SignOn Gate 2006

Introduction and installation

Version: 1.2.10.4, 04-Jul-2006

Index

1. Comtarsia SignOn Gate 2006

1.1 Introduction

1.1.1 What is SignOn Gate 2006?

SignOn Gate 2006 is an add-on to Comtarsia Logon Client 2006.

SignOn Gate 2003 is a technical implementation that allows for holding a **primary user management** on LDAP servers, while **resources** can be placed on Windows, Linux and Unix servers. It provides the possibility to manage user accounts automatically on Windows servers, Windows domains (NT 4.0 / ADS) and UNIX servers, offers also the possibility to integrate them into an LDAP user management.

The Comtarsia Logon Client and the Comtarsia Sign On Gate not only represents an optimal migration tool, additionally it offers also the advantage of separate user management and resource management maintenance. This means a determining independence compared to proprietary solutions. Herewith stands Comtarsia also for Single Sign On, Centralized User Management and Security Management.

1.1.2 Procedure

At each logon **Comtarsia Logon Client 2006** sends a synchronization request, so called **SignOn Sync Packet** to the server where SignOn Proxy is running, and the **SignOn Proxy** forwards it to the respective SignOn Agent.
The SignOn Agent makes sure that

- the user account exists
- a synchronous password is present
- suitable access permissions to the home directory are set
- the corresponding groups, where the user belongs, exist or will be created

1.1.3 How to be always up-to-date

At password change (either at logon with Comtarsia Logon Client 2003 or during the session) the SignOn Agent is in charge to **automatically and immediately update** the resource servers. This way the passwords are always synchronous unlike in systems that synchronize passwords via time managed procedures.

It is made sure at each logon that the user holds corresponding access permissions for all resources.

1.1.4 Security

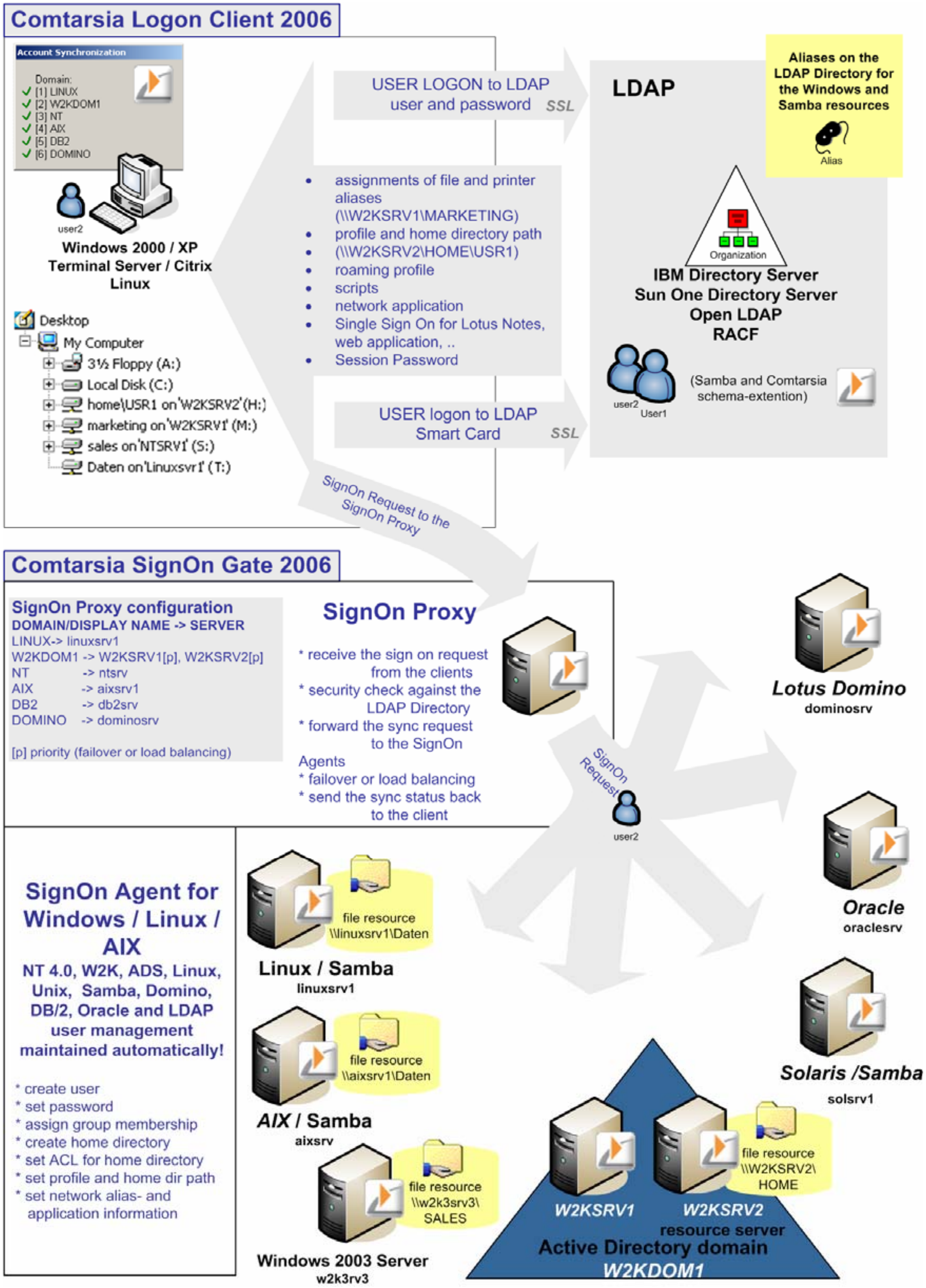
Logon data is transmitted with RSA encryption.
For further information on this matter please refer to the manual "SignOnGate_RSA_EN"

