



Comtarsia Logon Client 2016

Manual

Version: 6.2.15.0, 30th May, 2023

Contents

1. Introduction.....	3
2. Installation	5
2.1 Manual Installation.....	5
2.2 Software Distribution	6
3. Comtarsia Management Console (ComtMC)	7
3.1 Update Notification	7
4. Basic Configuraion	8
5. Usage Scenarios	11
5.1 LDAP over SSL.....	11
5.2 LDAP Users from Multiple OUs	12
5.2.1 Search for User.....	13
5.2.2 OU Searchlist.....	14
6. Configuration Parameters	17
6.1 Logon Client.....	17
6.1.1 Profile	17
6.1.2 Quick Logon.....	19
6.1.3 Scripts	20
6.1.4 User Environment	21
6.1.5 SSO.....	22
6.1.6 User Certificate	23
6.2 LDAP	24
6.2.1 Server.....	24
6.2.2 Users.....	25
Static DN	25
Search for User	26
OU Searchlist	27
6.2.3 User Object	28
6.2.4 Groups	30
6.3 SyncClient.....	32
6.4 Logon.....	34
6.4.1 Logon Policy	34
6.4.2 Logon Info	36
6.4.3 PKI	37
6.5 Groups	38
6.6 Variables.....	39
6.7 Logging	42
6.8 Licensing.....	44
7. Parameter Description.....	45
8. Disclaimer.....	57



1.Introduction

Comtarsia Logon Client 2016 for Windows Workstation and Server

Supported Platforms: Windows 7, Windows 8.1, Windows Server 2012 R2, Windows 10/11, Windows Server 2016/2019/2022 (minimum system requirements:1GB RAM, 1GB free disk space)

Primary LDAP authentication on the local or virtual Desktop via Password or Smart Card.

The Comtarsia Logon Client supports different Multi-Factor Authentication (MFA) types (TOTP, HOTP, FIDO2, COTP) to be used as a second factor for user authentication.

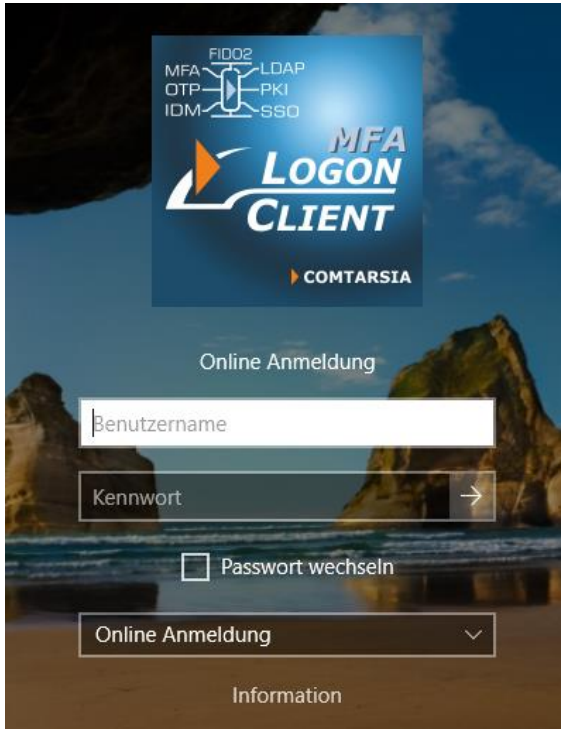
See the document "Comtarsia Multi-Factor Authentication Guide" for more details:

http://signon.comtarsia.com/Downloads/Englisch/Comtarsia_Multi-Factor_Authentication_Guide.pdf

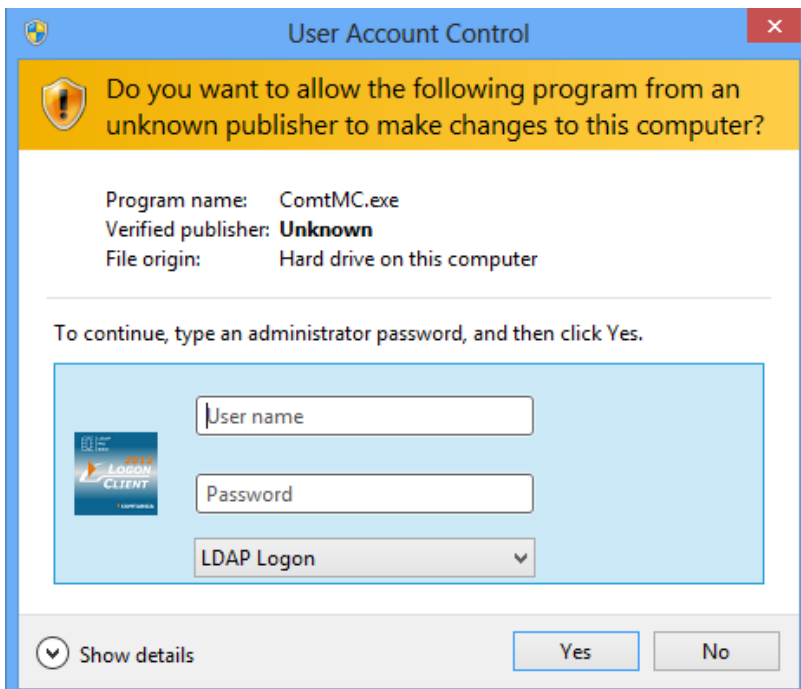
Direct LDAP authentication or via SignOn Proxy. Local User Mode or Domain User Mode with automatic User Managment by using the SignOn Agent for Active Directory

Supported LDAP Server: IBM Tivoli Directory Server, Open LDAP, Open Directory (Mac OS X), Fedora Directory Server, Novell eDirectory Server, IBM z/OS SecureWay (RACF), Sun DS Enterprise Edition, Lotus Domino, Microsoft Active Directory (via LDAP)





The Credential Provider interface is used by the Comtarsia Logon Client 2016 which replaces the Microsoft Logon tile by a Comtarsia Logon tile which enables the LDAP logon. It's possible to configure the Comtarsia Logon Client 2016 so that users can switch back to the Microsoft Logon tile, or to forbid any other authentication method beside LDAP/Comtarsia SignOn Proxy.

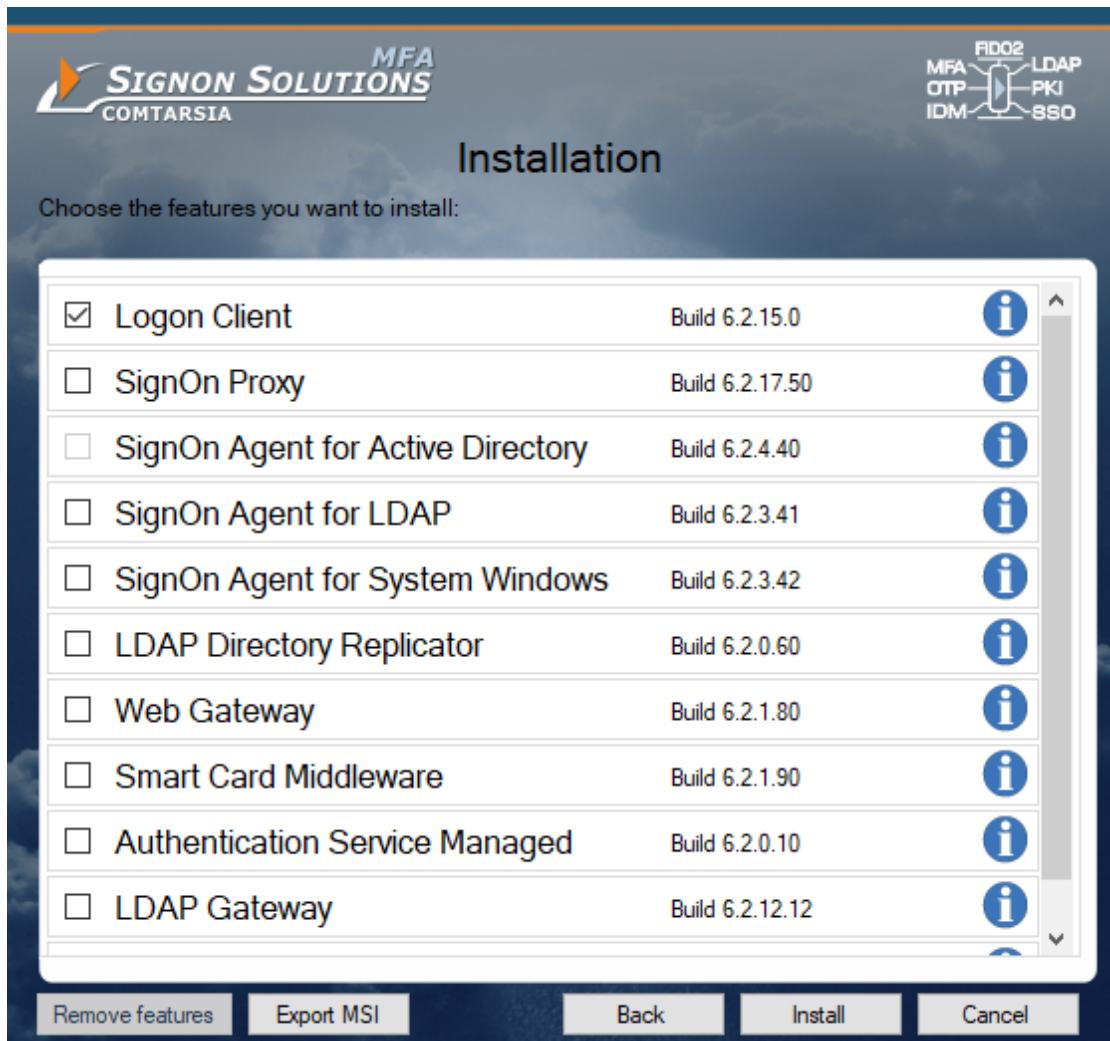


The Windows User Account Control (UAC) allows a specific authorisation for the execution of applications which need local Administrator rights. The Comtarsia Logon Client 2016 enables the possibility to use LDAP groups to control these temporary administrator privileges.

2. Installation

2.1 Manual Installation

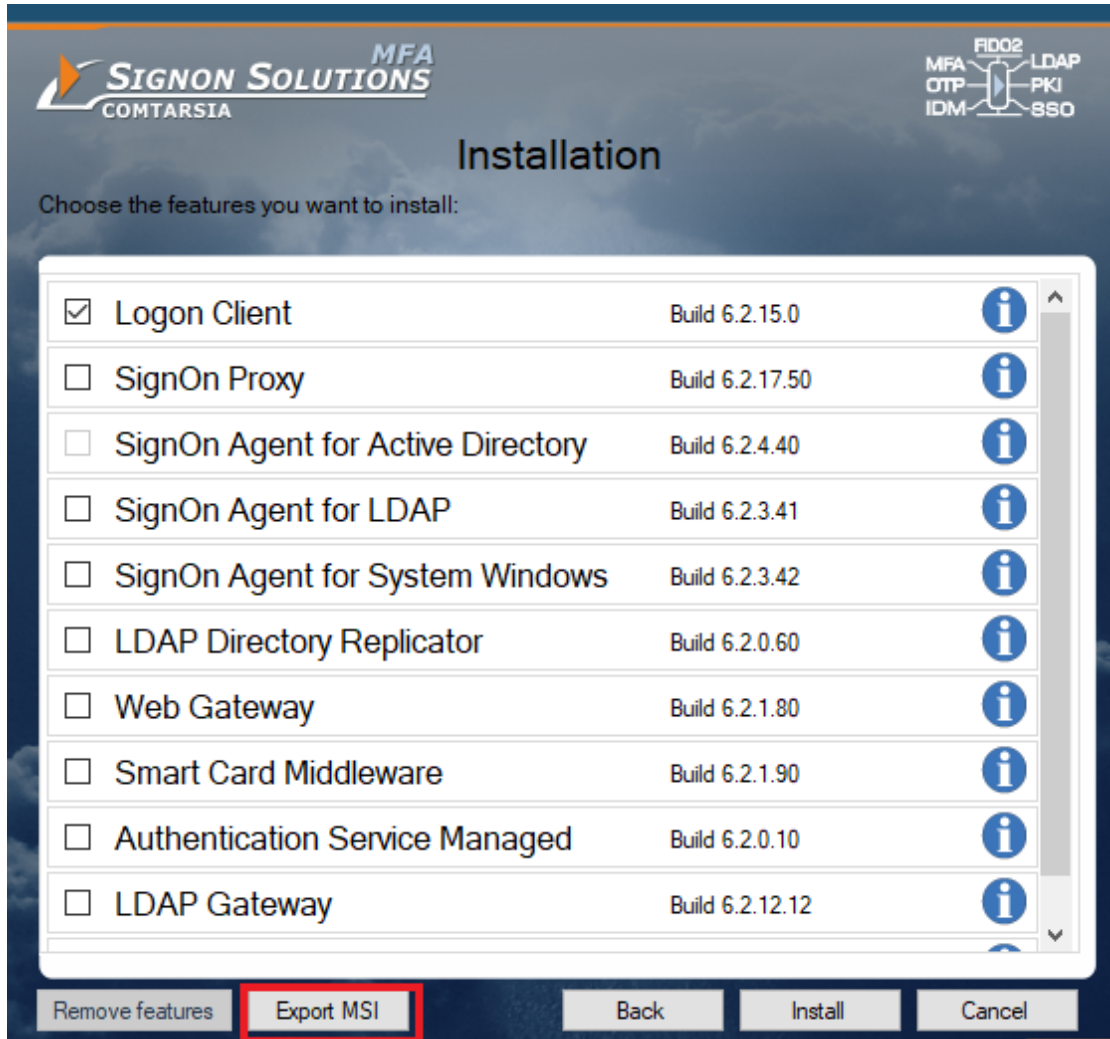
An installation or an update is done using the installation program "SOS2016-6.2.x.4.exe". When updating, the configuration is preserved and the license key will only be replaced if the validity of the installed key is shorter than the validity of the key shipped with the installation program. (Bought license keys usually won't be replaced.)



The installation program copies the necessary files and applies necessary registry changes to enable the Comtarsia Logon Client Credential Provider tile. It also writes a default configuration into the registry (except for those values which have already been set – no existing config will be replaced).

2.2 Software Distribution

All SignOn Solution 2016 components are provided as separate MSI packages. To get this packages, just run the SignOn Solutions 2016 bundle installer and on the feature selection screen press "Show MSI".



For some products an initial configuration is supplied in form of a mst-file (MSI Transform). If you prepare a package for software distribution, you should omit this initial mst file and replace it with your own configuration and support files (Licence key, certificates, customized images).

The complete Logon Client configuration is stored under the registry key "HKLM\Software\Comtarsia\SOSProfile 001".

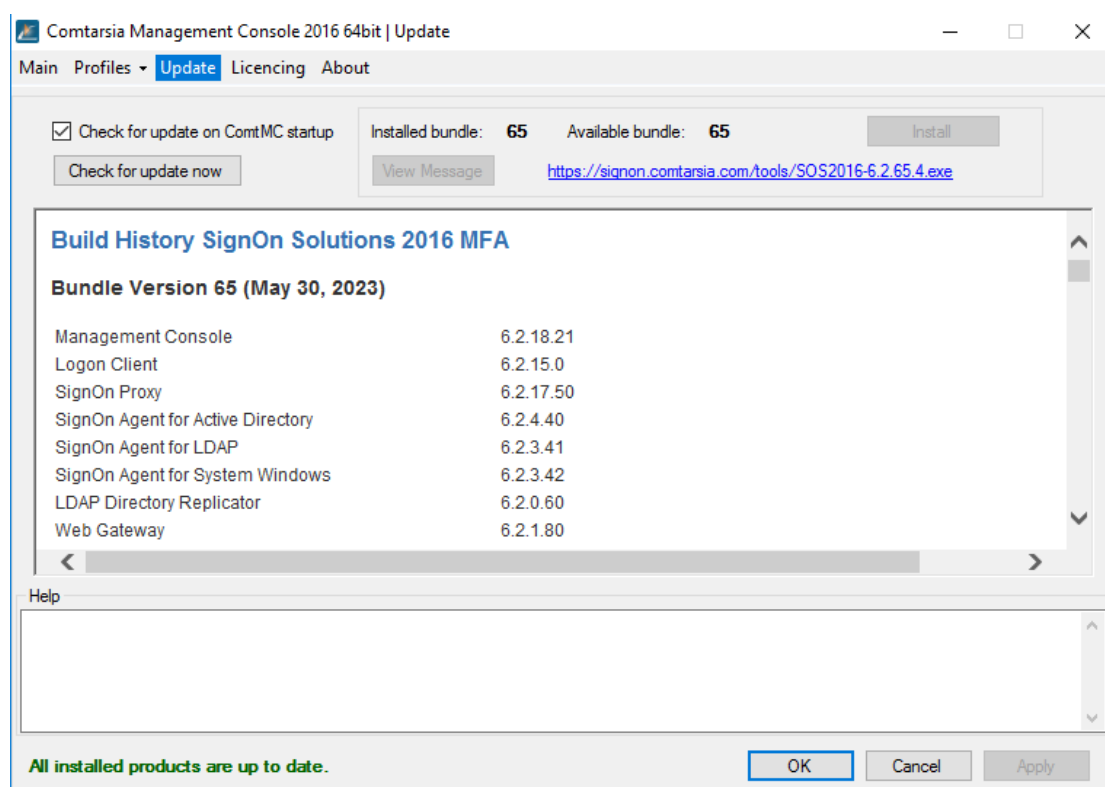
The licence key to use is configured under "HKLM\SOFTWARE\Comtarsia\SignOn Solutions 2016\LicenceKeys\003". This registry key and also the licence key file itself has to be included in the software distribution package.

