Comtarsia SignOn Proxy 2012

Manual

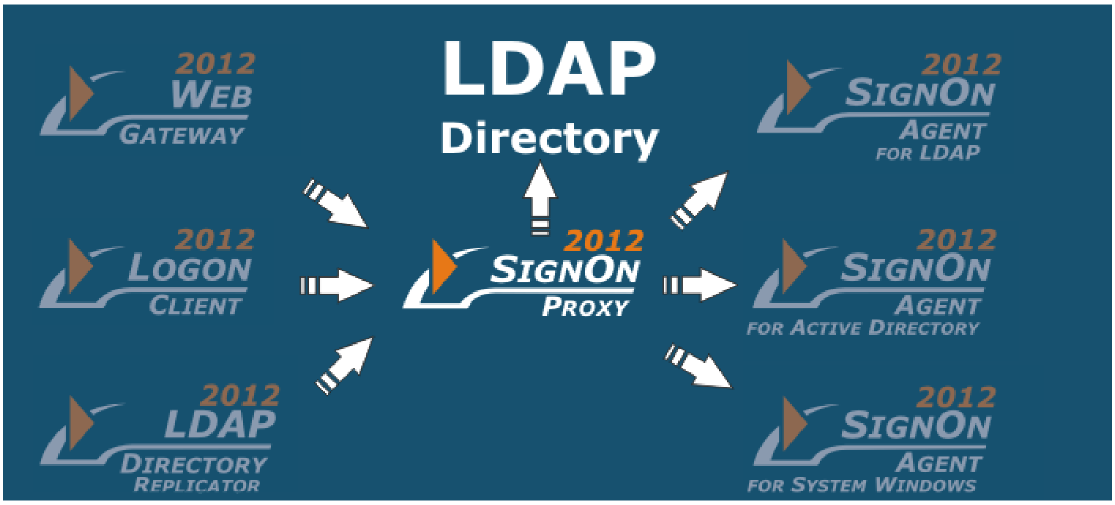
Version: 6.0.1.0, 6 th May, 2013

Contents

1.Introduction

Comtarsia SignOn Proxy 2012 for Windows Server 2008 / Windows Server 2012

LDAP Authentication, SignOn Agent Trigger
Proxy Authentication for Comtarsia Logon Client, Comtarsia Web Gateway and Comtarsia LDAP Directory Replicator


2012 Web Gateway
2012 Logon Client
2012 LDAP Directory Replicator
LDAP Directory
2012 SignOn Proxy
2012 SignOn Agent for LDAP
2012 SignOn Agent for Active Directory
2012 SignOn Agent for System Windows

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)

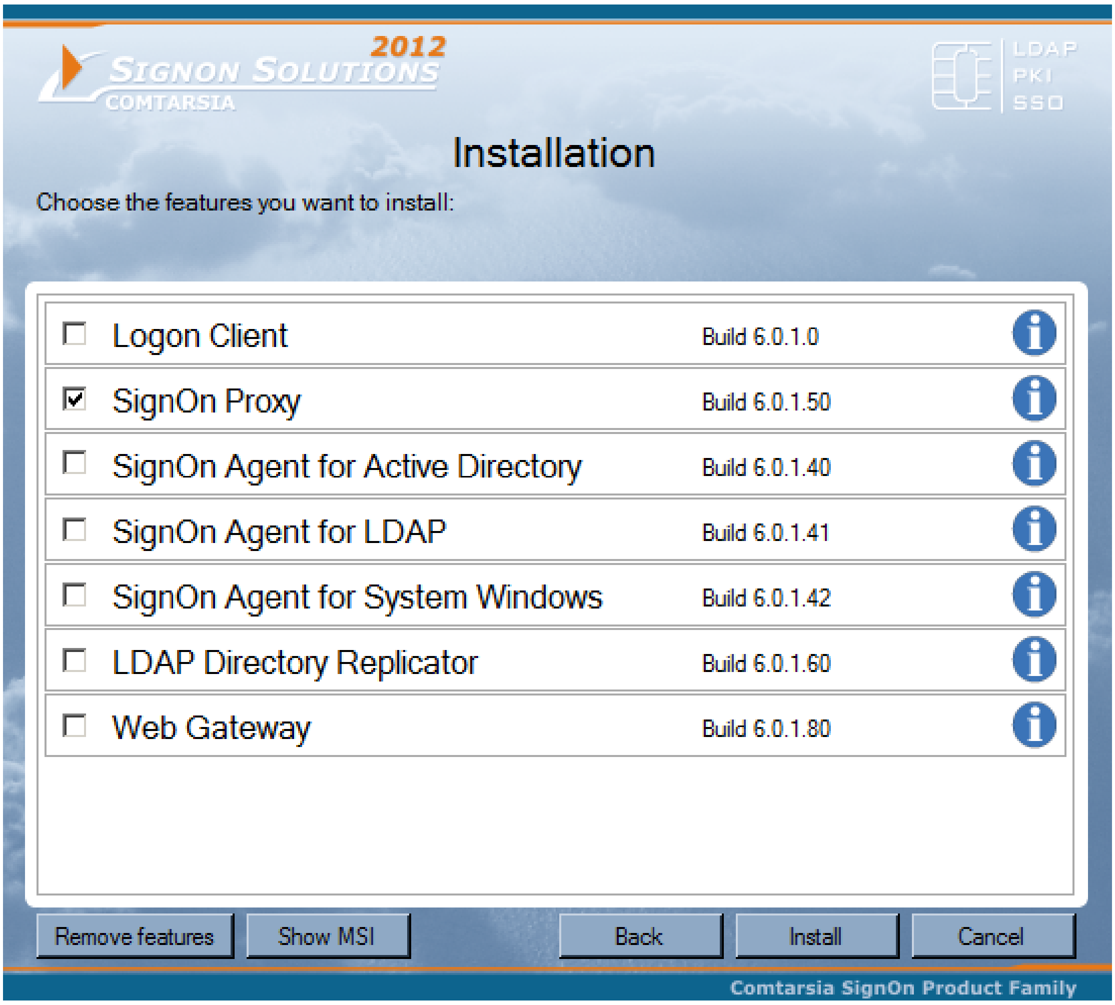
For more informations about the Comtarsia SignOn Solutions, please visit our webpage:
http://signon.comtarsia.com/index_en.html

2.Installation

2.1 Manual Installation

An installation or an update is done using the installation program “SOS2012-6.0.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.)

After the installation, the configuration utility „Comtarsia Management Console“ is started. See: Comtarsia Management Console (ComtMC)



Installation

Choose the features you want to install:

□	Logon Client	Build 6.0.1.0
☑	SignOn Proxy	Build 6.0.1.50
□	SignOn Agent for Active Directory	Build 6.0.1.40
□	SignOn Agent for LDAP	Build 6.0.1.41
□	SignOn Agent for System Windows	Build 6.0.1.42
□	LDAP Directory Replicator	Build 6.0.1.60
□	Web Gateway	Build 6.0.1.80

3.Comtarsia Management Console (ComtMC)

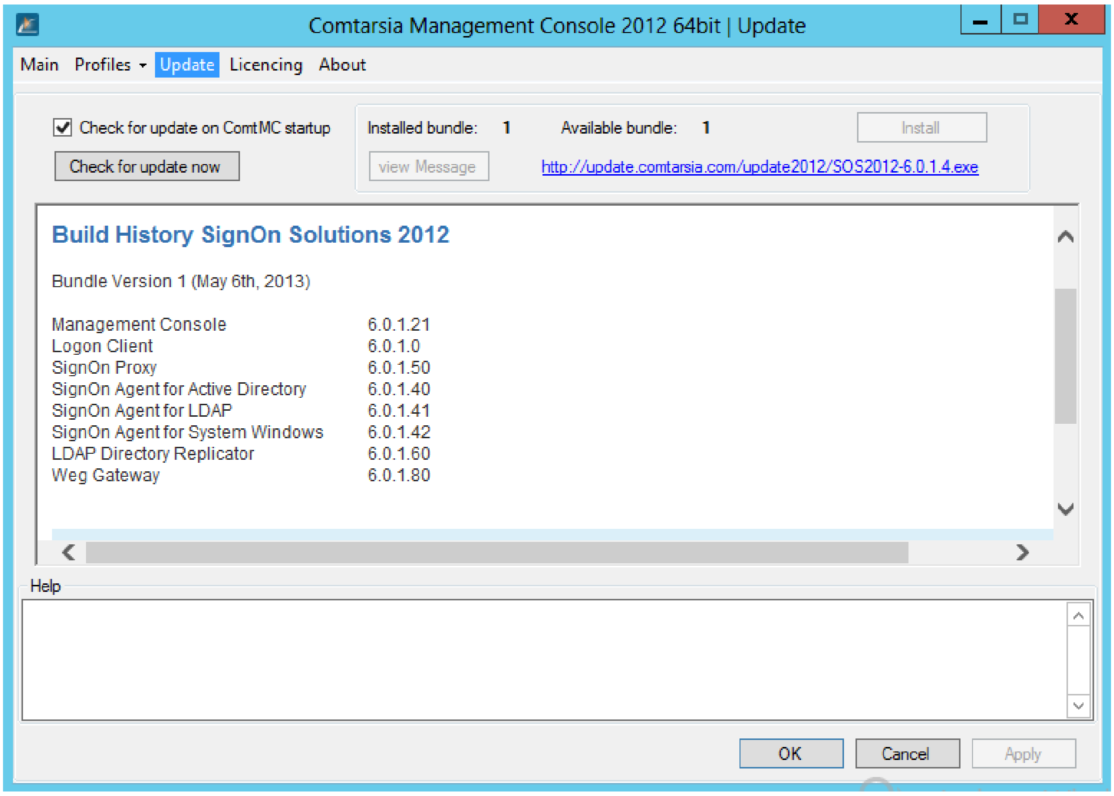
The Comtarsia Management Console (ComtMC) can be accessed trough the Start menu.

