Comtarsia Logon Client 2006

Technical Description

Version: 4.1.13.4, 04-Jul-2006

Content

1. Description

Comtarsia Logon Client 2006, LDAP Logon Client Module for Windows 2000 and Windows XP --- Build 4.1.13.4. (English and German).

The Comtarsia Logon Client 2006 for Windows allows for Windows 2000 and Windows XP Workstations as well as Terminal Service/Citrix sessions a primary authentication on a LDAP Directory.

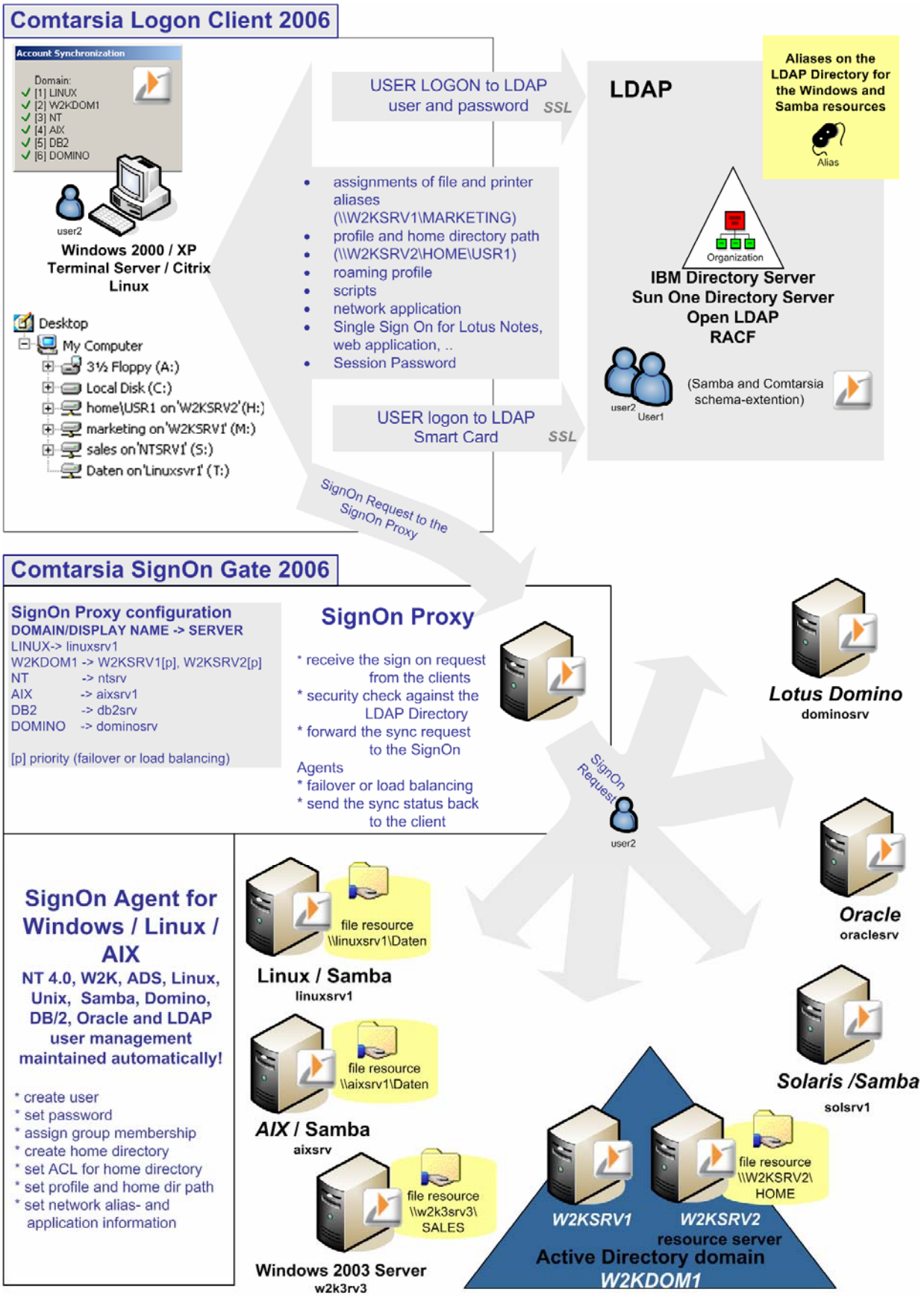
The additional product “Comtarsia SignOn Gate 2006” provides the further possibility to manage user accounts automatically on Windows servers, Windows domains (NT 4.0, W2K, W2K3/ ADS) and UNIX servers and to integrate them as resources in the central LDAP user management.

The products Comtarsia Logon Client and the Comtarsia SignOn Gate are optimal LDAP integration tools and offer also separate user management and resource management maintenance. This means a determining independence compared to proprietary solutions. Herewith stands Comtarsia also for Single Sign On, Centralized User Management and Security Management.

Please visit our web sites for further information about the Comtarsia SignOn Solutions .

http://signon.comtarsia.com

1.1 Comtarsia SignOn Overview



1.2 Server Requirements

LDAP:
Please see the manuals Comtarsia Logon Client 2006 and LDAP
http://signon.comtarsia.com/main/en/Manuals

1.3 Client Requirements

W2K Professional or Windows XP Professional, Windows Terminal Server 2003 (German or UK version)

1.4 Installation

1.4.1 Installation using Installer

Execute **CLC_2006-4.1.X.4.exe** and follow the on-screen instructions.
All parameters can also be modified after installation with the Logon Client Configurator. (Please see Comtarsia Logon Client LDAP manual, chapter 2)

The manual focuses on the registry parameters and is provided for the installation in big networks via software distribution.

1.4.2 Installation via Software Distribution

Call the Logon Client Installer with the parameter “MODE=UNPACK”.
This creates a directory with the name „CLC_2006-VERSION“, in which all files are provided which are necessary for a software distribution.

The installations consists of two steps, first the copying of the files and second the setting of the registry keys.

The following files are needed in the directory „%SYSTEMROOT%“ on the target system:

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

The following files are needed in the directory „%SYSTEMROOT%\SYSTEM32“on the target system:

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

The files CLCConfigurator.exe, as well as the Logon Client manuals are not needed on the target system.

The files for the SSL communication (certificate, Private Key, one or more CA-certificates) with the Proxy can be copied into an arbitrary folder, the paths then have to be set accordingly in the registry (“HKEY_LOCAL_MACHINE \Software\PCS\GINA\ComtSyncClient” [tlsCAFile/tlsCertFile/tlsKeyFile]). The default path is „%PROGRAMFILES%\Comtarsia\Logon Client 2006“.

In order to create a registry configuration, it is recommended to use the Logon Client Configurator and to subsequently export the registry branch under “HKEY_LOCAL_MACHINE \Software\PCS\GINA” and to import it to the workstations.

Furthermore registry key “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL” has to be set to “pcs_gina.dll”.

1.5 Uninstalling

Removal of Logon Client is achieved via "Control Panel / Add/Remove Programs".

Software Distribution

For software distribution execute the script ***uninstall.cmd***.
For uninstalling local administration permissions are required.

