommunikation des Clients mit dem LDAP Server findet unverschlüsselt statt. Diese Option eignet sich nur für den Testbetrieb und sollte keinesfalls in Produktionsumgebungen eingesetzt werden.

1 = SSL ohne "trusted server certificates"
Die Kommunikation mit dem LDAP Server wird verschlüsselt. Das Zertifikat des Servers wird nicht überprüft und auch der Client benötigt kein Zertifikat.

2 = SSL mit "trusted server certificates"
Der Logon Client überprüft das Zertifikat des LDAP Servers. Für diese Option muss ein „CA“-Zertifikat eingespielt werden (siehe LDAP-SSL). Der Client benötigt kein eigenes Zertifikat.

3 = SSL mit "trusted client certificates"
Der Logon Client überprüft das Zertifikat des LDAP Servers und sendet auch sein Zertifikat an den Server. Diese Option benötigt sowohl ein „CA“- als auch ein „Client“-Zertifikat. (siehe LDAP-SSL)

1.7.7 LDAPTimeout

“LDAPTimeout” = DWORD:30
Timeout in Sekunden pro LDAP-Server. Wenn die Funktion Failover (siehe LDAPEnableFailover) aktiviert ist und mehr als ein LDAP Server eingetragen sind, wird bei einem erfolglosen Verbindungsversuch zu einem Server nach dieser Zeitspanne automatisch zum nächsten übergegangen (siehe LDAPEnableFailover und LDAP LoadBalancing und Failover)

1.7.8 LDAPServerTyp

“LDAPServerTyp” = DWORD:1
Diese Einstellung legt den Typ des LDAP Servers fest.
Derzeit wird nur der IBM RACF (4) gesondert behandelt.

1 = iPlanet, 2 = Netscape, 3 = OpenLDAP, 4 = IBM RACF Directory Server,
5 = Domino, 6 = Novell eDirectory

1.7.9 LDAPEnableFailover

“LDAPEnableFailover” = DWORD:0
Aktiviert (1) die Failover und Load Balancing Funktionen im Logon Client. (siehe LDAP LoadBalancing und Failover und LDAPEnableDNS)

1.7.10 LDAPEnableDNS

“LDAPEnableDNS” = DWORD:0
Ist diese Option aktiviert, werden die LDAP Server nicht aus der Registry gelesen, sondern es wird ein DNS Server befragt.
Die Domäne des Clients muss richtig konfiguriert sein, entweder als „Primary DNS Suffix“ oder „Connection-specific DNS Suffix“.
Im Zone-File der Domäne müssen SRV-Records für die LDAP-Server angelegt werden (siehe LDAP LoadBalancing, und Failover sowie LDAPEnableFailover).

1.7.11 LDAPGroupTypes

“LDAPGroupTypes” = DWORD:3
Mit diesem Parameter wird definiert, in welchen LDAP Gruppen-Objektklassen der Logon Client nach einer Mitgliedschaft des Benutzers suchen soll. Dieser Wert ist ein Bitfeld, folgende Werte sind derzeit definiert:

Objektklasse	Wert
groupOfNames	1
groupOfUniqueNames	2
posixGroup	4

Bei einem Lotus Domino LDAP Server wird die Objektklasse „groupOfUniqueNames“ vom Logon Client nicht verwendet, auch wenn Sie angegeben wurde.
Ist der Registry Key nicht vorhanden, wird der Standartwert „3“ verwendet.

1.7.12 LDAPOUSearchList

“LDAPOUSearchList” = MULTI_SZ:“”
Mit diesem Registry Parameter kann eine OU SearchList definiert werden.
Die OUSerarchList ist eine Liste von OU’s, welche anstelle der OU vom Logon Panel, für den automatischen Zusammenbau der UserDN verwendet wird.
Der Logon Client versucht eine Anmeldung mit allen OUs in der definierten Reihenfolge, bis eine Anmeldung erfolgreich ist.
Die einzelnen OU Strings werden mit „;“ getrennt angegeben, z.B:
LDAPOUSearchList=“at;de;uk“

1.7.13 AttributeBasedGroups

“AttributeBasedGroups” = MULTI_SZ:“”

Mit diesem Parameter können dynamisch Gruppen zum aktuellen Benutzer anhand von LDAP Attributen hinzugefügt werden.