3. Comtarsia Management Console (ComtMC)

The Comtarsia Management Console (ComtMC) can be accessed through the Start menu.

On the first start of the ComtMC one will be asked whether “automatic update checking” should be enabled or disabled. If there’s no direct internet connection (internet accessible without proxy server), it’s advisable to disable automatic update checking for now. This setting can be adjusted at a later time. See: [Update Notification](#)

3.1 Update Notification



The version checking and notification is performed each time the ComtMC is started.

If there’s no direct internet connection (internet accessible without proxy server), it’s advisable to disable automatic update checking for now. The update check is carried out exclusively over <http://update.comtarsia.com>

A manual check (Check for update now) can be triggered via the “Update” tab of the ComtMC.

4. Basic Configuraion

The configuration of the LDAP settings builds the fundament on which all configuration scenarios build upon.

The following information is needed:

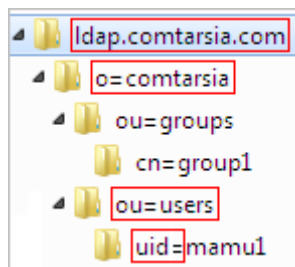
- LDAP-Server Adress/Port Non-SSL or SSL
- LDAP server type (eg: OpenLDAP, IBM Directory Server 6, etc)
- LDAP directory structure
- 1 LDAP user with password (for testing)

LDAP directories usually don't follow any rigid pattern and are usually tailored to fit company scenarios and applications. Therefore, the LDAP configuration of the Comtarsia Logon Client often just cannot be done by following a simple recipe. This section shows how to obtain a basis configuration which allows an LDAP logon, by following a few simple steps. Additional scenarios which can be used to refine that "simple configuration" follow later together with the required configuration steps. See: [Usage Scenarios](#)

To keep the fundamental configuration simple, it is assumed that all LDAP users are in the same container.

In the hirarchy of the example-LDAP server "ldap.comtarsia.com", the user "mamu1" is in the container "ou=users" which in turn is in "o=comtarsia". "o=comtarsia" is also the BaseDN. The naming-attribute of the example users is "uid". (usually "uid" or "cn")

The full DN (Distinguished Name) of the user is therefore: "uid=mamu1,ou=users,o=comtarsia".



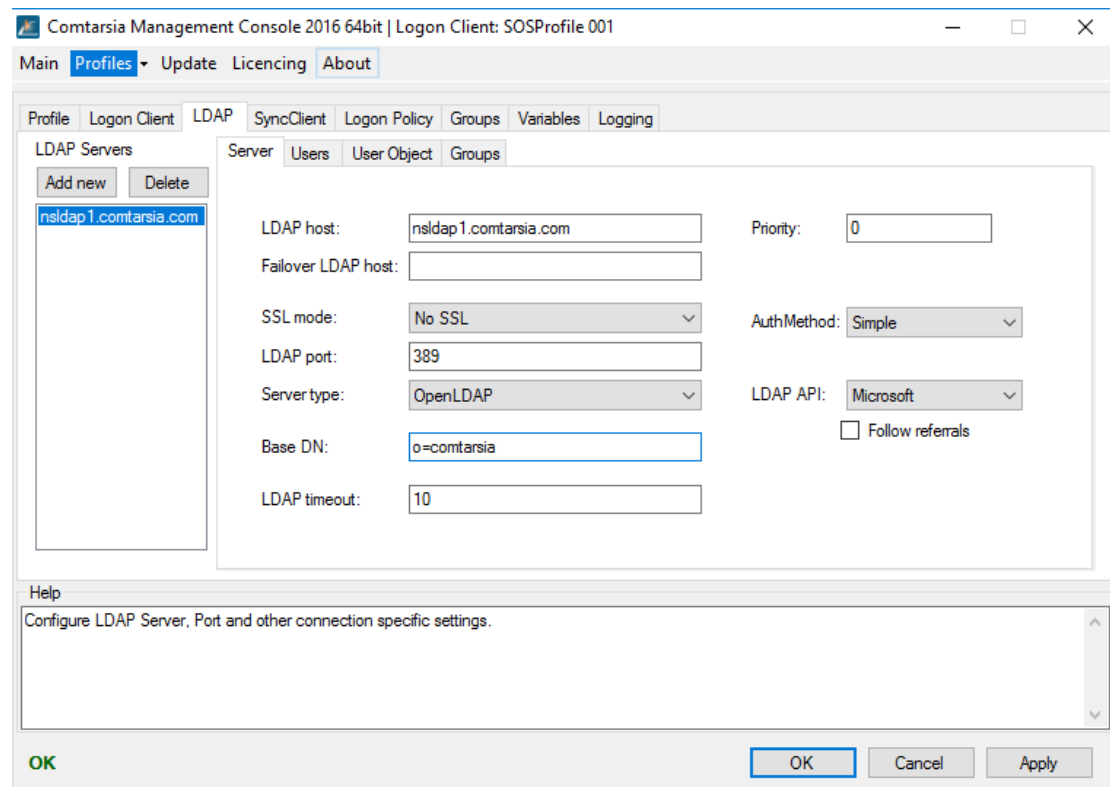
The syntax of full DNs is always from the lower level (leaf) to the base object (root or "baseDN").

LDAP servers can usually accessed unencrypted over the port 389, as well as SSL-encrypted over the port 636. For the first tests, with the test users, an unencrypted (clear text) communication is sufficient. In production environment, however, an encrypted communication is for security reasons strongly recommended; because otherwise, any communication between the client and the LDAP server (including login information) is held in clear text.

The first configuration to be made is in the Comtarsia Management Console (ComtMC) in the tab "[LDAP] -> [Server]"; The LDAP host name (or IP-address), the LDAP port and the corresponding SSL mode.

If the LDAP communication should be encrypted (over SSL), it's best to chose "SSL without trusted server certificate" instead of "No SSL" for now, for the sake of simplicity. For more information concerning the SSL modes, see: [LDAP over SSL](#)

Also important is the "BaseDN" which is the base of every LDAP-search.



The tab "[LDAP] -> [Users]" contains the configuration of the position of LDAP-users within the LDAP directory, or "how the authentication" should be performed.

The simplest "UserDN Mode" is "Static DN". In this mode, the Comtarsia Logon Client uses logon name entered by the user (at the logon tile) and uses it to construct an LDAP DN with that name and the configured "BaseDN, UserDN Suffix, and UserDN Prefix". Subsequently, the Comtarsia Logon Client uses that constructed LDAP DN and the password for an LDAP-bind to the configured LDAP server. If the LDAP server accepts that LDAP-bind with the constructed LDAP DN and password, the provided username is considered valid and the logon process continues.

The UserDN is constructed in the following way:
UserDN Prefix + <Logon-Name> + UserDN Suffix + Base DN
The assembly of those parts must result in a valid LDAP DN.

In the example, this results in:
UserDN Prefix="uid="
UserDN Suffix="ou=Users" (inclusive the comma)
BaseDN="o=Comtarsia"

The Comtarsia Management Console shows a preview of the resulting UserDN, so that one can see at a glance whether the chosen values are entered correctly and meet the existing LDAP structure. (marked red in the picture below)

Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001

Main Profiles Update Licencing About

Profile Logon Client LDAP SyncClient Logon Policy Groups Variables Logging

LDAP Servers

Server Users User Object Groups

Add new Delete

nsldap1.comtarsia.com

User Append BaseDN

UserDN Prefix: uid=

UserDN Suffix: .ou=User|

UserDN Mode: Static DN

System User

DN: cn=Directory Manager

Password:

Use System User for Group and Attribute Queries

DN: uid=<USERNAME>,ou=User,o=comtarsia

Help

User DN specific configuration for this LDAP server.

OK OK Cancel Apply

5. Usage Scenarios

5.1 LDAP over SSL

There are different modes of communication between the Comtarsia Logon Client 2008 and the LDAP server.

The basic idea of the SSL communication is the encryption of the plaintext data which is sent over the wire. (1st mode).

The 1st mode is the easiest to configure.

The settings are made in the ComtMC in [LDAP -> Server -> SSL mode].

Description of the modes:

Mode 1: SSL without "trusted server certificate"

Requirements:

Client: none

LDAP Server: SSL communication (ldaps) has to be enabled. The certificate doesn't have to be issued by a CA (Certificate Authority) – it may as well be a self-signed certificate.

Advantages: The communication between the Comtarsia Logon Client 2008 and the LDAP server, (which will otherwise be in clear text) will be encrypted.

Mode 2: SSL with "trusted server certificate"

Requirements:

Client: The client has to trust the CA (Certificate Authority) which issued the LDAP server certificate. Therefore, all CA-certificates in the chain have to be added to the "Trusted Root Authorities"-branch of the computer-certificates-store. (see figure below)

LDAP Server: The certificate of the LDAP server has to be issued by a certificate authority which is trusted by the client.

Advantages: Encryption. The Comtarsia Logon Client ensures that the LDAP server is trusted by checking its certificate. (prevents "man in the middle"-attacks)

Mode 3: SSL with "trusted client certificate"

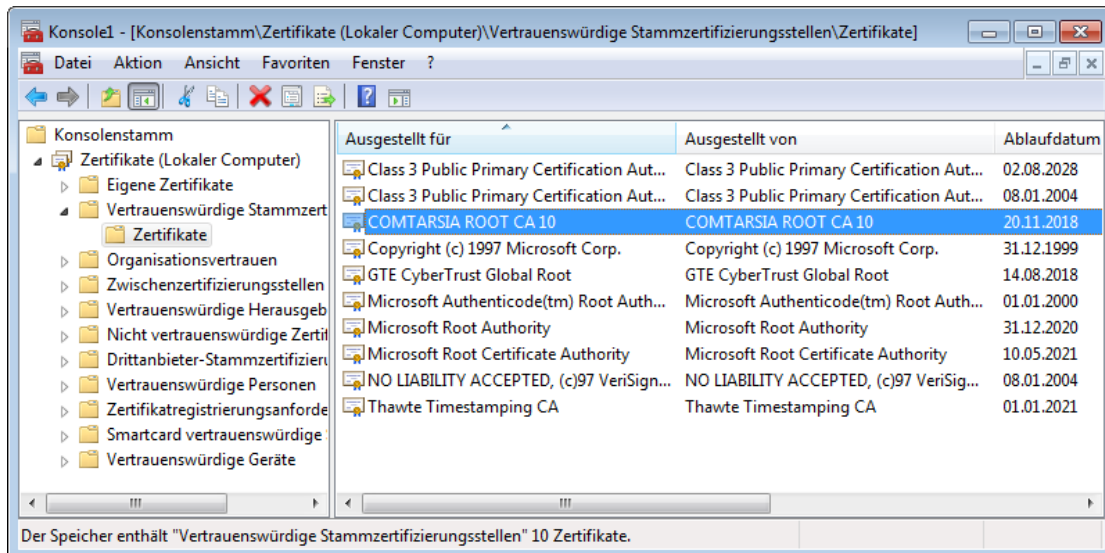
Requirements:

Client: As mode 2. In addition, the client needs a client certificate (inclusive key) in the "My"-branch of the computer certificates store. The certificate of each client has to have the computer name its client as part of the certificate CN (common name). (see figure below)

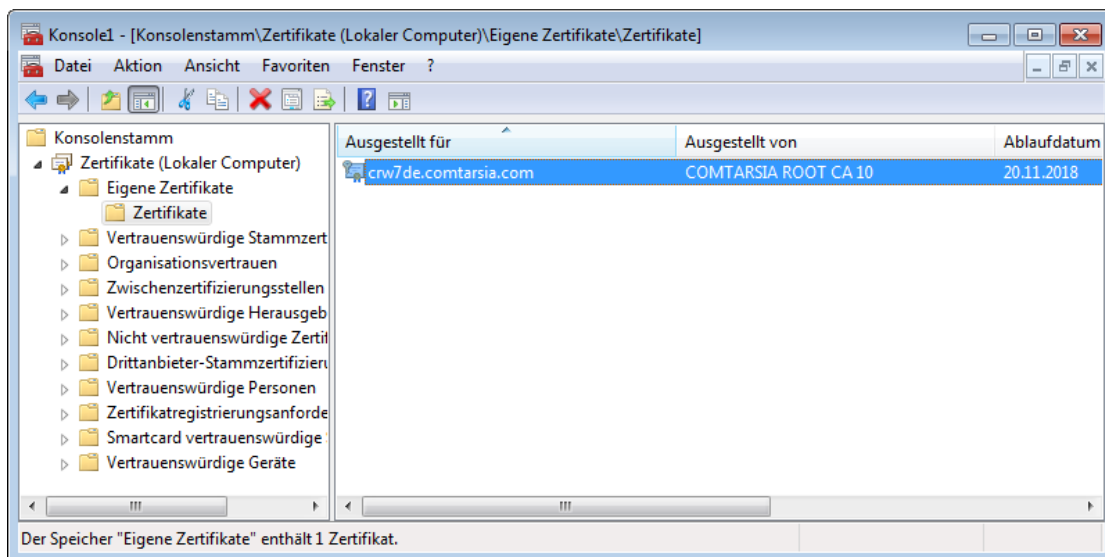
LDAP Server: As mode 2. In addition, the LDAP server has to trust the certificate authority which issued the client certificate.

Advantages: Like mode 2. The LDAP server can be configured to only accept connections from trusted clients.





[Figure: MMC: Trusted Root Certificates of the computer]



[Figure: MMC: My-store of the computer]

5.2 LDAP Users from Multiple OUs

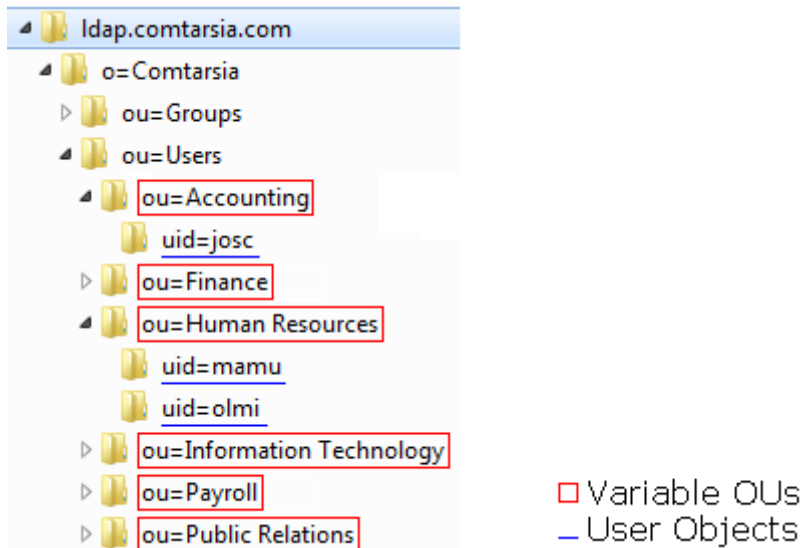
Often, the LDAP hierarchy isn't flat and the users are located in several organizational units (OU).

In the bases (example) configuration, all users are in the OU "ou=Users", which, in turn is within the organisation "o=Comtarsia". However, the following examples have an additional hierarchical level to show the configuration steps required to handle that "multiple Ous"-scenario.

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

eg:

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



[Figure: LDAP example: multiple OUs]

There are different ways to configure this (and similar) scenarios for the Comtarsia Logon Client 2008. The first option ([Search for User](#)), simply searches for the LDAP user within the configured RootDN (on a sub-tree level). The second option ([OU Searchlist](#)) uses a list of allowed OUs, and the Comtarsia Logon Client 2008 searches in each of those OUs for the provided LDAP-user.

In both cases, the LDAP-search either has to be allowed for "anonymous", or a "LDAP system user" has to be used who has the rights to search within the desired parts of the LDAP directory. This system user can be set in the ComtMC and will be used by the Comtarsia Logon Client for those search operations.