1.6 Parameter Description – General Settings

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

1.6.1 EnableSyncClient

„EnableSyncClient“=DWORD:1
This switch enables the Comtarsia SignOn Gate.
(refer to SignOn Gate Support)
Default: 0

1.6.2 PolicyPath

Defines the full path of the policy file.
e.g.: "PolicyPath"="%LOGONSERVER%\\netlogon\\ntconfig.pol"
(refer to Windows Policy)

1.6.3 DefaultUserProfile

This key defines the path for the default profile. If this path cannot be found the local default profile is used.
e.g.:"DefaultUserProfile"="%OS2_LOGONSERVER%\\netlogon\\default profile"

1.6.4 ProfilePath

Defines the path for the profile:
e.g. “PofilePath”=\\SERVER1\profiles\%USERNAME%
(refer to RoamingUserGroup)

1.6.5 HomeDirDrive

"HomeDirDrive"="H:"
If no drive letter is defined on the LAN Server, the Logon Client will use this drive letter.

Note: "HomeDirPath" is mandatory!
(refer to Figure 8)

1.6.6 HomeDirPath

If no home directory path is defined for the LAN Server domain it will be attempted to connect this network path as home directory.
e.g.: "HomeDirPath"="%OS2_LOGONSERVER%\\%USERNAME%"

Note: "HomeDirDrive" is mandatory!
(see Figure 8)

1.6.7 InitScript

This script is executed with system privileges during booting.
e.g.:“InitScript"="c:\cmd\init.cmd"

1.6.8 PreSystemLogonScript

This script is executed with system privileges at logon time.
The local user logon has not yet been carried out.
e.g.: "PreSystemLogonScript"="c:\cmd\cleanup.cmd"

1.6.9 SystemLogonScript

This Script gets executed at logon with system privileges.
e.g.:"SystemLogonScript” = “c:\cmd\system.cmd"

1.6.10 SysUsrLogonScript

This script is executed with system privileges at logon time within the user environment.
e.g.:"SysUsrLogonScript“=“c:\system.cmd"

1.6.11 UserLogonScript

This script is executed with user privileges at logon time in the user environment.
e.g.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.12 LocalUserLogonScript

This script is executed with user privileges at a local logon in the user environment.
e.g.: "LocalUserLogonScript"="c:\scripts\localLogon.cmd"

1.6.13 AdminUsrLogonScript

This script is executed with administrator privileges at logon time in the user environment.
e.g.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"
(Attention! This script is executed only at a domain logon or LDAP logon!)

1.6.14 LocalAdminUsrLogonScript

This script is executed at local logon time in the user environment with admin-privileges.
e.g.:
"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.15 UserLogoffScript

This script is executed with user privileges at logoff time in the user environment.
e.g.:"UserLogonScript"="%LOGONSERVER%\ibmlan$\dcdb\users\%USERNAME%\profile.cmd"

1.6.16 UserLogoffScriptErrorlevel

"UserLogoffScriptErrorlevel"=DWORD:0
By setting this value to “1” an error level of the UserLogoffScript not equal to zero will cause the logon client to cancel the logoff process.

1.6.17 SystemLogoffScript

This script is executed with system privileges at logoff time after the user has logged off (the environment will no longer be available).
e.g.: "systemLogoffScript"="c:\cmd\cleanup.cmd"

1.6.18 Script Overview:

	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
Executed On										
Local Logon	●	●	●		●	●		●	●	●
LDAP Logon	●	●	●	●		●	●		●	●
WTS / CITRIX Logon	●	●	●			●	●		●	●
WTS / Citrix Passthrough Logon	●	●	●			●	●		●	●
Citrix Anonymous Logon	●	●	●			●	●		●	●
Time of execution (before ➔● after ●➔)										
SystemBoot	●➔									
WTS/Citrix Session establishment	●➔									
The Logon Dialog appears	➔●									
Successful Local User Password Verfication (Local Logon)	➔●	●➔								
Successful LDAP User Password Verfication		●➔								
User Environment Preparation		➔●								
Load User Environment			●➔	●➔	●➔	●➔				
Load User Profile			●➔	●➔	●➔	●➔				
Assign Network Aliases			➔●	●➔		●➔	●➔			
Assign Network Applications			➔●	●➔		●➔	●➔	●➔		
Release the User Desktop				➔●	➔●	➔●	➔●	➔●		
User logoff or shutdown attempt									●➔	●➔
Close the User Desktop									➔●	●➔
WTS/Citrix Session Termination									➔●	➔●
Permissions										
Local System Permissions	●	●	●			●				
Local User Permissions							●	●		
Local Administrator Permission				●	●					
System Environment	●	●	●			●			●	●
User Environment				●	●		●	●		
Network Access				●	●		●	●		
Access to HKEY_CURRENT_USER				R/W	R/W		R/W	R/W	R/W	
Access to HKEY_LOCAL_MASCHINE	R/W	R/W	R/W	R/W	R/W	R/W	R/W*	R/W	R/W*	R/W
Access to SYSTEMROOT	R/W	R/W	R/W	R/W	R/W	R**	R**	R**	R**	R/W

* Depends on the effective User Policy
** Depends on the effective User File Access Rights

1.6.19 ScriptTimeout

"ScriptTimeout"=19
Number of seconds that scripts are waited for.

1.6.20 DisplayScriptError

„DisplayScriptError“=DWORD:1
A pop-up message appears if a script does not finish within the defined interval. Also refer to ScriptTimeout parameter and Script Overview.

1.6.21 DisablePasswordChange

"DisablePasswordChange"=1
„0“ allows the user to change the password (the logon client will change the LAN Server and the local password).
“1“ does not allow the user to change the password and causes a POP-UP message to appear the text of which can be defined with the parameter “ChangePasswordInfo".

Example: „ChangePasswordInfo“=“Password change is not allowed under Windows and only possibly by using the Web-Interface!“

1.6.22 ForceUnlockTime

"ForceUnlockTime"=258
This value defines the time, specified in seconds, after which a “forced logoff” in the locked mode will be possible.
If it is set to „0“ this function is disabled.
(see Figure 3 and Figure 4)

1.6.23 DisplayWError

"DisplayWError"=1
If this value is “1” internal errors will be displayed with a POP-UP message. If it is “0” then internal errors will only be written to the file “%systemroot%\gina.log”.
This function can be turned on or off in the logon dialog by simultaneously depressing the L and Shift keys and clicking into the window with the left mouse button.

1.6.24 DisplayProgressBox

"DisplayProgressBox"=DWORD:1
Use this entry to enable or disable the logon progress dialog.

1.6.25 RoamingUserGroup

"RoamingUserGroup"="USERS"
A group membership on the LAN server defines whether or not a user is provided a roaming profile.
This value defines the LAN Server group for roaming users.
For example if there is a defined group ROAMINGP then all users that should have a roaming profile in their home directory will be members of this group.
"RoamingUserGroup"="ROAMING"
If this value is set to the group “USERS” then all users on the LAN Server will be treated as roaming users.
(see Figure 5)

1.6.26 AdminLogonGroup

"AdminLogonGroup"="ADMIN"
default=""
A group membership on the LAN server / LDAP defines which user is authorized for Admin Logon. E.g. the group „ADMIN“ on the LAN server / LDAP is defined, and the user specified in the group may proceed Admin Logon.
Please see „Admin Logon“
Is this parameter not set, Admin Logon is deactivated.