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



☑ Check for update on ComtMC startup

Installed bundle: 1

Available bundle: 1

http://update.comtarsia.com/update2012/SOS2012-6.0.1.4.exe

Build History SignOn Solutions 2012

Bundle Version 1 (May 6th, 2013)

Management Console	6.0.1.21
Logon Client	6.0.1.0
SignOn Proxy	6.0.1.50
SignOn Agent for Active Directory	6.0.1.40
SignOn Agent for LDAP	6.0.1.41
SignOn Agent for System Windows	6.0.1.42
LDAP Directory Replicator	6.0.1.60
Weg Gateway	6.0.1.80

4. Basic Configuraion

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

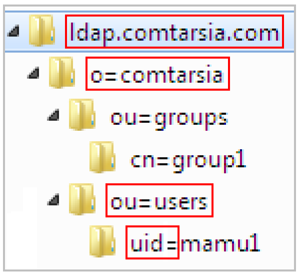
The following information is needed:

- 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 can not 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 (Distinquished Name) of the user is therefore:
"uid=mamu1,ou=users,o=comtarsia".



```
ldap.comtarsia.com
  o=comtarsia
    ou=groups
      cn=group1
    ou=users
      uid=mamu1
```

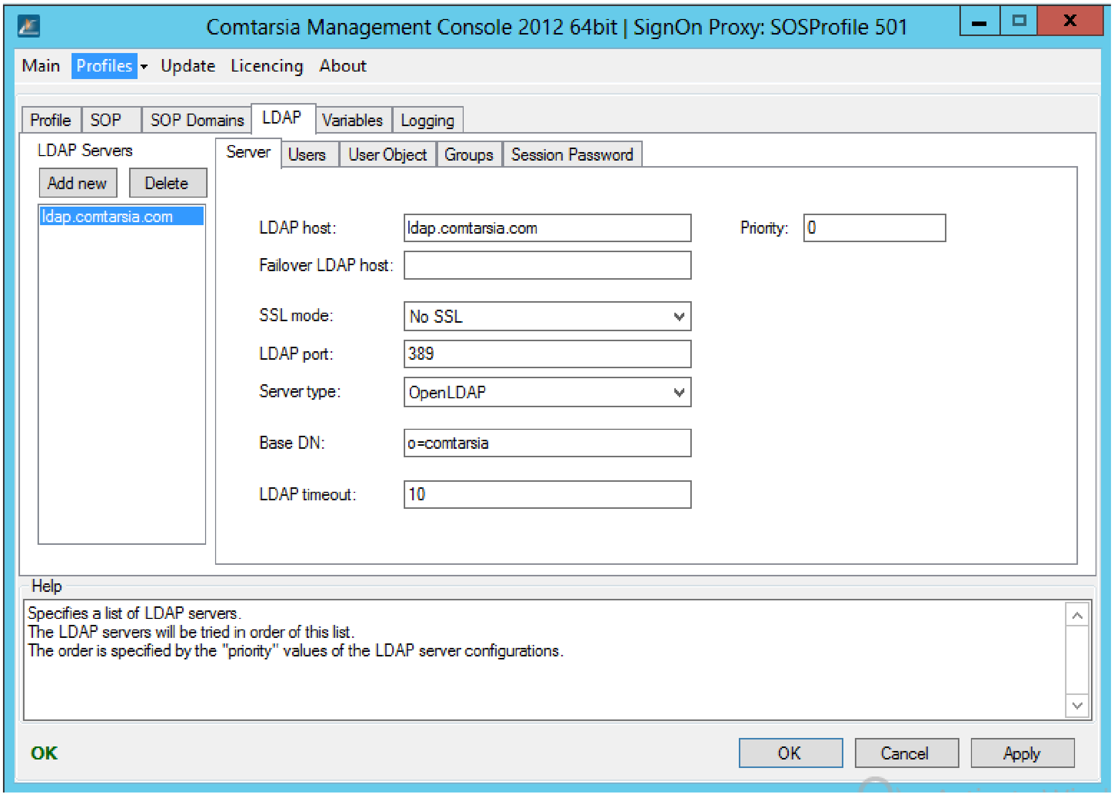
The syntax of full DNs is always from the lower level (leaf) to the base object (root or "baseDN").

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.



LDAP host: ldap.comtarsia.com
Priority: 0
Failover LDAP host:
SSL mode: No SSL
LDAP port: 389
Server type: OpenLDAP
Base DN: o=comtarsia
LDAP timeout: 10

Help
Specifies a list of LDAP servers.
The LDAP servers will be tried in order of this list.
The order is specified by the "priority" values of the LDAP server configurations.

OK

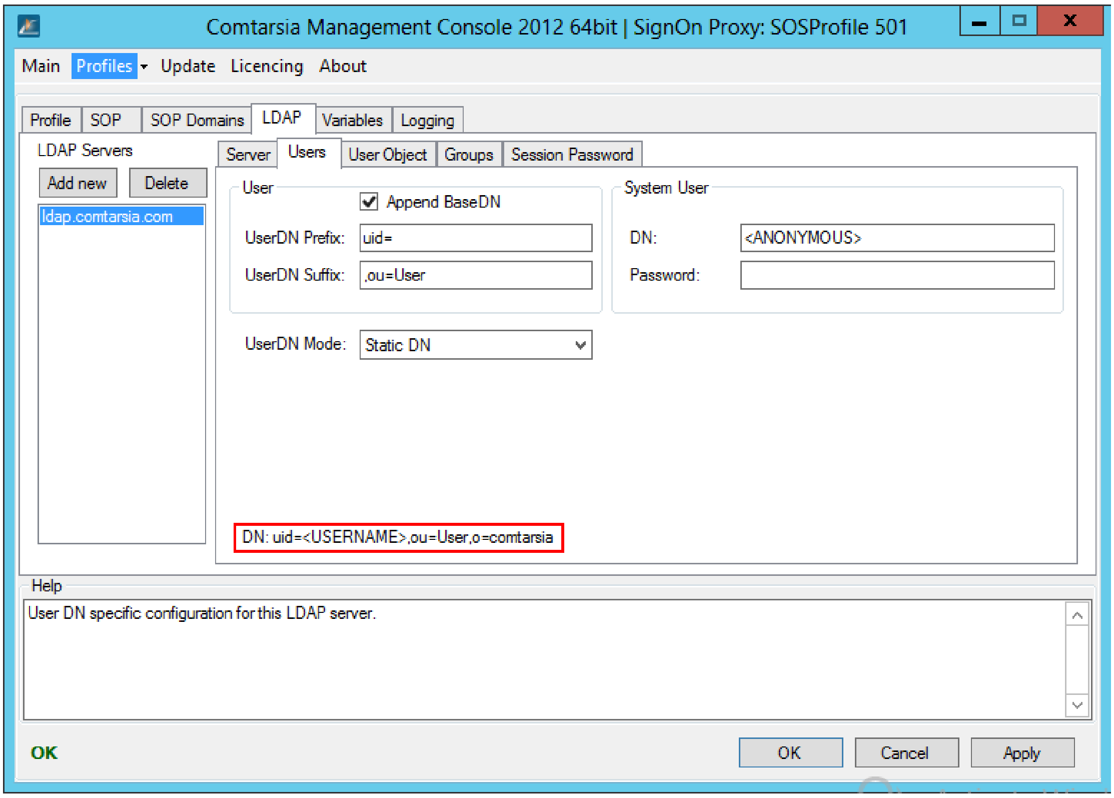
The tab “[LDAP] -> [Users]” contains the configuration of the position of LDAP-users within the LDAP directory, or “how the authentication” should be performed.

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)



ldap.comtarsia.com

☑ Append BaseDN

UserDN Prefix: uid=

UserDN Suffix: ,ou=User

DN: <ANONYMOUS>

Password:

UserDN Mode: Static DN

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

Help

User DN specific configuration for this LDAP server.

OK

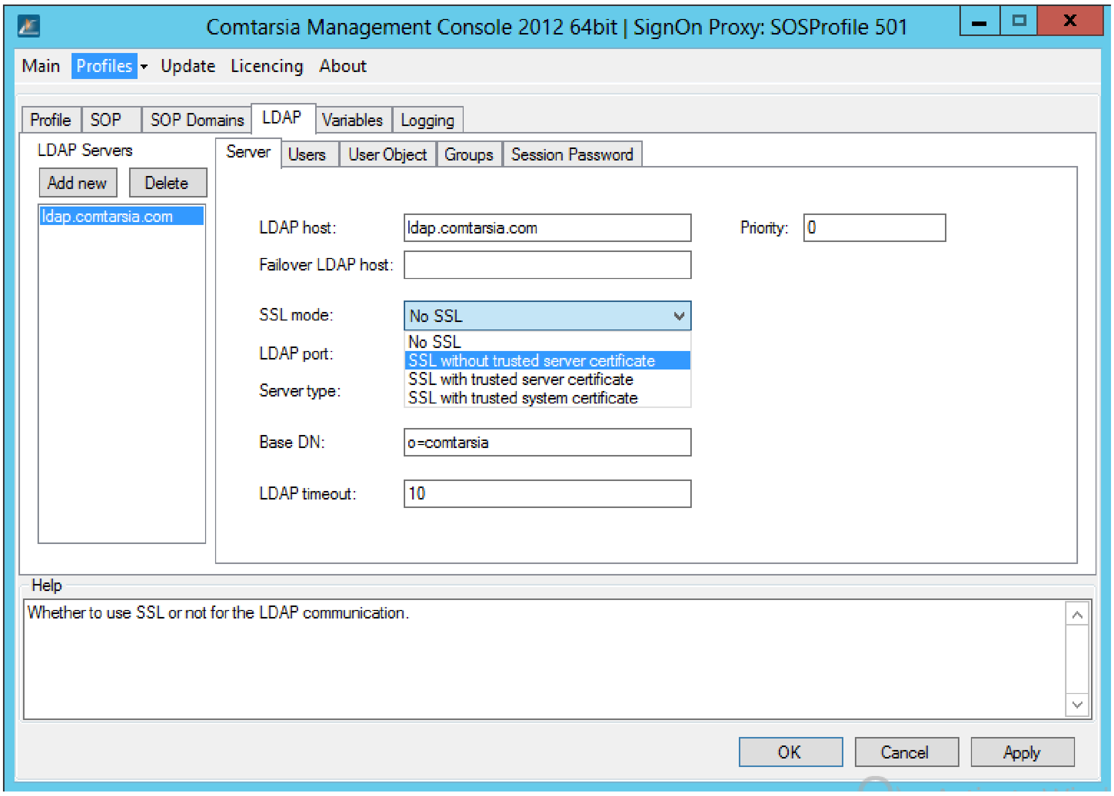
5. Usage Scenarios

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].