Beispiel:
AttributeBasedGroups: physicalDeliveryOfficeName=ATQA%s01_G

Bei der Anmeldung des Benutzers versucht der Logon Client, das LDAP Attribut „physicalDeliveryOfficeName“ aus dem Benutzerobjekt auszulesen und fügt

anschließend dem Benutzer eine dynamische Gruppe „ATQA%s01_G“ hinzu, wobei „%s“ durch den Inhalt des Attributes „physicalDeliveryOfficeName“ ersetzt wird. Es werden ebenso multivalue LDAP-Attribute mit bis zu 10 Einträgen unterstützt.
Ebenso gibt es die Möglichkeit das erste Zeichen des LDAP-Attributes abschneiden zu lassen, indem man ein „>“ hinter das „=“ setzt.

Beispiel:
AttributeBasedGroup: physicalDeliveryOfficeName=**>**ATQA%s01_G

1.7.14 AttributeBasedEnvironment

“AttributeBasedEnvironment” = “”

Mit diesem Parameter wird ein dynamisches Setzen von Environment-Variablen am Arbeitsplatz anhand bestimmter LDAP Attribute ermöglicht.

Beispiel:
AttributeBasedEnvironment: physicalDeliveryOfficeName

Bei der Anmeldung des Benutzers versucht der Logon Client, das LDAP Attribut „physicalDeliveryOfficeName“ aus dem Benutzerobjekt auszulesen und exportiert den Inhalt des Attributes als Environment-Variable „physicalDeliveryOfficeName“.

Bei Bedarf kann auch ein Mapping vorgenommen werden, z.B.:
AttributeBasedEnvironment: physicalDeliveryOfficeName=officeName

In diesem Fall wird der Inhalt des LDAP Attributes „physicalDeliveryOfficeName“ als Environment-Variable „officeName“ exportiert.

Ebenso gibt es die Möglichkeit, das erste Zeichen des LDAP-Attributes abschneiden zu lassen, indem man ein „>“ hinter das „=“ setzt.

Beispiel:
AttributeBasedEnvironment: physicalDeliveryOfficeName=**>**officeName

1.7.15 HwAdminGroup

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadmingroup"="hwadmin"
Dieser Parameter definiert, in welcher Gruppe der Benutzer Mitglied sein muss, um HWadmin (Hardware-Administrator) werden zu können.

1.7.16 HwAdminAttribute

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadminattribute"="machines"
Gibt an, welches Attribut des LDAP-Benutzerobjektes eine Liste mit Rechnernamen enthält, für welche dieser Benutzer hwadmin werden darf.

Bei der Anmeldung wird überprüft ob der Benutzer der "LDAP-hwadmingroup" zugehörig ist.
Anschließend wird überprüft, ob die Workstation, von welcher aus sich der Benutzer anmeldet, im "LDAP-hwadminattribute" existiert.
Wenn beides der Fall ist, wird der Benutzer lokaler Administrator.

1.7.17 EnableLocation

“EnableLocation” = DWORD:0
Der Location Modus ermöglicht ein standortabhängiges Erlauben / Verbieten, der Anmeldung eines Benutzers, sowie standortabhängiges Zuweisen von Environment -Variablen.

Der LocationCode wird aus dem Sub-Domain Part des FQDN der Workstation ermittelt.
z.B: test1.vien.comtarsia.com (LocationCode = ‘vien’)

1.7.18 LocationAllowedAttributes

“LocationAllowedAttributes” = „ANPrimaer, ANAlternativ“
Gibt an in welchen Attributen des LDAP-Benutzerobjekts definiert ist, d.h. von welchen Standorten aus der Benutzer sich anmelden darf.

1.7.19 LocationObjectClass

“LocationObjectClass” = „ANSubsiddiary“
Gibt die Objektklasse des LDAP-Location Objektes an.

1.7.20 LocationObjectCode

“LocationObjectCode” = „ANCode“
Gibt das LDAP-Attribut des LocationObjects an, welches den Standortcode enthält. z.B.: „vien“

1.7.21 LocationObjectAttribute

“LocationObjectAttribute” = „L“
Gibt an in welchem LDAP-Attribut des LocationObjects, der Standortname vermerkt ist. zB.: „Wien“

1.7.22 LocationBasedEnvironment

“LocationBasedEnvironment” = „“
Mit dieser Einstellung kann man Werte von Attributen des LocationObjects, als Environment Variablen exportieren.
zB.: “LocationBasedEnvironment” = „L=Standort“
siehe: AttributeBasedEnvironment

1.7.23 Die Variable VALID_LOCATION

Die Variable %VALID_LOCATION% ist immer dann gesetzt, wenn eine Lokationsüberprüfung stattgefunden hat. Ist der aktuelle Benutzer für die Anmeldung an der momentanen Lokation zugelassen, so enthält die Variable den Wert „1“. Findet keine Lokationsüberprüfung statt, zB weil eine lokale Anmeldung durchgeführt wurde, so ist diese Variable nicht gesetzt.