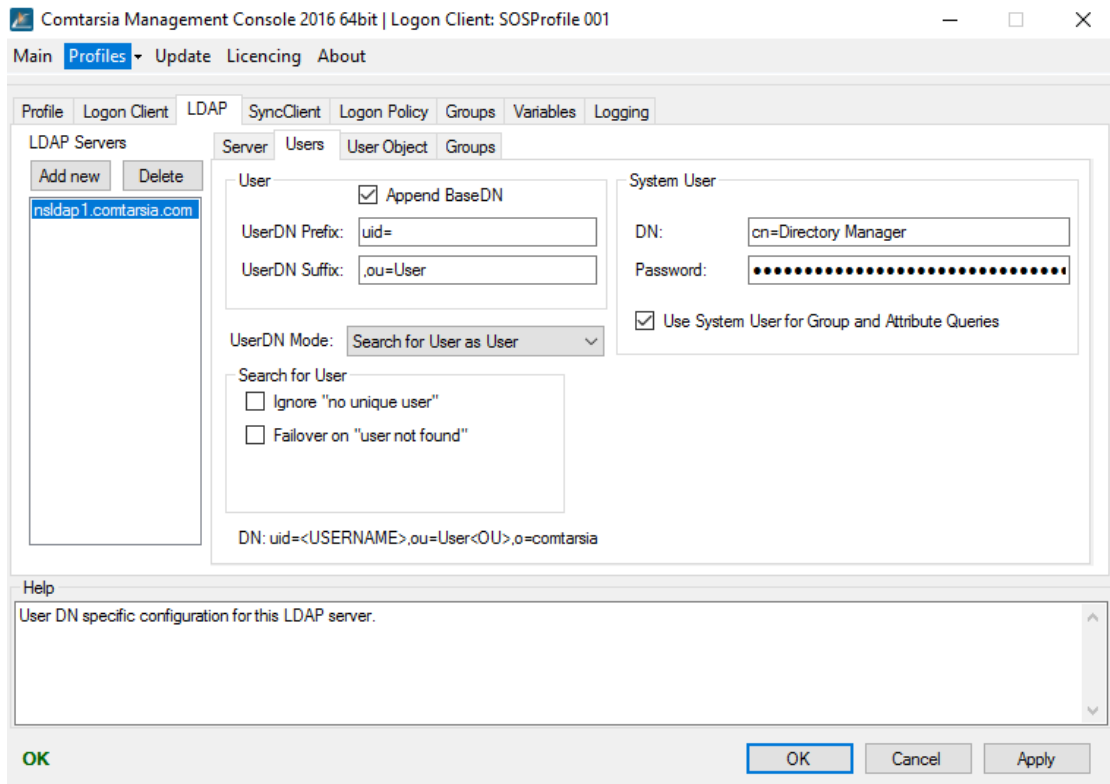
5.2.1 Search for User

The Comtarsia Logon Client authenticates itself against the LDAP server, using the configured "System User".

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

Then, the Logon Client issues an LDAP search, which is composed as follows.:

- (&(uid=<USERNAME>)(objectclass=person)) basedN: o=Comtarsia
- "<USERNAME>": The username entered by the user.
 - "uid=": the configured "UserDN Prefix"
 - "person": the configured "User Object > Object Class" (see figure)
 - "o=Comtarsia" the configured "baseDN"



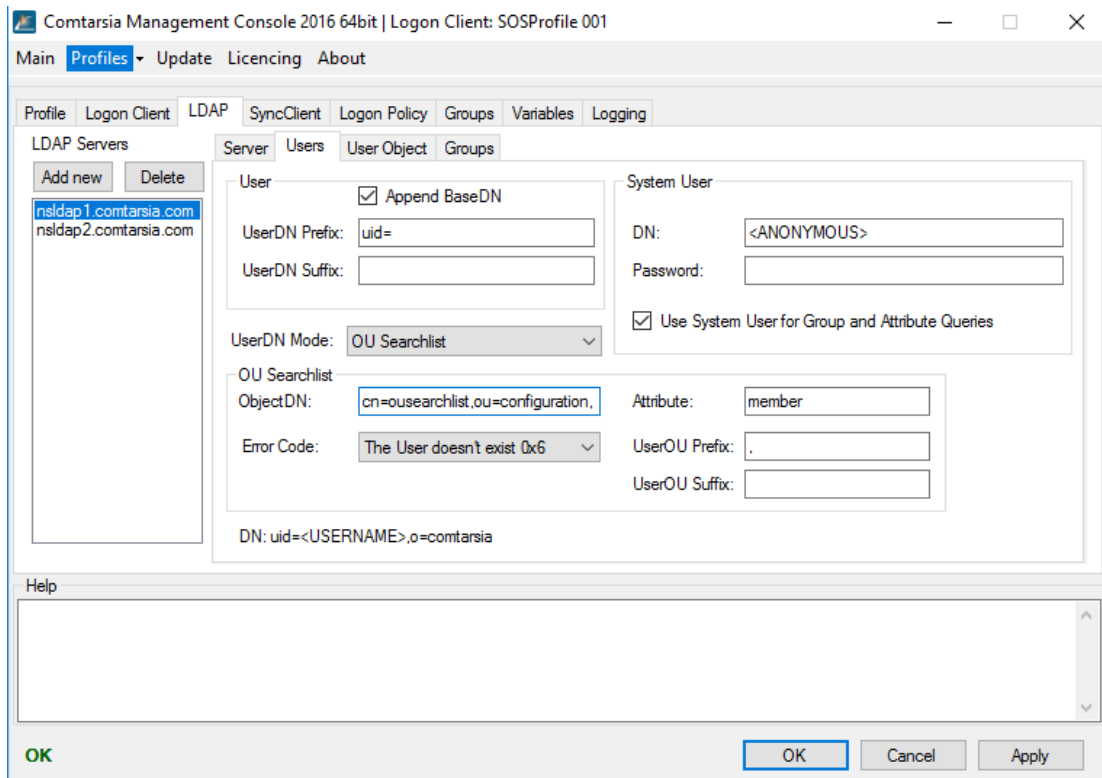
[Figure: ComtMC: LDAP > User Object > Object Class]

If an unique LDAP userobject is found, the full DN of this object is used for the LDAP bind request, together with the password provided by the user. In all further steps (eg: group search), this determined LDAP-user DN is used. If the user is not unique (more than one LDAP objects got returned by that LDAP-search), the logon process will be terminated with an error message.

5.2.2 OU Searchlist

The Comtarsia Logon Client authenticates itself against the LDAP server, using the configured "System User".

.After that, the Comtarsia Logon Client requests the configured "OU Searchlist > ObjectDN" and its "OU Searchlist > Attribute". This object contains a list of valid "<OU>"-values in the configured "OU Searchlist > Attribute".



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

The configured OU Searchlist Object could be an LDAP group (default configuration); but it can as well be any other LDAP object. By default the "Member"-attribute of a specific LDAP group would contain all the allowed "OUs".

Example LDIF of the OU Searchlist object:

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

The Comtarsia Logon Client uses the following values to generate possible valid User-DNs:

<UserDN Prefix><USERNAME><UserDN Suffix><UserOU Prefix><OU><UserOU Suffix>,<baseDN>

In the example configuration, this results in:
uid=<USERNAME>,<jeweilige OU>,o=Comtarsia

- "<UserDN Prefix>": configured in "LDAP > Users > User > UserDN Prefix"
- "<USERNAME>": entered by the user at the login screen
- "<UserDN Suffix>": configured in "LDAP > Users > User > UserDN Suffix"
- "<UserOU Prefix>": configured in "LDAP > Users > OU Searchlist > UserOU Prefix"
- "<OU>": replaced by the respective OUs
- "<UserOU suffix>": configured in "LDAP > Users > OU Searchlist > UserOU Suffix"
- "<baseDN>": configured in "LDAP > Server > baseDN"

The Comtarsia Logon Client checks each of the resulting DN to see if any of them is a valid LDAP user.

Once a user has been found, the full DN of that user is used, together with the password provided by the user, to issue an LDAP bind. If the LDAP bind succeeds, the logon process continues and the full DN of this user is used for all further steps (eg: group search).

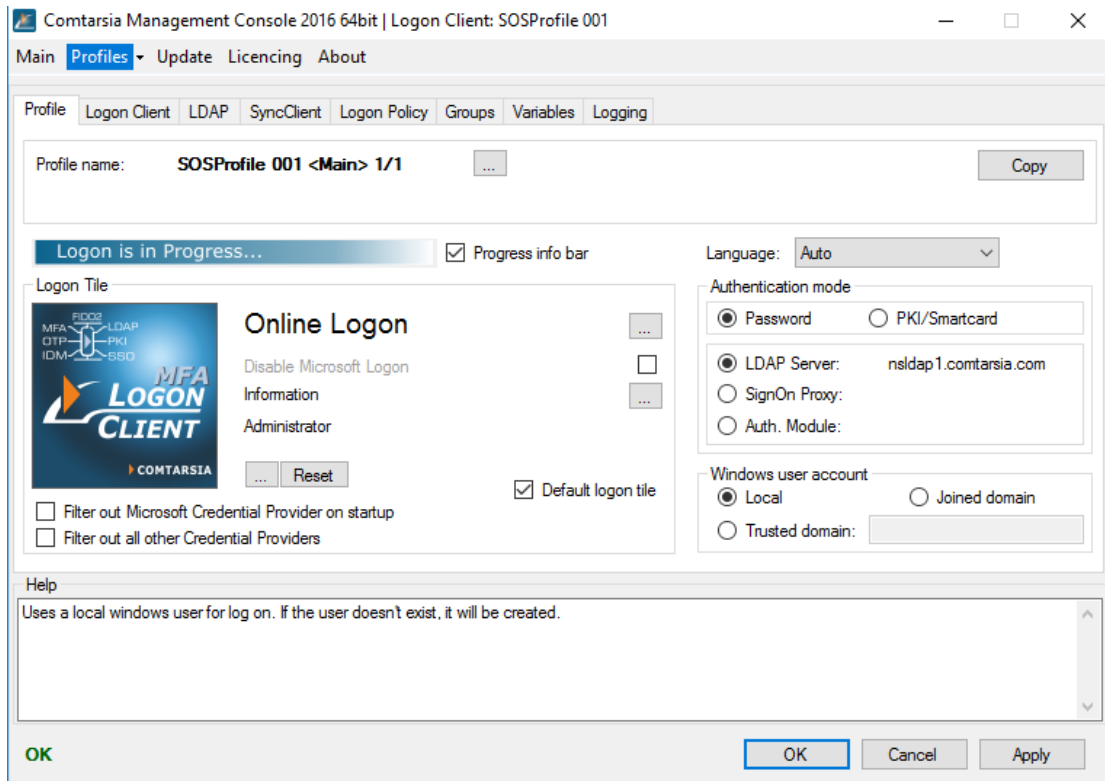
If none of the resulting user-DNs is a valid user, the logon process will be cancelled and the user receives the configured "error code" (LDAP > Users > OU Searchlist > Error Code).



6. Configuration Parameters

6.1 Logon Client

6.1.1 Profile



Language

Defines the user interface language. Currently the following languages are available: German, English, and French.

Authentication mode

enableSmartcard: Allows to chose between "user password" logon or "pki" (smartcard) logon.

enableProxyLogon: "Direct": the user is authenticated (directly) against the LDAP server. "Proxy": the user credentials (user/passwor or PKI handshake) is taking place over the Comtarsia SignOn Proxy server which handles the authentication via an LDAP server.

Windows user account

This option activates/deactivates [Enable Domain Logon](#). When set to "Local", the "Local User Mode" is active; "Joined domain" activates the "Domain User Mode".

Local User Mode:

After a successful LDAP logon a local user account is used for the workstation logon. The user account management (create, activation, password synchronization, etc..) is performed by the Comtarsia Logon Client.

Domain User Mode:

After a successful LDAP logon a domain user account is used for the workstation logon. In order for the automatic domain logon to work, two conditions have to be met:

- The workstation has to be a member of the domain
- Since the Comtarsia Logon Client doesn't have the necessary privileges to manage AD-users, the Comtarsia SignOn Gate has to be used on one of the AD servers, and the Comtarsia Logon Client has to be configured to use it. See: [SyncClient Configuration](#).

Microsoft Credential Provider – Filter:

The Comtarsia Logon Client allows you to filter out the standard Microsoft Credential Provider. I.e. Users can't switch to the Microsoft Credential Provider at the the logon- or unlock-screen. The Button "other user" is no longer available.

[Unregister on Startup](#)

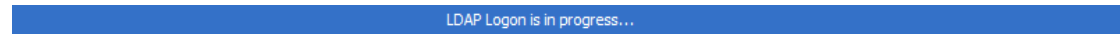
If this parameter is enabled, the Microsoft Credential Provider won't be loaded during the system start. (Comtarsia Credential Provider will be shown as default, but unless "[Disallow temporary activation/deactivation](#)" is also enabled, users can still switch to the Microsoft Credential Provider)

[Disable Microsoft Logon](#)

If this option is active, the link "Enable/Disable Microsoft Logon" (at the login screen) is no longer available.

[Display progress info bar](#)

If this parameter is activated, a progressbar is displayed on top of the screen during the logon.



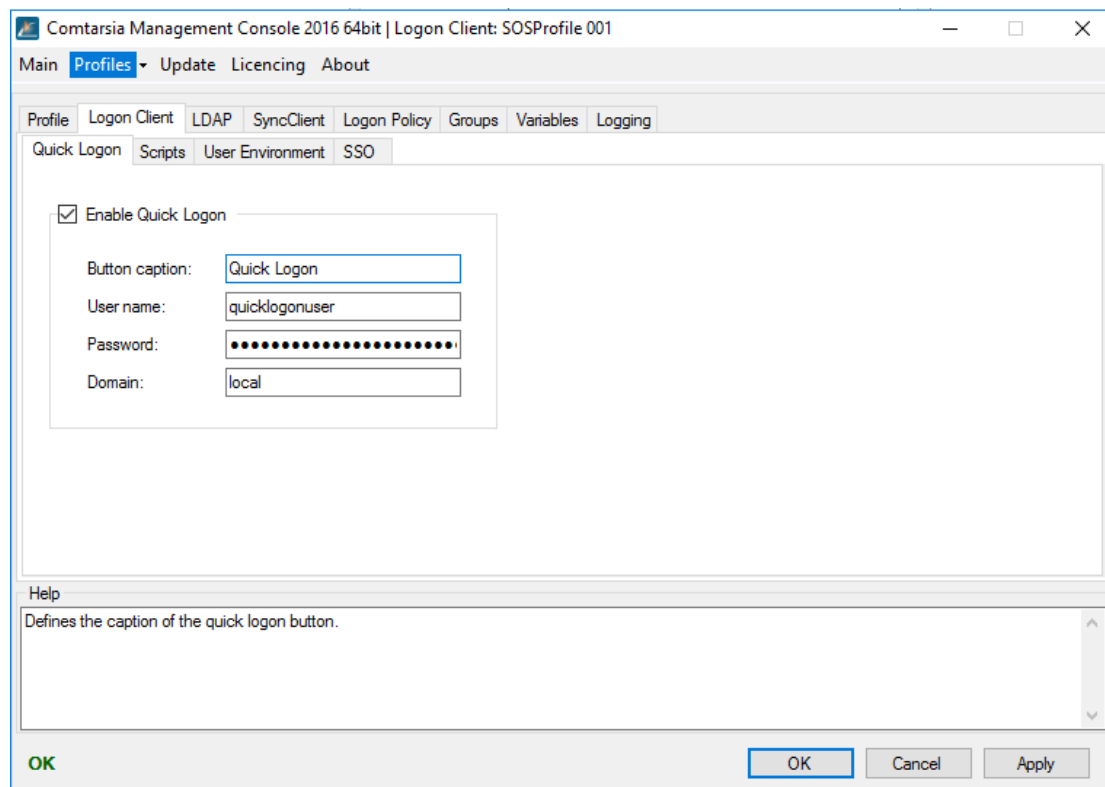
LDAP Logon is in progress...

[Logon Panel Bitmap](#)

With this parameter, an alternate bitmap (for example a company logo) can be chosen which replaces the Comtarsia logo in the Logon tile.

The bitmap has to have a resolution of 126x126 pixel and has to be locally available to the system during the logon.

6.1.2 Quick Logon



[Enable Quick Logon](#)

Activates a "Quick Logon" button on the logon screen which allows users to log on with predefined credentials (1-click logon)

[Button caption](#)

Specifies the text of the quick-logon button.

[User name](#)

Defines the username which has to be used for the quick logon.