Comtarsia Management Console 2012 64bit | SignOn Proxy: SOSProfile 501
Main
Profiles
Update
Licencing
About
Profile
SOP
SOP Domains
LDAP
Variables
Logging
LDAP Servers
Add new
Delete
Server
Users
User Object
Groups
Session Password
No SSL
SSL without trusted server certificate
SSL with trusted server certificate
SSL with trusted system certificate
Help
OK
Cancel
Apply

ldap.comtarsia.com

LDAP host: ldap.comtarsia.com

Priority: 0

Failover LDAP host:

SSL mode: No SSL

LDAP port:

Server type:

Base DN: o=comtarsia

LDAP timeout: 10

Whether to use SSL or not for the LDAP communication.

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.

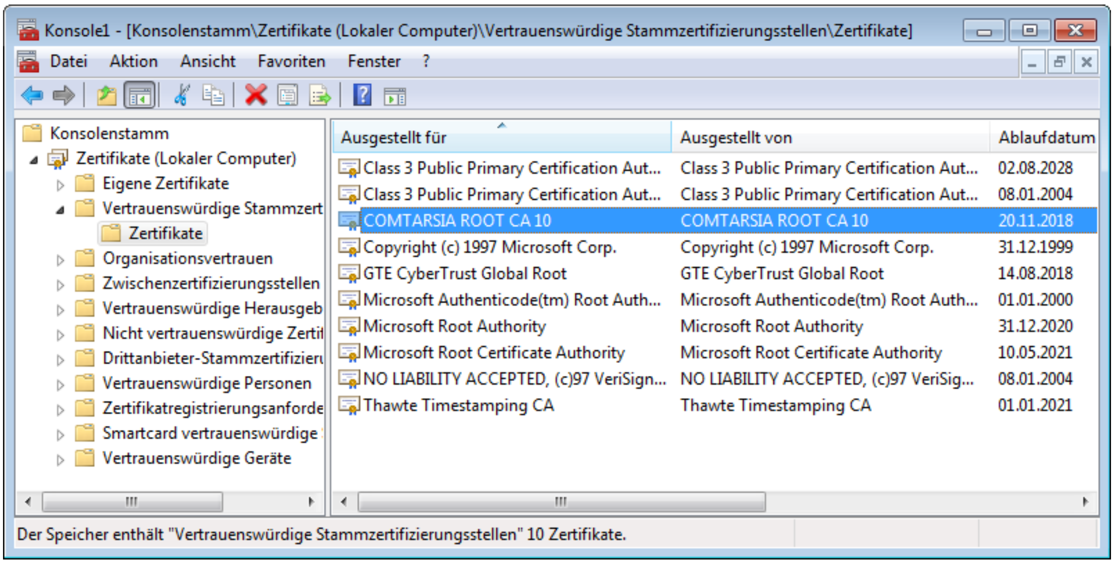
Mode 2: SSL with "trusted server certificate"
Requirements:

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.



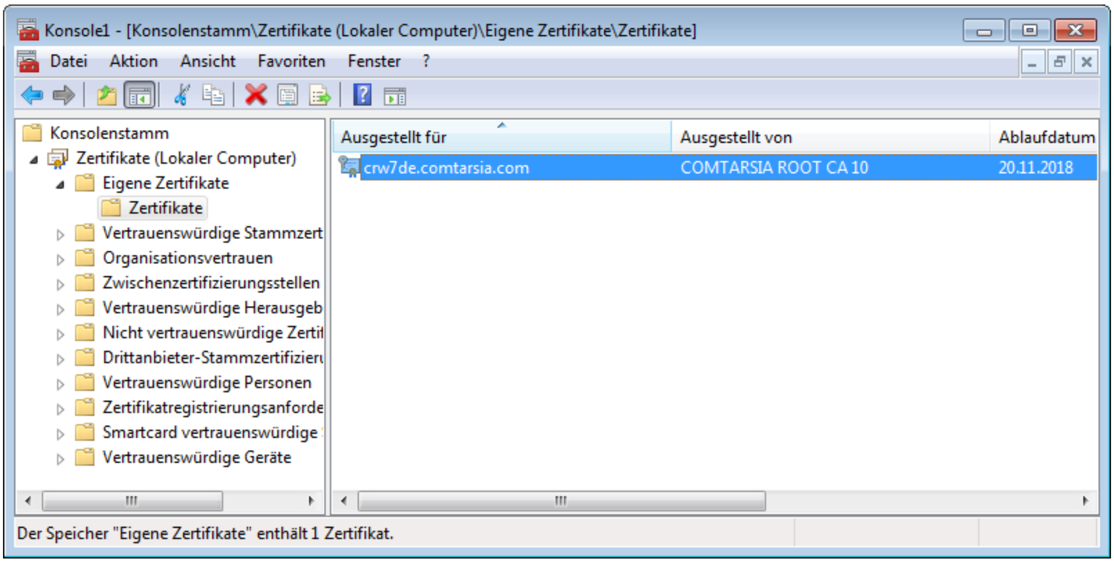
Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Vertrauenswürdige Stammzertifizierungsstellen\Zertifikate]

Konsolenstamm
- Zertifikate (Lokaler Computer)
  - Eigene Zertifikate
  - Vertrauenswürdige Stammzert
    - Zertifikate
  - Organisationsvertrauen
  - Zwischenzertifizierungsstellen
  - Vertrauenswürdige Herausgeb
  - Nicht vertrauenswürdige Zertif
  - Drittanbieter-Stammzertifizieru
  - Vertrauenswürdige Personen
  - Zertifikatregistrierungsanforde
  - Smartcard vertrauenswürdige
  - Vertrauenswürdige Geräte

Ausgestellt für	Ausgestellt von	Ablaufdatum
Class 3 Public Primary Certification Aut...	Class 3 Public Primary Certification Aut...	02.08.2028
Class 3 Public Primary Certification Aut...	Class 3 Public Primary Certification Aut...	08.01.2004
COMTARSIA ROOT CA 10	COMTARSIA ROOT CA 10	20.11.2018
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31.12.1999
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.08.2018
Microsoft Authenticode(tm) Root Auth...	Microsoft Authenticode(tm) Root Auth...	01.01.2000
Microsoft Root Authority	Microsoft Root Authority	31.12.2020
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10.05.2021
NO LIABILITY ACCEPTED, (c)97 VeriSign...	NO LIABILITY ACCEPTED, (c)97 VeriSig...	08.01.2004
Thawte Timestamping CA	Thawte Timestamping CA	01.01.2021

Der Speicher enthält "Vertrauenswürdige Stammzertifizierungsstellen" 10 Zertifikate.

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


Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Eigene Zertifikate\Zertifikate]
Datei
Aktion
Ansicht
Favoriten
Fenster
?
Konsolenstamm
Zertifikate (Lokaler Computer)
Eigene Zertifikate
Zertifikate
Vertrauenswürdige Stammzert
Organisationsvertrauen
Zwischenzertifizierungsstellen
Vertrauenswürdige Herausgeb
Nicht vertrauenswürdige Zertif
Drittanbieter-Stammzertifizieru
Vertrauenswürdige Personen
Zertifikatregistrierungsanforde
Smartcard vertrauenswürdige
Vertrauenswürdige Geräte

Ausgestellt für	Ausgestellt von	Ablaufdatum
crw7de.comtarsia.com	COMTARSIA ROOT CA 10	20.11.2018

Der Speicher "Eigene Zertifikate" enthält 1 Zertifikat.