1.6.27 Language

"Language"="german"
This defines the language used for dialog messages.
Choose between „english“ and „german“.

1.6.28 PanelBitmap

“PanelBitmap” = “c:\logo.bmp”
This parameter defines the bitmap to display instead of the Comtarsia Logo on the logon panel. See Figure 1.
Format: Bitmap 450x120 RGB

1.6.29 AlphaNumPwd

"AlphaNumPwd"=dword:1
Use this parameter to restrict the Logon Client password to alphanumeric characters. (a-z u. 0-9)

1.6.30 DontDisplayLastUserName

„DontDisplayLastUserName“=dword:1
This parameter disables display of the last user name in the logon dialog.

1.6.31 DisableMsGina

„DisableMsGina“=DWORD:1
This parameter turns off the possibility of switching to the Microsoft Logon Dialog. Refer to Microsoft GINA.

1.6.32 DisableEqualGroupMapping

„DisableEqualGroupMapping“=dword:1
This parameter turns off the group allocation by the same name and turns on manual group allocation. Refer to the function GroupMapping.

1.6.33 GroupAdministrator

"GroupAdministrator"="ADMIN"
This parameter defines the LDAP group of users which get administrative privileges. This parameter has to be defined at the same time as: DisableEqualGroupMapping“=DWORD:1

1.6.34 GroupPowerUser

"GroupPowerUser"="PUSER"
This parameter defines the LDAP group of users which get power user privileges. This parameter has to be defined at the same time as: DisableEqualGroupMapping“=DWORD:1

1.6.35 NWAFolderActive

„NWAFolderActive“=DWORD:1
This switch activates LDAP network application support.
Refer to chapter Network Applications

1.6.36 NWAFolderNamePath

„NWAFolderNamePath“=“%USERPROFILE%\Desktop“,“%ALLUSERSPROFILE%\Desktop“
This defines the directories in which a folder named “NWAFolderName” will be created. If this parameter is not defined the user desktop will be used per default.

1.6.37 NWAFolderName

„NWAFolderName“=“OS2-Anwendungen“
In this folder the shortcuts for network applications will be created.
If this parameter is not set, all shortcuts will be created in the folder defined by NWAFolderNamePath.

1.6.38 NWAAppFilter

„NWAAppFilter“=“*W2K*“
Only applications defined by this application filter with a suitable application ID will be created.

Filter matching IDs
„XP“ XP
„XP*“ XP, XPAA, XPBBB
„*XP“ XP, AAXP, BBBXP
„*XP*“XP, XPAA, AAXP, XPBBB, BBBXP

1.6.39 NWADefaultIconPath

„NWADefaultIconPath“=“\\os2srv\daten\icons“
Optional. An absolute path to an icon file which will be used for shortcuts without an icon of their own.

1.6.40 NWADefaultIcon

„NWADefaultIcon“= “default.ico“
Optional. An UNC path where a program icon will be searched for if none is found at the program location.

1.6.41 NWAIconPath

„NWAIconPath“=“c:\temp“
Optional. An absolute path to a directory where the icons are stored temporarily.
Default: c:\

1.6.42 NWATimeout

„NWATimeout“=dword:60
The maximum runtime for the “Network Applications” in seconds.

Default: 60

1.6.43 MinPwdLen

„MinPwdLen“=dword:8
Defines the minimum amount of character of the new user password at password change on the LDAP server.
Default:0

1.6.44 EnableDomainLogon

„EnableDomainLogon“=DWORD:1
default = 0

This switch defines, if the Logon Client uses for the Windows User-Session a local user, or a Windows domain user. If the value is set to “1” the Logon Client tries after each successful LDAP logon to execute a Windows Logon with the domain specified in the parameter “strLocalDomain”.
So that instead of the local user a domain user can be used, the workstation has to be member of this domain and the user with the same password has to exist already in the Windows domain. This mode is therefore only executable together with the product Comtarsia SignOnGate, which automates the user management in the Windows domain.
If this parameter is set to “0”, the Logon Client uses the local user.

1.6.45 strLocalDomain

„strLocalDomain“=“W2KDOM“
default = “ “

This parameter defines the local domain for the Windows Logon Session in the DomainLogon- as well as in the Terminal Server Mode.

1.6.46 WTSMode

„WTSMode“=DWORD:1
default= DWORD:0
If the Logon Client is installed on a Terminal Server this value has to be set to “1”.
In the Terminal Server Mode the additional product Comtarsia SignOn Gate for the automatic user management on the WTS Standalone Server or on the domain controller for the automatic user management must be already installed!
The domain name must be defined in the parameter “strLocalDomain”.

1.6.47 ExpireTime

“ExpireTime”=DWORD:3600 (1 hour)
Default = DWORD:0

Through this parameter the time period can be defined (in seconds) while the user account, created by the Logon Client on the local machine, is available. After this time period the account will expire through the operating system, and the user can not log on locally.
This expiry time is updated at each successful LDAP logon.
When "ExpireTime" = 0, this function is deactivated and all users will be created without expiry time.

1.6.48 RemoveUser

„RemoveUser“=dword:2
Default=dword:0

If this parameter is set, the user created by the Logon Client at the logon will be deleted from the local machine at logout.
When RemoveUser = 1, only the user will be deleted, if RemoveUser = 2, the locally saved user profile will be deleted as well.
When RemoveUser = 0, this function is deactivated.
NOTE: Users such as Administrator, or user not created by the Logon Client, will NOT be deleted.

1.6.49 AutoLogonUserName

„AutoLogonUserName“=“U00101“

If this parameter is set, the logon client will switch to “AutoLogon Mode”. With this parameter the user name for the automatically logon can be defined.
If this parameter is not defined or blank the function „Autologon“ will be disabled.
The parameters AutoLogonPassword and AutoLogonDomain must be defined too.

1.6.50 AutoLogonPassword

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

If the function „Autologon“ is activated via the parameter „AutoLogonUserName“, the Autologon password must be defined via this parameter.

The password can be set in clear text or can be set encrypted via the tool „SetAutoPwd.exe“ (syntax: SetAutoPwd mypassword).

1.6.51 AutoLogonDomain

„AutoLogonDomain“=“DOM01“
If the function „Autologon“ is activated via the parameter „AutoLogonUserName“, the Autologon Domain must be defined via this parameter.

For LDAP logon the string „LDAP LOGON“ and for local logon the string „LOCAL WORKSTATION“ must be used.

1.6.52 UserNameCase Policy

„UserNameCasePolicy“=DWORD:1

This parameter defines the possible upper and lower case at the input of the username at the logon dialog.

0 = allow upper and lower case
1 = only allows upper case
2 = only allows lower case

Note!
To set this parameter to “allow upper and lower case” is only recommended, if the primary logon domain, respectively the LDAP server is case-sensitive! For example: If the LDAP server accepts the input “user1” or “User1” for the user object “USER1”, it is not guaranteed, that the user is right and uniformly synchronised on a non case-sensitive resource system by the module Comtarsia SignOn Gate.