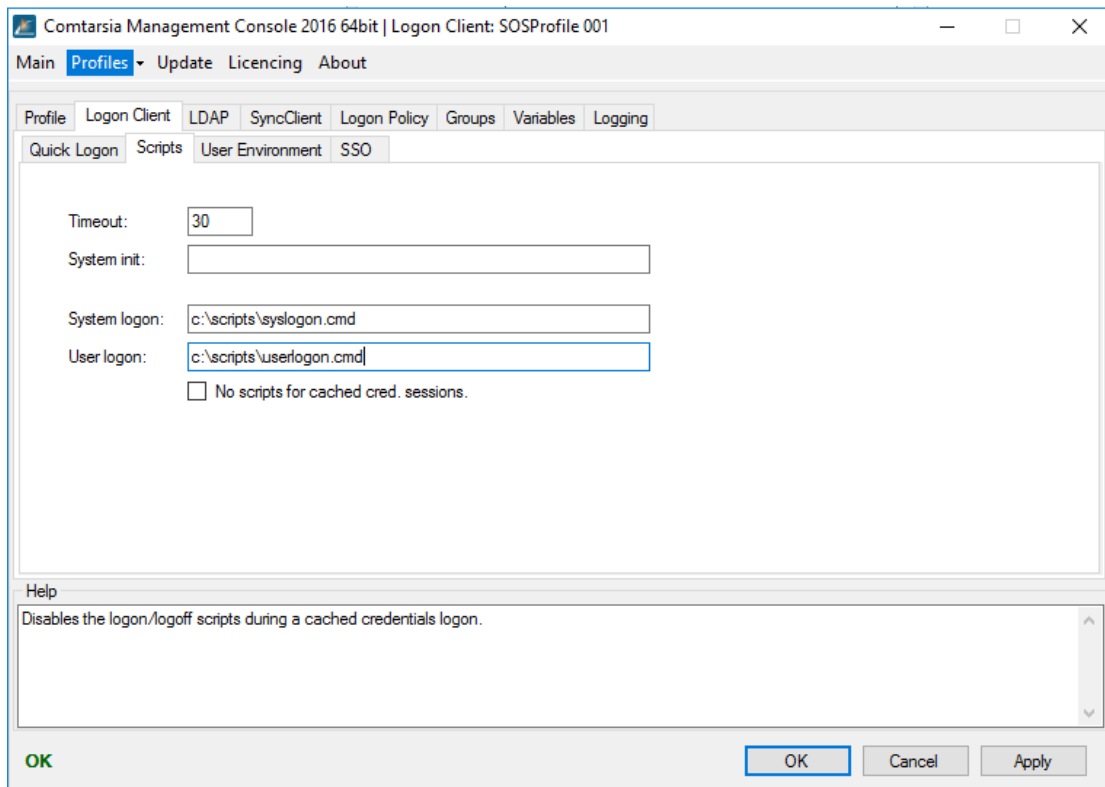
[Password](#)

Defines the password which has to be used for the quick logon.

[Domain](#)

Specifies the quick logon domain. To use an existing local user, this value has to be set to "local" or "%computername%"; otherwise an LDAP logon is performed with the predefined user credentials.

6.1.3 Scripts



The [Timeout](#) parameter specifies the time in seconds within which the scripts have to complete before the Comtarsia Logon Client terminates them.

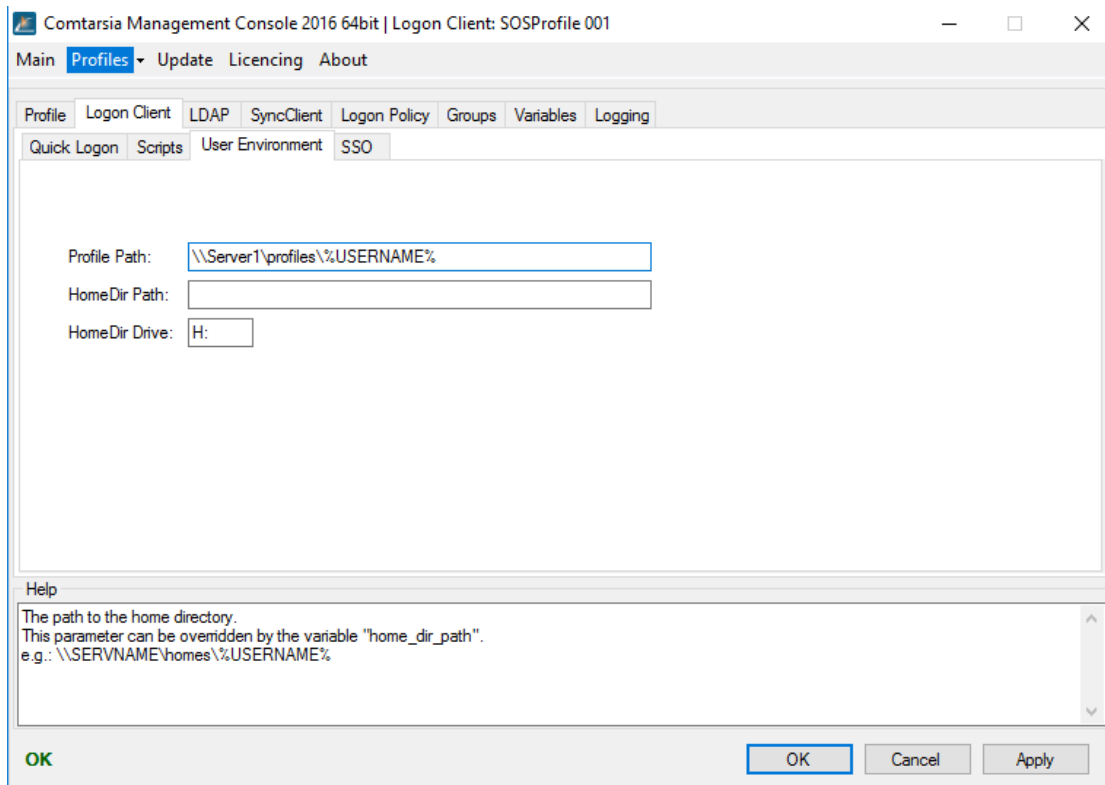
The [System Init Script](#) is run in the system context at the system startup.

The [System Logon Script](#) is run with system privileges in the system context at each logon.

The [User Logon Script](#) is run with user privileges in the user context at each logon.

If the parameter [No Logon/Logoff scripts for cached cred. Sessions](#) is enabled, the "logon scripts" will be inactive during an offline-/cached credentials logon.

6.1.4 User Environment



The parameter [Profile Path](#) specifies the path to the user profile which has to be assigned to local users.

The parameter [HomeDir Path](#) specifies which path should be assigned as local user's as the "home dir path".

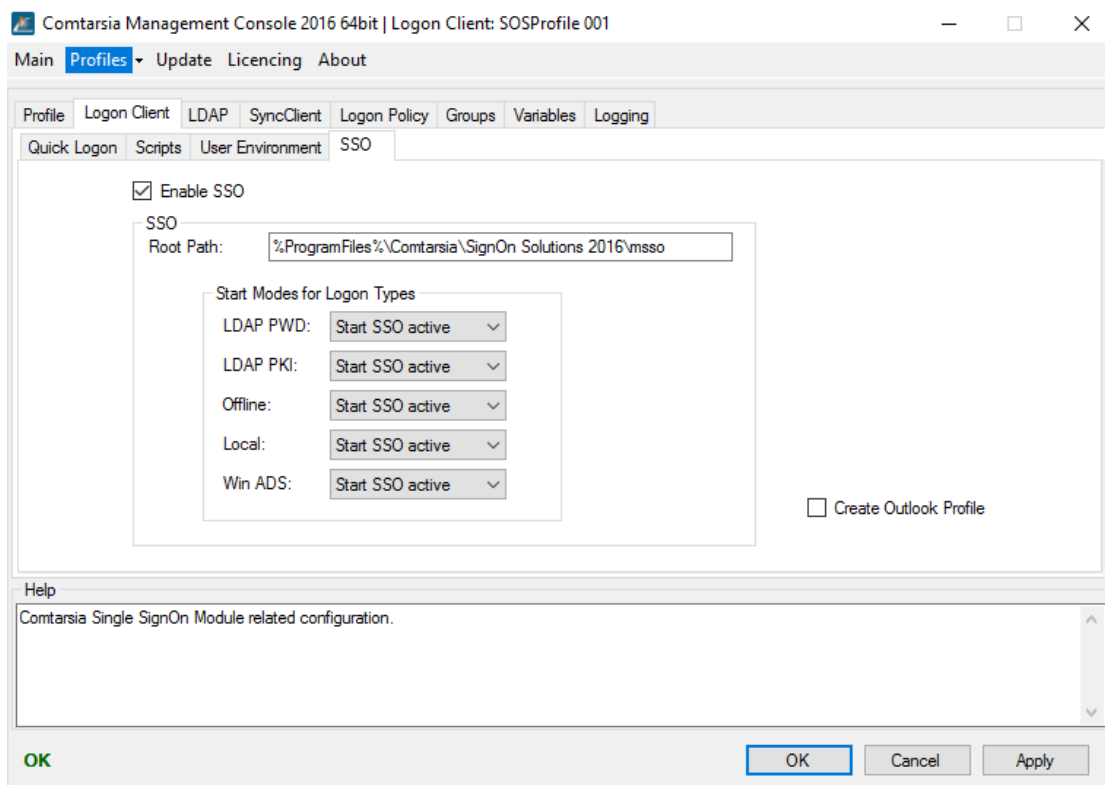
The parameter [HomeDir Drive](#) defines which drive letter should be assigned as the local user's "home dir drive".

In "Domain user mode" (activated [Enable Domain Logon](#)), the Comtarsia Logon Client is unable to assign these values to the domain users (due to privileges). Instead, the Comtarsia SignOn Gate (Agent Configuration) has to handle the user paths.

The default profile path can be assigned via the following value in the Windows System Registry:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\Default

Useful tips about customizing default user profiles and mandatory user profiles under Windows Vista, Windows 7 and Windows Server 2008 can be found in this Microsoft article: <http://support.microsoft.com/kb/973289/de>

6.1.5 SSO



[Enable SSO](#)

Enables the Comtarsia Managed Single SignOn (ComtMSSO) module. (this module has to be installed separately)

[Root Path](#)

Defines the path to the root directory of the ComtMSSO installation.

Start Modes for Logon Types

Specifies the desired start mode for the Comtarsia Single SignOn module dependant on the logon mode.

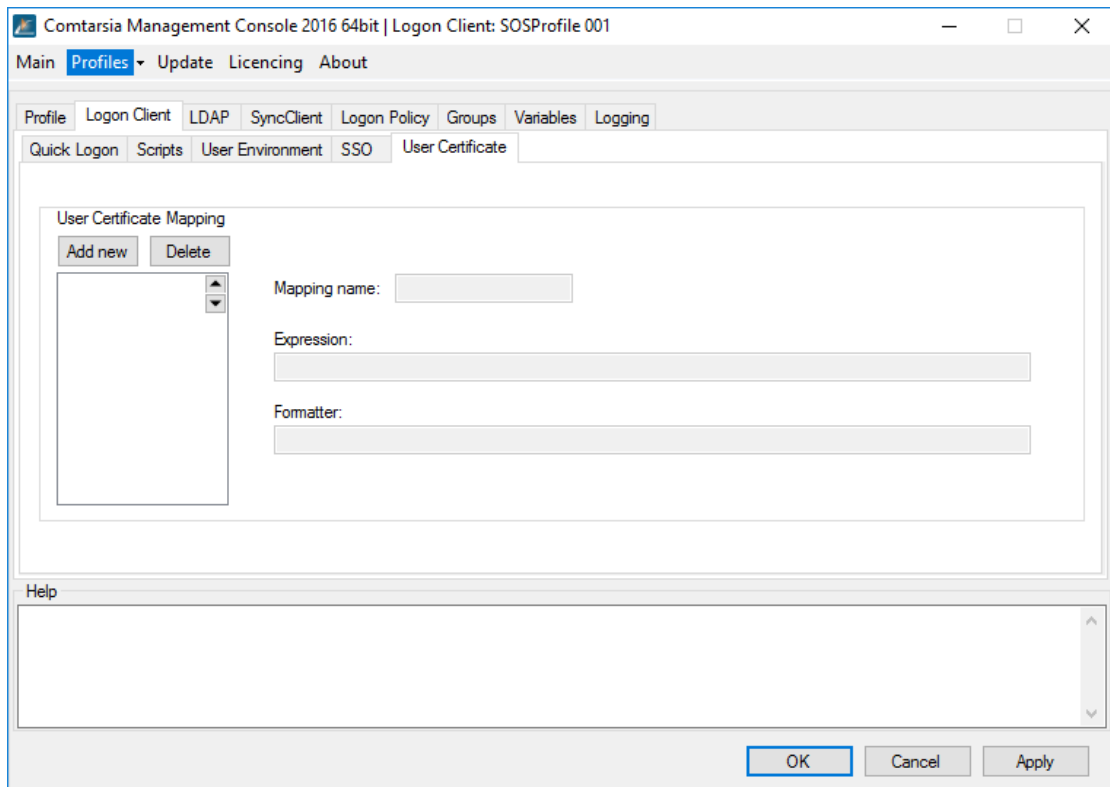
Start Modes:

- Don't start SSO: The ComtMSSO module won't be loaded
- Start SSO inactive: The ComtMSSO module will be loaded, but is set "inactive". (The user can enable it via the tray icon, when needed)
- Start SSO active: The ComtMSSO module will be loaded normally.

Logon Types: (via the Comtarsia logon tile)

- [LDAP PWD](#): LDAP-logon via user-password authentication
- [LDAP PKI](#): LDAP-logon via smartcard/token authentication
- [Offline](#): offline logon
- [Local](#): local logon
- [Win ADS](#): active directory logon

6.1.6 User Certificate



This tab is only available in PKI Mode. (see: [Logon Client - General - Authentication mode](#))

A [User Certificate Mapping](#) specifies a regular expression to map the Certificate DN (subject) of the user to an LDAP user dn. Several User Certificate Mappings can be defined which will be tried in order (top to bottom). The first matching [expression](#) will be used by the Logon Client to determine the LDAP user DN.

The [Mapping name](#) can be any name as it only serves organisational purposes.

The parameter [Expression](#) specifies the regular expression. If the certificates DN (subject) matches with this expression, the [Formatter](#) will be used to determine the resulting LDAP User. (The resulting string will be used to determine the LDAP User)

The parameter [Formatter](#) defines how to map the matching regular expression.

Example:

[Expression:](#) `^[Cc][Nn]=([^\,]*)\,`

[Formatter:](#) `uid=$1,ou=users,dc=company,dc=com`

Certificate DN: `cn=mustermann, ou=example, cn=controlling`

Resulting LDAP DN: `uid=musterman,ou=users,dc=company,dc=com`

Certificate DN: `cn=mustermann2, dc=company`

Resulting LDAP DN: `uid=musterman2,ou=users,dc=company,dc=com`

6.2 LDAP

6.2.1 Server

LDAP server specific configuration.

The screenshot shows the 'LDAP Servers' configuration window in the Comtarsia Management Console. The window title is 'Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001'. The main menu includes 'Main', 'Profiles', 'Update', 'Licencing', and 'About'. The 'LDAP' tab is active, with sub-tabs for 'Server', 'Users', 'User Object', and 'Groups'. On the left, there is a list of LDAP servers: 'nsldap1.comtarsia.com' (selected) and 'nsldap2.comtarsia.com'. Below the list are 'Add new' and 'Delete' buttons. The main configuration area contains the following fields:

LDAP host:	nsldap1.comtarsia.com	Priority:	0
SSL mode:	SSL without trusted server certificate	AuthMethod:	Simple
LDAP port:	636	LDAP API:	Microsoft
Server type:	OpenLDAP	<input type="checkbox"/> Follow referrals	
Base DN:	o=comtarsia		
LDAP timeout:	10		

At the bottom, there is a 'Help' section with the text: 'Configure LDAP Server, Port and other connection specific settings.' and buttons for 'OK', 'Cancel', and 'Apply'.

[LDAP host](#)

Specifies the primary LDAP server.

[Failover LDAP host](#)

Specifies a failover LDAP server. This host will only be contacted if the first LDAP server couldn't be reached.

[SSL mode](#)

This parameter specifies if, and which SSL mode should be used for the LDAP communication. (See: [LDAP over SSL](#))

[LDAP port](#)

The port of the LDAP servers. (default: 389). If another SSL mode is used, the port has to be changed to that LDAP-SSL port. (default for SSL-communication: 636)

[Server type](#)

Defines which LDAP server software is in use. This is necessary so that the Comtarsia Logon Client is able to evaluate server specific responses properly (eg: LDAP password policy controls).

[Base DN](#)

Specifies the baseDN of all LDAP-operations.

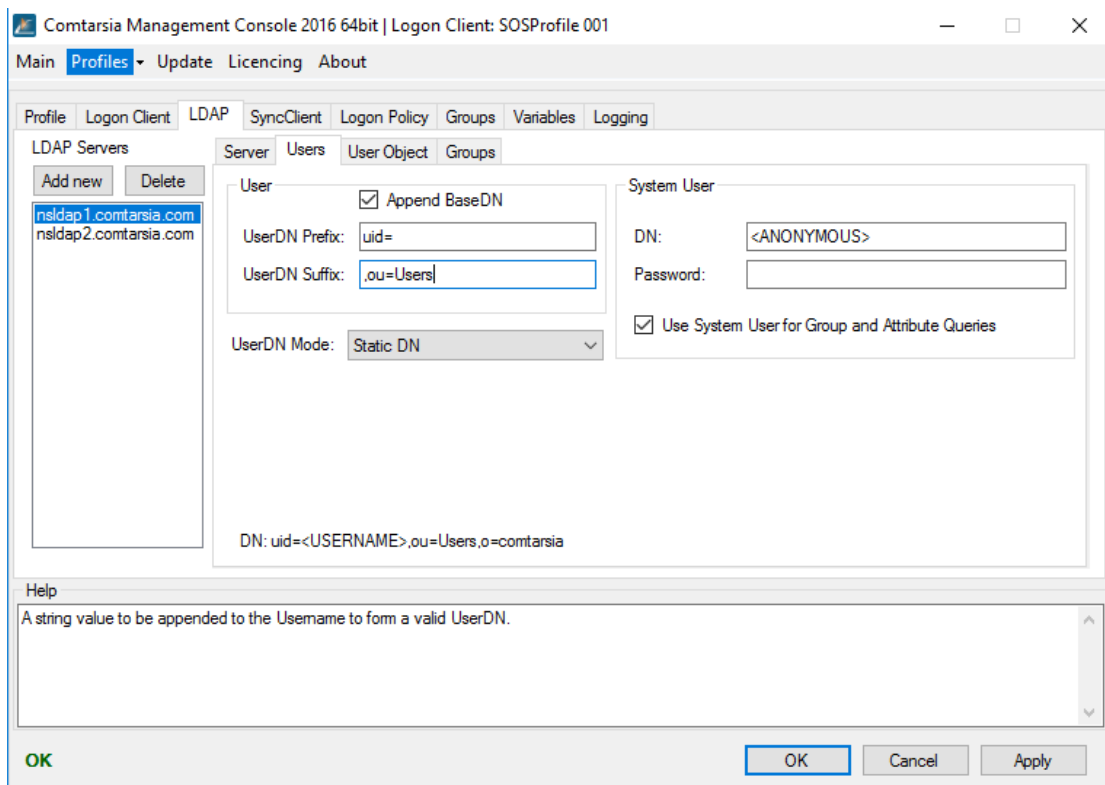
[LDAP timeout](#)

Specifies the timeout within which the LDAP-communication has to be finished; otherwise the logon process will be cancelled.