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

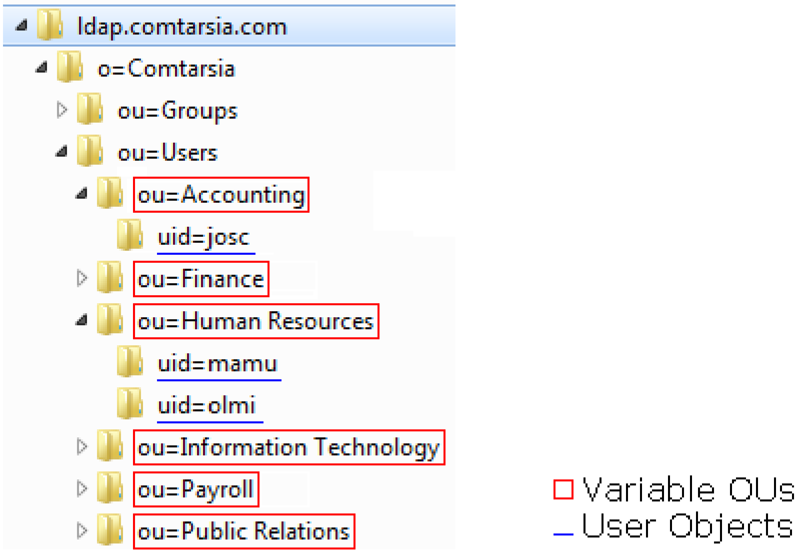
5.2 LDAP Users from Multiple OUs

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
```



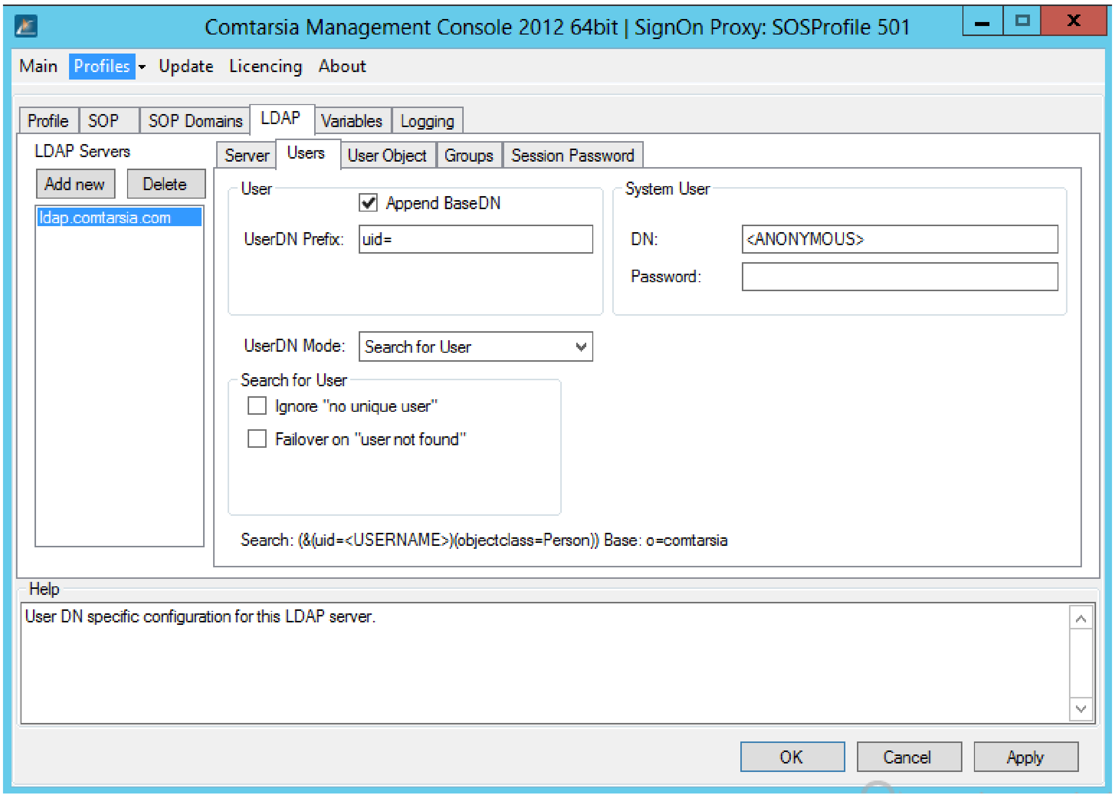
[Figure: LDAP example: multiple OUs]

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”.



☑ Append BaseDN

UserDN Prefix: uid=

DN: <ANONYMOUS>

Password:

UserDN Mode: Search for User

☐ Ignore "no unique user"

☐ Failover on "user not found"

Search: (&(uid=<USERNAME>)(objectclass=Person)) Base: o=comtarsia

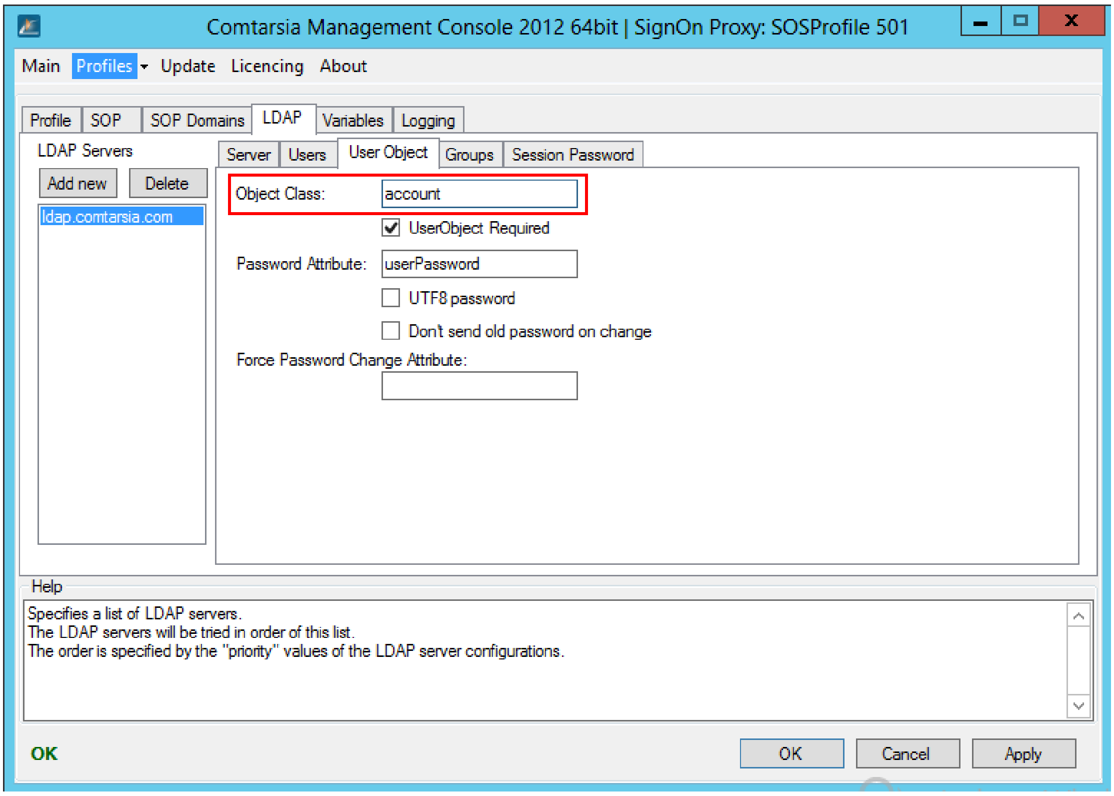
User DN specific configuration for this LDAP server.

[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"



Object Class: account

☑ UserObject Required

Password Attribute: userPassword

□ UTF8 password

□ Dont send old password on change

Force Password Change Attribute:

Specifies a list of LDAP servers.
The LDAP servers will be tried in order of this list.
The order is specified by the "priority" values of the LDAP server configurations.

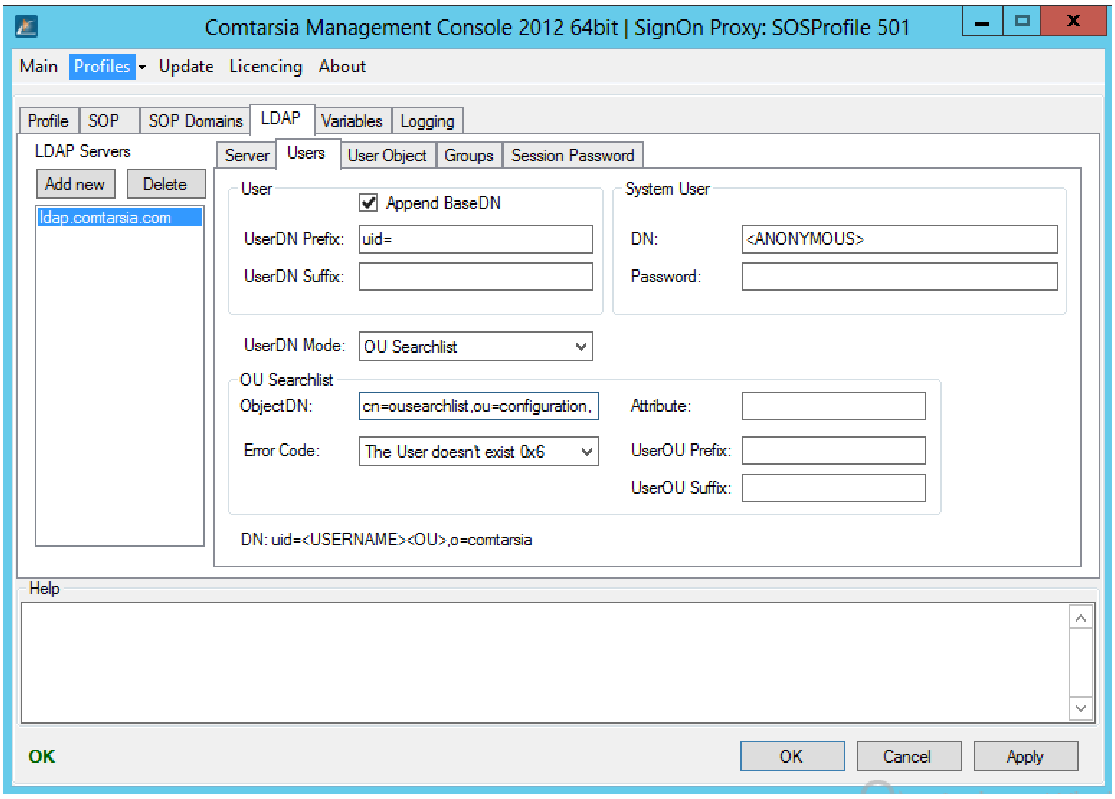
[Figure: ComtMC: LDAP > User Object > Object Class]

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".



User

☑ Append BaseDN

UserDN Prefix: uid=

UserDN Suffix:

System User

DN: <ANONYMOUS>

Password:

UserDN Mode: OU Searchlist

OU Searchlist

ObjectDN: cn=ousearchlist,ou=configuration,

Error Code: The User doesn't exist 0x6

Attribute:

UserOU Prefix:

UserOU Suffix:

DN: uid=<USERNAME><OU>,o=comtarsia

[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
```

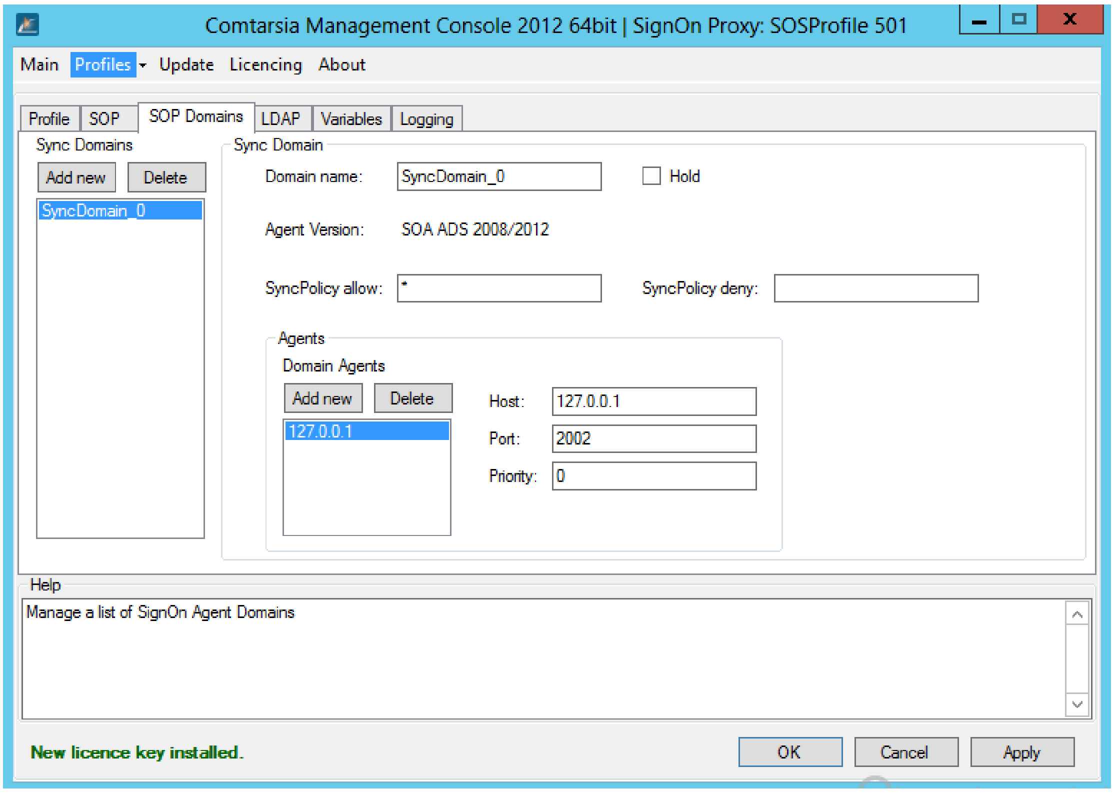
- "<UserDN Prefix>": configured in "LDAP > Users > User > UserDN Prefix"
- "<USERNAME>": entered by the user at the login screen
- "<UserDN Suffix>": configured in "LDAP > Users > User > UserDN Suffix"
- "<UserOU Prefix>": configured in "LDAP > Users > OU Seachlist > UserOU Prefix"
- "<OU>": replaced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