1.7 LDAP – Logon Client Settings

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\LDAP

1.7.1 LDAPVersion

„LDAPVersion“ = DWORD:3
Specifies which LDAP protocol version is used. Logon Client supports LDAP version 2 (refer to http://www.ietf.org/rfc/rfc1777.txt) as well as LDAP version 3 (refer to http://www.ietf.org/rfc/rfc2251.txt).
All currently shipping servers support LDAP version 3 which also allows for automatic recognition of the LDAPBaseDN (refer to LDAPBaseDN).

1.7.2 LDAPBaseDN

“LDAPBaseDN” = ""
Defines the LDAP base DN e.g.: „dc=comtarsia,dc=com“

How Logon Client discovers the LDAPBaseDN:
If LDAPBaseDB is set in the registry it will be used.
If the LDAP server supports LDAP version 3 and the LDAP version is set to „3“ in the registry, Logon Client tries to discover the BaseDN via LDAP query.
Note: Most LDAP server support more than a single BaseDN. You have to make sure that the BaseDN to be used by the Client gets returned as first entry. You can check this for example with an LDAP browser. (http://www-unix.mcs.anl.gov/~gawor/ldap/)
If no BaseDN was found the BaseDN is tried to be constructed out of the local computer's domain name.
e.g.: domain = „comtarsia.com“
BaseDN = „dc = comtarsia, dc= com“

1.7.3 LDAPUserDNPrefix

“LDAPUserDNPrefix “= "uid="
The UserDN is constructed out of multiple parts:
LDAPUserDNPrefix + USERNAME + LDAPUserDNSuffix + „,“ + LDAPBaseDN

LDAPBaseDN only gets added to the UserDN if LDAPAppendBaseDN is activated.

You have to set the following for a User-DN “cn=User1,ou=People,dc=comtarsia,dc=com”:
LDAPUserDNPrefix=’’cn=“
LDAPUserDNSuffix=“,ou=People“
LDAPBaseDN=’dc=comtarsia,dc=com“

1.7.4 LDAPUserDNSuffix

“LDAPUserDNSuffix” = ""
see LDAPUserDNPrefix

1.7.5 LDAPAppendBaseDN

“LDAPAppendBaseDN” = DWORD:1
If this setting is activated (1) the LDAPBaseDN gets appended to the UserDN.
Default: 1

1.7.6 LDAPEnableSSL

“LDAPEnableSSL” = DWORD:1

0 = no SSL
All communication of client and LDAP server is sent in plain text. This option is useful for testing only and should never be used in production environments.

1 = SSL without "trusted server certificates"
Communication with the LDAP server gets encrypted.
The server certificate does not get verified and the client does not need a certificate.

2 = SSL with "trusted server certificates"
Logon Client verifies the LDAP server certificate. To use this option a CA certificate has to be installed (refer to LDAP-SSL). The client does not need its own certificate.

3 = SSL with "trusted client certificates"
Logon Client verifies the LDAP server certificate and sends its own certificate to the server. This option requires a CA certificate as well as a client certificate. (refer to LDAP-SSL)

1.7.7 LDAPTimeout

“LDAPTimeout” = DWORD:30
Timeout in seconds per LDAP server. If Failover (see LDAPEnableFailover) is activated and more than one LDAP server is entered, automatically the next one is tried after failure to connect to one server within this interval. (refer to LDAPEnableFailover as well as LDAP LoadBalancing and Failover)

1.7.8 LDAPServerTyp

“LDAPServerTyp” = DWORD:1
This setting configures the type of the LDAP server
Currently only IBM RACF (4) is treated differently.

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

1.7.9 LDAPEnableFailover

“LDAPEnableFailover” = DWORD:0
Activates (1) Logon Client Failover and Load Balancing Functions. (refer to LDAP LoadBalancing as well as Failover and LDAPEnableDNS)

1.7.10 LDAPEnableDNS

"LDAPEnableDNS" = DWORD:0
If this option is activated no LDAP servers are read from the registry but a DNS server is queried instead.
The client domain has to be configured appropriately, either as „Primary DNS Suffix" or „Connection-specific DNS Suffix".
SRV records for the LDAP servers have to be added to the domain's zone file. (refer to LDAP LoadBalancing and Failover as well as LDAPEnableFailover).

1.7.11 LDAPGroupTypes

"LDAPGroupTypes" = DWORD:3

This parameter defines in which LDAP group object classes the logon client should search for a user membership. This value is a bitfield. The following values are defined:

object class	value
groupOfNames	1
groupOfUniqueNames	2
posixGroup	4

On a Lotus Domino LDAP server the object class is not used by the Logon Client, even if it is specified.
If there is no registry key, the default value is set to '3'.

1.7.12 LDAPOUSearchList

"LDAPOUSearchList" = MULTI_SZ:""
This parameter defines an OU Search List. The OUSearchList is a list of OU's, which is used instead of the OU of the Logon Panel, to automatically construct the UserDN.
The Logon Client tries to login with all OUs in a defined order until one login is successful.
Each OU string is separated with ";", for example LDAPOUSearchList="at;de;uk"

1.7.13 AttributeBasedGroups

"AttributeBasedGroups" = MULTI_SZ:""

This parameter adds dynamic groups to the current user considering LDAP attributes.

Example:
AttributeBasedGroups: physicalDeliveryOfficeName=ATQA%s01_G

At the user login the Logon Client tries to read the LDAP attribute "physicalDeliveryOfficeName" out of the user object and afterwards adds the dynamic group „ATQA%s01_G" to the user, in which the content of the attribute „physicalDeliveryOfficeName" replaces "%s". Multivalue LDAP attributes with up to 10 entries are supported too.
There is also the possibility to cut off the first character of the LDAP attribute by placing a ">" after the "=".

Example:
AttributeBased Group: physicalDeliveryOfficeName=**>**ATQA%s01_G

1.7.14 AttributeBasedEnvironment

"AttributeBasedEnvironment" = ""

This parameter allows the setting of environment variables on workstations dynamically considering specific LDAP attributes.

Example:
AttributeBasedEnvironment: physicalDeliveryOfficeName

At the user login the Logon Client tries to read the LDAP attribute "physicalDeliveryOfficeName" out of the user object and exports the content of this attribute as environment variable "physicalDeliveryOfficeName".

If needed a Mapping can be made, for example:
AttributeBasedEnvironment: physicalDeliveryOfficeName=officeName

In this case the content of the LDAP attribute „physicalDeliveryOfficeName" is exported as environment variable "officeName".

There is also the possibility to cut off the first character of the LDAP attribute by placing a ">" after the "=".

Example:
AttributeBasedEnvironment: physicalDeliveryOfficeName=**>**officeName

1.7.15 HwAdminGroup

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadmingroup"="hwadmin"

This parameter defines which group the user has to be member off, so it can be HWadmin (Hardware-Administrator).

1.7.16 HwAdminAttribute

KEY: HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA
"hwadminattribute"="machines"

Determines, which attribute of the LDAP-user object contains a list of workstation names and for which of these this user can be HWadmin.