Complete trust from a security point of view between SignOn Proxy server and LDAP directory is enforced.

Please see more under "Setting up SignOn Proxy"/ "Security".

The Security Agent provides a high security level in combination with the SignOn Agent: To prohibit the use of the central user management no uncontrolled user accounts remain active longer than defined, since Security Agent automatically deactivates these. The execution time is precisely configurable.

1.2 Comtarsia SignOn Overview



Comtarsia Logon Client 2006

Account Synchronization

Domain:
✓ [1] LINUX
✓ [2] W2KDOM1
✓ [3] NT
✓ [4] AIX
✓ [5] DB2
✓ [6] DOMINO

Windows 2000 / XP
Terminal Server / Citrix
Linux

Desktop
My Computer
3½ Floppy (A:)
Local Disk (C:)
home\USR1 on 'W2KSRV2' (H:)
marketing on 'W2KSRV1' (M:)
sales on 'NTSRV1' (S:)
Daten on 'Linuxsvr1' (T:)

USER LOGON to LDAP
user and password SSL

- assignments of file and printer aliases (\\W2KSRV1\MARKETING)
- profile and home directory path
- (\\W2KSRV2\HOME\USR1)
- roaming profile
- scripts
- network application
- Single Sign On for Lotus Notes, web application, ..
- Session Password

USER logon to LDAP
Smart Card SSL

LDAP

Aliases on the LDAP Directory for the Windows and Samba resources

IBM Directory Server
Sun One Directory Server
Open LDAP
RACF

(Samba and Comtarsia schema-extention)

SignOn Request to the SignOn Proxy

Comtarsia SignOn Gate 2006

SignOn Proxy configuration
DOMAIN/DISPLAY NAME -> SERVER
LINUX-> linuxsrv1
W2KDOM1 -> W2KSRV1[p], W2KSRV2[p]
NT -> ntsrv
AIX -> aixsrv1
DB2 -> db2srv
DOMINO -> dominosrv

[p] priority (failover or load balancing)

SignOn Proxy

* receive the sign on request from the clients
* security check against the LDAP Directory
* forward the sync request to the SignOn Agents
* failover or load balancing
* send the sync status back to the client

SignOn Request

SignOn Agent for Windows / Linux / AIX

NT 4.0, W2K, ADS, Linux, Unix, Samba, Domino, DB/2, Oracle and LDAP user management maintained automatically!