6.2.2 Users

The configuration of "how to determine the LDAP user".

Static DN



[Append BaseDN](#)

If this parameter is enabled, the BaseDN is appended to the UserDN. (Default and recommended)

[UserDN Prefix](#)

Defines the naming attribute of the LDAP user. The specified value is used for the "Bind as User" operation (static DN), as well as for the LDAP user search (if enabled).

[UserDN Suffix](#)

This suffix is appended to the user name for the "Bind as User" (static DN) operation.

UserDN Mode ([searchForUser](#), [ouSearchListMode](#))

Defines how the Logon Client should determine the LDAP DN of the LDAP user object. „Static DN" defines that the UserDN should be constructed from the specified values, and that this resulting userDN should be used directly for the LDAP bind operation. (Also see: [LDAP Users from Multiple OUs](#))

DN: Shows the resulting userDN which will be used for the LDAP bind; or, in case of a different "UserDN Mode", the resulting LDAP search string.

Search for User

The screenshot shows the 'LDAP' configuration window in the Comtarsia Management Console. The window title is 'Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001'. The main menu includes 'Main', 'Profiles', 'Update', 'Licencing', and 'About'. The 'LDAP' tab is active, with sub-tabs for 'Server', 'Users', 'User Object', and 'Groups'. On the left, there is a list of LDAP Servers with 'nsldap1.comtarsia.com' and 'nsldap2.comtarsia.com'. The 'User' configuration section includes a checked 'Append BaseDN' checkbox, 'UserDN Prefix' set to 'uid=', and 'UserDN Suffix' set to ',ou=Users'. The 'UserDN Mode' is set to 'Search for User as User'. Below this, there are two unchecked checkboxes: 'Ignore "no unique user"' and 'Failover on "user not found"'. The 'System User' section has 'DN' set to '<ANONYMOUS>' and a checked 'Use System User for Group and Attribute Queries' checkbox. At the bottom, the resulting DN is displayed as 'DN: uid=<USERNAME>,ou=Users,<OU>,o=comtarsia'. A 'Help' section at the bottom left contains the text 'LDAP specific configuration.'. The window has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

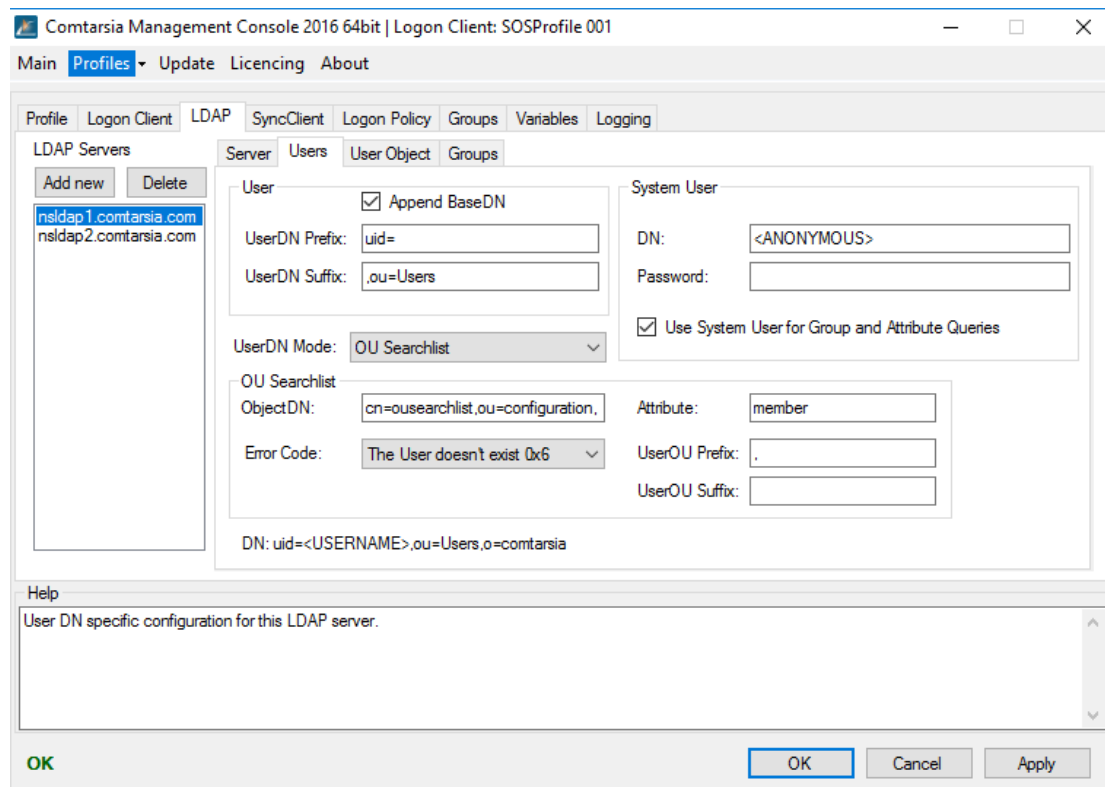
[System User > DN](#)

Defines a full LDAP DN of a dedicated LDAP system user which will be used for the LDAP search operation (Both for "UserDN Mode: Search for User", and "UserDN Mode: OU Searchlist"). UserDN Modes, other than "static DN" are needed to find LDAP users in case they're in different containers/OUs. (Also see: [LDAP Users from Multiple OUs](#), and [Search for User](#))

[System User > Password](#)

Defines the password of the LDAP system user. The password is stored encrypted.

OU Searchlist



OU Searchlist

Also see: [LDAP Users from Multiple OUs](#), and [OU Searchlist](#)

OU Searchlist > ObjectDN

Specifies which LDAP object contains the list of OUs ([OU Searchlist](#)).

OU Searchlist > Attribute

Specifies which LDAP attribute of that OU Searchlist LDAP object contains the single OU-values. (multivalue attribute)

OU Searchlist > Error Code

Defines which LDAP error should be returned in case the User wasn't found in any of the OUs.

OU Searchlist > UserOU Prefix

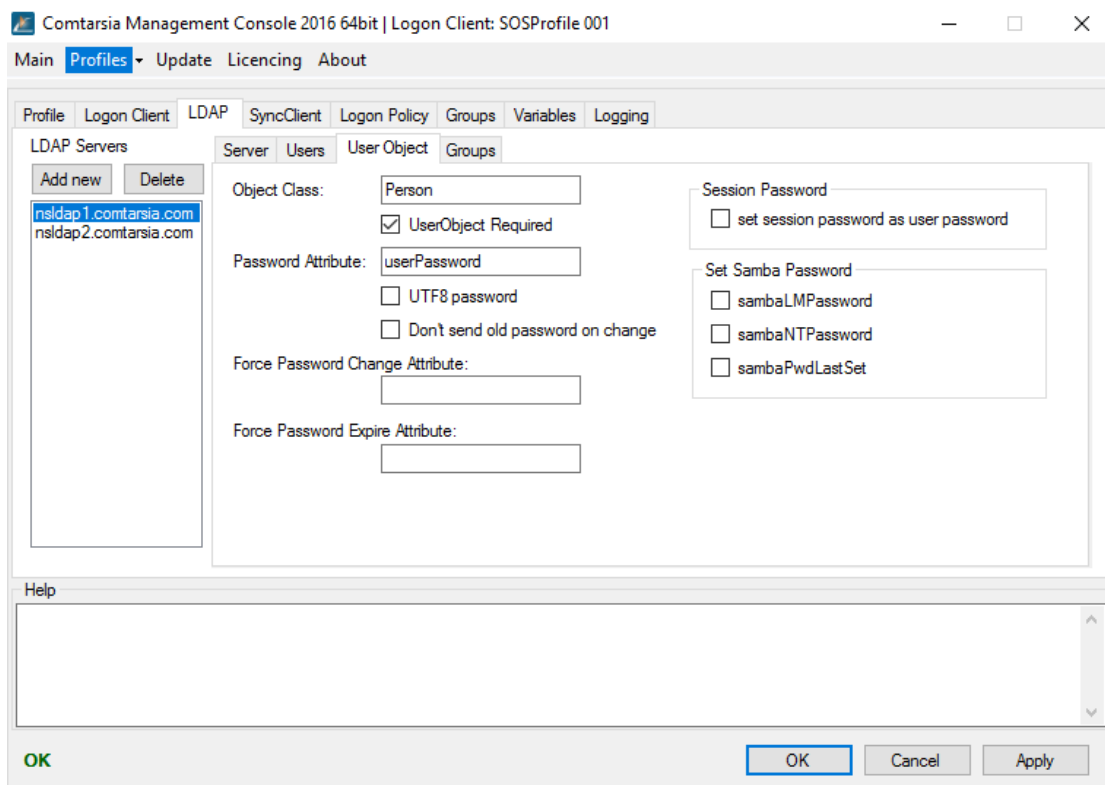
Defines a prefix which will be used to construct the particular user DNs.

The possible UserDNs are constructed in the following way:

<UserDN Prefix><USERNAME><UserDN Suffix><UserOU Prefix><OU><UserOU Suffix>, <baseDN>

(Also see: [LDAP Users from Multiple OUs](#), and [OU Searchlist](#))

6.2.3 User Object



User Object

[Object Class](#)

Defines which LDAP ObjectClass has to be used to determine the LDAP-user (for Search For User and OU Searchlist).

[UserObject Required](#)

If this option is enabled, a logon will only be allowed if the LDAP-user was actually found in the LDAP directory. This usually isn't necessary, unless the LDAP server allows bind requests of non-existent/wrong users.

[Password Attribute](#)

Defines in which LDAP attribute of the LDAP user object the password is stored.

[UTF8-password](#)

If this option is enabled, the password will be sent UTF8-encoded during the logon, as well as during password-changes. This also affects the system user password.

[Don't send old password on change](#)

If this option is enabled, the old password won't be sent together with the new password during a password change request. (Default: old password will be sent. Recommended)

[Set Samba Password](#)

The following options can be used to synchronize the LDAP user password with the Samba Password of the LDAP user object. This is useful if the LDAP user objects are also used as samba users.

[sambaLMPassword](#)

Updates the LDAP user attribute "sambaLMPassword" with the LM-hash of the user password.

[sambaNTPassword](#)

Updates the LDAP user attribute "sambaNTPassword" with the NT-hash of the user password.

[sambaPwdLastSet](#)

Updates the LDAP user attribute "sambaPwdLastSet" with the current time stamp (at each logon), to avoid an expiration of the samba password.

Session Password

During a smartcard logon, a session password is generated (dependant on the session password mode), by using the user's private key. The generated session password will be set as Windows user password and if the Sync Client is enabled, it will also be sent to the SignOn Proxy for synchronisation.

[set session password](#)

The session password will be written into the configured "password attribute" of the LDAP user object.

Warning: As the users don't know their generated session passwords, they won't be able to authenticate via the LDAP directory via user+password.

[password template](#)

This value specifies a template for the generation of the session password.

Following characters can be used:

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

[interval mode](#)

This option sets the config "[smartCardSessionPasswordMode](#)" to 1. (interval mode). The interval mode ensures that the generated password stays the same over specified time spans, but also that different workstations generate the same session password. This prevents synchronisation/network-resource access problems if users work on different computers on the network.

[validity](#)

Specifies the amount of '[validity units](#)' a session password remains the same.

[validity units](#)

Specifies the unit of the "[validity](#) (amount)".

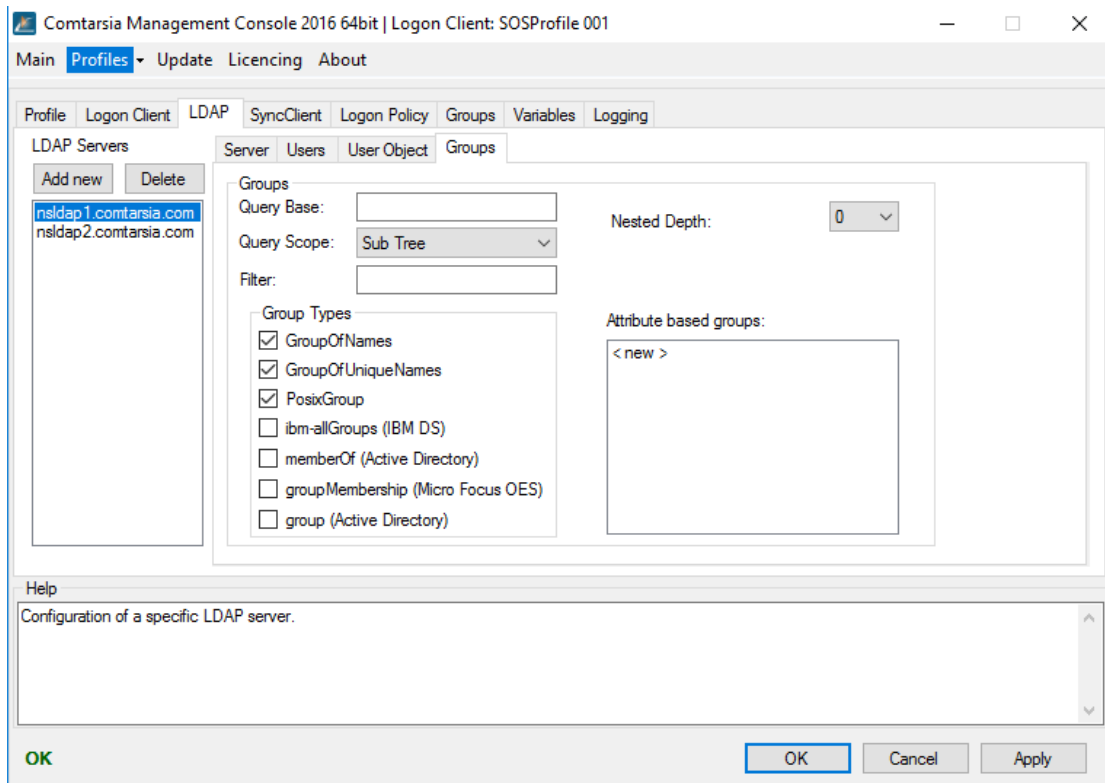
[offset](#)

Specifies an offset in minutes.

For example: A "validity: 1, validity units: days" password always changes at 0:00 each day. Via the offset, this point in time can be changed (in minutes).



6.2.4 Groups



Query Base

With this option, a different base DN can be defined for the group search. By default (if this option is empty), the configured [LDAP > Server > [Base DN](#)] is used.

Query Scope

Specifies the scope of the LDAP group search

- Base: Only the "Query Base" itself.
- One Level: All entries directly within the "Query Base"
- Sub Tree: The whole tree below the "Query Base"

Filter

Specifies an additional LDAP search filter which will be incorporated into the LDAP group search. Groups that do not match this filter will be left out.

With this, it's possible to (examples):

- Check if a specific attribute is existant: (description=*)
- Check if an attribute starts with/ends with/contains a value: (description=Logon*)
- Check if an attribute has a specific value: (GroupUsage=LogonGroup)
- Check if one of several, or several group-requirements are met: (|(GroupUsage=LogonGroup)(GroupUsage=WinGroup))

Group Types

Specifies which types of groups the Comtarsia Logon Client has to look for. This configuration depends on the group types actually used on the LDAP server.

- GroupOfNames
- GroupOfUniqueNames

- PosixGroup
- ibm-AllGroups: a special LDAP user attribute, which only exists on IBM-Directory servers. (ignores [Query Base](#) and [Filter](#))
- memberOf: a special LDAP user attribute, which only exists on Microsoft Active Directory servers (ignores [Query Base](#) and [Filter](#))

Attribute based groups

With "attribute based groups", it's possible to use attributes of the LDAP user object as if they were groups.

For example, the LDAP user objects have an LDAP attribute "department", it is possible to define "department" as "attributes based group" and use the values of the LDAP attribute "department" as an additional group.