At logon it is checked if the user is member of the "LDAP-hwadmingroup". Afterwards it is checked that the workstation on which the user logs on exists in the "LDAP-hwadminattribute". If both are the case, the user is going to be local administrator.

1.7.17 EnableLocation

"EnableLocation" = DWORD:0
The Location Mode enables a location dependent permission/prohibition of the logon of a user, as well as a location dependent assignment of environment-variables.

The LocationCode is looked up out of the sub domain part of the workstations FQDN.
For example: test1.vien.comtarsia.com (LocationCode = 'vien')

1.7.18 LocationAllowedAttributes

“LocationAllowedAttributes” = „ANPrimaer, ANAlternativ“
Determines, which attributes of the LDAP user object is defined that means from which locations the user can log in.

1.7.19 LocationObjectClass

“LocationObjectClass” = „ANSubsiddiary“
Indicates the object class of the LDAP location object.

1.7.20 LocationObjectCode

“LocationObjectCode” = „ANCode“
Indicates the LDAP attribute of the location object, which contains the location code, i.g. “vien”.

1.7.21 LocationObjectAttribute

“LocationObjectAttribute” = „L“
Indicates in which LDAP attribute of the Location Object the location name is noted, for example: “Vienna”

1.7.22 LocationBasedEnvironment

“LocationBasedEnvironment” = „“
With this setting one can export values of attributes of the LocationObject as environment variables.
For example: “LocationBasedEnvironment” = „L=Location“
Please see: AttributeBasedEnvironment

1.7.23 The variable VALID LOCATION

The variable %VALID LOCATION% is always set, if a location check has taken place. If the current user is valid for the logon on the current location, then the variable contains the value “1”. If a location check has not taken place, for example because a local logon was executed, then this variable is not set.

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

Here all available LDAP servers are configured.
If appropriately configured DNS servers are available you can also choose to let the LDAP servers be discovered via DNS (refer to LDAPEnableDNS).

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

The key names consist of the host names or IP addresses of the LDAP server. e.g.: „ldap.comtarsia.com“.

1.7.26 Priority

“Priority” = DWORD:0
Server priority defining the order of contacting as defined in RFC 2052.
0 - 65535 = smaller number equals higher priority

1.7.27 Weight

„Weight“ = DWORD:0
Load Balancing as described in RFC 2052.
0 = no load balancing, 1 - 65535 = load balancing factor

1.7.28 PortLDAP

„PortLDAP“ = DWORD:389
Port address of the LDAP servers used for unencrypted communication.
„389“ is the default for all LDAP servers.

1.7.29 PortLDAPS

„PortLDAPS“ = DWORD:636
Port address of the LDAP servers used for SSL encrypted communication.
„636“is the default for all LDAP servers.

1.8 SignOn Gate support

Comtarsia Logon Client sends at each logon a synchronization package to the SignOn Proxy Server which forwards it to the SignOn Agent.
The response details, i.e. which domains and/or servers were synchronized, will automatically be displayed in the Sync Status box at client side.
The logon session has access to all those systems because the users and passwords are synchronous.
The SynClient functionality is activated with the “EnableSyncClient” registry setting. (see EnableSyncClient)

[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\ComSyncClient]

1.8.1 SyncProxy

"SyncProxy"="192.68.14.245"
or
"SyncProxy"="signonproxy.comtarsia.com"

This parameter defines IP address or host name of the SignOn Proxy server.

1.8.2 ProxyPort

"ProxyPort"=DWORD:7d1
This parameter defines the IP port to be used for communicating with the Proxy Server.

1.8.3 ConnectTimeout

"ConnectTimeout"=DWORD: 5
This parameter defines the time out in seconds for establishing a connection with the Proxy Server.

1.8.4 SyncPacketTTL

"SyncPacketTTL"=DWORD:1770
This parameter defines the time out in seconds for processing SyncPackets.

For more information on the Comtarsia SignOn Gate 2003, please refer to the document SignOnGate2003.doc.

1.9 Functional Description LDAP Logon

LDAP logon enables the Logon to the local workstation via an LDAP directory.
(see Figure 1)
Additionally groups, windows policy, drive and printer mappings, home directory, profile paths and network applications can be defined within the LDAP directory.
Together with the Comtarsia SignOn Agent for Windows and UNIX you can maintain users via an LDAP directory and allow for access to Windows and UNIX resources.
For more information please refer to:
http://signon.comtarsia.com/main/en/Manuals

1.10 Windows Policy

1.10.1 General Information

The NT 4.0 policy functionality continues to be supported under Windows 2000. While it has been replaced with the GPOs which are administered in ADS (Active Directory Service) the “classical” policy method will be used if no ADS is available. The templates “winnt.adm” and “common.adm” are no longer functional for the administration of Win2000 restrictions. These templates need to be manually recreated for Win2000.
Policy settings which are defined in “.pol files” will be processed during a logon, i.e. during the logon process policy settings for "default computer" are updated in "HKEY_LOCAL_MACHINE" and policy settings for "default user" in "HKEY_CURRENT_USER".
Settings in "HKEY_LOCAL_MACHINE" are stored in the "system" registry file and are user independent.
Settings in "HKEY_CURRENT_USER" are stored in profiles of the respective user (file: ntuser.dat) and “follow” roaming users.
Note: Policy Settings must be considered both ways! If you want to disable a defined policy you will not achieve this by removing the policy file from the Server but only by setting a new policy that counters the old one.
This is controlled in the policy editor (**“poledit.exe" supplied with Microsoft NT 4.0 servers** or with the NT server resources kit) with the checkboxes that can assume the following three modes:
Checkbox is greyed: No entry in the Policy file, everything remains unchanged.
Checkbox is checked: The policy entry is activated.
Checkbox is unchecked: The policy entry is deactivated (Activated in the opposite direction.).
During specifying a new value for text fields the related checkbox needs to remain checked.

1.10.2 Logon Client

The Login Client passes the full path of the policy file which is defined under „PolicyPath“ to the Winlogon Process. You should release this file on each Domain Controller on the same share with read permissions for all users.
We recommend the use of the directory replicator service. Therefore the path should be: "%OS2_LOGONSERVER%\netlogon\ntconf1.pol"

1.10.3 Administration of the Logon Clients

Since all parameters of the Logon Clients are stored in the MACHINE hive of the registry it is also possible to configure by means of policy settings.

First load the template „pcs_gina.adm“ into the policy editor. (see Figure 12)

Next you are able to open the local registry with this template to locally configure and test the Logon Client. (see Figure 11)

Click on "local computers" to see the settings of the Logon Client.
(see Figure 14)

Use the menu option File-Save to update the local registry with your changes. Note that these changes will only become effective the next time an LDAP login occurs.

For central administration you need to either open an existing policy file or create a new one. **(Note: open existing policy files always with the same templates!)**

With this function you have central control over the settings of all Logon Clients in your network.

If you would like to administer additional policy settings for the Windows workstations you need to load the Windows templates too when you create the policy. (see Figure 13)

Assigning of specific policies for individual users or groups is not possible but you can circumvent this limitation by defining several groups and allocating different policies to them.