* create user
* set password
* assign group membership
* create home directory
* set ACL for home directory
* set profile and home dir path
* set network alias- and application information

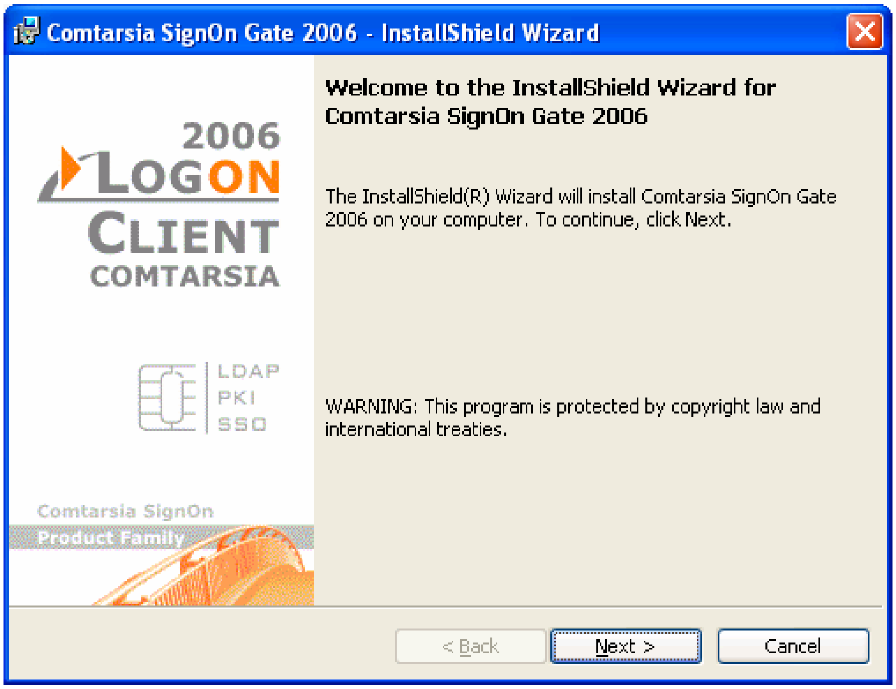
1.3 Installation

This manual contains Comtarsia SignOn Proxy and SignOn Agent installation instructions in order to setup SignOn Gate 2003 with InstallShield installer.

Administrator privileges are required for installation!

1.3.1 Start with InstallShield

Please start setup by **SignOnGate-1.1.x.4.exe** file.



Welcome to the InstallShield Wizard for Comtarsia SignOn Gate 2006

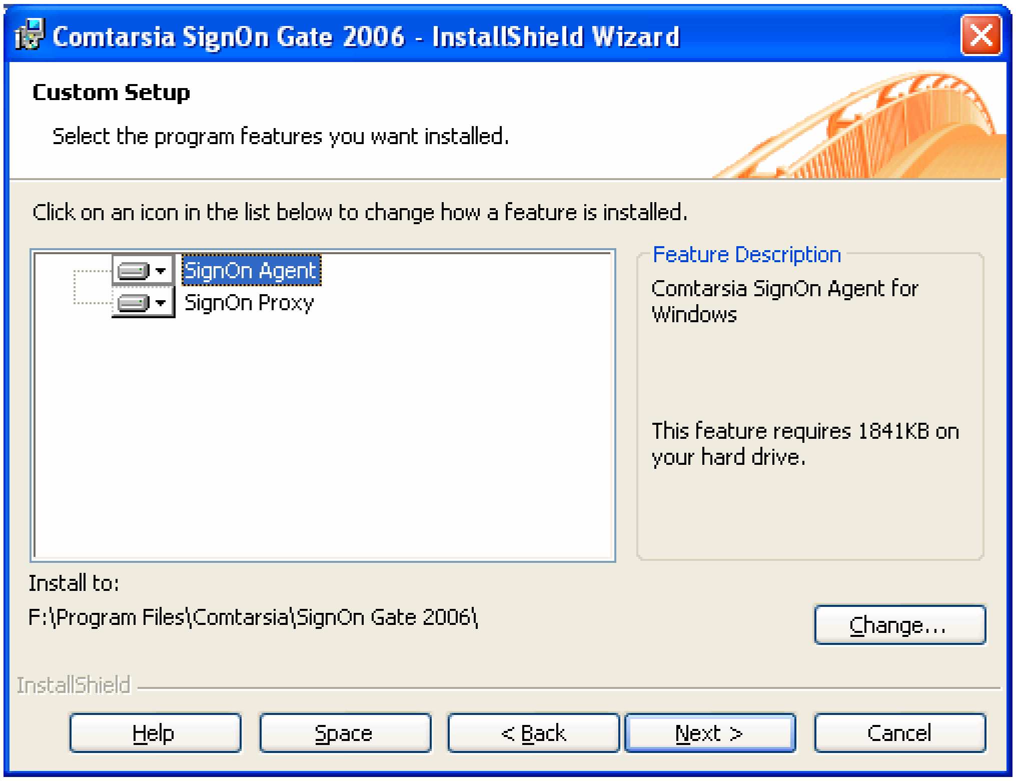
The InstallShield(R) Wizard will install Comtarsia SignOn Gate 2006 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

