Servolution Logon Client Version 3.0

Technische Beschreibung

August 2002

Version 3.0 – Build 3.0.x.15

Inhaltsverzeichnis

1. Beschreibung

Servolution LDAP/OS2 Logon Client Modul für Windows 2000 and Windows XP 3.0, Build 3.0.X.15
(english und german)

Die Vorgänger Versionen 1.0 – 2.1, wurden für große Umgebungen entwickelt, in denen die Benutzerverwaltung und das File- und Print-Service auf OS/2 Servern betrieben und im Frontoffice Windows 2000 bzw. Windows XP eingesetzt wird.

In diesen Netzwerken steht der Bedarf an GUI's für Installation und Konfiguration im Hintergrund, auf der Anwenderseite hingegen sind Funktionen wie zentrale Konfiguration, einfache Möglichkeit der SW-Verteilung, individuelle Anpassung in das IT-Umfeld sehr wichtig.
Genau für diesen Einsatzbereich wurde der Servolution Logon Client entwickelt, er ist aber auf Grund seiner sehr einfachen Handhabung auch für den Einsatz in kleinen Netzwerken geeignet.

Mit dem Servolution Logon Client Version 3.0 wurden alle Funktionalitäten der Vorgänger Versionen übernommen, und er ermöglicht es für Windows 2000 und Windows XP Workstations, sich an LDAP und OS/2 Server anzumelden.
Optional besteht die Möglichkeit, das Passwort auf anderen OS/2 und NT Domänen synchron zu halten.

Mit dem Zusatzprodukt „Servolution Sync Agent for Windows / Sync Agent für UNIX" besteht die Möglichkeit, Benutzerkonten auf Windows Servern, Windows Domänen (NT 4.0 / ADS) und UNIX Servern automatisch verwalten zu lassen und als Ressourcen im OS/2 Netzwerk oder in der LDAP Benutzerverwaltung zu integrieren.

Im Rahmen von Großkundenprojekten wurde der *„Servolution Migration Path"* entwickelt, mit welchem eine weiche Migration der OS/2 Server Ressourcen auf Windows und UNIX ermöglicht wird und weiters die Benutzerverwaltung von OS/2 auf ein LDAP Directory verlagert werden kann.

Der Servolution Logon Client sowie der Servolution Sync Agent stellt nicht nur eine optimale Migrationshilfe dar, sondern der Vorteil, die Benutzerverwaltung von der Ressourcenverwaltung losgelöst zu betreiben, bedeutet eine sehr entscheidende Unabhängigkeit gegenüber Hersteller propräterer Lösungen. Somit steht Servolution auch für Single Sign On, Centralized User Management und Security Management.

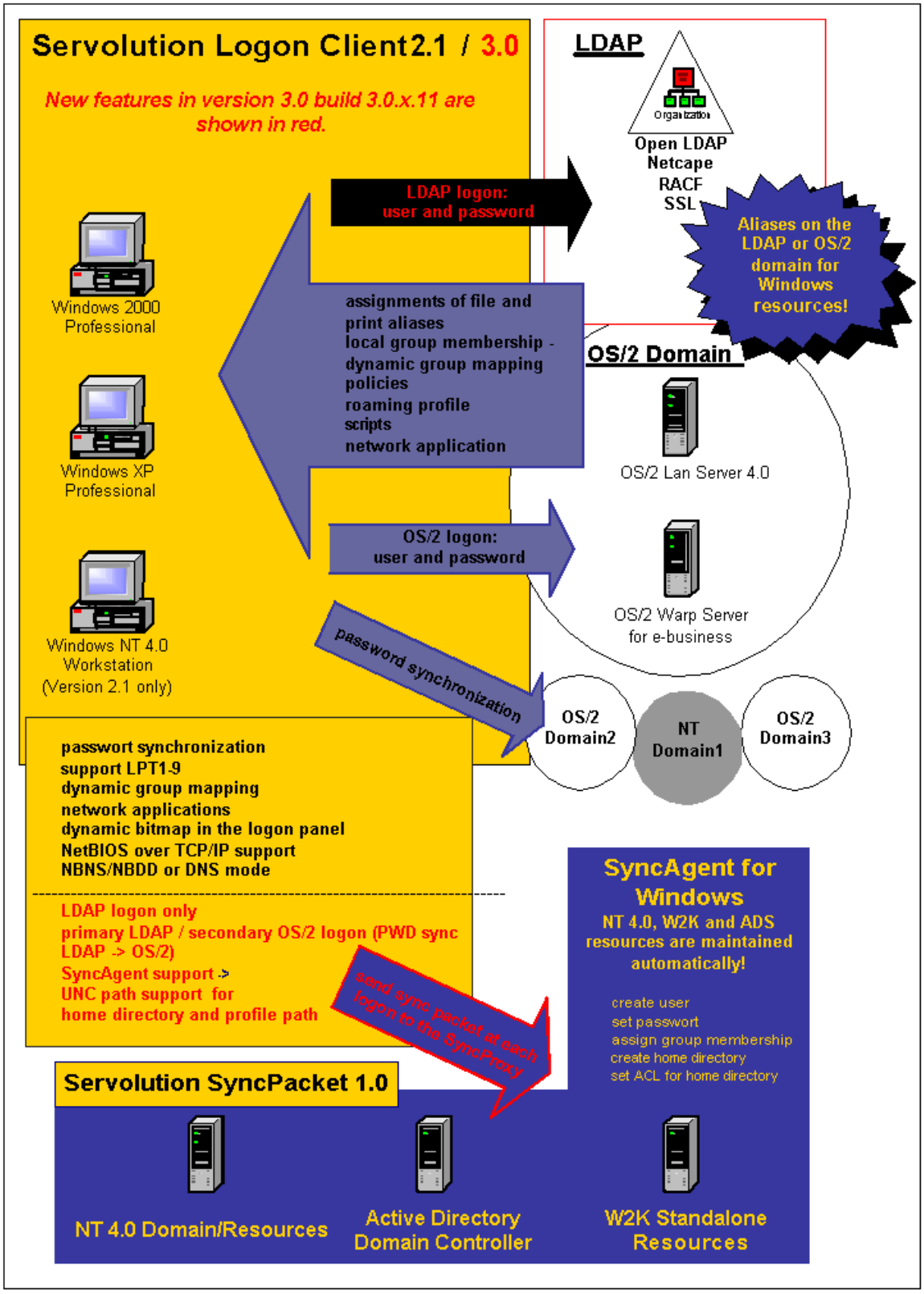
Weitere Informationen bezüglich LDAP und den Servolution Migration Path entnehmen Sie bitte unseren Web Sites.

http://servolution.comtarsia.com/main/de/Migration

http://www.comtarsia.com/main/de/Services/Netzwerk/Directories

Informationen über die Verfügbarkeit und Funktionsumfang der Produkte „Sync Agent" entnehmen Sie bitte dem Servolution Roadmap:
http://servolution.comtarsia.com/main/de/Roadmap

1.1 Servolution Übersicht



1.2 Voraussetzungen am Server:

LDAP:
Siehe LDAP Quickstart

OS/2:
LAN Server 4.0, 5.0, WARP Server oder WARP Server for e-business (German od. UK)
Protokoll NetBEUI , (TCP/IP u. NetBIOS over TCP/IP)

1.3 Voraussetzungen am Client:

W2K Professional oder Windows XP Professional (German od. UK)
Protokoll NetBIOS over TCP/IP od. NetBEUI.
Achtung für Windows XP: Das Protokoll NetBEUI wird ohne Gewährleistung unterstützt!
Begründung:
Microsoft gibt keinen offiziellen Support für das Protokoll NetBEUI!

Produkte, welche auf tiefer Kernelebene den Netzwerkstack verändern, wie z.B. VMWARE, sind gemeinsam mit dem Produkt Servolution Logon Client nicht zu betreiben.

Die Terminal Server Funktionalitäten auf der XP Workstation wird mit dem derzeitigen Build nicht unterstützt.

1.4 Installation:

Die Datei **SetupIc.exe** ausführen und die Anweisungen befolgen.
Die Einstellungen sämtlicher Parameter können nach der Installation über den Configurator durch geführt werden.
Das Handbuch orientiert sich auf die Registry Parameter, und ist für die Installation in großen Netzwerken via SW-Verteilung vorgesehen.

SW-Verteilung:

Die Datei ***pcs_gina.reg*** anpassen und die Datei ***install.cmd*** ausführen.
Für die Installation sind lokale Administrator-Rechte notwendig!
Neustart des Systems.

Alle Einstellungen werden in der Registry unter dem Key
"HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA" verwaltet.

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 EnableLDAP

„EnableLDAP“=DWORD:1
Mit diesem Schalter wird der Logon Client von OS/2 auf LDAP umgeschaltet.