- "`<UserOU Suffix>`": configured in "LDAP > Users > OU Seachlist > 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

6.1.1 Domains



SyncDomain_0

Domain name: SyncDomain_0

□ Hold

Agent Version: SOA ADS 2008/2012

SyncPolicy allow: *

SyncPolicy deny:

127.0.0.1

Host: 127.0.0.1

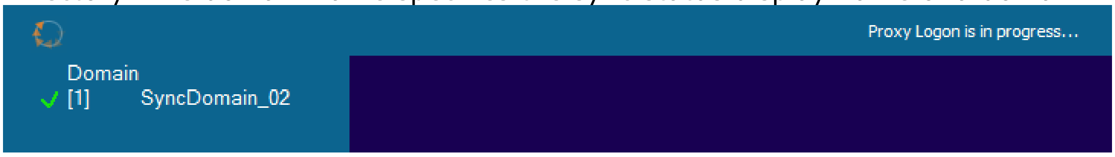
Port: 2002

Priority: 0

Manage a list of SignOn Agent Domains

New licence key installed.

The SOP Sync Domains defines a SignOn Agent synchronization target. A SOP Sync Domain can be an Active Directory Domain, a Windows System or LDAP Directory. The domain name specifies the sync status display name of a domain:



Proxy Logon is in progress...

Domain
✓ [1] SyncDomain_02

As Agent Version must be specified the corresponding Agent type:

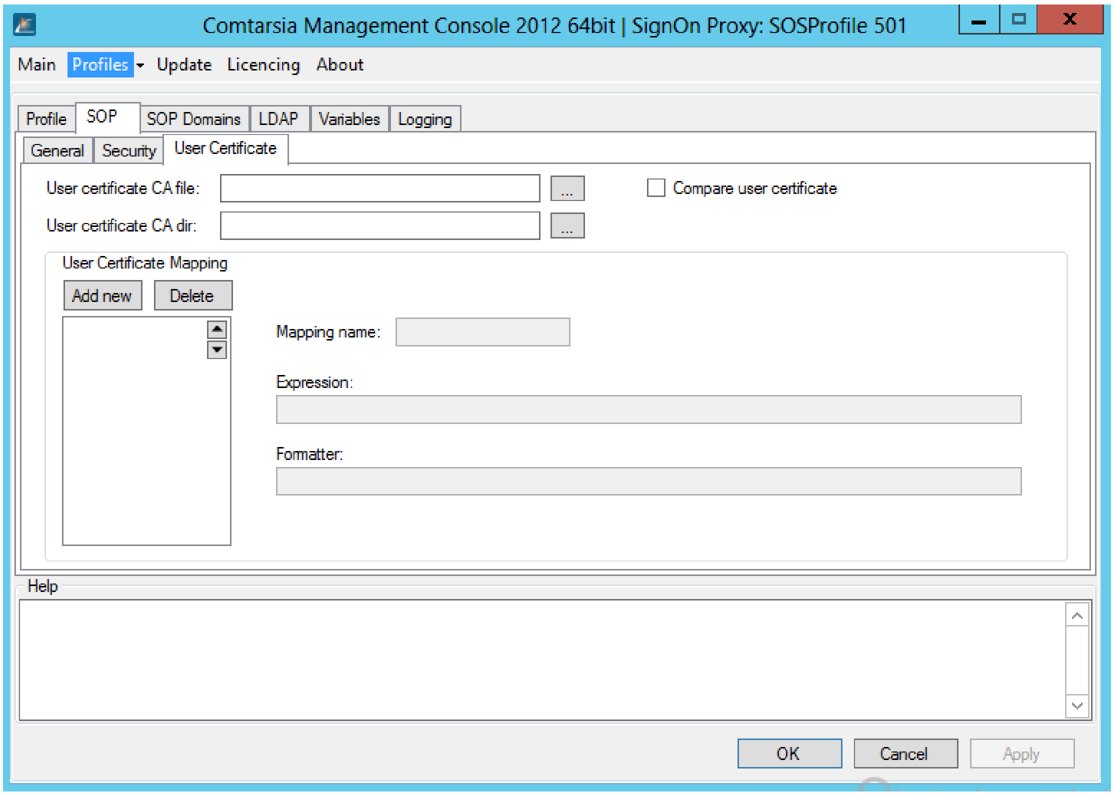
- SOA ADS 2008/2012
- SOA LDAP 2008/2012
- SOA SystemWin 2012

The Sync Policy specifies a list of groups whose users should be synchronized in this domain. Groups have to be separated with a comma ",".
Groups can be wildcard matched at the end with an asterisk.
The Sync Policy allow specifies a list of groups whose users must not be synchronized in this domain. Groups have to be separated with a comma ",".
Groups can be wildcard matched at the end with an asterisk.
A single asterisks matches all groups.
The SyncPolicyDeny list has priority over the SyncPolicy allow list.
This function is based on the internal variable __GROUP__ which contains the LDAP groups of a user. By using the variable manager client or proxy variables

can be added to the __GROUP__ variable and can used for the sync allow or deny policy.

By activated checkbox Hold the domain is skipped by the synchronization.

6.1.2 User Certificate



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 SignOn Proxy 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=controling

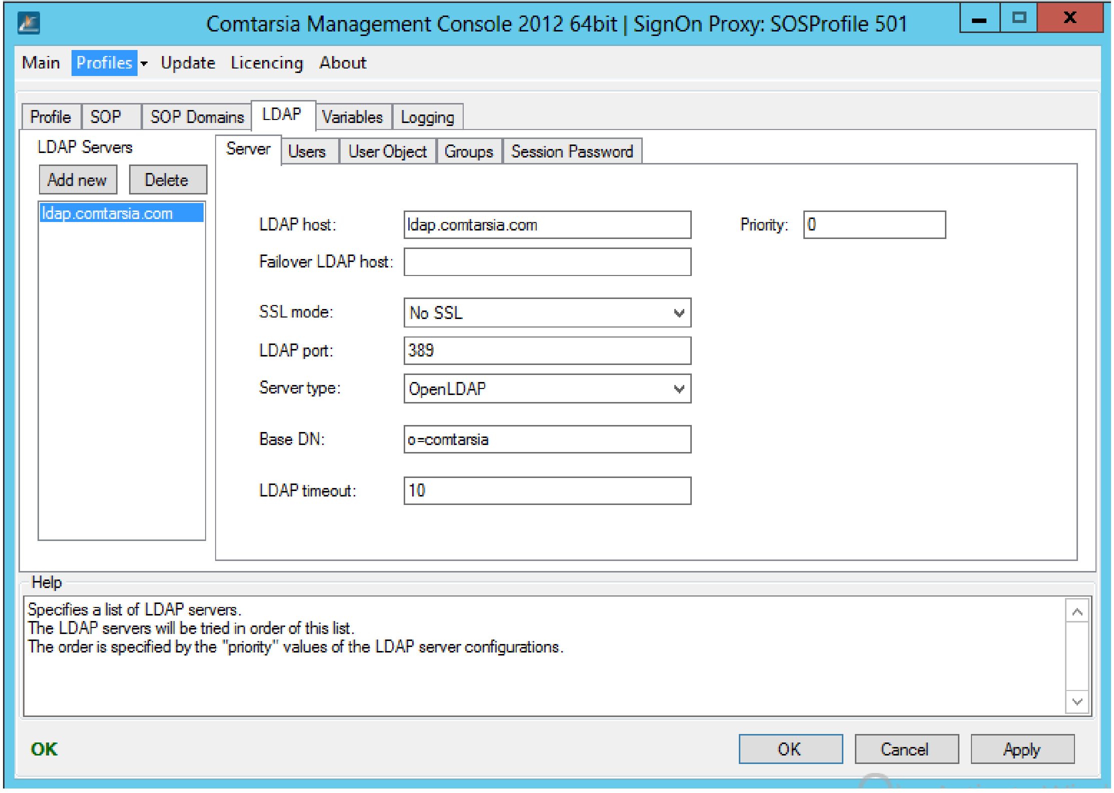
Resulting LDAP DN: uid=musterman,ou=users,dc=company,dc=com

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.



ldap.comtarsia.com

LDAP host: ldap.comtarsia.com

Priority: 0

Failover LDAP host:

SSL mode: No SSL

LDAP port: 389

Server type: OpenLDAP

Base DN: o=comtarsia

LDAP timeout: 10

Specifies a list of LDAP servers.
The LDAP servers will be tried in order of this list.
The order is specified by the "priority" values of the LDAP server configurations.

OK

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).