1.7.24 KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAPServers

Hier werden die verfügbaren LDAP-Server angegeben.
Falls entsprechend konfigurierte DNS-Server zur Verfügung stehen, können die LDAP Server auch über DNS ermittelt werden (siehe LDAPEnableDNS).

1.7.25 KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\[Hostname oder IP]

Der Name der Keys entspricht dem Hostnamen oder der IP-Adresse des LDAP-Servers, z.B.: „ldap.comtarsia.com“.

1.7.26 Priority

“Priority” = DWORD:0
Server-Priorität, beschreibt die Kontaktierungsreihenfolge wie in RFC 2052 definiert.
0 - 65535 = je kleiner, desto höher die Priorität

1.7.27 Weight

„Weight“ = DWORD:0
Load Balancing, wie in RFC 2052 beschrieben
0 = kein load balancing, 1 - 65535 = load balancing factor

1.7.28 PortLDAP

„PortLDAP“ = DWORD:389
Port-Adresse des LDAP-Servers für unverschlüsselte Kommunikation.
„389“ ist die Standardeinstellung bei allen LDAP-Servern.

1.7.29 PortLDAPS

„PortLDAPS“ = DWORD:636
Port-Adresse des LDAP-Servers für SSL-verschlüsselte Kommunikation.
„636“ ist die Standardeinstellung bei allen LDAP-Servern.

1.8 SignOn Gate Unterstützung

Der Comtarsia Logon Client sendet bei jedem Logon ein Synchronisation Paket zum SignOn Proxy Server, welche dann an den SignOn Agents weitergeleitet werden.
Die Antwort, welche Domänen bzw. Server automatisch synchronisiert werden konnte, werden in der Sync Status Box am Client angezeigt.
Die Logon Session hat aufgrund der Benutzer- und Passwortsynchronität auf alle diese Systeme Zugriff.
Die SyncClient Funktionalität wird mit dem Parameter „EnableSyncClient“ in der Registry aktiviert. (siehe EnableSyncClient)

[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\ComSyncClient]

1.8.1 SyncProxy

"SyncProxy"="192.168.14.245"
oder
"SyncProxy"="signonproxy.comtarsia.com"

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

1.8.2 ProxyPort

"ProxyPort"=DWORD:7d1
Dieser Parameter definiert den IP-Port für die Kommunikation mit dem ProxyServer.

1.8.3 ConnectTimeout

"ConnectTimeout"=DWORD: 5
Dieser Parameter definiert den Timeout in Sekunden für den Verbindungsaufbau mit dem Proxy Server.

1.8.4 SyncPacketTTL

"SyncPacketTTL"=DWORD:1770
Dieser Parameter definiert den Timeout in Sekunden für die Bearbeitung der SyncPackets.

Weitere Informationen über das Produkt Comtarsia SignOn Gate 2006, entnehmen Sie bitte dem Dokument SignOnGate2006.
http://signon.comtarsia.com/main/de/Manuals

1.9 Funktionsbeschreibung LDAP Logon

Der LDAP Logon ermöglicht den Logon auf der lokalen Workstation über ein LDAP Directory. (siehe Bild 1.)
Zusätzlich können Gruppen, Windows Policy, Laufwerks- und Printerzuordnungen, Homedirectory und Profilepfad und Netzwerkapplikationen über das LDAP Directory definiert werden.
Gemeinsam mit dem Comtarsia SignOn Agent für Windows und UNIX besteht die Möglichkeit, die Benutzerverwaltung über ein LDAP Directory zu betreiben und den Zugriff auf Windows und UNIX Ressourcen zu gewährleisten.

Weitere Informationen über die LDAP Konfiguration finden Sie im Handbuch Comtarsia Logon Client 2006 und LDAP.
http://signon.comtarsia.com/main/de/Manuals