Default: 0

Beispiel:
„EnableLDAP“=DWORD:1
Der LDAP Modus ist aktiviert. In diesem Modus kann zwischen dem „LDAP LOGON“ und einem LDAP-OS/2 LOGON gewählt werden. Ein reiner OS/2 Login ist in diesem Modus nicht möglich. (siehe LDAP-OS/2 LOGON)

„EnableLDAP“=DWORD:0
Der OS2 Modus ist aktiviert, es ist nur ein OS/2 Login möglich.
(siehe Funktionsbeschreibung OS/2 Logon)

1.6.2 EnableSyncClient

„EnableSyncClient“=DWORD:1
Mit diesem Schalter wird der Servolution Synchronisation Agent aktiviert.
(Siehe Servolution Sync Client)
Default: 0

1.6.3 PolicyPath

Definiert den vollen Pfad des Policy-Files.
z.B.: "PolicyPath"="%OS2_LOGONSERVER%\\netlogon\\ntconfig.pol"
(siehe Windows Policy)

1.6.4 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"="%OS2_LOGONSERVER%\\netlogon\\default profile"

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"="%OS2_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"="%OS2_LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.12 AdminUsrLogonScript

Dieses Script wird beim Logon im User Environment mit Admin-Privilegs ausgeführt.
z.B.:"UserLogonScript"="%OS2_LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.13 UserLogoffScript

Dieses Script wird beim Logoff im User Environment mit User-Privilegs ausgeführt.

z.B.:"UserLogonScript"="%OS2_LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.14 UserLogoffScriptErrorlevel

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

1.6.15 SystemLogoffScript

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

1.6.16 Script Übersicht:

Script	Zeitpunkt und Reihenfolge der Ausführung	lokale Berechtigung	Environment	Zugriff auf Netzwerk-ressourcen	Zugriff auf HKEY_CURRENT_USER	Zugriff auf HKEY_LOCAL_MACHINE
InitScript	System Boot	System	System	Nein	Nein	Ja
PreSystemLogonScript	Vor lokalem Logon(1)	System	System	Nein	Nein	Ja
SystemLogonScript	Logon (2)	System	System	Nein	Nein	Ja
AdminUsrLogonScript	Logon (3)	User mit Lokalen Admin Rechten	User	Ja	Nein	Ja
SysUsrLogonScript	Logon (4)	System	User	Nein	Nein	Ja
UserLogonScript	Logon (5)	User	User	Ja	Ja *	Ja *
UserLogoffScript	Logoff (1)	User	User	Ja	Ja *	Ja *
SystemLogoffScript	Logoff (2)	System	System	Nein	Nein	Ja

* Abhängig von der effektiven User Policy

1.6.17 ScriptTimeout

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

1.6.18 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.

1.6.19 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!“

1.6.20 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)

1.6.21 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.

1.6.22 DisplayProgressBox

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

1.6.23 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.)

1.6.24 Language

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

1.6.25 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 RBG

1.6.26 AlphaNumPwd

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

1.6.27 DontDisplayLastUserName

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

1.6.28 DisableMsGina

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

1.6.29 DisableEqualGroupMapping

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

1.6.30 GroupAdministrator

"GroupAdministrator"="ADMIN"
Dieser Parameter definiert die OS/2 Gruppe, in welcher der Benutzer Mitglied sein muß, damit er das lokale Administrator Privileg bekommt. Der Parameter DisableEqualGroupMapping“=dwor:1 muß ebenfalls definiert sein.

1.6.31 GroupPowerUser

"GroupPowerUser"="PUSER"
Dieser Parameter definiert die OS/2 Gruppe, in welcher der Benutzer Mitglied sein muß, damit er das lokale Hauptbenutzer Privileg bekommt. Der Parameter DisableEqualGroupMapping“=dword:1 muß ebenfalls definiert sein.

1.6.32 CheckPWDinAllDomains

"CheckPWDinAllDomains“=dword: 1
Dieser Parameter schaltet die Passwortüberprüfung in allen definierten Domänen der Passwort Synchronisation ein.
(Siehe Bild 19.) und Kapitel Passwort Synchronisation.

1.6.33 NWAFolderActive

„NWAFolderActive“=dword:1
Dieser Schalter aktiviert die Unterstützung für OS/2 Netzwerkapplikationen.
Siehe Kapitel Netzwerkapplikationen

1.6.34 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.

1.6.35 NWAFolderName

„NWAFolderName“=“OS2-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.

1.6.36 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

1.6.37 NWADefaultIconPath

„NWADefaultIconPath“=“\\os2srv\daten\icons“
Optional ein UNC-Pfad, in dem alternativ nach dem Programmicon gesucht wird, wenn dieses in der Programmposition nicht gefunden wird.

1.6.38 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.

1.6.39 NWAIconPath

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

1.6.40 NWATimeout

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

1.7 OS/2 Logon Client Einstellungen

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA

1.7.1 PrefDomain

"PrefDomain"="OS2DOMT"
Gibt die Standard Domäne an, welche im Logon Dialog immer angezeigt wird.

1.7.2 NBDDADDR

„NBDDADDR“=“192.168.2.215“
Ist dieser Parameter definiert, schaltet der Logon Client in den NetBIOS over TCP/IP Modus und benützt den definierten NetBIOS Datagram Distributor, um den entsprechenden Domain Controller zu finden.
Achtung! In diesem Fall muß in der TCP/P Konfiguration der NetBIOS Name Server (WINS Server) definiert sein.

1.7.3 BNBDDADDR

„BNBDDADDR“=“192.168.2.216“
Dieser Parameter definiert den Backup NetBIOS Datagram Distributor.
Zusätzlich sollte der Backup NetBIOS Nameserver definiert sein. (WINS Server)

1.7.4 EnableDNS

"EnableDNS"=dword:1
Mit diesem Parameter wird der DNS Modus eingeschaltet.
DNS Modus: Protokoll ist NetBIOS over TCP/IP, und die Namensauflösung erfolgt nur über DNS.

Siehe DNS Modus:
NetBIOS Datagram Distributor und WINS Server dürfen nicht definiert sein. Unter NT 4.0 muß zusätzlich der Schalter „EnableDNS“ in der TCP/IP/WINS Konfiguration eingeschaltet sein.

1.8 LDAP – Logon Client Einstellungen

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP

1.8.1 LDAPVersion

„LDAPVersion“ = DWORD:3
Version des LDAP-Protokolles, 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).

1.8.2 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“

1.8.3 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“

1.8.4 LDAPUserDNSuffix

“LDAPUserDNSuffix” = ""
siehe LDAPUserDNPrefix

1.8.5 LDAPAppendBaseDN

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

1.8.6 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)

1.8.7 LDAPTimeout

“LDAPTimeout” = DWORD:30
Timeout in Sekunden pro LDAP-Server. Wenn dir 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)

1.8.8 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

1.8.9 LDAPEnableFailover

“LDAPEnableFailover” = DWORD:0

Aktiviert (1) die Failover und Load Balancing Funktionen im Logon Client. (siehe LDAP LoadBalancing und Failover und LDAPEnableDNS)

1.8.10 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).

1.8.11 KerberosEnable

“KerberosEnable” = DWORD:0
Aktivieren von Kerberos V5 Support.
Diese Option ist mit Build 3.0.4.10 noch nicht verfügbar.
Default: 0

1.8.12 KerberosEnableDNS

„KerberosEnableDNS“ = DWORD:1
Kerberos KDC und Realm werden über DNS ermittelt.
Diese Option ist mit Build 3.0.4.10 noch nicht verfügbar.

1.8.13 KerberosRealm

„KerberosRealm“ = ""
Kerberos Realm
Diese Option ist mit Build 3.0.4.11noch nicht verfügbar.

1.8.14 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).

1.8.15 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“.

1.8.16 Priority

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

1.8.17 Weight

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

1.8.18 PortLDAP

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

1.8.19 PortLDAPS

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

1.9 Servolution Sync Client

Der Servolution Sync Client sendet bei jedem Logon ein Sync Packet zum Servolution Proxy Server, welche dann an den Sync 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]

1.9.1 SyncProxy

"SyncProxy"="192.68.14.245"
oder
"SyncProxy"="syncproxy.comtarsia.com"

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

1.9.2 ProxyPort

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

1.9.3 ConnectTimeout

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

1.9.4 SyncPacketTTL

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

Weitere Informationen über das Produkt Servolution Sync Agent – Sync Packet 1.0, entnehmen Sie bitte dem Dokument syncpacket_1.0_.doc.

1.10 Funktionsbeschreibung OS/2 LOGON:

1.10.1 System Start:

Der Logon Client überprüft beim Start von Windows, ob alle notwendigen Dienste bereit sind, erst dann wird ein OS2 Logon möglich.
Kann z.B. der Workstationdienst nicht gestartet werden, kommt eine Fehlermeldung, und es wird auf die Microsoft Gina umgeschaltet.

1.10.2 Logon:

Nach Angabe im Logon Dialog (siehe Bild 1.) von Username, Paßwort, Domäne und Bestätigung durch ENTER oder OK, wird der OS2 Logon gestartet.
Zuerst wird ein Domain Controller für die angegebene Domäne und den User gesucht.
Kann diese nicht gefunden werden, wird ein lokaler Loginversuch auf ein bereits lokal vorhandenes Userprofil angeboten und bei richtigem Paßwort durchgeführt.
Wird ein OS/2 Domain Controller gefunden, wird das Paßwort am LAN Server geprüft.
Stimmt die User/Paßwort Kombination am LAN Server, wird ein LAN-Server Logon durchgeführt (siehe Bild 9) und der lokale User wird vorbereitet.
Ist noch kein lokaler Benutzer vorhanden, wird dieser mit demselben Usernamen und Paßwort angelegt. Die Gruppenmitgliedschaft am LAN Server wird abgefragt und nach Möglichkeit auch auf lokale Gruppen zugewiesen. (siehe Bild 5.)
Z.B. ist der User am LAN Server in der Gruppe „Hauptbenutzer“, wird er auch lokal Mitglied der Gruppe „Hauptbenutzer“.
Für LAN Server 4.0 (max 8 Zeichen für Gruppen und User Definition) wird die Abfrage der Gruppen „PUSERS“ und „WSADMIN“ je nach Betriebssystemsprache auf die lokalen Gruppenmitgliedschaften von Hauptbenutzern/Administratoren durchgeführt bzw. auf die lokalen Gruppen Power User/Administrators übertragen.
Z.B.: Ist der User in der LS Domäne Mitglied der Gruppe WSADMIN, wird er Mitglied der lokalen Gruppe Administratoren.
Diese Gruppenmitgliedschaften lassen sich beliebig erweitern und werden bei jedem Logon auch auf bereits existierende User aktualisiert.
(Siehe GroupMapping)

Dynamische Shares für Homedirectories am LAN Server werden bei Bedarf freigegeben.
Die User-Assignments, Aliases und Printer, der LS Domäne werden abgearbeitet und verbunden.
Netzwerkapplikationen werden in einem definierten Folder am Desktop erstellt.
(siehe OS2 Netzwerkapplikationen).
Der Desktop wird für den User freigegeben. (siehe Bild 7., Bild 8 und Bild 10.)