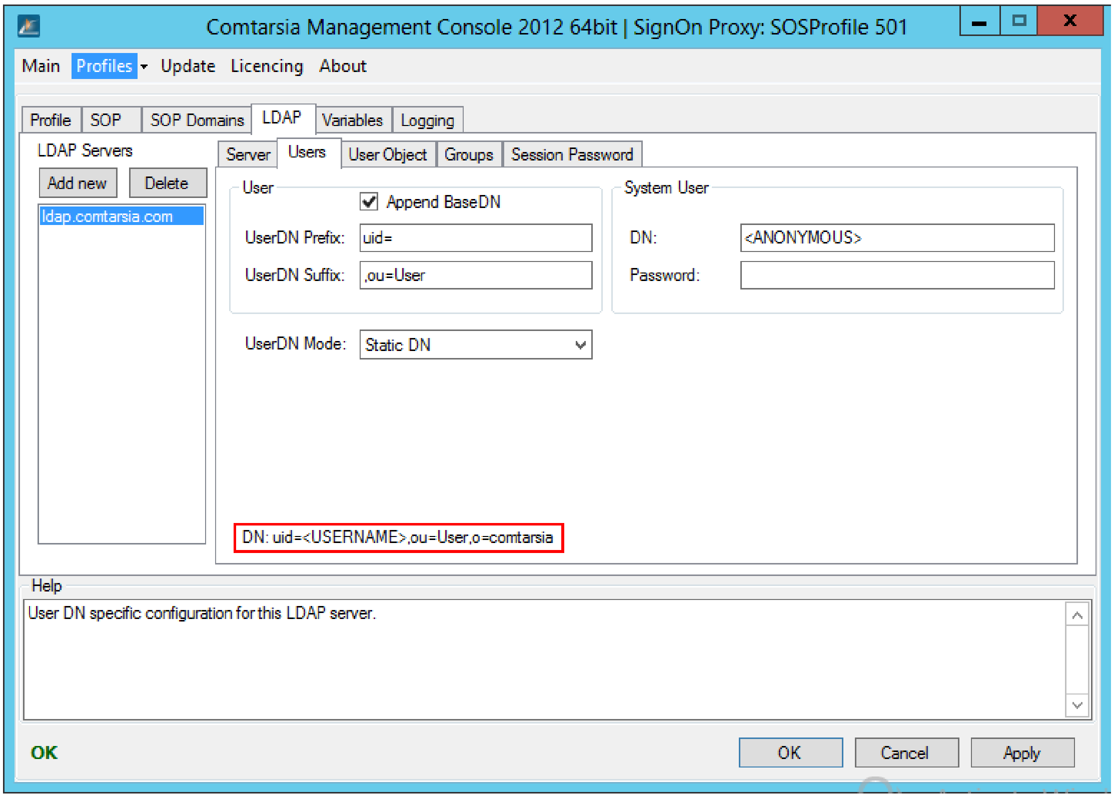
Base DN
Specifies the baseDN of all LDAP-operations.

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



ldap.comtarsia.com

☑ Append BaseDN

UserDN Prefix: uid=

UserDN Suffix: ,ou=User

DN: <ANONYMOUS>

Password:

UserDN Mode: Static DN

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

User DN specific configuration for this LDAP server.

OK

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).

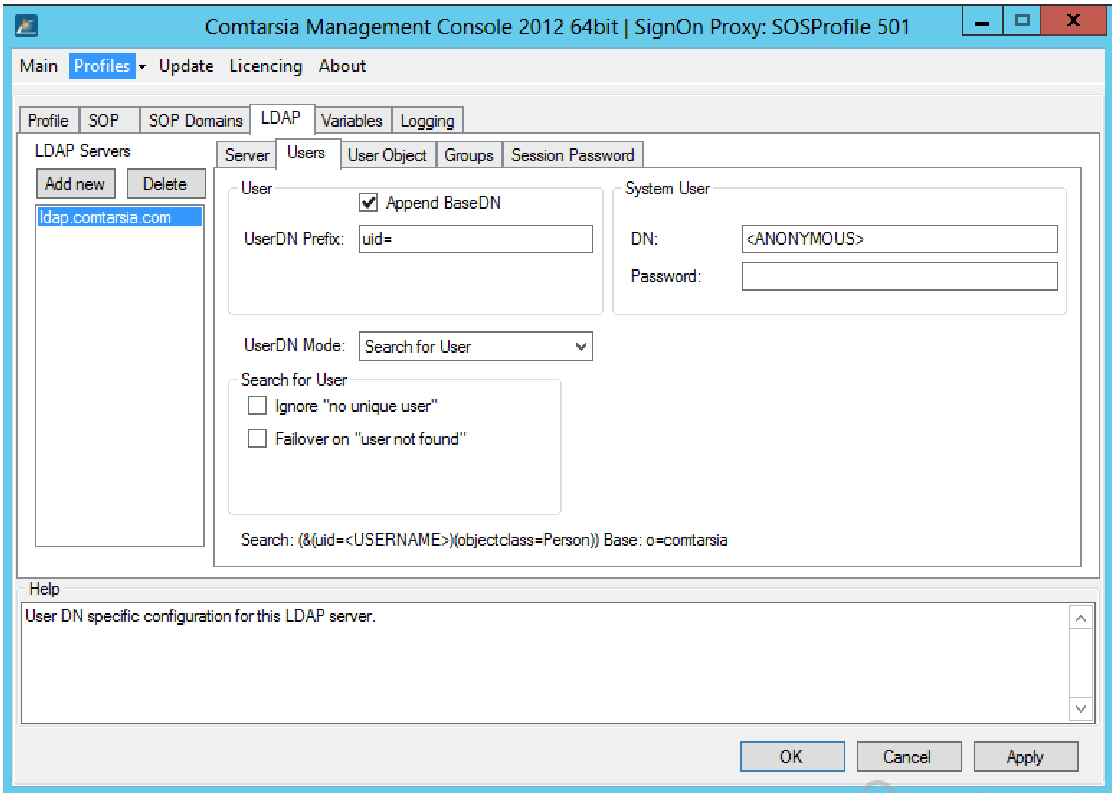
UserDN Suffix
This suffix is appended to the user name for the "Bind as User" (static DN) operation.

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.

6.2.3 Search for User



Comtarsia Management Console 2012 64bit | SignOn Proxy: SOSProfile 501

ldap.comtarsia.com

User

☑ Append BaseDN

UserDN Prefix: uid=

System User

DN: <ANONYMOUS>

Password:

UserDN Mode: Search for User

Search for User

□ Ignore "no unique user"

□ Failover on "user not found"

Search: (&(uid=<USERNAME>)(objectclass=Person)) Base: o=comtarsia

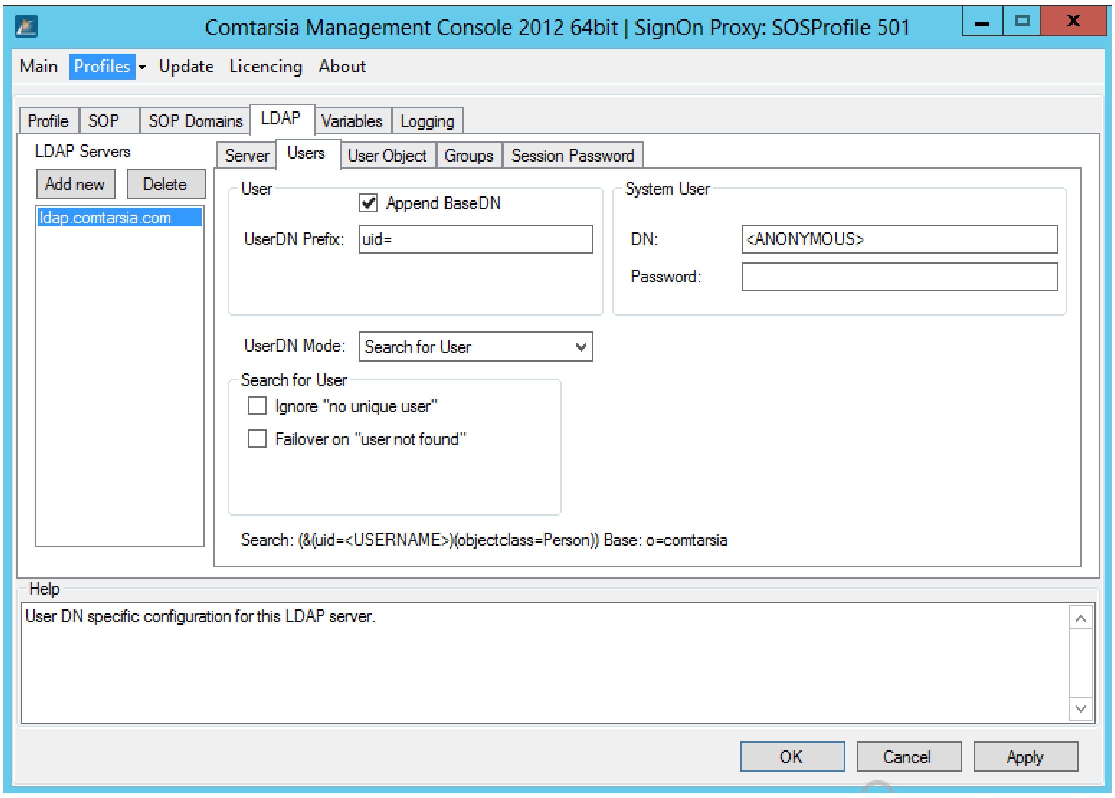
Help

User DN specific configuration for this LDAP server.

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, und Search for User)

System User > Password
Defines the password of the LDAP system user. The password is stored encrypted.

6.2.4 OU Searchlist



ldap.comtarsia.com

☑ Append BaseDN

UserDN Prefix: uid=

DN: <ANONYMOUS>

Password:

UserDN Mode: Search for User

□ Ignore "no unique user"

□ Failover on "user not found"

Search: (&(uid=<USERNAME>)(objectclass=Person)) Base: o=comtarsia

User DN specific configuration for this LDAP server.