1.10 Windows Policy

1.10.1 Allgemein

Die Registry Based Policy Funktionalität von NT 4.0 ist unter Windows 2000, Windows XP weiterhin funktionsfähig.
Sie wurde von den GPO's, welche im Active Directory verwaltet werden, abgelöst. Steht aber kein ADS zu Verfügung, muß auf die alte klassische Policy Methode zurückgegriffen werden. Es lassen sich sämtliche GPO's Templates auf Poledit fähige Templates konvertieren.
Für die Verwaltung von Win2000 bzw. XP Workstations müssen die Templates dem jeweiligen Betriebsystem verwendet werden.
Policy Settings, welche in den sogenannten „*.pol" Files definiert sind, werden abgearbeitet, d.h. beim Logon Prozess werden Policy Settings für „default Computer" in den HIVE „HKEY_LOCAL_MACHINE" und Policy Settings für „default User" in den HIVE „HKEY_CURRENT_USER" aktualisiert.
Settings im HIVE „HKEY_LOCAL_MACHINE" werden im Registry-File "system" gespeichert und sind benutzerunabhängig.
Settings im HIVE „HKEY_CURRENT_USER" werden im Profil des jeweiligen Benutzers abgespeichert (File: ntuser.dat) und wandern bei einem Roaming-User-Konzept mit dem User mit.
WICHTIG: Policy Settings müssen in beide Richtungen berücksichtigt werden, d.h. möchten Sie eine bereits gesetzte Policy wieder aufheben, reicht es nicht, das Policy File vom Server zu entfernen. Policy Settings müssen durch neue Policy Definitionen wieder zurückgesetzt werden.
Im Policy Editor („**poledit.exe" im Lieferumfang von NT 4.0 Server** oder NT Server Ressource Kit) passiert das mit den Schaltflächen, welche drei Modi annehmen können:
Feld ist grau: Kein Eintrag im Policy File, alles bleibt, wie es ist.
Feld ist angehakt: Der Policy Eintrag wird aktiviert.
Feld ist weiß: Der Policy Eintrag wird in die Gegenrichtung aktiviert.
Bei Textfeldern muß bei einer neuen Wertzuweisung das Feld angehakt bleiben.

1.10.2 Logon Client

Der Logon Client übergibt beim Logon den vollen Pfad des Policy-Files, welches im Parameter „PolicyPath“ definiert ist, dem Winlogon Prozeß.
Dieses File sollte auf jedem Domain Controller im selben Share mit Leserechten für alle freigegeben sein.
Die Verwendung des Directory Replicator Service wird empfohlen. Daher ergibt sich z.B. dieser Pfad: „%OS2_LOGONSERVER%\netlogon\ntconf1.pol“

1.10.3 Verwaltung des Logon Clients

Da alle Parameter des Logon Clients im MACHINE HIVE der Registry gespeichert sind, kann die Konfiguration auch über Policy Settings erfolgen.
Dafür muß zuerst das Template „pcs_gina.adm“ im Policy Editor geladen werden. (siehe Bild 12).
Dann kann mit dieser Schablone die lokale Registry geöffnet werden, z.B. für die lokale Konfiguration und Tests mit dem Logon Client. (siehe Bild 11).
Durch Klicken auf „Local Computer“ werden die Logon Clients Einstellungen angezeigt. (siehe Bild 14).
Änderungen werden durch die Menüauswahl "Datei, Speichern" in der lokalen Registry aktualisiert.
Diese Änderungen werden erst beim nächsten LDAP Logon vom Logon Client übernommen.
Für eine zentrale Verwaltung muß entweder ein bestehendes Policy File geöffnet werden, oder ein neues erstellt werden. **(Achtung: Bestehende Policy Files immer mit den gleichen Templates öffnen!)**.
Mit dieser Funktion haben Sie die Einstellung des Logon Clients zentral unter Kontrolle.
Möchten Sie zusätzliche Policy Einstellungen für die Windows Workstation verwalten, müssen bei der Erstellung des Policy Files die Windows Schablonen zusätzlich geladen werden.
(siehe Bild 13).
Das Zuordnen von Policy Einstellungen für bestimmte Benutzer oder Gruppen ist nicht möglich.
Durch das Definieren von mehreren Gruppen und deren Zuweisung unterschiedlicher Policy Files kann jedoch eine individuelle Verwaltung erreicht werden.

1.10.4 Die Variable USER_PRIV

Die Environment Variable USER_PRIV wird abhängig von den LDAP Gruppenmitgliedschaft gesetzt:

Benutzer ist Mitglied der LS Gruppe	USER_PRIV erhält den Wert	Lokale Gruppen Mitgliedschaft
-, USERS, keine zusätzliche Gruppen Definition	USER	Benutzer/Users
PUSER	PUSER	Hauptbenutzer/Power User
WSADMIN	WSADMIN	Administratoren/Administrators

Administrator Logon

USER_PRIV erhält den Wert	Lokale Gruppen Mitgliedschaft
ADMIN	Administratoren/Administrators

1.10.5 Vorschlag für den Einsatz von Policy Files in Verbindung mit dem Comtarsia Logon Client:

Benutzer, Hauptbenutzer, Workstation Administratoren sollen verschiedene Policy Einstellungen erhalten.
Über die LDAP Gruppenmitgliedschaft und der Definition mehrerer Policy Files läßt sich diese Funktionalität realisieren.

Es werden vier Policy Files mit dem Policy Editor (Poledit.exe, Lieferumfang NT/W2K Server, für die Verwaltung von W2K Arbeitsstationen muß der Poledit 5.0 und die Schablonen von einem W2K Server verwendet werden) erstellt und auf alle Domain Controller im Netlogon Share freigegeben.
User.pol, puser.pol, wsadmin.pol, admin.pol.