1.10.3 Logoff:

Handelt es sich um einen Roaming User, wird das lokale User-Profil mit dem am Server gespeicherten Profil (\\Server\Homedir\profile) synchronisiert.
Ein LAN-Server Logoff wird durchgeführt (siehe Bild 9).

1.11 Funktionsbeschreibung LDAP – OS/2 LOGON

Diese Funktion ermöglicht das Passwortsynchronisieren von LDAP Benutzerkonten (z.b. LDAP – RACF System) auf OS/2 Domänen.

Die Funktion „LDAP–OS/2 LOGON“ führt nach einer vorgeschalteten LDAP Benutzer/Passwort Überprüfung einen vollständigen OS/2 Logon durch.
(siehe Funktionsbeschreibung OS/2 LOGON)
Ist der LDAP Server nicht erreichbar, wird mit dem OS/2 Login fortgesetzt.
Ist das Passwort auf der OS/2 Domäne nicht synchron mit dem Passwort im LDAP Directory, bekommt der Anwender im Zuge der Anmeldung die Möglichkeit, das aktuelle Passwort einzugeben. Kann mit diesem Passwort ein OS/2 Login erfolgen, wird das Passwort vom Logon Client automatisch auf das LDAP Passwort geändert.
Wird im Zuge der Anmeldung ein Passwortwechsel durchgeführt (z.B. LDAP Passwort abgelaufen), wird das Passwort auf der OS/2 Domäne automatisch vom Logon Client geändert und anschließend der Logon mit dem neuen Passwort durchgeführt.
Um den Logon Client in diesen Modus zu bringen, muß die Funktion LDAP aktiviert werden (siehe LDAPEnable), und es muß im Logon Dialog im Feld Domäne die OS/2 Domäne angebeben werden (siehe Bild 1).
Dieser Modus erfordert eine vollständige Konfiguration der OS/2 und LDAP Einstellungen.
(siehe LDAP – Logon Client Einstellungen und OS/2 Logon Client Einstellungen)

1.12 Funktionsbeschreibung LDAP Logon

Der LDAP Logon wird durch den Parameter LDAPEnable und durch der Angabe „LDAP LOGON“ im Logon Dialog aktiviert und ermöglicht den Logon auf der lokalen Workstation über ein LDAP Directory. (siehe Bild 1.)
Zusätzlich können Gruppen, Windows Policy, Laufwerks- und Printerzuordnungen, Homdirectory und Profilepfad und Netzwerkapplikationen über das LDAP Direktory definiert werden.
Gemeinsam mit dem Servolution Synchronisation 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 Inforamtionen entnehmen Sie bitte folgenden Quellen:

- SLCundLDAP.doc (Servolution Logon Client und LDAP)
- http://servolution.comtarsia.com/main/de/Migration
- http://www.comtarsia.com/main/de/Services/Netzwerk/Directories

1.13 Windows Policy

1.13.1 Allgemein

Die Policy Funktionalität von NT 4.0 ist unter Windows 2000 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.
Für die Verwaltung von Win2000 Workstations müssen die Templates „winnt.adm“ und „common.adm“ von einem Windows 2000 Server 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.

1.13.2 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“

1.13.3 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 OS/2 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 Zuorden 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.

1.13.4 Die Variable USER_PRIV

Die Environment Variable USER_PRIV wird abhängig von der LAN Server 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

1.13.5 Vorschlag für den Einsatz von Policy Files in Verbindung mit dem Servolution Logon Client:

Benutzer, Hauptbenutzer, Workstation Administratoren sollen verschiedene Policy Einstellungen erhalten.
Über die LAN Server 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 OS/2 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"="%OS2_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!).

1.14 Home-Directory- und Profile-Path

Dem Logon Client kann über eine Variable der Home-Directory- und Profilepfad sowie der lokale Laufwerksbuchstabe zugewiesen werden.
Das Benutzerprofil wird im Unterverzeichnis „Profile“ abgelegt.

Der Logon Client unterstützt vier Interpretationen der Home-Directory Zeichenkette.

1.14.1 OS/2 Syntax ohne Drive Letter

\\OS2SRV3\C$\HOME\USER1
Interpretation:
Der nächste freie Laufwerksbuchstabe wird dem UNC Pfad \\OS2SRV3\HOME\USER1 zugewiesen.
Der Profilepfad wird auf \\OS2SRV3\HOME\USER1\PROFILE eingestellt.

1.14.2 OS/2 Syntax mit Drive Letter

H:\OS2SRV3\C$\HOME\USER1
Interpretation:
Der Laufwerksbuchstabe H: wird dem UNC Pfad \\OS2SRV3\HOME\USER1 zugewiesen.
Der Profilepfad wird auf \\OS2SRV3\HOME\USER1\PROFILE eingestellt.

1.14.3 UNC Pfad ohne Drive Letter

\\COMTW2K\HOME\USER1
Interpretation:
Der nächste freie Laufwerksbuchstabe wird dem UNC Pfad \\COMTW2K\HOME\USER1 zugewiesen.
Der Profilepfad wird auf \\COMTW2K\HOME\USER1\PROFILE eingestellt.
Vorsicht: Das „$"-Zeichen darf in dieser Variante nicht verwendet werden!

1.14.4 UNC Pfad mit Drive Letter

H:\COMTW2K\HOME\USER1
Interpretation:
Der Laufwerksbuchstabe H: wird dem UNC Pfad \\COMTW2K\HOME\USER1 zugewiesen.
Der Profilepfad wird auf \\ COMTW2K \HOME\USER1\PROFILE eingestellt.
Vorsicht: Das „$"-Zeichen darf in dieser Variante nicht verwendet werden!

Die Verwaltung des HomeDirectory-Strings unter OS/2:

Der Home-Directory-String kann unter OS/2 mit dem folgenden Befehl zugewiesen werden:
net user USER1 /homedir:H:\COMTW2K\HOME\USER1

Unser TIP für die Migration! *Gemeinsam mit dem Servolution Sync-Agent für Windows können ALIAS- und Homedirectory-Ressourcen auf Windows Ressourcen verlagert werden, die Benutzerverwaltung bleibt vorerst auf OS/2!*
Der SyncAgent für Windows verwaltet die ACL Berechtigung für das Homedirectory automatisch!

Die Verwaltung des HomeDirectory-Strings unter LDAP:

Der Home-Directory-String wird im Attribut "CLCProfilePath" des "CLCPerson"-Objektes gespeichert. Das Attribut wird bei einer LDAP-Anmeldung automatisch ausgelesen.
Weiter Informationen entnehmen Sie bitte folgender Quellen:

- SLCundLDAP.doc (Servolution Logon Client und LDAP)
- http://servolution.comtarsia.com/main/de/Migration
- http://www.comtarsia.com/main/de/Services/Netzwerk/Directories

1.15 Zusätzliche Funktionen:

1.15.1 Microsoft GINA

Mit der Tasten Kombination **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.

1.15.2 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 gedrückter **linken „CTRL“ Taste und Klick auf das kleine „Servolution“ Logo** den Adminlogon Dialog aktivieren.
Es erscheint ein weiterer Dialog, in dem der Administrator aufgefordert wird, seinen Benutzernamen und sein Paßwort einzugeben.(siehe Bild 2)
Nun wird zuerst überprüft, ob der Administrator Account in der OS/2 Domäne gültig ist und mindestens „Account Operator“ Rechte besitzt (siehe Bild 6), dann wird ein Login des angegebenen Benutzers mit lokalen Administratorrechten durchgeführt.

Diese Funktion ist mit Build 3.0.x.11 nur im OS/2 Login Modus möglich!

2. NetBIOS over TCP/IP

2.1 LMHOSTS

Die einfachste Methode, den Logon Client über das Protokoll NetBIOS over TCP/IP zu betreiben, ist die Konfiguration über die LMHOSTS Datei.
Hier müssen alle Domainkontroller und Ressource Server mit der entsprechenden IP Adresse definiert werden:

c:\winnt\system32\drivers\etc\lmhosts

192.168.5.111 OS2DOM #PRE #DOM
192.168.5.111 OS2SRV #PRE
192.168.5.112 OS2SRV2 #PRE

Mit dem Befehl “nbtstat –R” wird die Datei LMHOSTS in den NetBIOS-Namecache geladen, dieser kann mit dem Befehl „nbtstat –c“ überprüft werden.
Bei jedem Systemstart wird diese Datei ebenfalls geladen.