1.10.4 USER_PRIV variable

The USER_PRIV environment variable gets set depending on the LAN Server group membership.

Lan Server group membership	USER_PRIV is assigned	Local Group Membership
-, USERS, no additional group definitions	USER	Benutzer/Users
PUSER	PUSER	Hauptbenutzer/Power User
WSADMIN	WSADMIN	Administratoren/Administrators

Administrator Logon

USER_PRIV is assigned	Local Group Membership
ADMIN	Administratoren/Administrators

1.10.5 Suggestion On How To Use Policy Files with Comtarsia Logon Client:

USERS, POWER USERS, Workstation Administrators should receive different policy settings.
This can be achieved by defining different policy files and LAN Server group memberships.

You create four policy files with the Policy Editor (Poledit.exe, part of NT/W2K server; use Poledit 5.0 and W2K server templates exclusively to administer W2K workstations) and release them in the Netlogon share on the domain controller: User.pol, puser.pol, wsadmin.pol, admin.pol.

The parameter PolicyPath includes the variable USR_PRIV.
.: "PolicyPath"="%LOGONSERVER%\\netlogon\\%USER_PRIV%.pol"

NOTE: All four policy files must consider the exact same policy settings e.g.:
Users should not be allowed to execute the registry tools. Therefore this policy must be set in *user.pol* and must be reset in all other files. (Checkbox is checked or unchecked, NOT greyed!!)

1.11 Home Directory and Profile Path

The home directory path, the local directory letter as well as the profile path for the Roaming-Profile functionality can be assigned to the Logon Client via the local configuration as well as via LDAP.

For the local configuration the following parameters are to be used: „HomeDirPath“, „HomeDirDrive“ and „ProfilePath“.

For the configuration via the LDAP directory with the Comtarsia schema-extension the following attributes of the “CLCPerson”-object are to be used.
CLCHomeDirPath”, “CLCHomeDirDrive” and “CLCProfilePath”.

Maintaining the HomeDirectory String under LDAP:

For the configuration via the LDAP directory with the Comtarsia schema-extension the following attributes of the “CLCPerson”-object are to be used.
CLCHomeDirPath”, “CLCHomeDirDrive” and “CLCProfilePath”.
For more information please refer to:

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

1.12 Additional Features:

1.12.1 Microsoft GINA

By pressing SHIFT + ENTER in the logon dialog you can switch to the Microsoft Gina. In this mode the logon behaves as if the Logon Client were not installed. This functionality can be prevented with the switch “DisableMsGina”.

1.12.2 Administrator Logon

This function enables the login (the profile of the respective user is loaded) with local administrator rights. The user becomes a temporarily member of the local group of administrators for the duration of this session.

This mode is meant to allow for adjustments in the user’s profile, install software packages or carrying out maintenance work.

For security reasons the user must first enter its username and password in the logon dialog (see Figure 1) but instead of pressing "ENTER" or "OK", the admin logon dialog can be activated by pressing **“CTRL+ALT+ENTER” keys**.
This dialog allows an administrator to enter his/her username and password (see Figure 2).

At first it is going to be checked, whether the administrator account in the LDAP Directory is member of the “AdminLogonGroup”, then the logon will be processed with local Administrator rights (please see AdminLogonGroup).

1.12.3 Directory Replicator

The Directory Replicator replicates directories during the Logon process simply and efficiently.
Because only modified files are copied, this function can be used for system management and software updates on a large scale.
Files/directories are also deleted according to the reference directory.

Call via scripts

Example:

Replicate \\Server\program c:\program

Parameter Description:

-a copies the ACL information
-s also copies the Security Attribute

Example

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

2. GroupMapping

The „DisableEqualGroupMapping“ switch turns on manual group allocation.
Only groups will be allocated which are defined in the GroupMapping key.
Groups for local administrators and power users can now be defined with the „GroupAdministrator“ and „GroupPowerUser“ keys (the LDAP groups „WSADMIN“ and „PUSER“ will not be assigned automatically to the local groups „Administrator“ and „Poweruser“.)

Example for manual group allocation:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA]
"DisableEqualGroupMapping"=dword:00000001
"GroupAdministrator"="WSADMIN"
"GroupPowerUser"="PUSER"

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

3. Network Applications

For further Information please see the Comtarsia Logon Client 2006 and LDAP Manual, chapter Network Applications.

4. Glossary

4.1.1 GINA

This specification is used by developers who want to replace the component of Windows NT respectively Windows 2000 that performs identification and authentication of interactive users. This replaceable functionality is implemented as a dynamic-link library (DLL) which is loaded and called by WINLOGON.EXE. This DLL is referred to as the Graphical Identification and Authentication DLL or abbreviated: GINA.

4.1.2 GPO

GPO is short for "Windows 2000 Group Policy".

4.1.3 SAS

SAS is short for “Secure Attention Sequence” for which the default trigger is key combination “Ctrl-Alt-Del”.

5. Disclaimer

Errors and Changes expected!

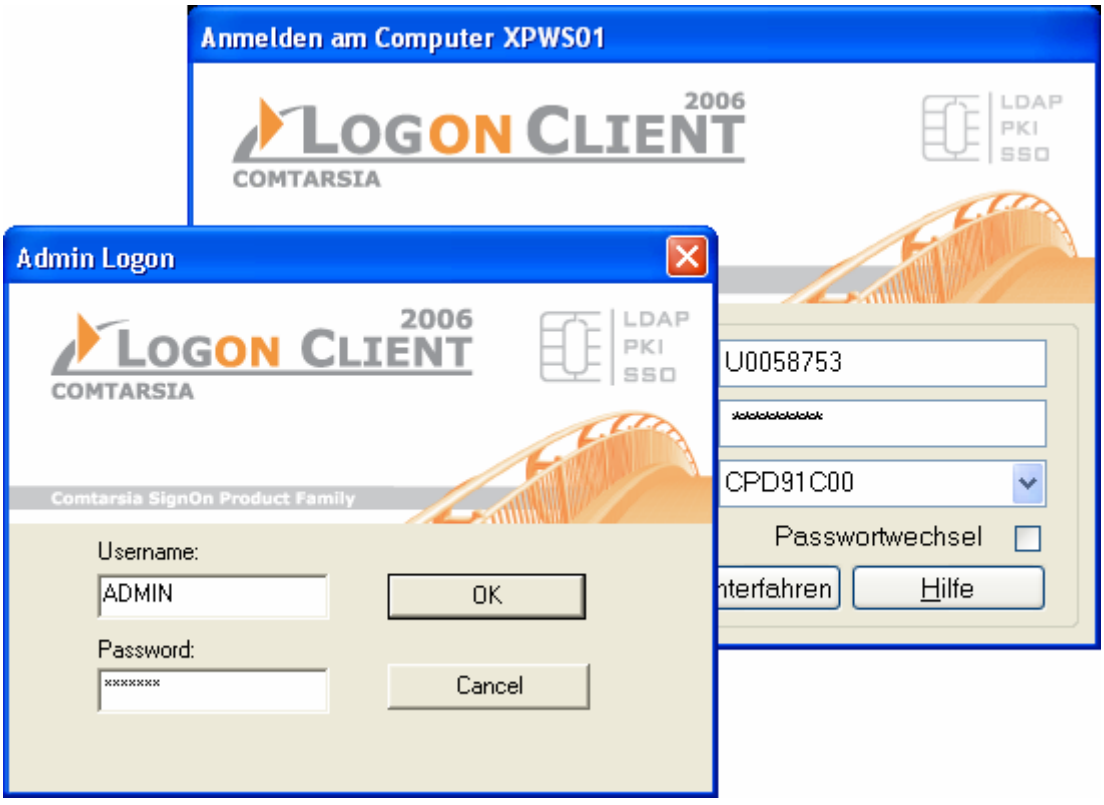
Comtarsia IT Services does not give any assurance or guarantee for other websites, to which we refer in this manual. If you access a non-Comtarsia IT Services Website, it is an independent site beyond our control.
It is also valid, if this site contains the Comtarsia IT Services logo.