After entering User and Company name, please define, for whom the program shall be available (current user/all users of the computer).

Specify program destination folder, or leave default setting.

Select features which you want to install: Comtarsia SignOn Proxy and/or Comtarsia SignOn Agent.


Comtarsia SignOn Gate 2006 - InstallShield Wizard
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
SignOn Agent
SignOn Proxy
Feature Description
Comtarsia SignOn Agent for Windows
This feature requires 1841KB on your hard drive.
Install to:
F:\Program Files\Comtarsia\SignOn Gate 2006\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

After InstallShield has copied and registered all necessary files, the Configurator of the chosen service will appear.

1.3.2 Setting up the SignOn Agent

General Agent Parameters

Please set the **IP Address** of the server where the SignOn Proxy service is running (“**Proxy Server(IP address)**”).
In case SignOn Agent and SignOn Proxy are running on the same computer, please leave default value (127.0.0.1).

The “**SOA Policy Options**” allow carrying out extended settings which regard the user synchronization.

Check Password: the password will be automatically synchronized.

Create User: If a user account does not yet exist, it will be automatically created.

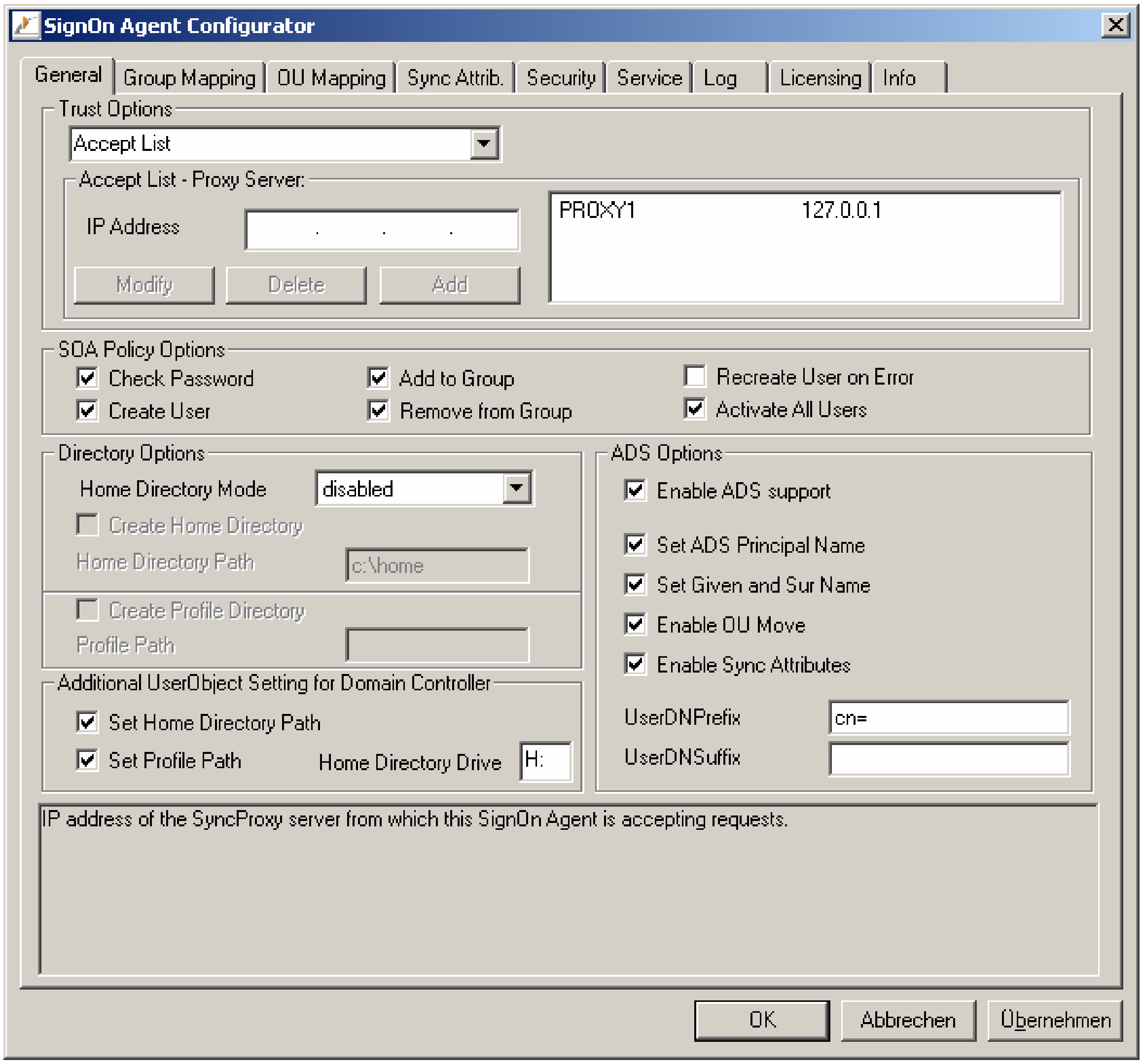
Add to group, Remove from Group: the group membership will be adjusted according to the global user management and the “groupmapping List”.