6.3 SyncClient

Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001

Main Profiles Update Licencing About

Profile Logon Client LDAP SyncClient Logon Policy Groups Variables Logging

Enable Sync Client

SignOn Proxy

Primary host: proxy.comtarsia.com

Failover host:

Port: 2003

Connect Timeout: 5

Sync Packet TTL: 20

Display Sync Client Box

Trust Options Client

Certificate OIDs Certificate FQDN

TLS

TLS Key Type PKCS12

CA File: %ProgramFiles%\Comtarsia\SignOn Solution

Cert File: %ProgramFiles%\Comtarsia\SignOn Solution

Key File: %ProgramFiles%\Comtarsia\SignOn Solution

Additional SignOn Request on

CREDUI LDAP Logon

Logged on Password change

Workstation unlock Time span (min): 720

Help

Host name / IP-address of the Proxy Server or placeholder string "SRV_RECORD"(without quotes) for SignOn proxy automatically registered SRV record (_comtsop, _tcp, Port: 2003, Weight: 1, Priority: 1).

OK Cancel Apply

[Enable Sync Client](#)

This option enables the Sync Client. After each successful logon, a Sync-User request will be sent to a specified Comtarsia SignOn Proxy.

SignOn Proxy

[Primary host](#)

Specifies the IP-address or host name of the primary Comtarsia SignOn Proxy.

[Failover host](#)

Specifies the IP-address or host name of a failover Comtarsia SignOn Proxy.

[Port](#)

Specifies the IP-port for the communication to the SignOn Proxy. (default: 2003)

[Connect Timeout](#)

Specifies a connect-timeout in seconds.

[Sync Packet TTL](#)

Specifies a timeout in seconds for the whole synchronization process.

[Display Sync Client Box](#)

If this parameter is enabled, the status of the synchronization is displayed on the upper left corner of the logon screen.



TLS

[CA File](#)

This option specifies the path to the CA-certificate.

[Cert File](#)

This option specifies the path to the user/computer-certificate.

[Key File](#)

This option specifies the path to the user/computer private key.

For more information about the Comtarsia Logon Client <-> SignOn Proxy communication, please refer to the manual [Architectural Manual – SSL Certificates](#) Chapter 2.1.

Additional SignOn Request on

If the parameter [CREDUI LDAP Logon](#) is enabled, a Sync-User request will also be sent after every successful CREDUI LDAP logon.
(eg: For a Windows UAC)



If the parameter [Logged on Password change](#) is enabled, a Sync-User request will also be sent after each LDAP-password change during an active logon session.

If the parameter [Workstation Unlock](#) is enabled, a Sync-User request will also be sent each time the workstation is unlocked.
A time span that has to pass after the last Sync-User request before a new Sync-User request is sent, can be configured via [Time span \(min\)](#).

6.4 Logon

6.4.1 Logon Policy

Comtarsia Management Console 2016 64bit | Logon Client: SOSProfile 001

Main Profiles Update Licencing About

Profile Logon Client LDAP SyncClient Logon Policy Groups Variables Logging

General Session Password PKI MFA / OTP

LogonPolicy - General

Disable local logon

Display offline logon option

Offer offline logon if LDAP server unreachable

Username case policy: auto Lower Case

Disallow grace period login

Don't display last username

Disable user Remove user

RDP mode: 0 - RDP Auto Logon

Force RDP Authentication Windows Policy Setting

Logon Groups

Groups: []

Mode: Allow logon

Check Credentials

Offline session Online session

Check interval (minutes): 10

Logoff session Disable user

Set Account Expire

Account Expire in Minutes: 0

Help

OK OK Cancel Apply

If the parameter [Disable local logon](#) is enabled, the option „LOCAL LOGON“ won't be available on the logon form below the logon tile.

[Display offline logon option](#)

[Offer offline logon if LDAP server unreachable](#)

The parameter [Username case policy](#) specifies whether to force upper- or lower-case letters for the user name, or to allow upper and lower case letters on the logon form.

No Case Policy: Upper- and lowercase is allowed.
Auto Upper Case: All characters will be converted to upper case letters.
Auto Lower Case: All characters will be converted to lower case letters.

If the option [Disallow grace period login](#) is enabled, a password change dialog which will be shown due to a "LDAP logon during the grace login period", can't be cancelled. (The cancel button is disabled)

If the parameter [Don't display last username](#) is enabled, the username of the last successful logon won't be shown in the logon form.

If the parameter [Remove user](#) is enabled, the local user and his/her user profile will be removed after logging off from an LDAP-logon session. This only affects users who have been created by the Comtarsia Logon Client during an LDAP-logon (marked with the user description: "SERV_TEMP_USER").

In domain mode (i.e. there are no local users), this option is ignored. However, one may use the following Windows policy to remove local roaming profiles after each logon session:
REG_DWORD:HKLM\Software\Policies\Microsoft\Windows\System\DeleteRoamingCache = 1

[Disable RDP autologon](#)

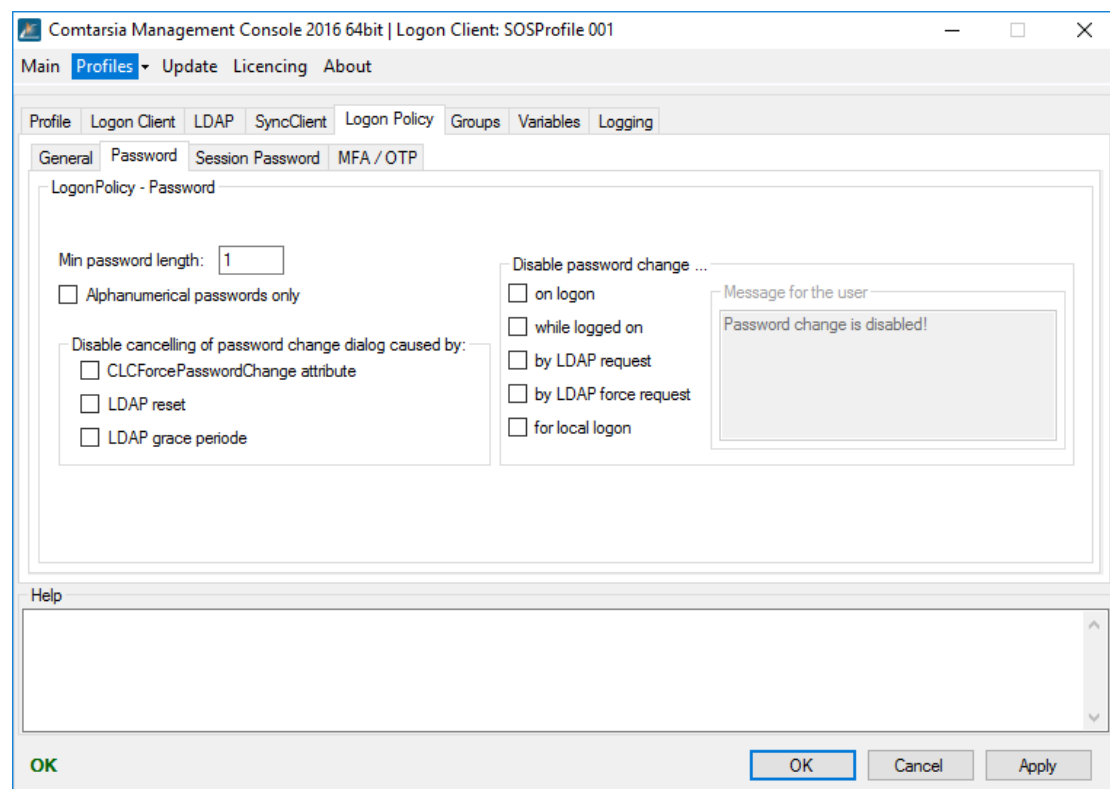
Logon Groups

Logon Groups can be used to allow/deny the logon of users, based on their LDAP group membership (LDAP groups, attribute based groups).

The field [Groups](#) contains a comma-separated list of group names.

The parameter [Mode](#) defines whether the membership of one of the Logon Groups is required for a logon, or forbids the logon. If the [Groups](#) list is empty, the Logon Groups functionality is inactive.

(See: [LDAP-groups](#) and parameter [Attribute based groups](#))



Password

The parameter [Min password length](#) specifies the minimum length an LDAP password must have during a password change or an LDAP logon. If the current LDAP password is shorter, the user will be prompted to change it in order to log on.

The parameter [Alphanumerical passwords only](#) can be used to make sure that users can use alphanumeric characters only, in their passwords. (no special characters are allowed)

Cancelling of the password change dialog can be prevented in the following cases:

- [CLCForcePasswordChange attribute](#): if the password dialog is shown due to the set LDAP attribute "CLCForcePasswordChange" of the LDAP user object.

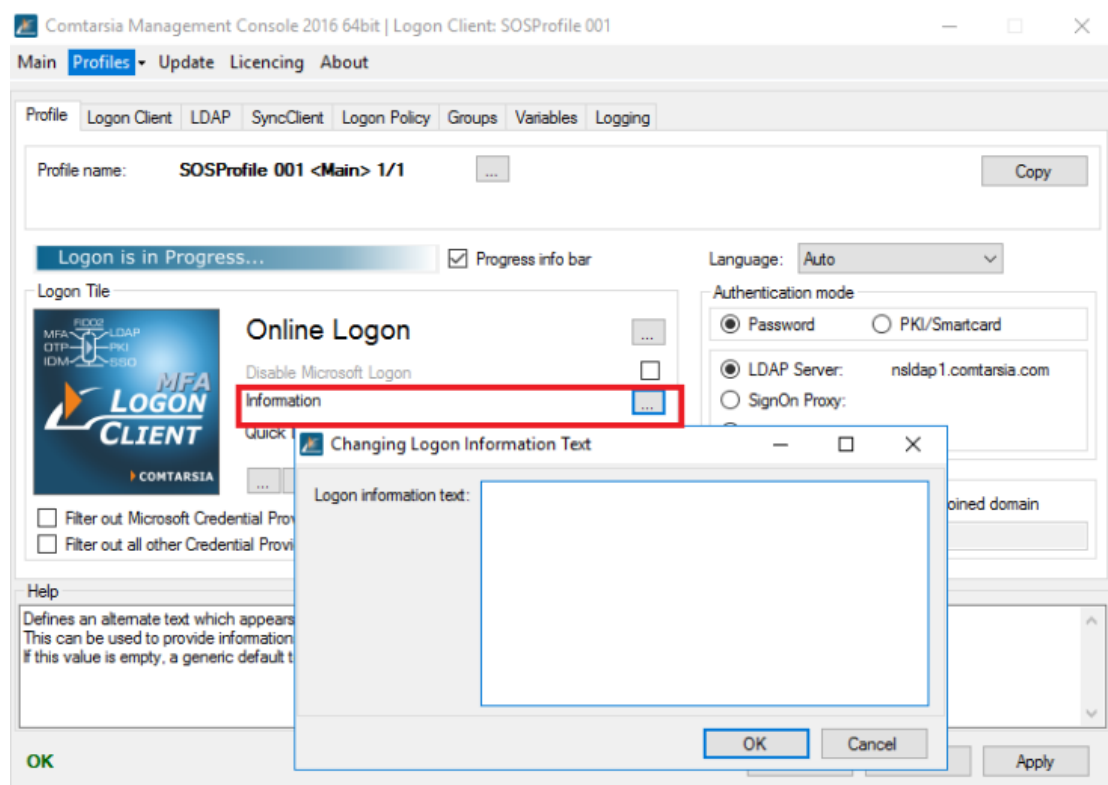
- [LDAP reset](#): if the password dialog is shown due a “must change on reset”-password policy control returned by the LDAP server.
- [LDAP grace periode](#): if the password dialog is shown due to a “grace period login” (returned password policy control by the LDAP server).

It’s possible to prevent the password change in the following cases:

- [on logon](#): via the check box “change password” on the logon screen
- [while logged on](#): during a logged-on session. (Ctrl+Alt+Del screen)
- [by LDAP request](#): if the LDAP server requested a password change (eg: via a “warn expire”).
- [by LDAP force request](#): if the LDAP attribute “CLCForcePWDchange” is set for the LDAP user, or the LDAP server returned a “must change password” (eg: due to the LDAP password policy “must change on reset”).
- [for local logon](#): during a local logon.

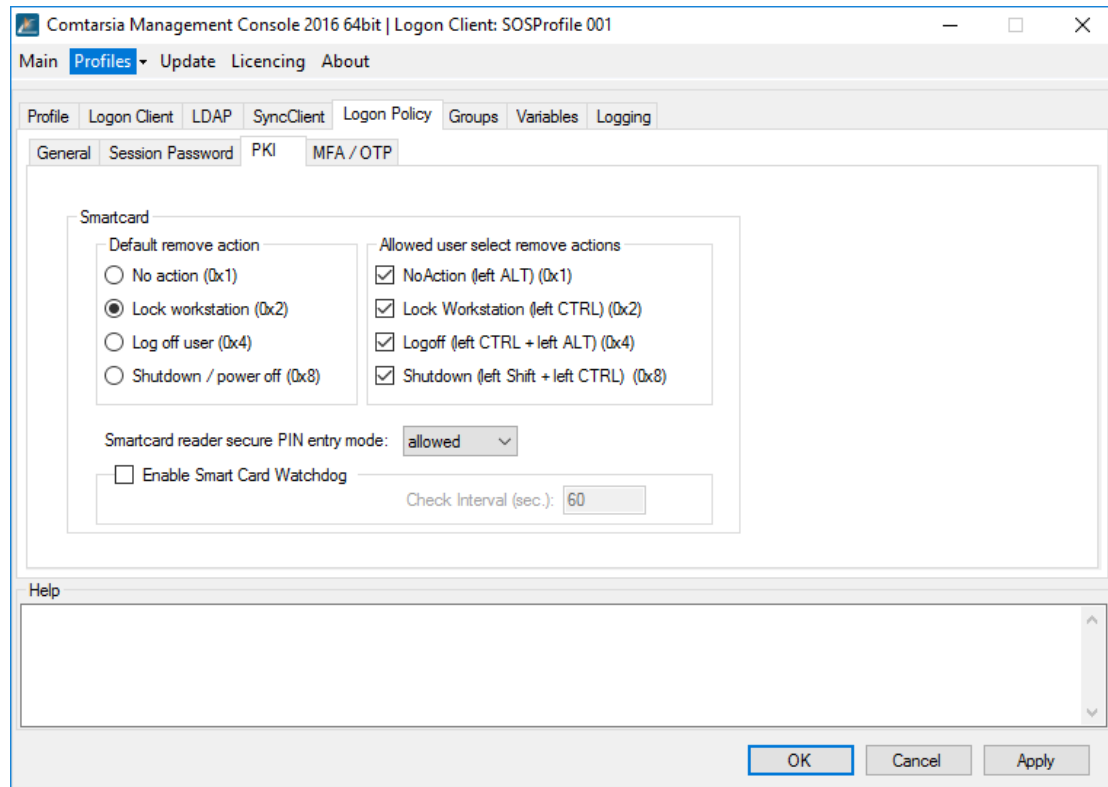
If a password change is prevented due to one of the aforementioned policies, the user will receive the message configured in [Message for the user](#). This is useful if it’s required that the users change their LDAP passwords over a web interface.

6.4.2 Logon Info

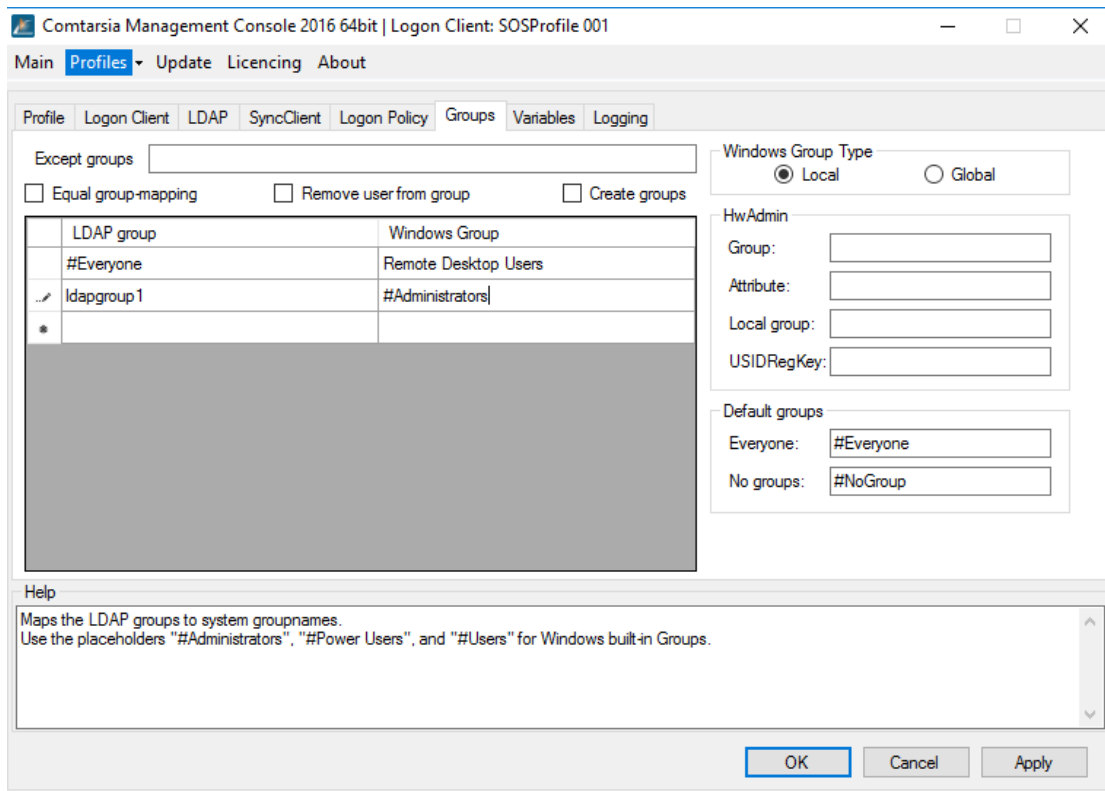


The parameter [Logon Info Text](#) specifies an alternative text users will see if they click on the “Information” link on the logon form. By default (if the text isn’t set), a generic text will be displayed. It’s suggested to enter support information, like a phone hotline, users need in case they can’t log on (eg: password expired, account locked, etc.)