Moreover a link from our site to an other does not mean we identify ourselves with their contains or support their use.

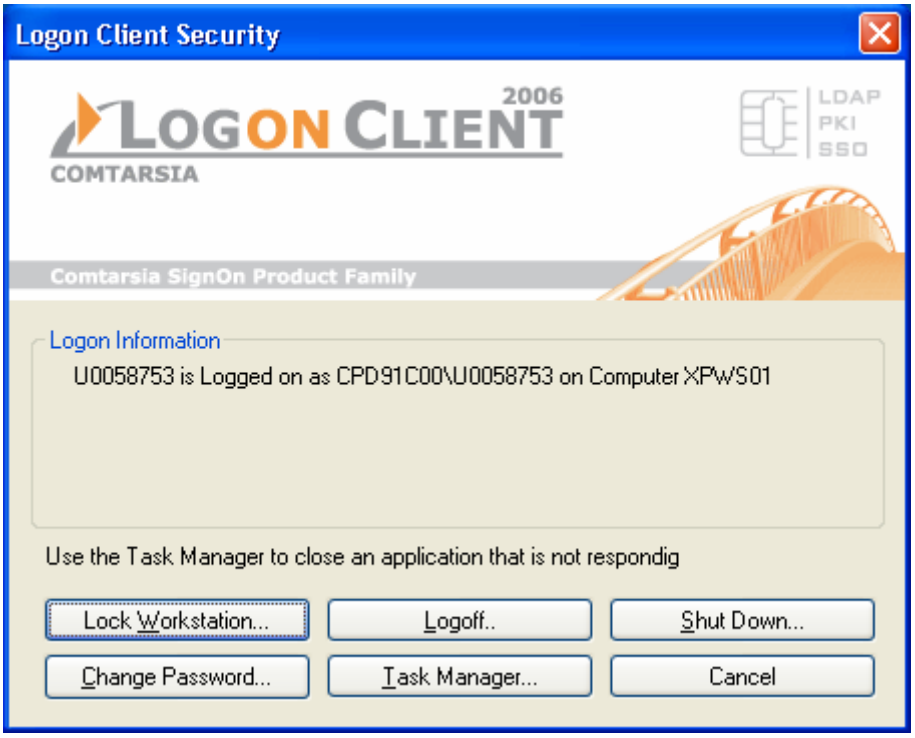
6. Screen Shots

6.1.1 Figure 1. Logon Dialog

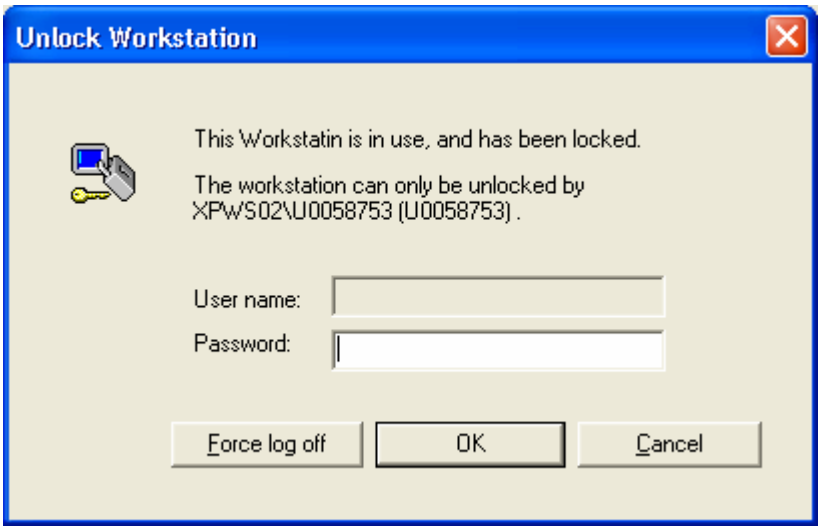
6.1.2 Figure 2. Admin Logon Dialog



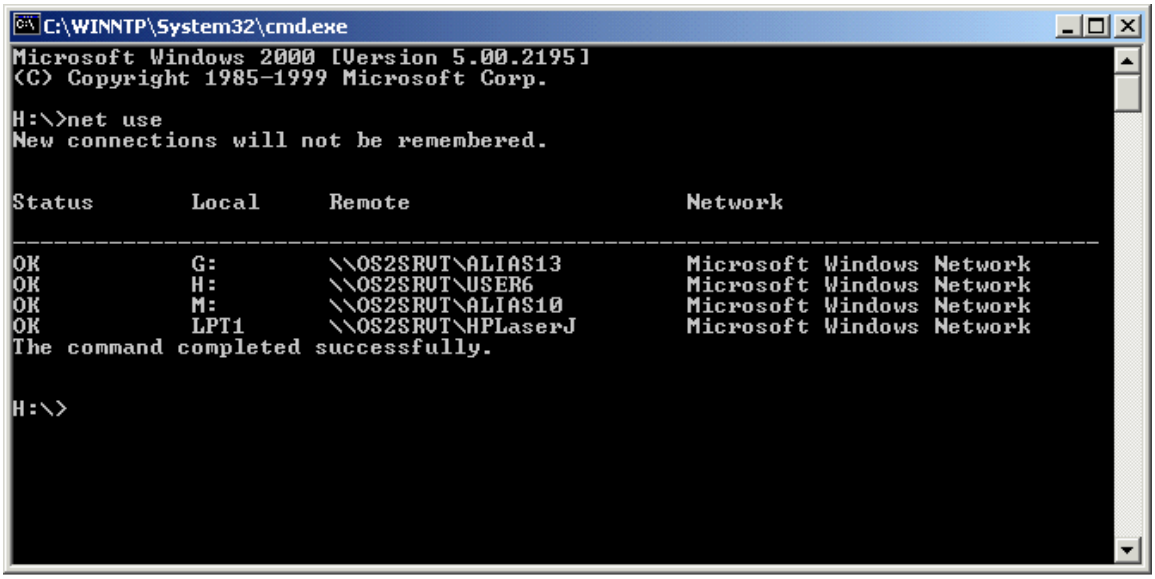
6.1.3 Figure 3. ON SAS Dialog



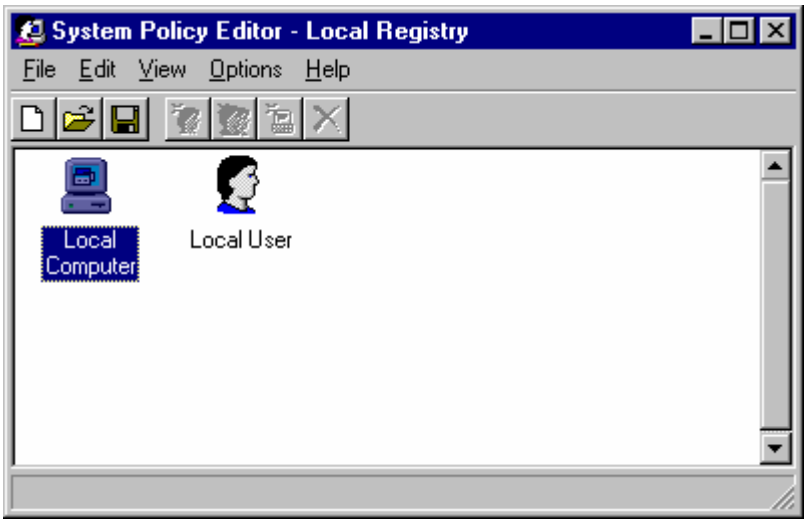
6.1.4 Figure 4. Unlock Dialog



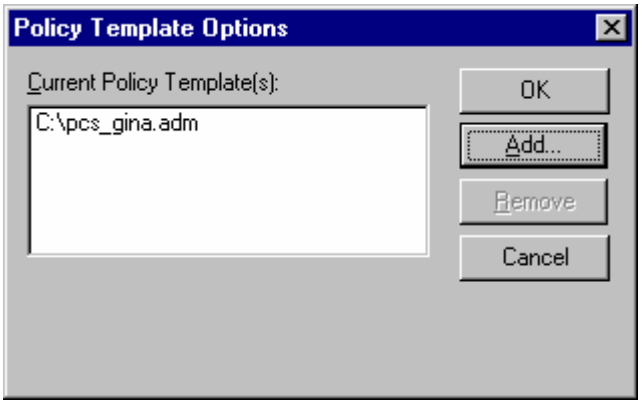