Der Parameter PolicyPath wird mit Verwendung der USR_PRIV Variable gesetzt.
.: "PolicyPath"="%LOGONSERVER%\\netlogon\\%USER_PRIV%.pol"

WICHTIG! Alle vier Policy Files müssen exakt dieselben Policy Settings berücksichtigen.
z.B.: Benutzern soll das Ausführen der Registry Tools verboten werden, somit muß dieses Setting im Policy-file: *user.pol* gesetzt sein und bei allen anderen wieder zurückgesetzt werden (Kästchen ist angehakt oder weiß, NICHT grau!).

Weiter sehr nützliche Information über GPO's ohne Active Directory finden Sie unter: http://www.gruppenrichtlinien.de

1.11 Home-Directory- und Profile-Path

Dem Logon Client kann über die lokale Konfiguration bzw. über LDAP der Home-Directory-Pfad, der lokale Laufwerksbuchstabe, sowie der Profile-Pfad für die Roaming-Profile Funktionalität zugewiesen werden.

Für die lokale Konfiguration sind folgende Parameter zu verwenden: „HomeDirPath“, „HomeDirDrive“ und „ProfilePath“.

Für die Konfiguration über das LDAP Directory mit der Comtarsia Schema-Erweiterung sind folgende Attribute des “CLCPerson”-Objektes zu verwenden: “CLCHomeDirPath”, “CLCHomeDirDrive” und “CLCProfilePath”.

Die Verwaltung unter LDAP:

Für die Konfiguration über das LDAP Directory mit der Comtarsia Schema-Erweiterung sind folgende Attribute des “CLCPerson”-Objektes zu verwenden: “CLCHomeDirPath”, “CLCHomeDirDrive” und “CLCProfilePath”.

- LDAP Logon Client.doc (Comtarsia Logon Client 2006 und LDAP)
- http://signon.comtarsia.com/main/de/Manuals

1.12 Zusätzliche Funktionen:

1.12.1 Microsoft GINA

Mit der Tastenkombination **SHIFT + ENTER im Logon Dialog** kann auf die Microsoft Gina umgeschaltet werden.
Damit wird ein Modus erreicht, der sich verhält, als würde der Logon Client nicht installiert sein. Über den Schalter „DisableMsGina” kann diese Funktionalität unterbunden werden.

1.12.2 Administrator Logon

Diese Funktion ermöglicht einem Benutzer das Login (das Profil des jeweiligen Benutzers wird geladen) mit lokalen Administratorrechten.
Der Benutzer wird temporär (nur für diese Sitzung) Mitglied der lokalen Administratorgruppe.

Mit diesem Modus können Einstellungen am Benutzerprofil, Installationen von SW-Pakten oder Wartungs- Arbeiten vorgenommen werden.
Aus Sicherheitsgründen muß zuerst der Anwender wie gewohnt seine Benutzer ID und Paßwort im Logon Dialog eintragen. (siehe Bild 1) Anstelle der Bestätigung mit „ENTER“ oder „OK“ kann nun ein Administrator mit **CTRL+ALT+ENTER** den Adminlogon Dialog aktiviert werden, in welcher der Administrator aufgefordert wird, seinen Benutzernamen und sein Paßwort einzugeben (siehe Bild 2).

Nun wird zuerst überprüft, ob der Administrator Account im LDAP Directory Mitglied der Gruppe „AdminLogonGroup“ ist, dann wird ein Login des angegebenen Benutzers mit lokalen Administratorrechten durchgeführt (siehe AdminLogonGroup).

1.12.3 Directory Replicator

Der Directory Replicator ermöglicht sehr einfach und effizient Verzeichnisse während des Logon Vorganges zu replizieren.
Da nur veränderte Dateien kopiert werden, kann diese Funktion für umfangreiche Systemmanagement – Softwareaktuallisierungsfunktionen verwendet werden.
Ebenfalls werden entsprechend dem Referenzverzeichnis Dateien/Verzeichnisse gelöscht.

Aufruf über Scripts:

Beispiel:
Replicate \\Server\program c:\program

Parameter Beschreibung:

-a Die ACL Information wird mitkopiert
-s Die Security Attribute werden mitkopiert

Beispiel:
Replicate \\Server\program c:\program -as

2. GroupMapping

Der Schalter „DisableEqualGroupMapping“ schaltet die automatische Gruppenzuordnung nach gleichen Namen aus und die manuelle Gruppenzuordnung ein.
Es werden nur Gruppen zugeordnet, welche unter dem Key GroupMapping definiert sind.
Die Gruppen für das lokale Administrator- und Hauptbenutzer Privileg sind nun über die Parameter „GroupAdministrator“ und „GroupPowerUser“ zu definieren (die LDAP Gruppen „WSADMIN“ und „PUSER“ werden nicht mehr automatisch den lokalen Gruppen „Administrator“ und „Hauptbenutzer“ zugewiesen.)