2.2 NetBIOS Name Server & NetBIOS Datagram Distributor Service (NBNS & NBDD)

In größeren Netzwerken ist die Verwendung der LMHOSTS Datei absolut nicht sinnvoll, hier werden NetBIOS Nameserver und das NetBIOS Datagram Distributor Service verwendet.
In einer reinen Microsoft Umgebung wird die Dynamische Netbios Namensauflösung mit den sogenannten WINS Server (Windows Internet Name Server) gelöst.
OS/2 verwendet zusätzlich das NetBIOS Datagram Service, um beim Logon Request und beim Paßwortwechsel den richten Domain Controller zu finden.
Das Produkt Shadow IP-Server von der Firma NTS (www.nts.com) stellt eine ausgereifte NBNS/NBDD Serverlösung dar. Damit wird der Betrieb von Windows und OS/2 Servern in einem NetBIOS over TCP/IP Netzwerk abgedeckt.
Der Shadow IP-Server unterstützt das Microsoft Protokoll (WINS) und das OS/2 Protokoll NBNS/NBDD.

Download Möglichkeit einer Testversion des Shadow IPservers:
http://www.nts.com/evalsoftware/ipservernt/ipservernteval.zip

Ein ausführliche Beschreibung über den Einsatz von OS/2 Warp Server in Verbindung mit dem Shadow IPserver ist im IBM Redbook “SG242009” dokumentiert.
(http://www.redbooks.ibm.com/)

2.3 Beispielkonfiguration, NetBIOS over TCP/IP mit Shadow IP

Die wichtigsten Einstellungen am OS/2 Server und am Shadow IPserver wird mit dieser Beispielkonfiguration beschrieben.

2.3.1 Shadow IP Server Konfiguration

Im Bild 17. und im Bild 18. ist die Server Konfiguration abgebildet.
Das Bild 16. zeigt den IP Manager mit der aktuellen NetBIOS Namensdatenbank.
Das Bild 15. zeigt die IP Shadow Server Console. Diese kann bei der Fehlersuche sehr hilfreich sein.

2.3.2 OS/2 LAN Server Konfiguration

a) Protocol.ini

[tcpbeui_nif]

DriverName = tcpbeui$
Bindings = ,RTL8139_nif
NODETYPE = "H-Node"

(a) ***NBNSADDR = "192.168.2.215"*** (definiert die IP Adresse des Shadow IPservers.)

NBDDADDR = "192.168.2.215"
OS2TRACEMASK = 0x0

NCBS = 225
NAMES = 21

USEMAXDATAGRAM = "NO"
NETBIOSTIMEOUT = 500

NAMECACHE = 1000
PRELOADCACHE = "NO"
NAMESFILE = 0
DATAGRAMPACKETS = 20
PACKETS = 50
INTERFACERATE = 300

(i) *SESSIONS = 130*

(ii) *SELECTORS = 15*

(iii) *NETBIOSRETRIES = 2*

Der Browser Dienst muß gestartet werden, damit sich der Server im NBNS dynamisch registriert!
Command Line Befehl: *C:\net start browser*

Am Servolution Logon Client muß im Parameter NBDDADDR die IP Adresse des Shadow IPservers definiert werden.
NBDDADDR = „192.168.2.215“

2.4 NetBIOS over TCP/IP im DNS Modus

(Neu ab BUILD 2.0.x.5)

Client Konfiguration:
Der Logon Client wird mit dem Parameter „EnableDNS“ eingeschaltet.
Zusätzlich dürfen keine NBDD, NBNS bzw. WINS Server definiert sein. Unter NT 4.0 muß zusätzlich der Schalter „EnableDNS“ in der TCP/IP/WINS Konfiguration eingeschaltet sein!
Voraussetzung ist, daß sämtliche Domänennamen und Servernamen ohne Domain-Suffix über DNS auflösbar sind, z.B. der OS/2 Server „OS2SRV“ muß von der Workstation mit „ping OS2SRV“ auflösbar sein.
Dazu muß die entsprechende DNS Domäne in der TCP/IP Konfiguration als Domain-Suffix eingetragen werden, z.B: comtarsia.com, entspricht: OS2DOM.comtarsia.com.

DNS Server Configuration:
Die IP-Adresse aller Domaincontroller einer Domäne müssen über Round Robbin im DNS Server eingetragen sein. Die Antwort eines DNS Lookups auf den Domänennamen soll die Liste aller Domaincontroller der Domäne sein. Der Logon Client versucht bei jeden Logon bzw. Passwort Wechsel über die DNS Anwort Liste einen Server zu finden.

3. Passwort Synchronisation

(Neu ab BUILD 2.1.x.x)
Die Funktion “Passwort Synchronisation” ermöglicht die Synchronisation des Benutzerkontos an mehreren OS/2 und NT 4.0 Domänen. Voraussetzung ist, daß der Benutzer mit dem gleichen Namen in den anderen Domänen vorhanden ist. Ist das Passwort in allen Domänen synchron, ist der Logon Client in der Lage, bei allen definierten Domänen das Passwort automatisch anzugleichen siehe Bild 20.
Sollte bei einer Domäne das aktuelle Passwort nicht mit der Logon Domäne synchron sein, bekommt der Benutzer ein PopUp siehe Bild 21, in dem er die Möglichkeit bekommt, das aktuelle (bzw. alte) Passwort für diese Domäne einzugeben, und der LogonClient führt einen erneuten Passwortabgleich durch.
Ist Schalter „CheckPWDinAllDomains“ gesetzt, werden bei jedem Logon die definierten Domänen auf die Synchronisation überprüft siehe Bild 19. Sollte das Passwort in einer Domäne nicht synchron sein, bekommt der Benutzer ein Popup siehe Bild 21, bei dem er die Möglichkeit erhält, das aktuelle (bzw. alte) Passwort einzugeben, und der Logon Client führt einen Passwortabgleich durch.
Die zu synchronisierenden Domänen werden folgendermaßen in der Registry definiert.
In diesen Beispiel werden die Domänen OS2DOM1, OS2DOM2 und OS2DOM3 synchron gehalten.

Der Parameter “Type” definiert den Type der Domäne:
“Type” = dword:0 = Auto (nicht implementiert Build 3.0.x.11)
“Type” = dword:1 = OS/2
“Type” = dword:2 = NT / W2K –non ADS
“Type” = dword:3 = ADS (nicht implementiert Build 3.0.x.11)

[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\DomainSync\OS2DOM1]
“Type” = dword:1
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\DomainSync\OS2DOM2]
“Type” = dword:1
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\DomainSync\OS2DOM3]
“Type” = dword:1

4. GroupMapping

Der Schalter „DisableEqualGroupMapping“ schaltet die automatische Gruppenzordnung 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 OS/2 bzw. 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]
"OS2GROUP1"="LOCALGROUP1"
"OS2GROUP2"="LOCALGROUP2"

5. OS/2 Netzwerkapplikationen

Diese Funktion wird von allen Servolution Logon-Clients ab der Version 2.0.x.21 unterstützt.

Der Logon Client stellt eine Funktionalität zur Nutzung von OS/2 Anwendungsdefinitionen unter Windows zur Verfügung. Während des Logins werden die verfügbaren Anwendungen vom Server abgefragt, und es werden entsprechend diverser Einstellung in der lokalen Registry (NWA*) Shortcuts für die Anwendungen erzeugt.

OS/2 Applikationsdefinition	Windows-Shortcut
ApplikationsID	-
Beschreibung	Name des Shortcuts(*.lnk) Beschreibung des Shortcuts
Programmposition/Befehl/Parameter	wie OS/2
Arbeitsverzeichnis	Ausführen in

Falls im Verzeichnis der Programmposition ein Icon mit dem Namen APPLIKATIONSID.ico hinterlegt ist, wird dieses für den Shortcut verwendet.
Alle benötigten Icons werden vom OS/2-Server auf den lokalen Rechner ins das unter NWAIconPath definierte Verzeichnis kopiert.
Falls im Verzeichnis der Programmposition ein Shortcut mit dem Namen APPLIKATIONSID.lnk hinterlegt ist, wird dieses verwendet, und somit alle anderen applikationsspezifischen Parameter ignoriert.

Die Shares für Programmposition sowie Arbeitsverzeichnis müssen dem Benutzer bereits mit dem richtigem Laufwerksbuchstaben zugeordnet sein (Es wird auch die OS/2 Netwerkapplikations-Option „on Requester“ unterstützt).

Erstellen und Löschen der Shortcuts:
Nach einem erfolgreichen Login des Benutzers werden ev. noch vorhandene Shortcuts, die dem Filter entsprechen, gelöscht (falls der PC nicht ordnungsgemäß abgedreht wurde) und danach dem Filter entsprechend wieder angelegt, bzw. falls am OS/2-Server ein lnk-File vorhanden ist, wird dieses nur kopiert. Andere Shortcuts in diesem Verzeichnis bleiben unberührt, solange der Name nicht mit dem Filter kollidiert.

Die unter NWAFolderNamePath sowie NWAFolderName definierten Verzeichnisse werden mit Administrator-Rechten erzeugt, und können somit auch auf Verzeichnisse zeigen, wo der User normalerweise keine Schreibrechte hat (z.B.: %ALLUSERSPROFILE%).