OU Searchlist
Also see: LDAP Users from Multiple OUs, und 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)

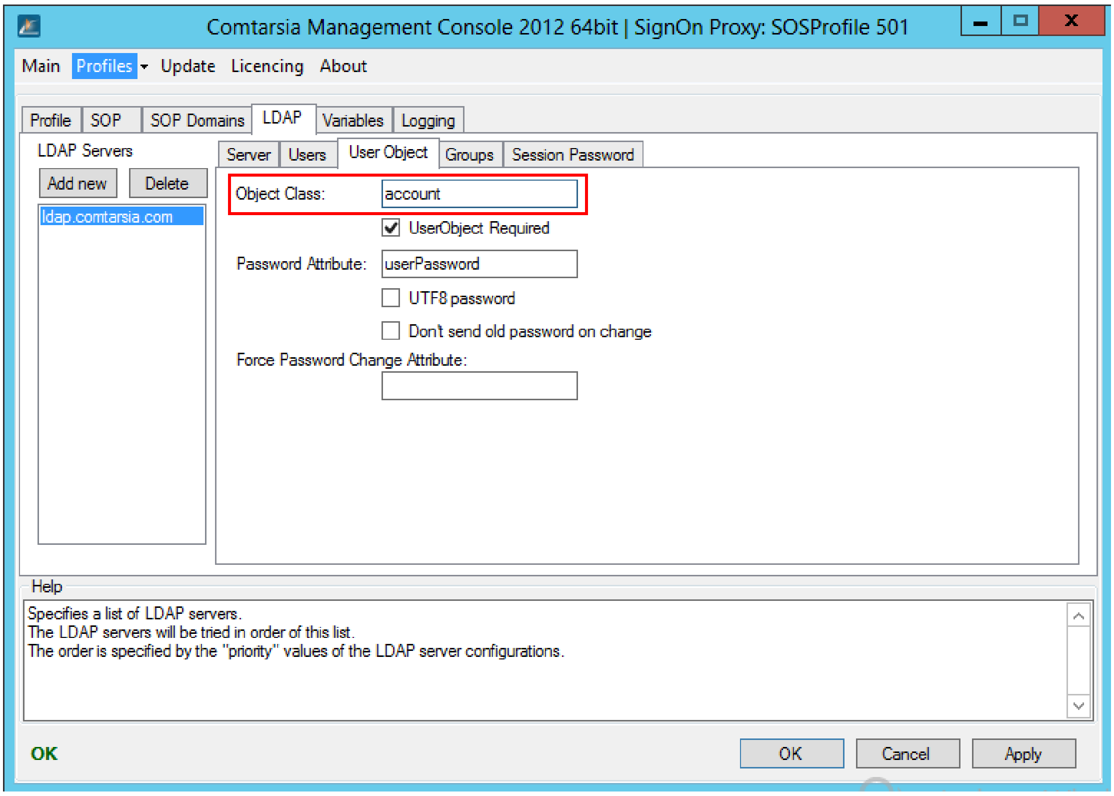
OU Searchlist > Error Code
Defines which LDAP error should be returned in case the User wasn’t found in any of the OUs.

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)

6.2.5 User Object



Comtarsia Management Console 2012 64bit | SignOn Proxy: SOSProfile 501

Object Class: account

☑ UserObject Required

Password Attribute: userPassword

□ UTF8 password

□ Dont send old password on change

Force Password Change Attribute:

Specifies a list of LDAP servers.
The LDAP servers will be tried in order of this list.
The order is specified by the "priority" values of the LDAP server configurations.

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)

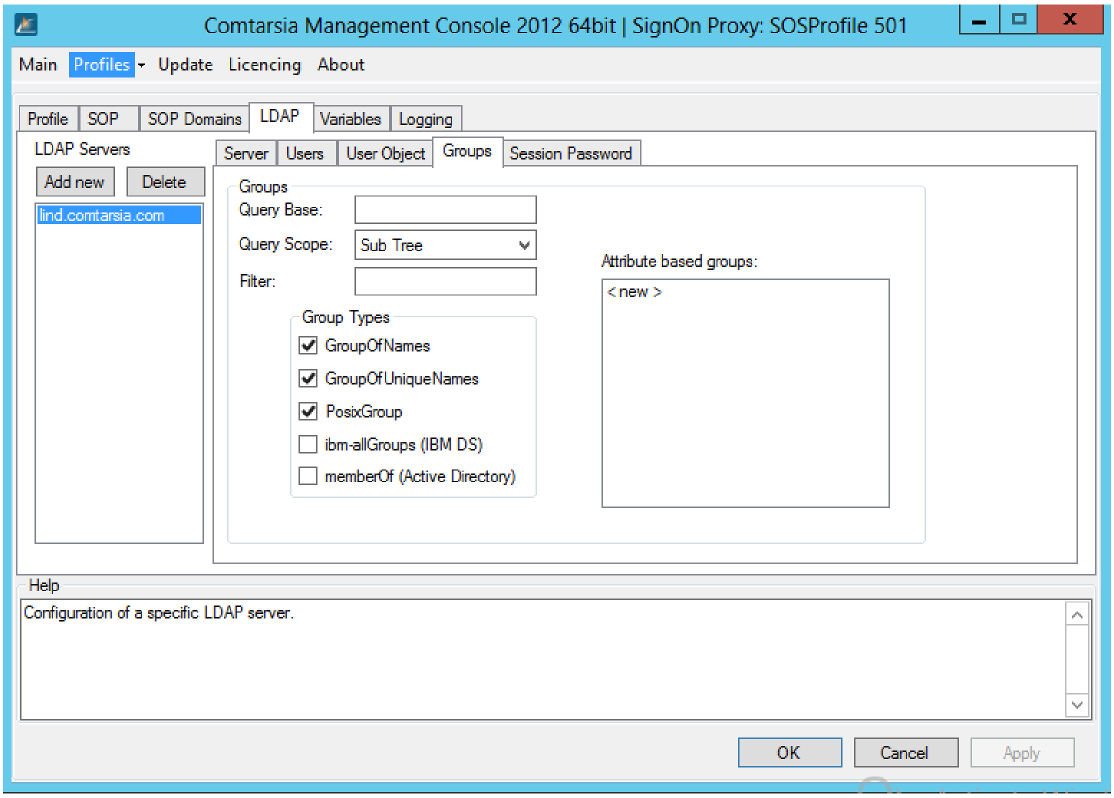
interval mode
This option sets the config "smartCardSessionPasswordMode" to 1. (interval mode). The interval mode ensures that the generated password stays the same over specified time spans, but also that different workstations generate the same session password. This prevents synchronisation/network-resource 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).

6.2.6 Groups



lind.comtarsia.com

Groups

Query Base:

Query Scope: Sub Tree

Filter:

Group Types

☑ GroupOfNames
☑ GroupOfUniqueNames
☑ PosixGroup
☐ ibm-allGroups (IBM DS)
☐ memberOf (Active Directory)

Attribute based groups:
< new >

Configuration of a specific LDAP server.

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 existent: (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.

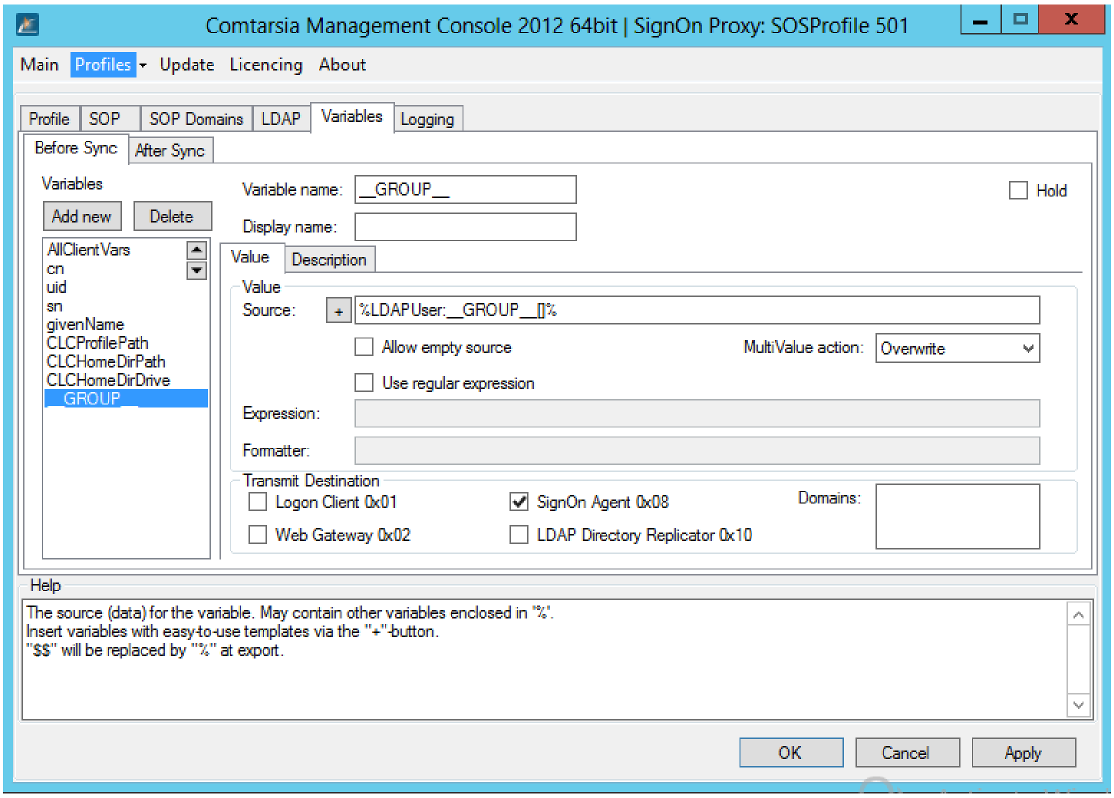
- GroupOfNames

- 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 Variables



Variable name: __GROUP__

Display name:

□ Hold

Value

Source: + %LDAPUser:__GROUP__[]%

□ Allow empty source

MultiValue action: Overwrite

□ Use regular expression

Expression:

Formatter:

Transmit Destination

□ Logon Client 0x01 ☑ SignOn Agent 0x08 Domains:

□ Web Gateway 0x02 □ LDAP Directory Replicator 0x10

Help

The source (data) for the variable. May contain other variables enclosed in "%".
Insert variables with easy-to-use templates via the "+"-button.
"$$" will be replaced by "%" at export.

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 synchronization (thus they can also be sent to the SignOn Agent)
After Sync: Variables will be processed after the user synchronization Thus values can be sent back by the SignOn Agent 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 temporally.