Beispiel für die manuelle Gruppenzuordnung:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA]
"DisableEqualGroupMapping"=DWORD:1
"GroupAdministrator"="WSADMIN"
"GroupPowerUser"="PUSER"

[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\GROUPMAPPING]
"LDAPGROUP1"="LOCALGROUP1"
"LDAPGROUP2"="LOCALGROUP2"
```

3. Netzwerkapplikationen

siehe Handbuch Comtarsia Logon Client 2006 und LDAP, Kapitel Netzwerkapplikationen.

4. Erklärungen:

4.1.1 GINA:

Diese Spezifikation wird in der SW-Entwicklung verwendet, wenn jener Bestandteil von Windows NT bzw. W2K ersetzt werden soll, der das Identifizieren und Beglaubigen der interaktiven Benutzer durchführt. Diese austauschbare Funktionalität wird als dynamic-link library (DLL) zu Verfügung gestellt, von WINLOGON.EXE geladen und aufgerufen. Diese DLL wird als "**G**raphical **I**dentification a**n**d **A**uthentication" oder GINA bezeichnet.

4.1.2 GPO:

GPO steht für "Windows 2000 Group Policy".

4.1.3 SAS:

SAS steht für "Secure Attention Sequence", welche im Standardfall über die Tastenkombination „Strg+Alt+Del" ausgelöst wird.

5. Disclaimer

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.

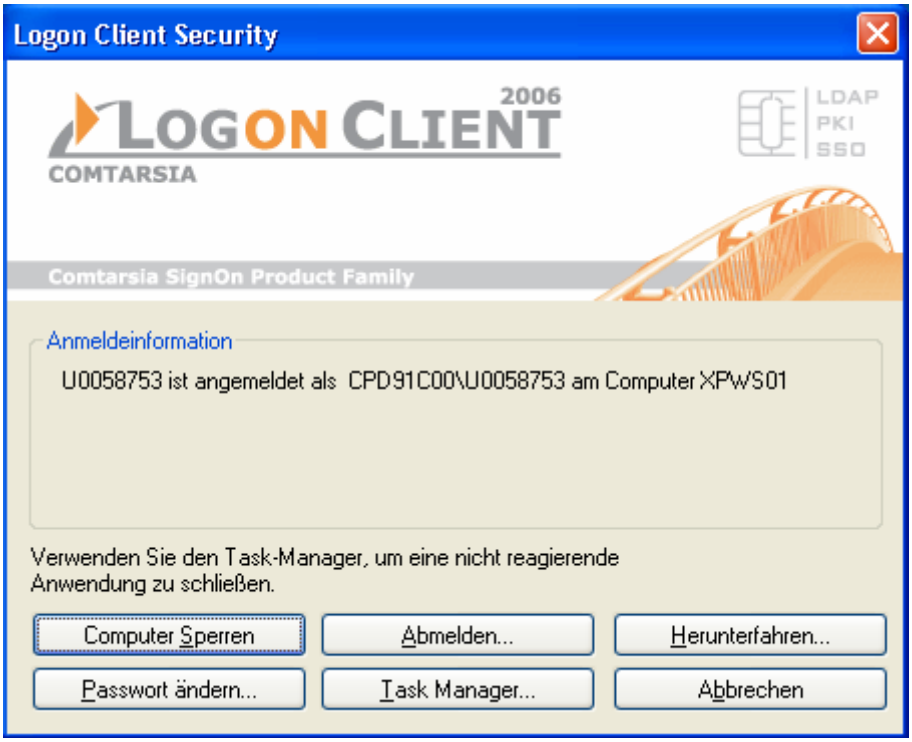
Darüber hinaus bedeutet ein Link aus unserer Site heraus auf eine andere nicht, daß wir uns mit deren Inhalt identifizieren oder deren Nutzung unterstützen.

6. Screen Shots