6.4.3 PKI



6.5 Groups



The parameter [Except groups](#) defines a comma separated list of group names for which no operation should be carried out. (The user won't be added to, nor removed from these groups.)

The parameter [Create groups](#) defines if LDAP groups (or groups resulting from the group mapping), which don't exist locally, should be created automatically.

The parameter [Windows Group Type](#) defines whether local or global groups should be used. "Global groups" can only be used on a windows domain controller. Global groups are domain global whereas local groups exist on the client computer only. On a client computer (any non-domain controller), this option has to be set to "Local".

If [Equal group-mapping](#) is enabled, the group names won't be altered by the mapping list. Each LDAP Group will be mapped to a system group one-to-one. Otherwise, a manual "group mapping" list can be specified. (also see: [LDAP-groups](#) and [AttributeBasedGroups](#))

HwAdmin

The HwAdmin functionality allows to specify a list of computers of which a user is Administrator. The list is stored in a specified [HwAdmin Attribute](#) of the LDAP user object. The parameter [HwAdmin Group](#) specifies which LDAP-groups enables the "HwAdmin" functionality for a user.

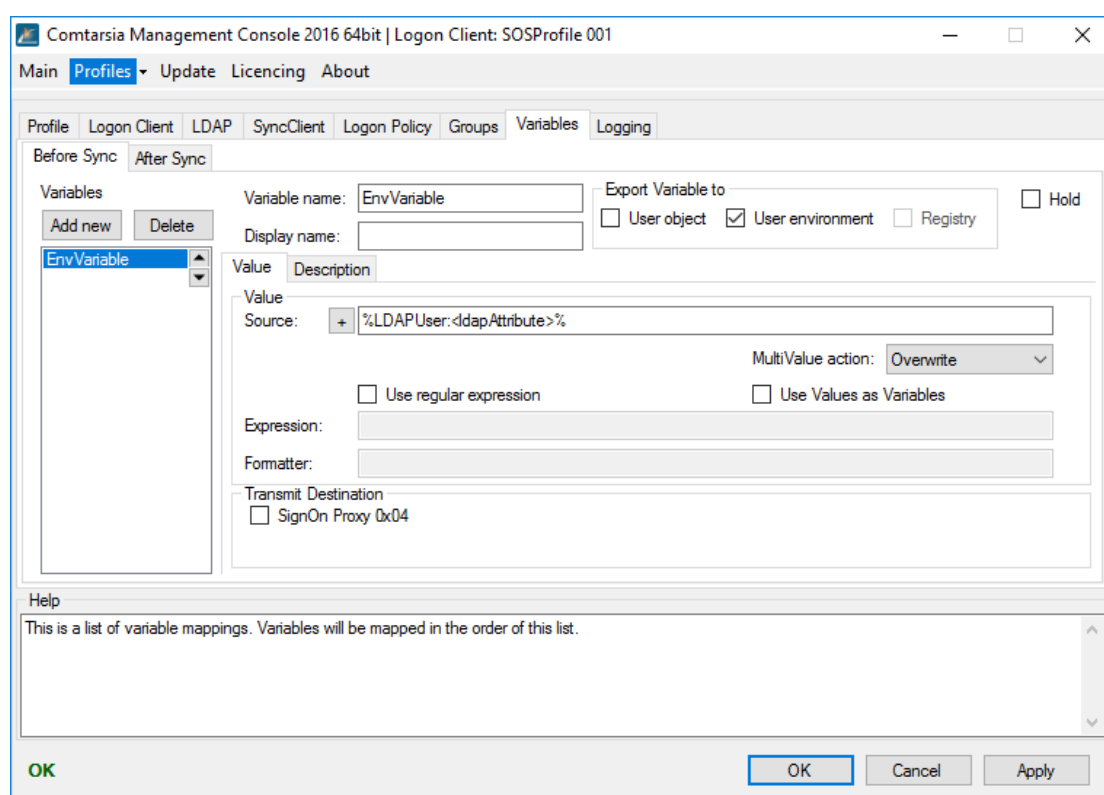
The parameter [HwAdmin Attribute](#) specifies which LDAP attribute of the LDAP user object contains the list of computer names for which that user is an administrator. If both criterias are met, the user will be added to the local administrators group. (The name of that group has to be specified via the parameter [LocalAdminGroup](#))

Default groups

Every user who successfully authenticated against the LDAP will be member of the dummy group specified in [Everyone](#). This group can also be used in the group mapping list.

The parameter [No groups](#) specifies a dummy group which should be assigned to every successfully authenticated user who has no LDAP groups (inclusive [AttributeBasedGroups](#)) This group can also be used in the group mapping list.

6.6 Variables



Variables are placeholders for variable values which can be obtained from different sources and processed and exchanged between the products within the Comtarsia product family. The values can also be exported to the respective target systems.

Examples for possible sources: LDAP user object; Windows registry, Computer environment variables, internally provided values.

Examples for possible export targets: Attributes of the Windows user object (ie. comment, home/profile path, full name); user environment.

The variables can be used/modified at two different points in time which are defined by the tabs "[Before Sync](#)" and "[After Sync](#)".

[Before Sync](#): Variables will be accessed before the user synchronisation (thus they can also be sent to the SignOn Proxy/SignOn Agent)

[After Sync](#): Variables will be processed after the user synchronisation. Thus values can be sent back by the SignOn Agent/SignOn Proxy and processed. The variables will also be processed in order (from top to bottom). The up/down arrow buttons can be used to change that order.

The [Variable name](#) specifies the name of the variable. If the value has to be exported, the name has to match with the name of the target variable and/or the name of the target attribute.

The [Display name](#) specifies the name to be displayed in the variables list (at the left side). This parameter is used by the configuration utility only and is meant to help organising the variables.

Via "[Export Variable to](#)", variables can be exported to different target systems.
[User object](#): The value of the user object (with the name of the value) will be set to the value of the variable.
[User environment](#): The variable will be exported into the user environment (Windows environment variable).

With [Hold](#) variables can be disabled temporarily.

Value

The [Source](#) defines the source/data of the variable. This field can contain text as well as other variables (between two '%'). To use '%' as part of the value '%%' has to be used and will be replaced by '%' rather than used as a variable. The "+" button offers a dialog to add easy-to-use variable source templates.

The [MultiValue action](#) defines how to handle multi value variables (variables which represent an array).

Overwrite: A possibly existing value will be overwritten.

Delete: The variable will be deleted.

DeleteValue: The resulting value will be removed from the existing variable (array).

AddValue: The resulting value will be added to the variable (array). (ie. to add a group to the existing list of groups)

[Use regular expression](#) enabled the 'regular expressions' functionality for this variable..

[Expression](#) defines the regular expression which has to be applied to the resolved value (content/data) of the source. If the source also contains variables, these will be replaced before the regular expression is applied.

The [Formatter](#) defines how to build the resulting value by applying the regular expression on the source value.

The [Index](#) can be used to refer to a specific match if a necessarily more ambiguous regular expression results in more than one match. Usually the index is 0 unless it's impossible to make the regular expression specific enough to result in only 1 match.

The [Flags](#) is a bitmask which specifies the operation mode of the regular expression.

Valid Flags:

```
match_default      0,  
match_not BOL     0x00000001, /* first is not start of line */  
match_not EOL     0x00000002, /* last is not end of line */
```




```

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

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

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

```

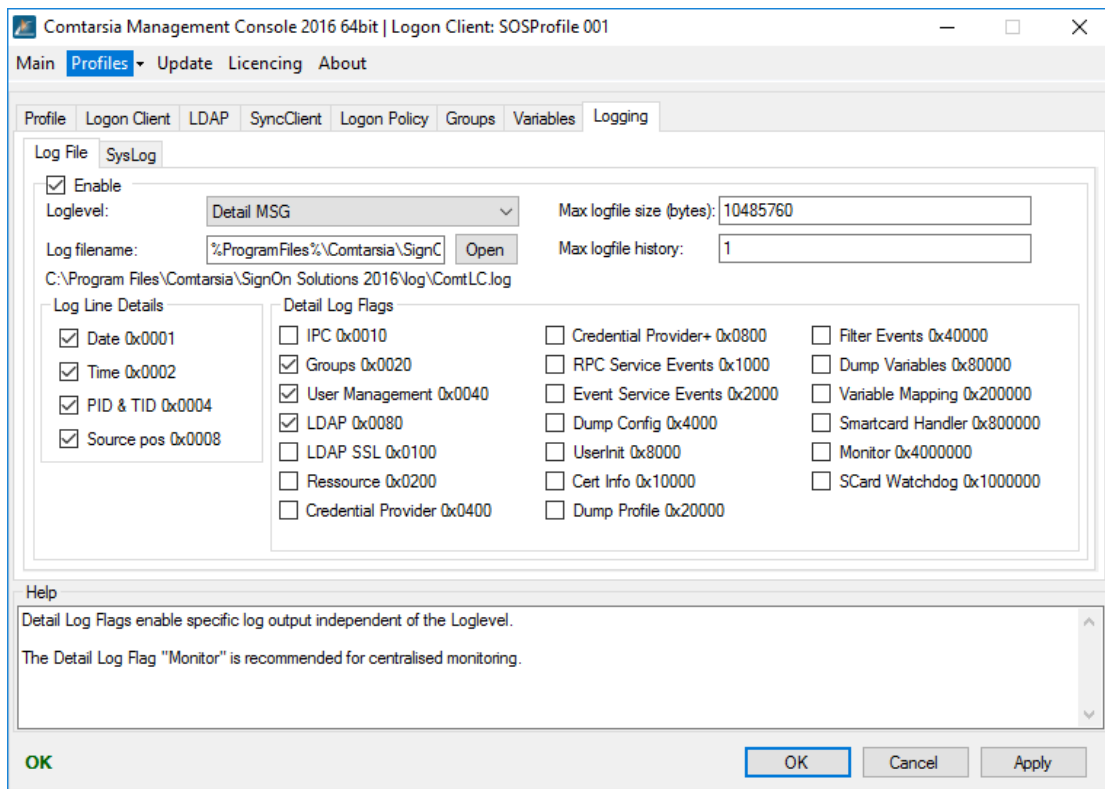
Transmit Destination

The [Transmit Destination](#) specifies to which other Comtarsia SignOn products this variable should be sent to. (Invalid destinations are greyed out)

If the [Transmit Destination](#) 'SignOn Agent 0x8' is set (only possible on the SignOn Proxy) the option [Domains](#) can be used to specify to which SignOn Agent domains this variable should be sent. If this field is empty, the variable will be sent to all SignOn Agents.



6.7 Logging



[Log File Enable](#)

Enables/disables writing to the log file.

[LogLevel](#)

The LogLevel defines the verbosity of the log written to the specified file. The "detail log flags" are handled independently of the LogLevel.

Eg: It's perfectly valid to use "LogLevel"=None, and "Detail Log Flags"=Monitor to only log "monitoring"-messages.

- None: No logging, except detail log flags.
- Error: Only errors and specified detail log flags.
- Exception: As Error, and exception messages.
- Warn: As Exception, and warnings.
- Info: As Warn, and additional information
- Detail MSG: Everything (except unspecified log flags which have to be enabled separately)

[Log filename](#)

Defines the path to the log file.

[Max logfile size](#)

Defines the size at which the logfile should be rotated.

[Max logfile history](#)

Defines the amount of logfiles to be rotated.

[Detail Log Flags](#)

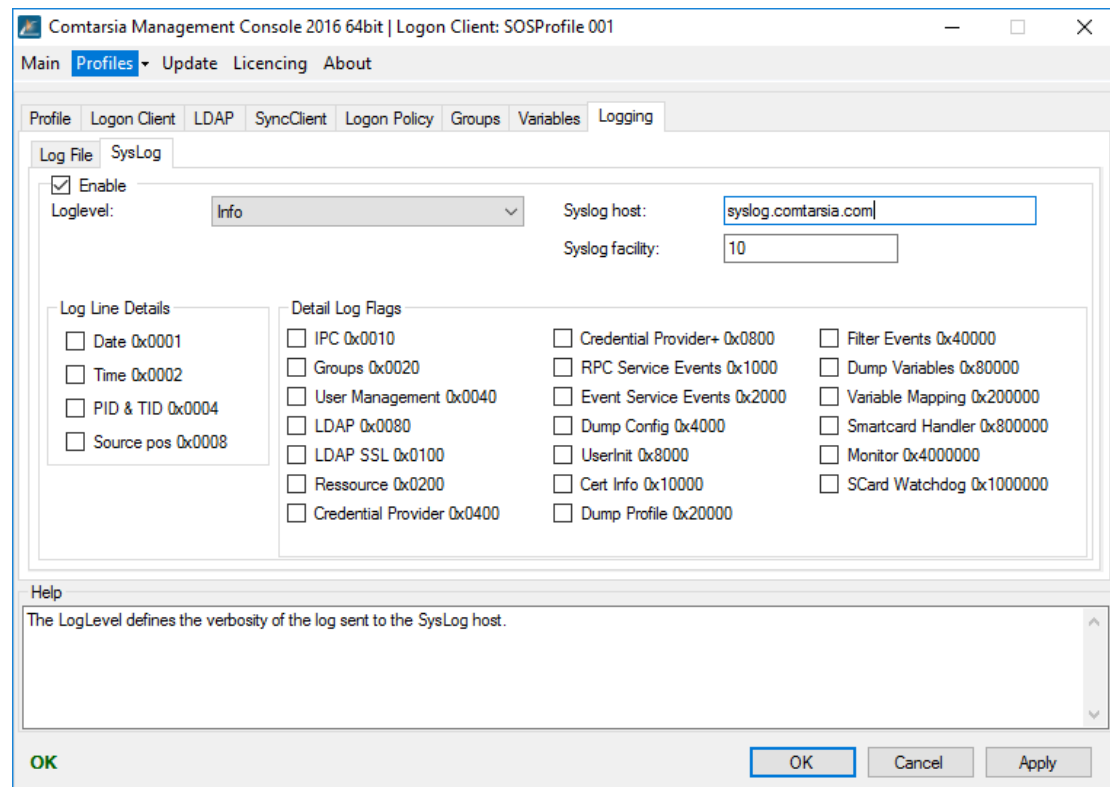
Detail Log Flags enable specific log output independent of the LogLevel.

The Detail Log Flag "Monitor" is recommended for centralized monitoring.

[Log Line Details](#)

Defines which details are to be included in each log line.

- Date
- Time
- PID & TID: Process and thread ID.
- Source pos: The position (line) in the source code.



[SysLog](#)

[Enable](#)

Enables/disables forward of log messages to a syslog server.

[LogLevel](#)

The LogLevel defines the verbosity of the log written to the specified file. The "detail log flags" are handled independently of the LogLevel.

E.g.: It's perfectly valid to use "LogLevel"=None, and "Detail Log Flags"=Monitor to only log "monitoring"-messages.

- None: No logging, except detail log flags.
- Error: Only errors and specified detail log flags.
- Exception: As Error, and exception messages.
- Warn: As Exception, and warnings.
- Info: As Warn, and additional information
- Detail MSG: Everything (except unspecified log flags which have to be enabled separately)

[Syslog host](#)

Defines the central SysLog host to which the SysLog messages will be sent.

[Syslog facility](#)

Specifies the SysLog facility of the log messages.