6.1.5 Figure 10. Windows Workstation „net use“



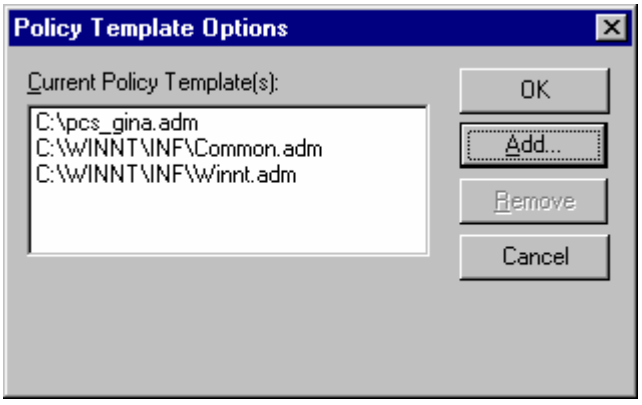
6.1.6 Figure 11. Policy Editor



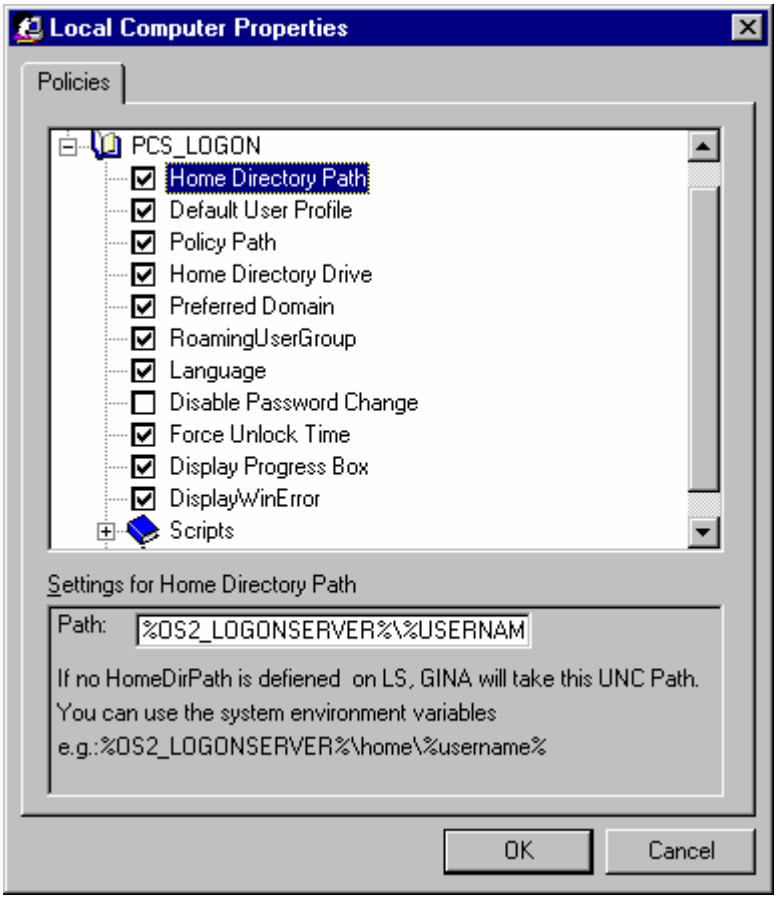
6.1.7 Figure 12. Policy Editor GINA Template



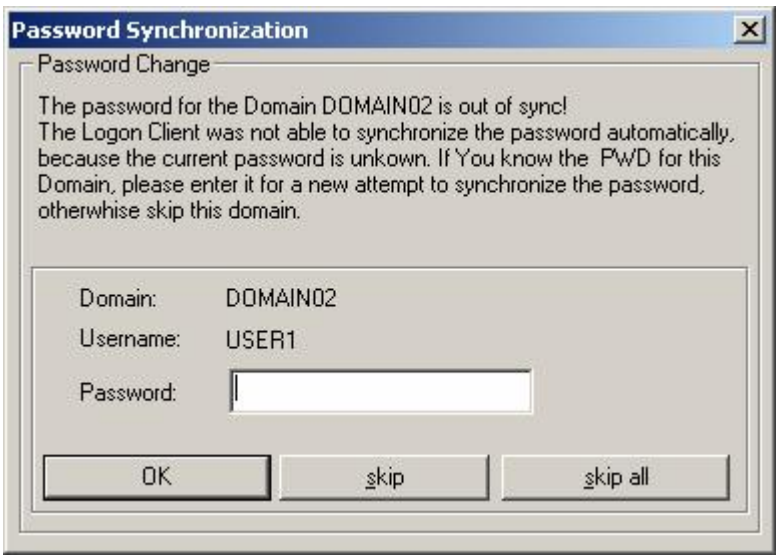
6.1.8 Figure 13. Policy Editor GINA and Windows Templates



6.1.9 Figure 14. Policy Editor GINA Configuration



6.1.10 Figure 21. Password Synchronization



6.1.11 Figure 22. Extended LDAP Logon