6.1.1 Bild 1. Logon Dialog

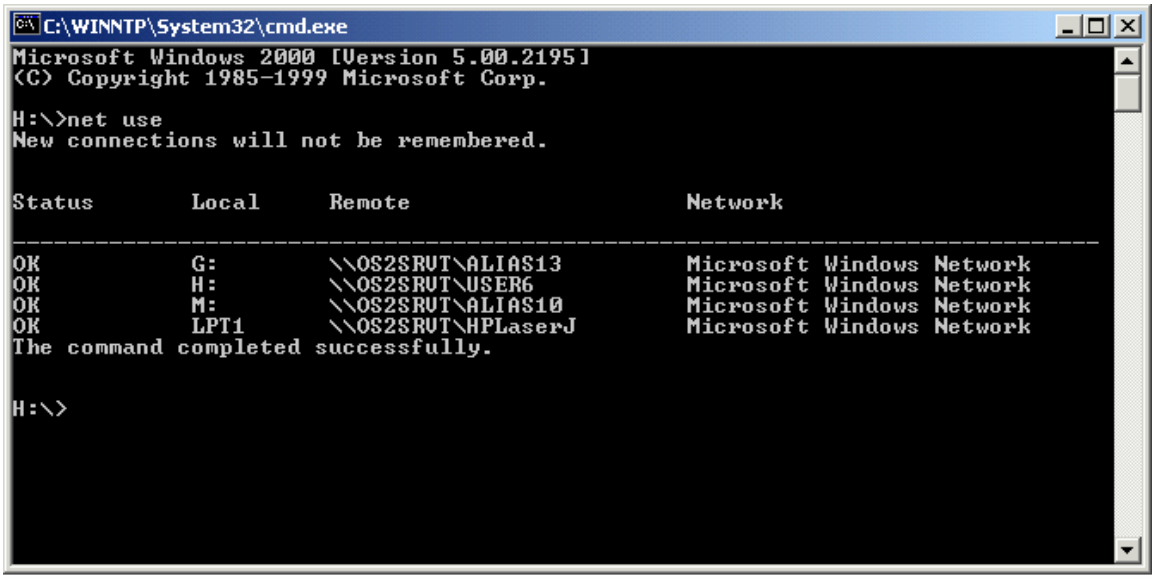
6.1.2 Bild 2. Admin Logon Dialog

6.1.3 Bild 3. ON SAS Dialog

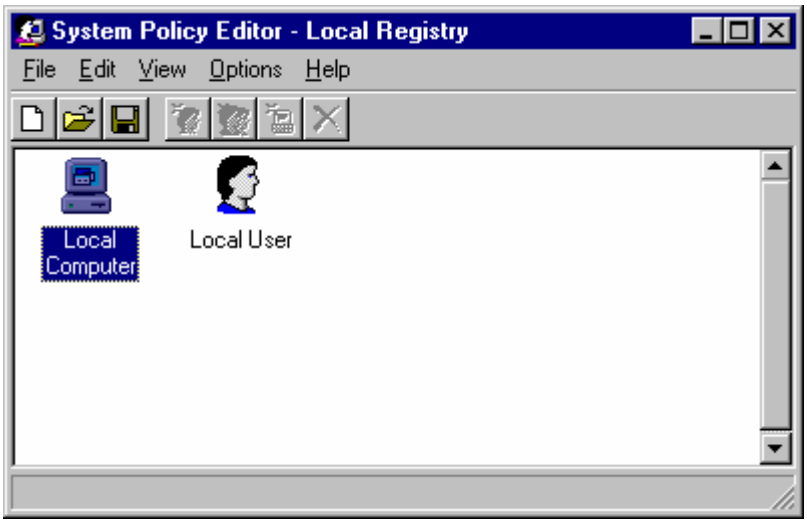


6.1.4 Bild 4. Unlock Dialog

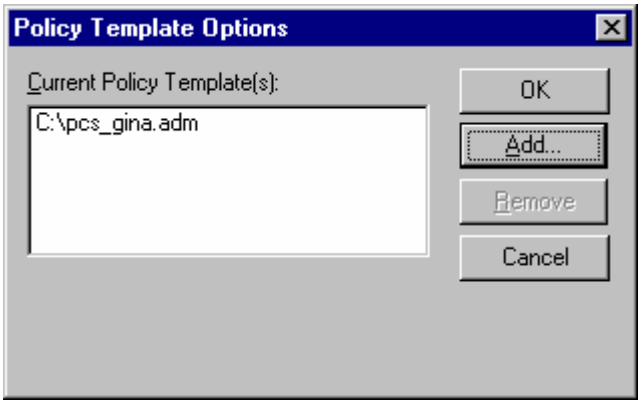
6.1.5 Bild 10. Windows Workstation „net use“



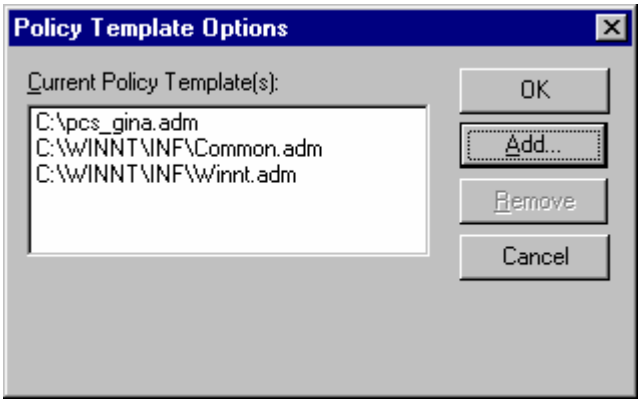
6.1.6 Bild 11. Policy Editor



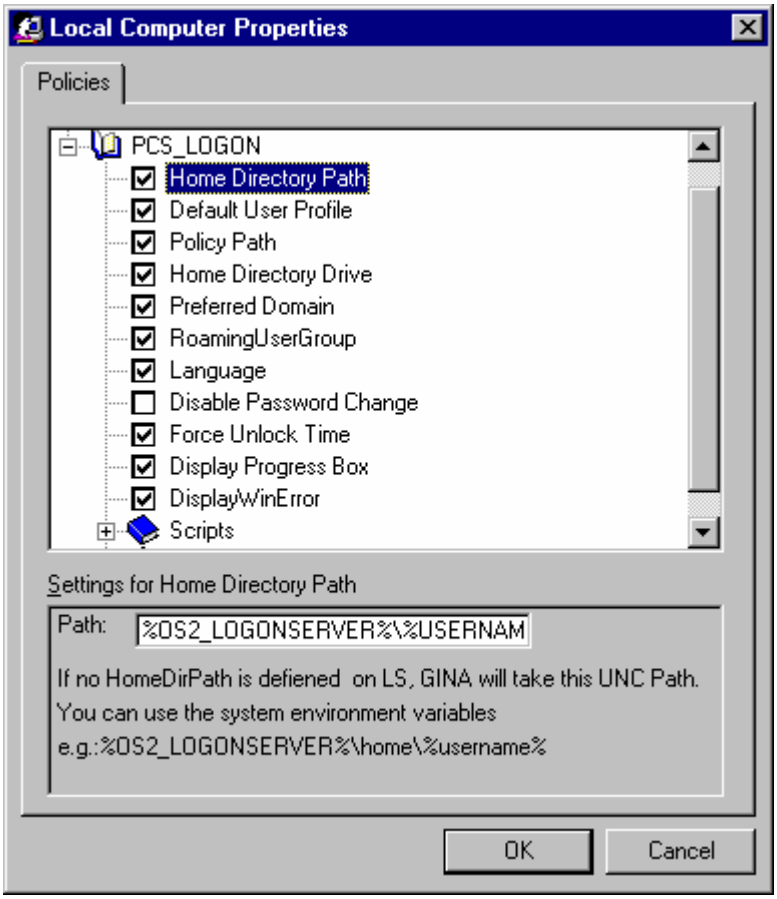
6.1.7 Bild 12. Policy Editor GINA Template



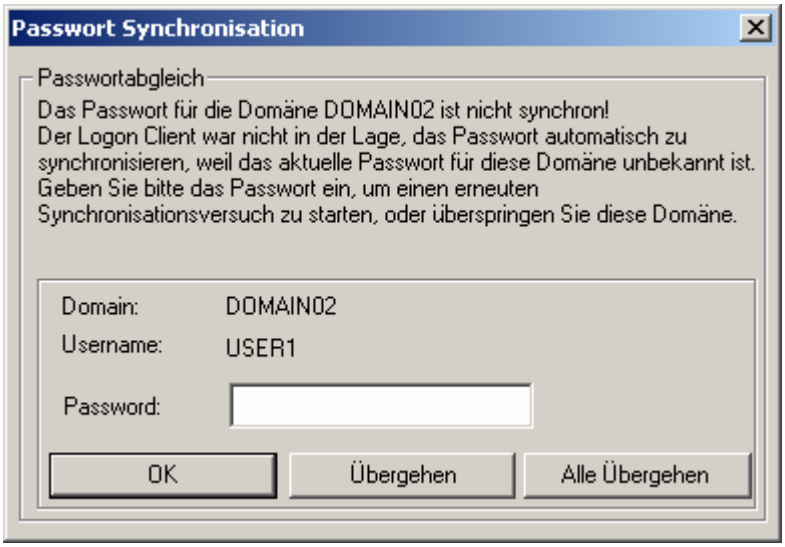
6.1.8 Bild 13. Policy Editor GINA und Windows Templates



6.1.9 Bild 14. Policy Editor GINA Konfiguration



6.1.10 Bild 21. Passwort Synchronisation – Passwortabgleich



6.1.11 Bild 22. Erweiterter LDAP Logon