Der Logon-Client trägt die folgenden dynamischen Userinformationen in die Registry ein, um bei Bedarf eine weitere Verarbeitung durch Scripts zu ermöglichen:
Netzwerkapplikationen: PCS\GINA\OS2ENVIRONMENT\NETAPPS
Shares: PCS\GINA\OS2ENVIRONMENT\NETDRIVE
Homedir: PCS\GINA\OS2ENVIRONMENT\HOMEDRIVE

6. Erklärung:

6.1.1 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.

6.1.2 GPO:

GPO steht für "Windows 2000 Group Policy".

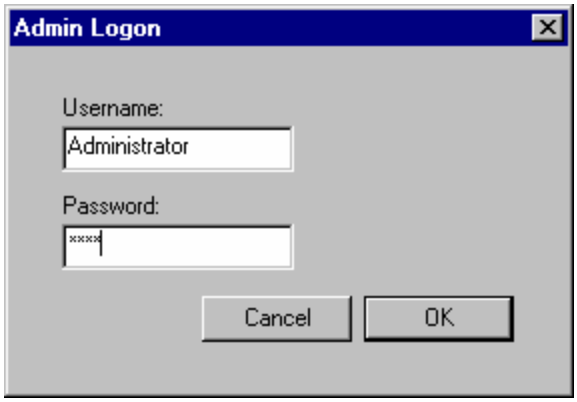
6.1.3 SAS:

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

7. Screen Shots

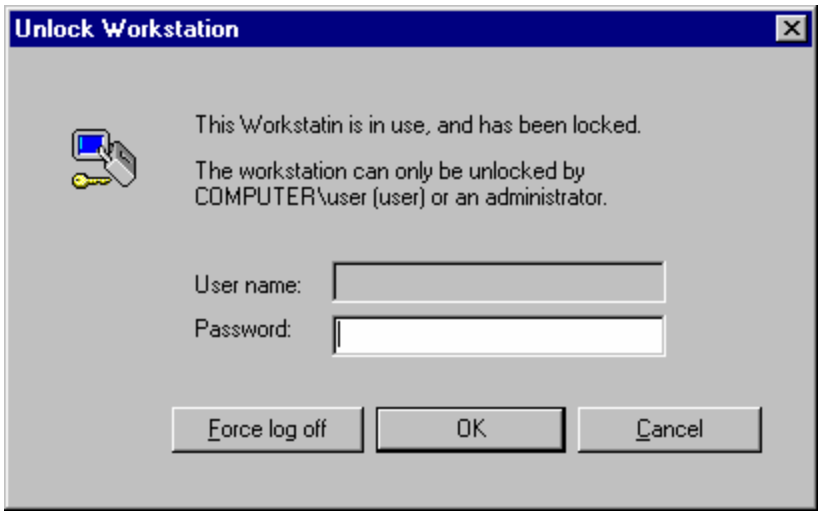
7.1.1 Bild 1. Logon Dialog

7.1.2 Bild 2. Admin Logon Dialog

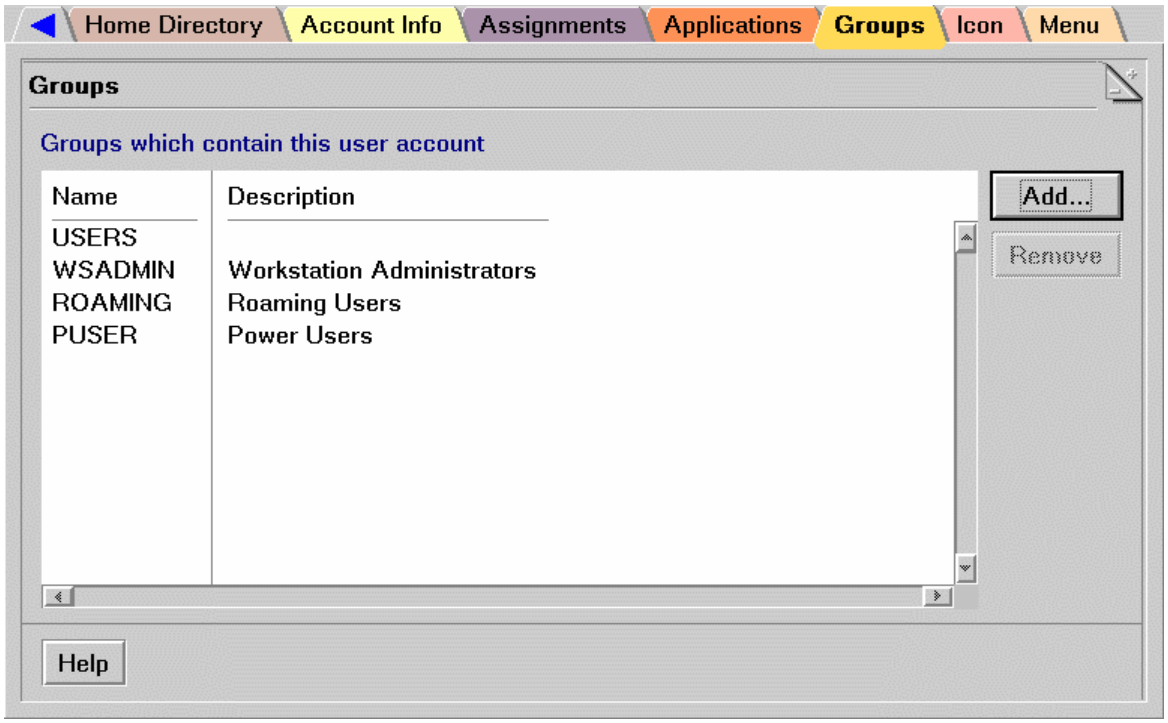


7.1.3 Bild 3. ON SAS Dialog

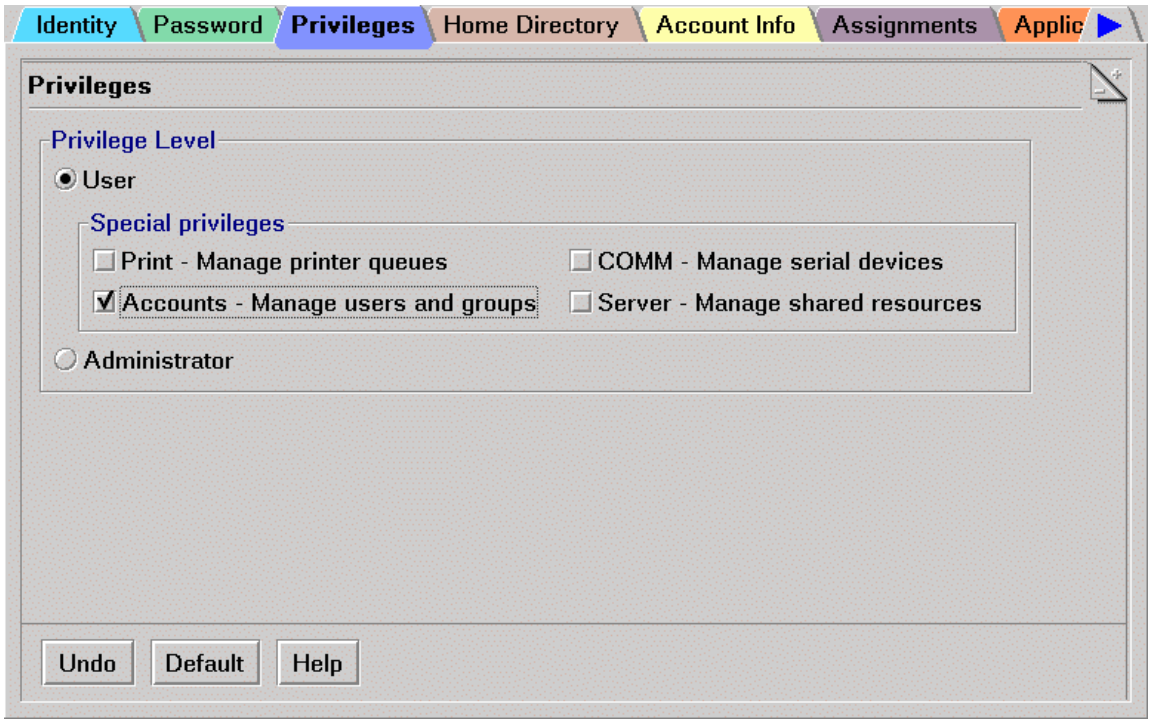
7.1.4 Bild 4. Unlock Dialog



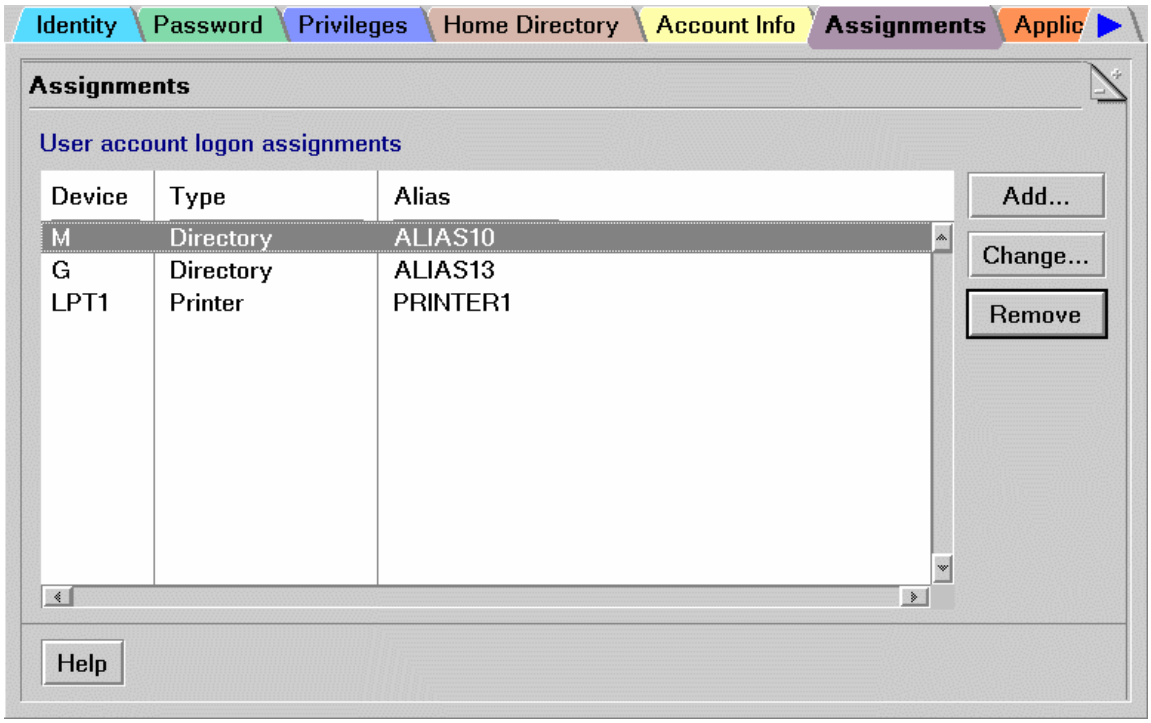
7.1.5 Bild 5. LAN-Server Gruppen Verwaltung



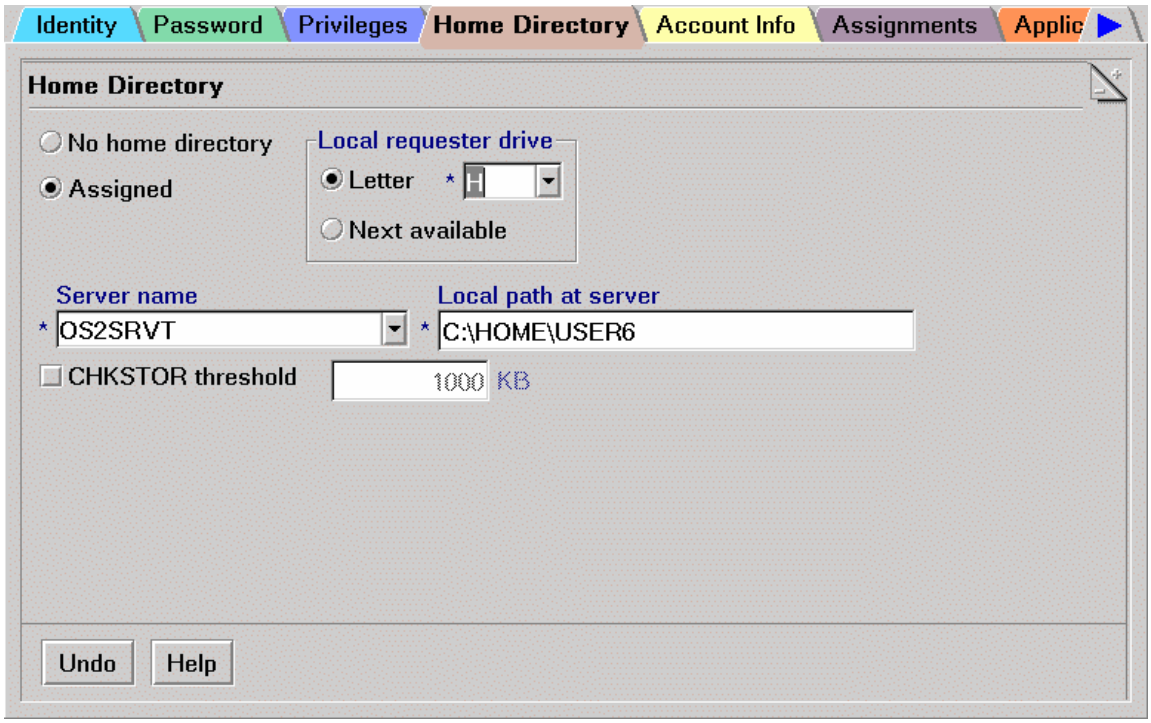
7.1.6 Bild 6. LAN-Server Benutzer Berechtigungen



7.1.7 Bild 7. LAN-Server Benutzer Verbindungen



7.1.8 Bild 8. LAN-Server Benutzer Homedirectory



7.1.9 Bild 9. LAN-Server Audit Log

User ID	Workstation	Event	Date	Time
USER6	PCS71P	Session logon	26.09.00	10:55:49
USER6	PCS71P	Logon to network	26.09.00	10:55:49
USER6	PCS71P	Session logon	26.09.00	10:55:50
USER6	PCS71P	Session logoff	26.09.00	10:55:50
***	PCS71P	Session logon	26.09.00	10:55:54
USER6	PCS71P	Logoff from network	26.09.00	10:57:56

7.1.10 Bild 10. Windows Workstation „net use“

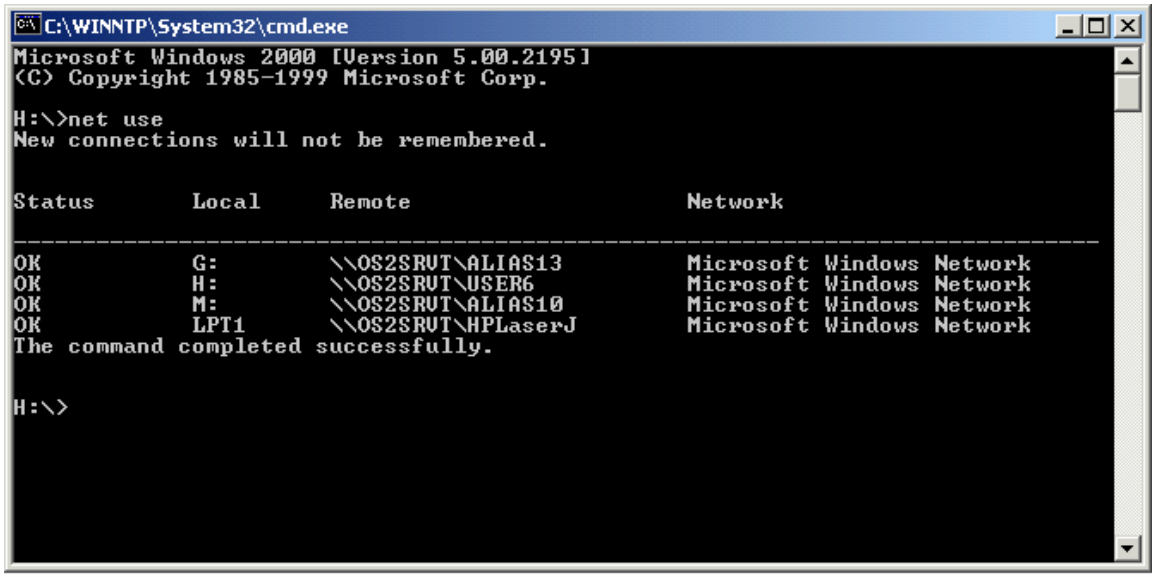
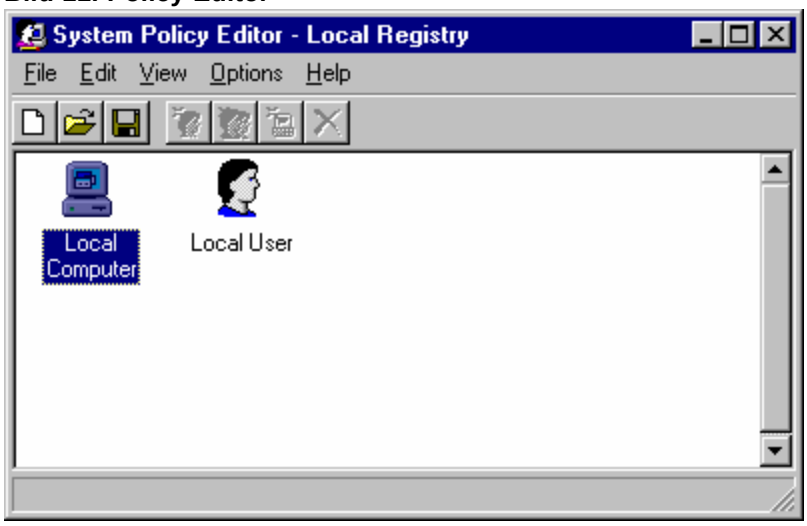
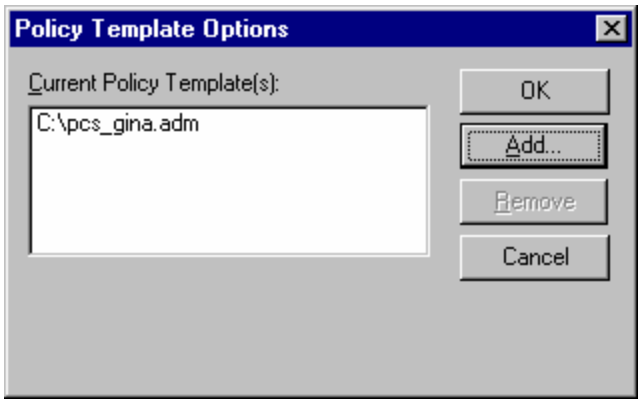