[Detail Log Flags](#)

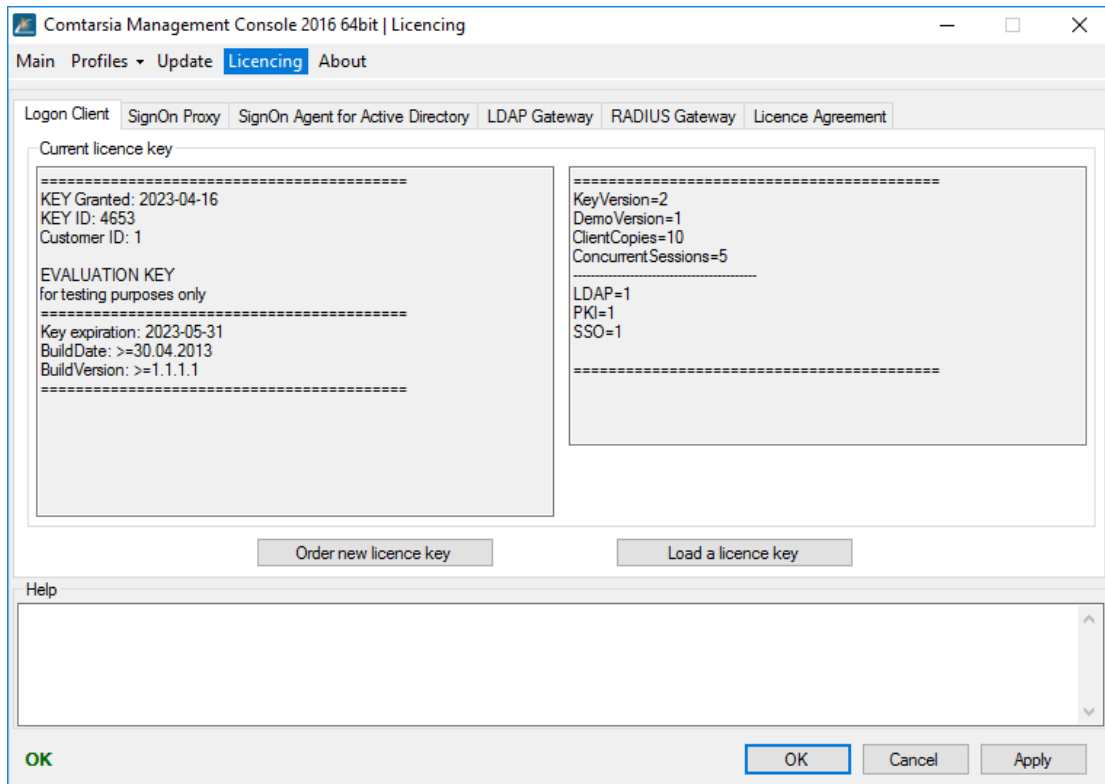
Detail Log Flags enable specific log output independent of the Loglevel. The Detail Log Flag "Monitor" is recommended for centralized monitoring.

[Log Line Details](#)

Defines which details are to be included in each log line.

- Date
- Time
- PID & TID: Process and thread ID.
- Source pos: The position (line) in the source code.

6.8 Licensing



Displays information about the installed license key. The button "Load another license key" opens a file chooser dialog and copies the specified license key to the directory %ProgramFiles%\Comtarsia\SignOn Solutions 2016\Key.

7. Parameter Description

[HKLM\SOFTWARE\Comtarsia]

[.\SignOn Solutions 2016]

path

path=REG_SZ:"C:\\Program Files\\Comtarsia\\SignOn Solutions 2016"
Product installation directory.

[.\SignOn Solutions 2016\Components]

[.\SignOn Solutions 2016\DefaultProfiles]

LogonClient

LogonClient=REG_SZ:"SOSProfile 001"

[.\SignOn Solutions 2016\LogonClient]

userInit

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

credProvMode

credProvMode=REG_DWORD:0

detectedCredProvMode

detectedCredProvMode=REG_DWORD:0

displayCredProvConfig

displayCredProvConfig=REG_DWORD:0

[.\SOSProfile *]

language

language=REG_SZ:"Auto"

Language of the user interface. (Logon screen, messages)

profileName

profileName=REG_SZ:""

profileComment

profileComment=REG_SZ:""

profileConfigVersion

profileConfigVersion=REG_SZ:""



[.\SOSProfile *\Group]

Configuration of the system specific groups.

equalGroupMapping

equalGroupMapping=REG_DWORD:0

0: use the groupmapping list to map LDAP groups to system groups

1: use the LDAP groups 1:1 without mapping

exceptGroups

exceptGroups=REG_SZ:""

A comma separated list of group names which should be ignored.

globalGroups

globalGroups=REG_DWORD:0

0: use local system groups

1: Use global groups (only valid on domain controllers)

HwAdminGroup

HwAdminGroup=REG_SZ:""

HwAdminAttribute

HwAdminAttribute=REG_SZ:""

HwAdminUSIDRegKey

HwAdminUSIDRegKey=REG_SZ:""

HwAdminSubOU

HwAdminSubOU=REG_SZ:""

localAdminGroup

localAdminGroup=REG_SZ:""

createGroups

createGroups=REG_DWORD:0

Create non-existing groups.

defaultEveryoneGroup

defaultEveryoneGroup=REG_SZ:"#Everyone"

A default group every LDAP user will be a member of. It can also be used with group mapping.

defaultNoGroup

defaultNoGroup=REG_SZ:"#NoGroup"

A default group every LDAP user who doesn't have any LDAP groups will be a member of.

[.\SOSProfile *\GroupMapping]

[.\SOSProfile *\LDAP]

[.\SOSProfile *\LDAP\Servers]

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

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

priority

priority=REG_DWORD:0

failoverHost

failoverHost=REG_SZ:""

baseDN

baseDN=REG_SZ:"o=comtarsia"

The LDAP baseDN

userDNPrefix

userDNPrefix=REG_SZ:"uid="

userDNSuffix

userDNSuffix=REG_SZ:",ou=sd"

userOUPrefix

userOUPrefix=REG_SZ:""

userOUSuffix

userOUSuffix=REG_SZ:""

userObjectClass

userObjectClass=REG_SZ:"Person"

userObjectRequired

userObjectRequired=REG_DWORD:0

userQueryScope

userQueryScope=REG_DWORD:2

groupTypes

groupTypes=REG_DWORD:7

groupQueryBase

groupQueryBase=REG_SZ:""

groupQueryScope

groupQueryScope=REG_DWORD:2

attributeBasedGroups

attributeBasedGroups=REG_MULTI_SZ:"System.String[]"

userPasswordAttribute

userPasswordAttribute=REG_SZ:"userPassword"

timeout

timeout=REG_DWORD:0xA



port

port=REG_DWORD:0x185

sslMode

sslMode=REG_DWORD:0

serverType

serverType=REG_DWORD:0x0

useUTF8Password

useUTF8Password=REG_DWORD:0

dontSendOldPasswordOnChange

dontSendOldPasswordOnChange=REG_DWORD:0

systemUserDN

systemUserDN=REG_SZ:""

systemUserPassword

systemUserPassword=REG_SZ:""

OUSearchListMode

OUSearchListMode=REG_DWORD:0

OUSearchListErrorCode

OUSearchListErrorCode=REG_DWORD:6

OUSearchListObjectDN

OUSearchListObjectDN=REG_SZ:""

OUSearchListAttribute

OUSearchListAttribute=REG_SZ:""

appendBaseDN

appendBaseDN=REG_DWORD:1

searchForUser

searchForUser=REG_DWORD:0

groupFilter

groupFilter=REG_SZ:""

ignoreNoUniqueUser

ignoreNoUniqueUser=REG_DWORD:0

failoverOnUserNotFound

failoverOnUserNotFound=REG_DWORD:0

setSessionPasswordasUserPassword

setSessionPasswordasUserPassword=REG_DWORD:0

followReferrals

followReferrals=REG_DWORD:1



[.\SOSProfile *\Log]

enable

enable=REG_DWORD:1

With this parameter, this logging-method can be enabled/disabled.

logFileName

logFileName=REG_SZ:"%ProgramFiles%\Comtarsia\SignOn Solutions 2016\log\ComtRPCSrv.log"

logLevel

logLevel=REG_DWORD:4

Specifies the log level.

URGENCY_ERROR = 1,

URGENCY_EXCEPTION = 2,

URGENCY_WARN = 3,

URGENCY_INFO = 4,

URGENCY_MSG = 5,

logMask

logMask=REG_DWORD:0

logDetails

logDetails=REG_DWORD:0xFFFFFFFF

Specifies the log details.

logDetails = 0x0 = No log details

logDetails = 0x1 = Date

logDetails = 0x2 = Time

logDetails = 0x4 = Process and thread ids.

logDetails = 0x8 = Source position

logDetails = 0xFFFFFFFF = All details

enableLogTransactions

enableLogTransactions=REG_DWORD:0

maxLogFileSize

maxLogFileSize=REG_DWORD:0xA00000

maxLogFileHistory

maxLogFileHistory=REG_DWORD:1

[.\SOSProfile *\Log\SysLog]

enable

enable=REG_DWORD:0

With this parameter, this logging-method can be enabled/disabled.

host

host=REG_SZ:""

Specifies the SysLog server.

facility

facility=REG_DWORD:10



Specifies the SysLog facility.

logLevel

logLevel=REG_DWORD:0

Specifies the log level.

URGENCY_ERROR = 1,
URGENCY_EXCEPTION = 2,
URGENCY_WARN = 3,
URGENCY_INFO = 4,
URGENCY_MSG = 5,

logMask

logMask=REG_DWORD:0

logDetails

logDetails=REG_DWORD:0x0

Specifies the log details.

logDetails = 0x0 = No log details
logDetails = 0x1 = Date
logDetails = 0x2 = Time
logDetails = 0x4 = Process and thread ids.
logDetails = 0x8 = Source position
logDetails = 0xFFFFFFFF = All details

[.\SOSProfile *\SyncClient]

connectTimeout

connectTimeout=REG_DWORD:5

proxyPort

proxyPort=REG_DWORD:0x7D3

syncPacketTTL

syncPacketTTL=REG_DWORD:0x14

syncProxy1

syncProxy1=REG_SZ:""

syncProxy2

syncProxy2=REG_SZ:""

tlsCAFile

tlsCAFile=REG_SZ:"%ProgramFiles%\Comtarsia\SignOn Solutions 2016\cert\ca.pem"

tlsCADir

vn=REG_SZ:""

tlsCertFile

tlsCertFile=REG_SZ:"%ProgramFiles%\Comtarsia\SignOn Solutions 2016\cert\client.pem"

tlsKeyFile

tlsKeyFile=REG_SZ:"%ProgramFiles%\Comtarsia\SignOn Solutions 2016\cert\client.key"



[.\SOSProfile *\UserCertificateMapping]

[.\SOSProfile *\UserCertificateMapping\ <UserCertificateMappingName>]

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

expression

expression=REG_SZ:""

formatter

formatter=REG_SZ:""

[.\SOSProfile *\Variables]

[.\SOSProfile *\Variables\BeforeSync]

[.\SOSProfile *\Variables\AfterSync]

[.\SOSProfile *\Variables\<<VariableEffectivePoint>]

The name of this key can be "BeforeSync" or "AfterSync" and defines when the variables under this key should be mapped.

[.\SOSProfile *\Variables\<<VariableEffectivePoint>\<VariableName>]

The name of this key (<VariableName>) is in the form NNN_Name, where 'N' are numbers and define the order of the mapping rules. The 'Name' is the resulting name of the variable.

displayName

displayName=REG_SZ:""

variableComment

variableComment=REG_SZ:""

source

source=REG_SZ:""

transmitDestination

transmitDestination=REG_DWORD:0x0

exportDestination

exportDestination=REG_DWORD:0x0



transmitDestinationDomains

transmitDestinationDomains=REG_MULTI_SZ:"System.String[]"

mappingType

mappingType=REG_DWORD:0

expression

expression=REG_SZ:""

formatter

formatter=REG_SZ:""

index

index=REG_DWORD:0

flags

flags=REG_DWORD:0x2000000

multivalueAction

multivalueAction=REG_DWORD:0

0:Override

1>Delete

2>DeleteValue

3:AddValue

hold

hold=REG_DWORD:0

This option can be used to temporarily disable a variable mapping.

[.\SOSProfile *\UserEnvironment]**defaultUserProfile**

defaultUserProfile=REG_SZ:""

profilePath

profilePath=REG_SZ:""

homeDirDrive

homeDirDrive=REG_SZ:"H:"

homeDirPath

homeDirPath=REG_SZ:""

[.\SOSProfile *\LogonClient]**displayProgressBox**

displayProgressBox=REG_DWORD:1

enableSyncClient

enableSyncClient=REG_DWORD:0



displaySyncBox

displaySyncBox=REG_DWORD:1

WTSMODE

WTSMODE=REG_DWORD:0

ADSLogonMode

ADSLogonMode=REG_DWORD:0

winDomain

winDomain=REG_SZ:""

enableDomainLogon

enableDomainLogon=REG_DWORD:0

userinit

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

GPUUpdate_Mask

GPUUpdate_Mask=REG_DWORD:0

GPUUpdate_CMD

GPUUpdate_CMD=REG_SZ:""

disableMsCredProviderToggle

disableMsCredProviderToggle=REG_DWORD:0

unregisterMsCredProvider

unregisterMsCredProvider=REG_DWORD:0

panelBitmap

panelBitmap=REG_SZ:""

refreshUnlockTimer

refreshUnlockTimer=REG_DWORD:720

removeUser

removeUser=REG_DWORD:0

bitmask: (only for local mode)

0x1 User Account

0x2 Profile // (0x1 User Account, 0x2 Profile), only local mode.

LDAPSetPasswordAsSambaPassword

LDAPSetPasswordAsSambaPassword=REG_DWORD:0

enableSmartCard

enableSmartCard=REG_DWORD:0

smartCardDefaultRemoveAction

smartCardDefaultRemoveAction=REG_DWORD:2

smartCardRemoveActionUserSelectMask

smartCardRemoveActionUserSelectMask=REG_DWORD:0xF



logonPanelTileDisplayName
logonPanelTileDisplayName=REG_SZ:""

enableProxyLogon
enableProxyLogon=REG_DWORD:0

sessionPasswordTemplate
sessionPasswordTemplate=REG_SZ:"LLUURR99SS"

smartCardSessionPasswordMode
smartCardSessionPasswordMode=REG_DWORD:0

smartCardSessionPasswordValidity
smartCardSessionPasswordValidity=REG_DWORD:1

smartCardSessionPasswordValidityUnits
smartCardSessionPasswordValidityUnits=REG_DWORD:0

smartCardSessionPasswordValidityOffset
smartCardSessionPasswordValidityOffset=REG_DWORD:0

smartCardSecurePINEntryMode
smartCardSecurePINEntryMode=REG_DWORD:1

displayMsgStrID
displayMsgStrID=REG_DWORD:0

[.\SOSProfile *\LogonPolicy]

minPwdLen
minPwdLen=REG_DWORD:0

alphaNumPwd
alphaNumPwd=REG_DWORD:0

userNameCasePolicy
userNameCasePolicy=REG_DWORD:1

disablePasswordChange
disablePasswordChange=REG_DWORD:0

disableLocalLogon
disableLocalLogon=REG_DWORD:0

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

denyCancelForcePWDChangeDlg
denyCancelForcePWDChangeDlg=REG_DWORD:0

disallowGraceLogin
disallowGraceLogin=REG_DWORD:0



dontDisplayLastUserName
dontDisplayLastUserName=REG_DWORD:0

logonAllowGroups
logonAllowGroups=REG_SZ:""

negateLogonAllowGroups
negateLogonAllowGroups=REG_DWORD:1

enableWkstLogonPolicy
enableWkstLogonPolicy=REG_DWORD:0

wkstLogonPolicyRetryTimer
wkstLogonPolicyRetryTimer=REG_DWORD:60

wkstLogonPolicyRootOUGroups
wkstLogonPolicyRootOUGroups=REG_MULTI_SZ:"System.String[]"

logonInformationText
logonInformationText=REG_SZ:""

offerOfflineLogonByUnreachableLDAP
offerOfflineLogonByUnreachableLDAP=REG_DWORD:1

offerOfflineLogonAsLogonOption
offerOfflineLogonAsLogonOption=REG_DWORD:0

enableQuickLogon
enableQuickLogon=REG_DWORD:0

quickLogonButtonCaption
quickLogonButtonCaption=REG_SZ:""

quickLogonUser
quickLogonUser=REG_SZ:""

quickLogonPassword
quickLogonPassword=REG_SZ:""

quickLogonDomain
quickLogonDomain=REG_SZ:""

disableRdpAutoLogon
disableRdpAutoLogon=REG_DWORD:0

setAsDefaultLogonTile
setAsDefaultLogonTile=REG_DWORD:1

[.\SOSProfile *\Script]

userLogon
userLogon=REG_SZ:""



userLogoff

userLogoff=REG_SZ:""

systemLogon

systemLogon=REG_SZ:""

systemLogoff

systemLogoff=REG_SZ:""

systemInit

systemInit=REG_SZ:""

timeout

timeout=REG_DWORD:0x1E

noScriptByCachedCredLogon

noScriptByCachedCredLogon=REG_DWORD:0

[.\SOSProfile *\SSO]**rootPath**

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

enableSSO

enableSSO=REG_DWORD:0

LDAP_PWD_MODE

LDAP_PWD_MODE=REG_DWORD:2

LDAP_PKI_MODE

LDAP_PKI_MODE=REG_DWORD:2

OFFLINE_MODE

OFFLINE_MODE=REG_DWORD:2

LOCAL_LOGON_MODE

LOCAL_LOGON_MODE=REG_DWORD:2

WIN_ADS_MODE

WIN_ADS_MODE=REG_DWORD:2



8.Disclaimer

All pages are subject to copyright and may only be copied or integrated in own offers with the written permission of Comtarsia IT Services.

All Rights reserved.

Subject to changes without notice!

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. This is also valid, if this site contains the Comtarsia IT Services logo.

In addition, a link from our site to another does not mean that we identify ourselves with their content or support their use.