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 */
```

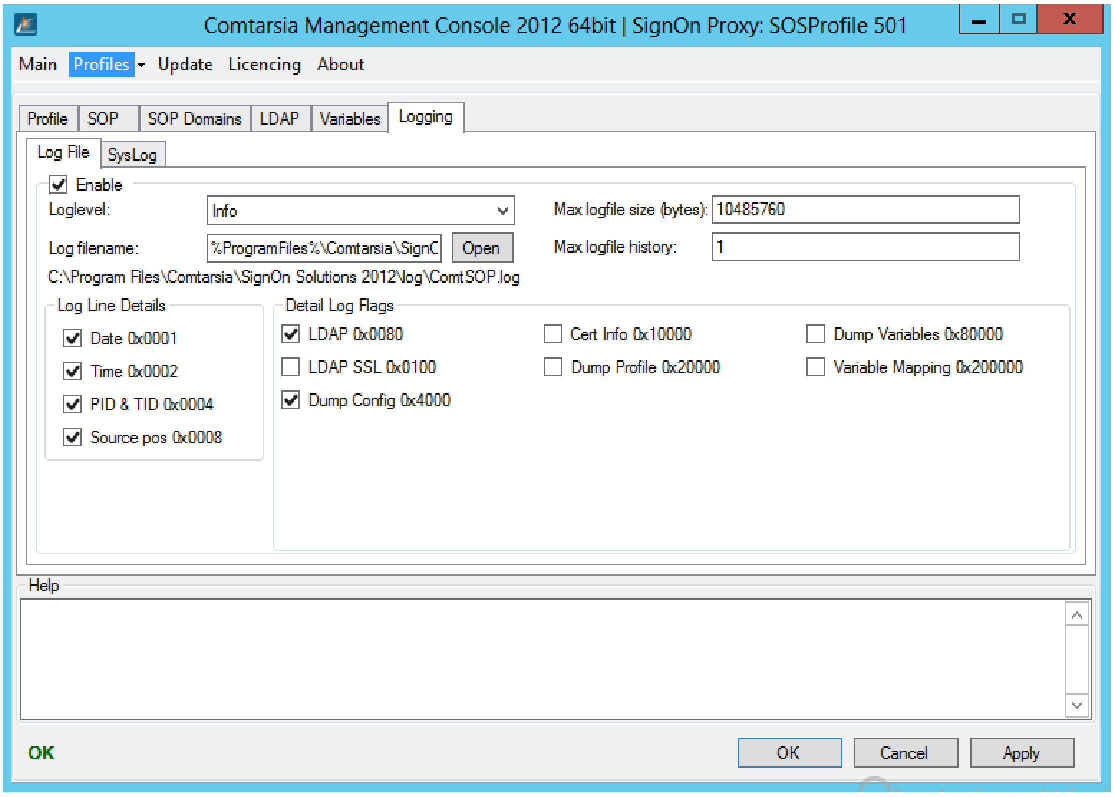
```
match_not_null          0x00000800, /* string can't be null */
match_continuous        0x00001000, /* each grep match must continue
*/
                                    /* uninterupted from the previous
one */
match_partial           0x00002000, /* find partial matches */

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

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

Transmit Destination

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 SignbOn 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.

6.4 Logging



☑ Enable

Loglevel: Info

Log filename: %ProgramFiles%\Comtarsia\SignC

C:\Program Files\Comtarsia\SignOn Solutions 2012\log\ComtSOP.log

Max logfile size (bytes): 10485760

Max logfile history: 1

Log Line Details

☑ Date 0x0001

☑ Time 0x0002

☑ PID & TID 0x0004

☑ Source pos 0x0008

Detail Log Flags

☑ LDAP 0x0080

□ LDAP SSL 0x0100

☑ Dump Config 0x4000

□ Cert Info 0x10000

□ Dump Profile 0x20000

□ Dump Variables 0x80000

□ Variable Mapping 0x200000

OK

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.

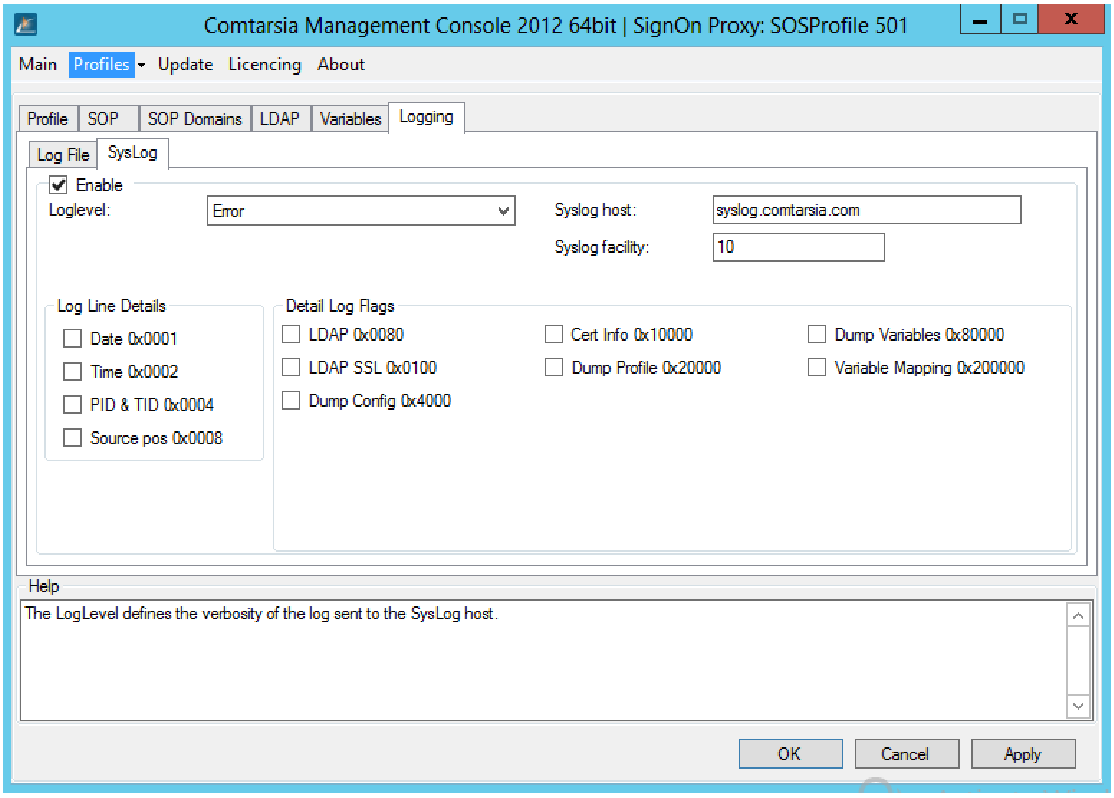
Detail Log Flags

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.



☑ Enable

Loglevel: Error

Syslog host: syslog.comtarsia.com

Syslog facility: 10

Log Line Details

☐ Date 0x0001
☐ Time 0x0002
☐ PID & TID 0x0004
☐ Source pos 0x0008

Detail Log Flags

☐ LDAP 0x0080
☐ LDAP SSL 0x0100
☐ Dump Config 0x4000
☐ Cert Info 0x10000
☐ Dump Profile 0x20000
☐ Dump Variables 0x80000
☐ Variable Mapping 0x200000

The LogLevel defines the verbosity of the log sent to the SysLog host.

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.

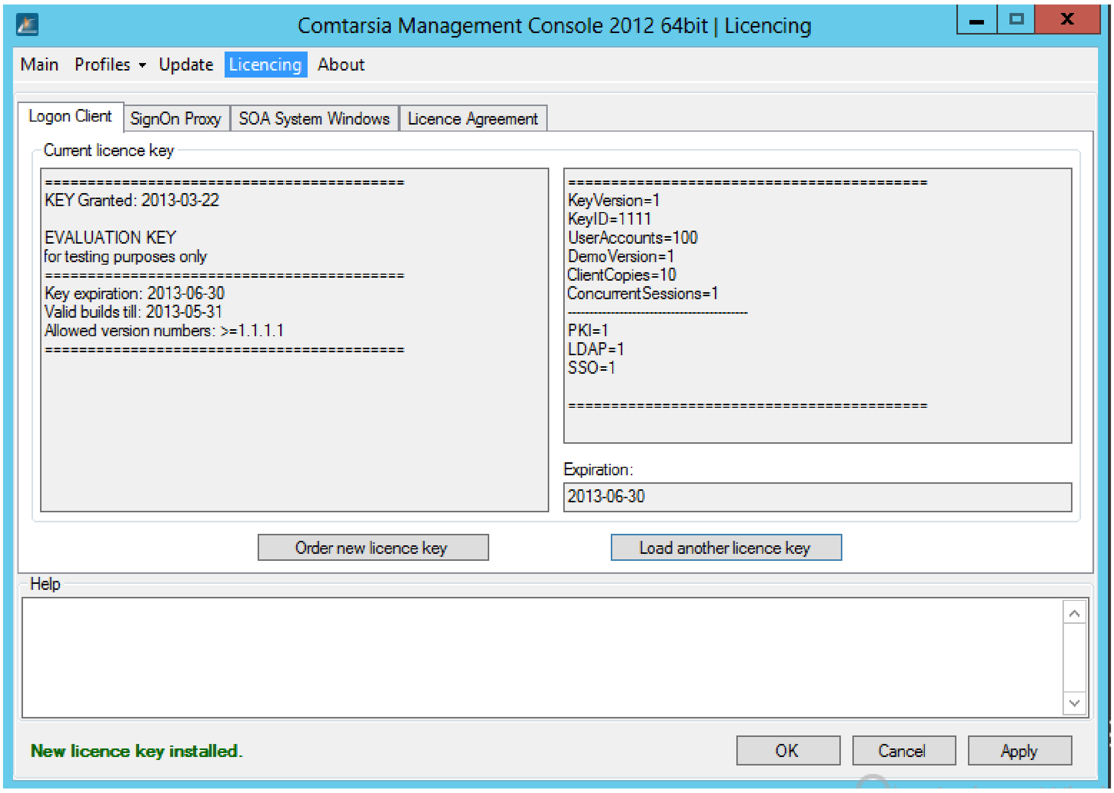
Syslog facility
Specifies the SysLog facility of the log messages.

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.

6.5 Licensing



```
==========================================
KEY Granted: 2013-03-22

EVALUATION KEY
for testing purposes only
==========================================
Key expiration: 2013-06-30
Valid builds till: 2013-05-31
Allowed version numbers: >=1.1.1.1
==========================================
```

```
==========================================
KeyVersion=1
KeyID=1111
UserAccounts=100
DemoVersion=1
ClientCopies=10
ConcurrentSessions=1
-----------------------------------------
PKI=1
LDAP=1
SSO=1

==========================================
```

Expiration: 2013-06-30

New licence key installed.

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 2012\Key.

7. 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.