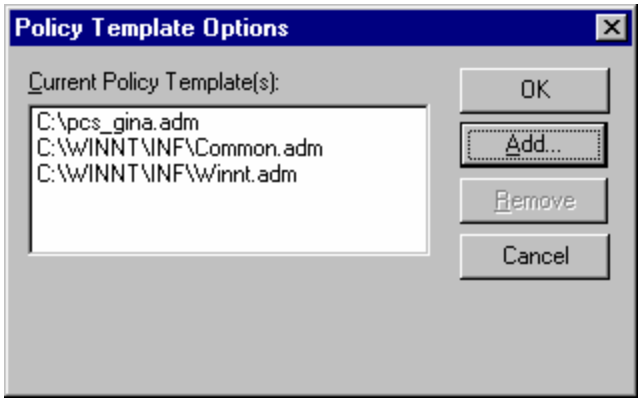
Bild 11. Policy Editor



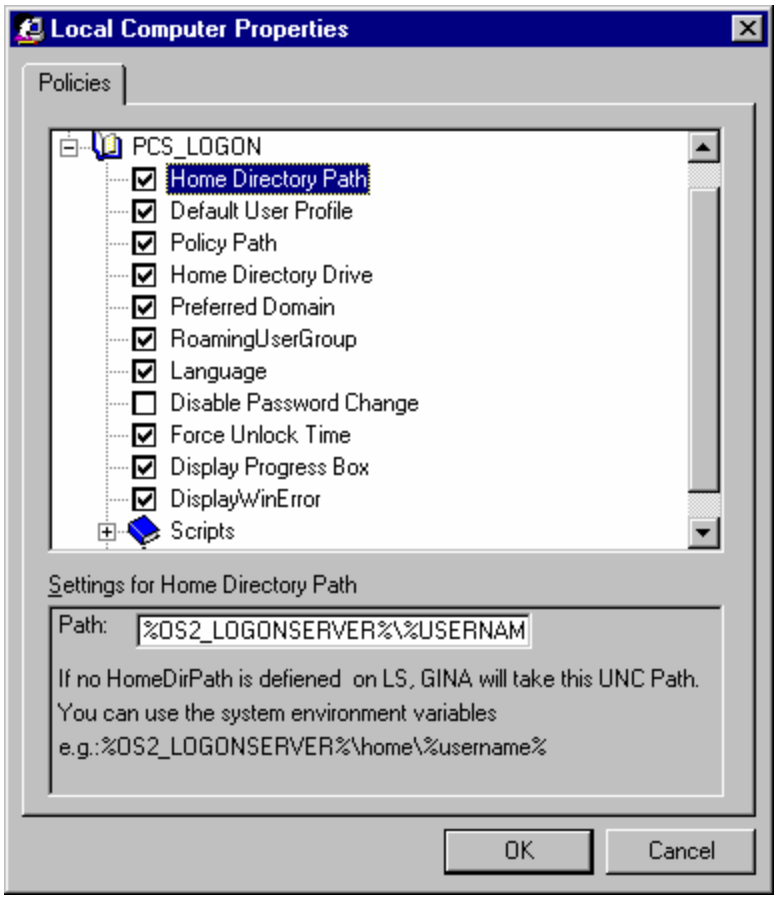
7.1.11 Bild 12. Policy Editor GINA Template



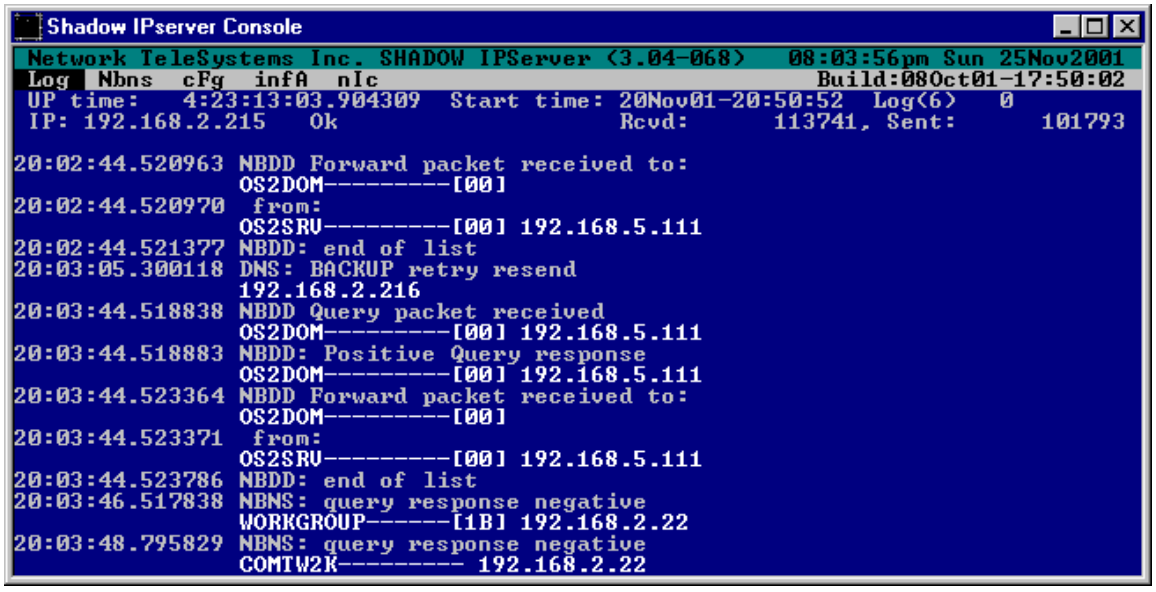
7.1.12 Bild 13. Policy Editor GINA und Windows Templates



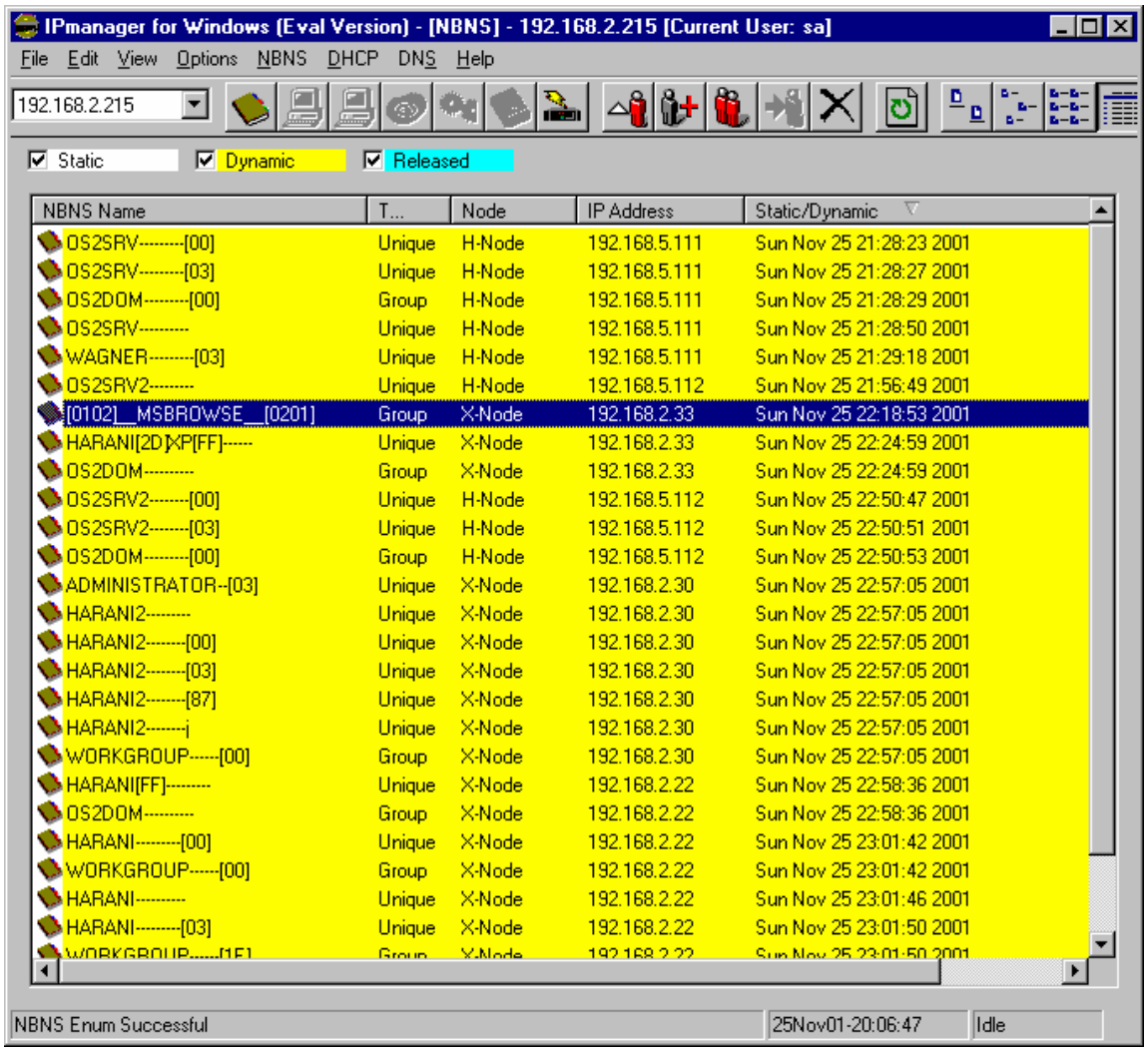
7.1.13 Bild 14. Policy Editor GINA Konfiguration



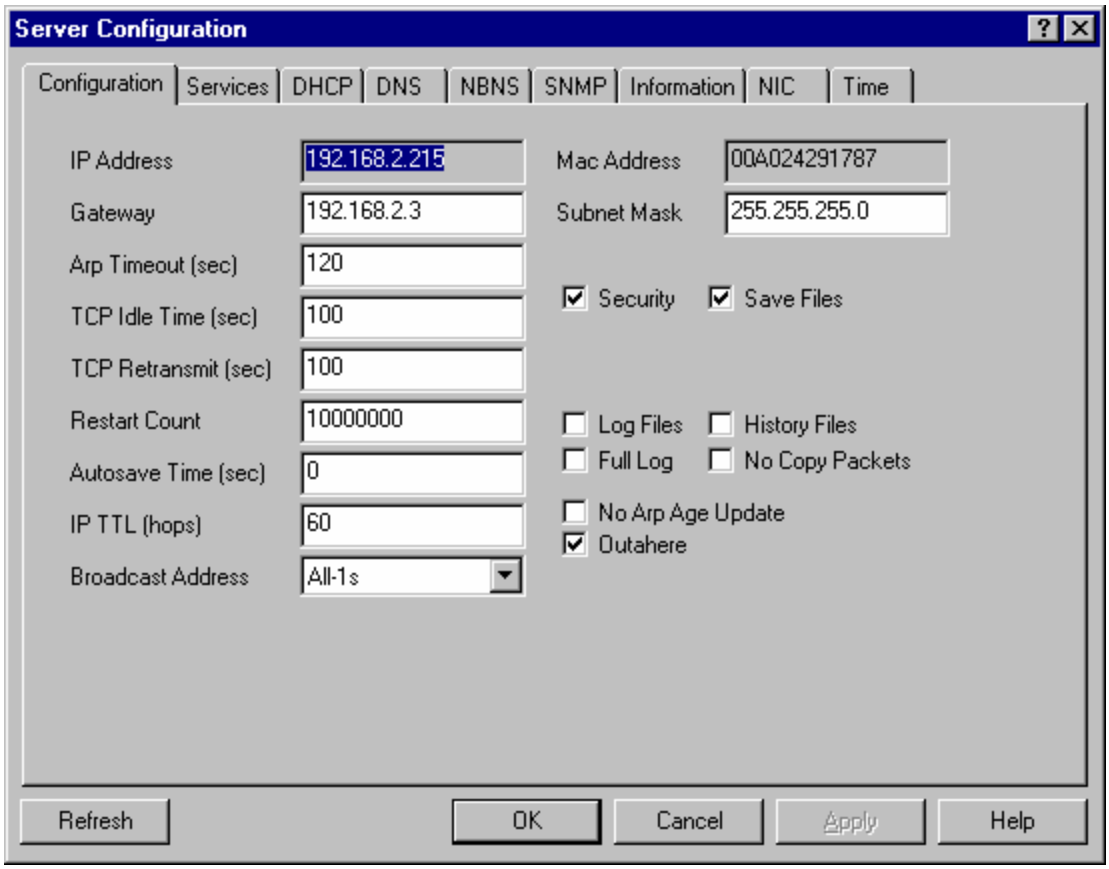
7.1.14 Bild 15. Shadow IPserver Console



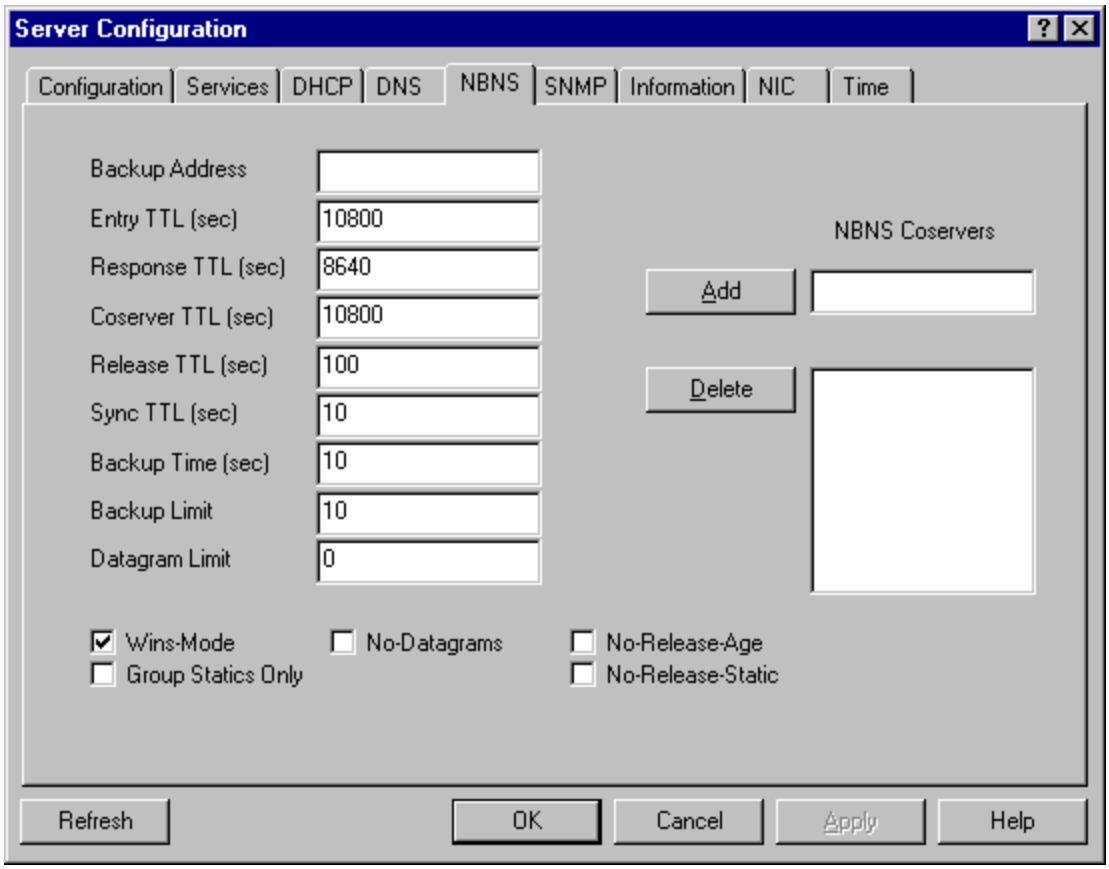
7.1.15 Bild 16. Shadow IPserver - IP Manager



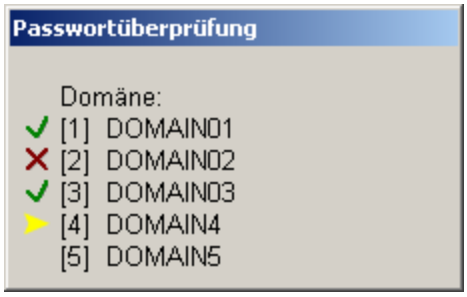
7.1.16 Bild 17. Shadow IPServer – Server Configuration



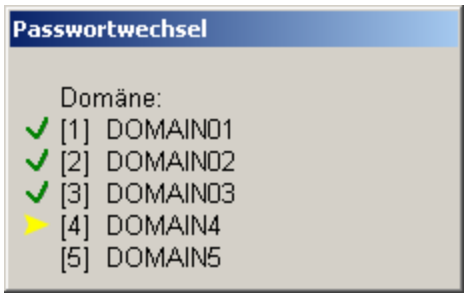
7.1.17 Bild 18. Shadow IPServer – Server Configuration - NBNS



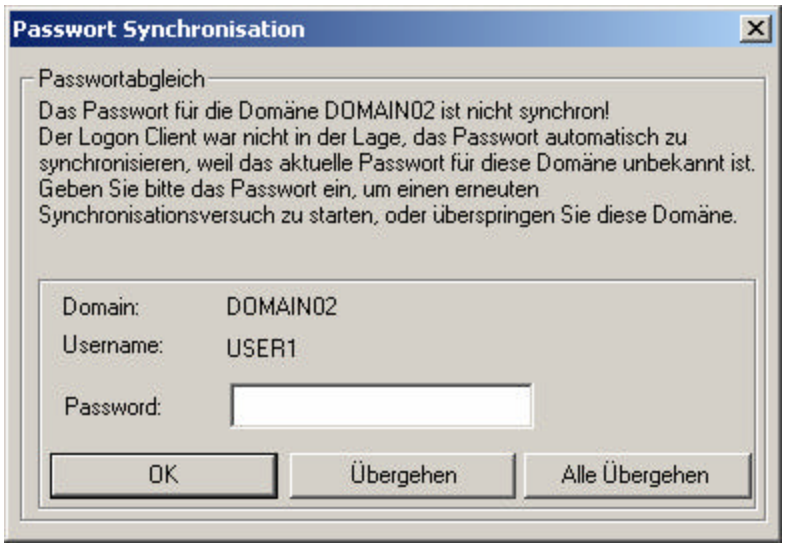
7.1.18 Bild 19. Passwort Synchronisation - Passwortüberprüfung



7.1.19 Bild 20. Passwort Synchronisation – Passwortwechsel



7.1.20 Bild 21. Passwort Synchronisation – Passwortabgleich



7.1.21 Bild 22. Erweiterter LDAP Logon