Recreate User on Error: If an error occurs in the user synchronization, for example the user account cannot be synchronized, the user account will be newly created and the password will be synchronized.

Activate All Users: If the user account which should be synchronized is deactivated, it will be activated again even if it is not created by the Agent. Otherwise just user accounts created by the Agent will be activated (marked with the "user description" "SERV_TMP_USER")

The "**Home Directory Options**" determines, by which means a home directory is created for the user.

If not disabled, the "**Standalone Server**" option requires enabled "**Create Home Directory**" checkbox and "**Home Directory Path**" checkbox, if the user accounts shall be automatically created. "**Home Directory Path**" can be set as for example "c:\home". User home directory will be created in "c:\home".



Trust Options: Accept List

Accept List - Proxy Server:

IP Address: . . .

PROXY1	127.0.0.1

SOA Policy Options

☑ Check Password ☑ Add to Group □ Recreate User on Error

☑ Create User ☑ Remove from Group ☑ Activate All Users

Directory Options

Home Directory Mode: disabled

□ Create Home Directory

Home Directory Path: c:\home

□ Create Profile Directory

Profile Path:

Additional UserObject Setting for Domain Controller

☑ Set Home Directory Path

☑ Set Profile Path Home Directory Drive: H:

ADS Options

☑ Enable ADS support

☑ Set ADS Principal Name

☑ Set Given and Sur Name

☑ Enable OU Move

☑ Enable Sync Attributes

UserDNPrefix: cn=

UserDNSuffix:

IP address of the SyncProxy server from which this SignOn Agent is accepting requests.

If the SignOn Agent is running on a Windows domain controller, "**Home Directory Path**" can be defined with the word "**CLIENT**", and the SignOn Agent uses the settings specified in the Logon Client. If an UNC path is specified, a user directory can be on an other server in the same Windows domain as the SignOn Agent. The

UNC path must contain the name of the server! Do not use here IP addresses!

If checkboxes "**Set Home Directory Path**" and "**Set Profile Path**" are enabled, the profile path and the home directory path will be created according to the user object.

In case that no drive letter is set for the user directory in the master domain, it is possible to create it here for the Windows user database via the SignOn Agent.

These options are only useful on a domain controller when migrating Windows server(s).

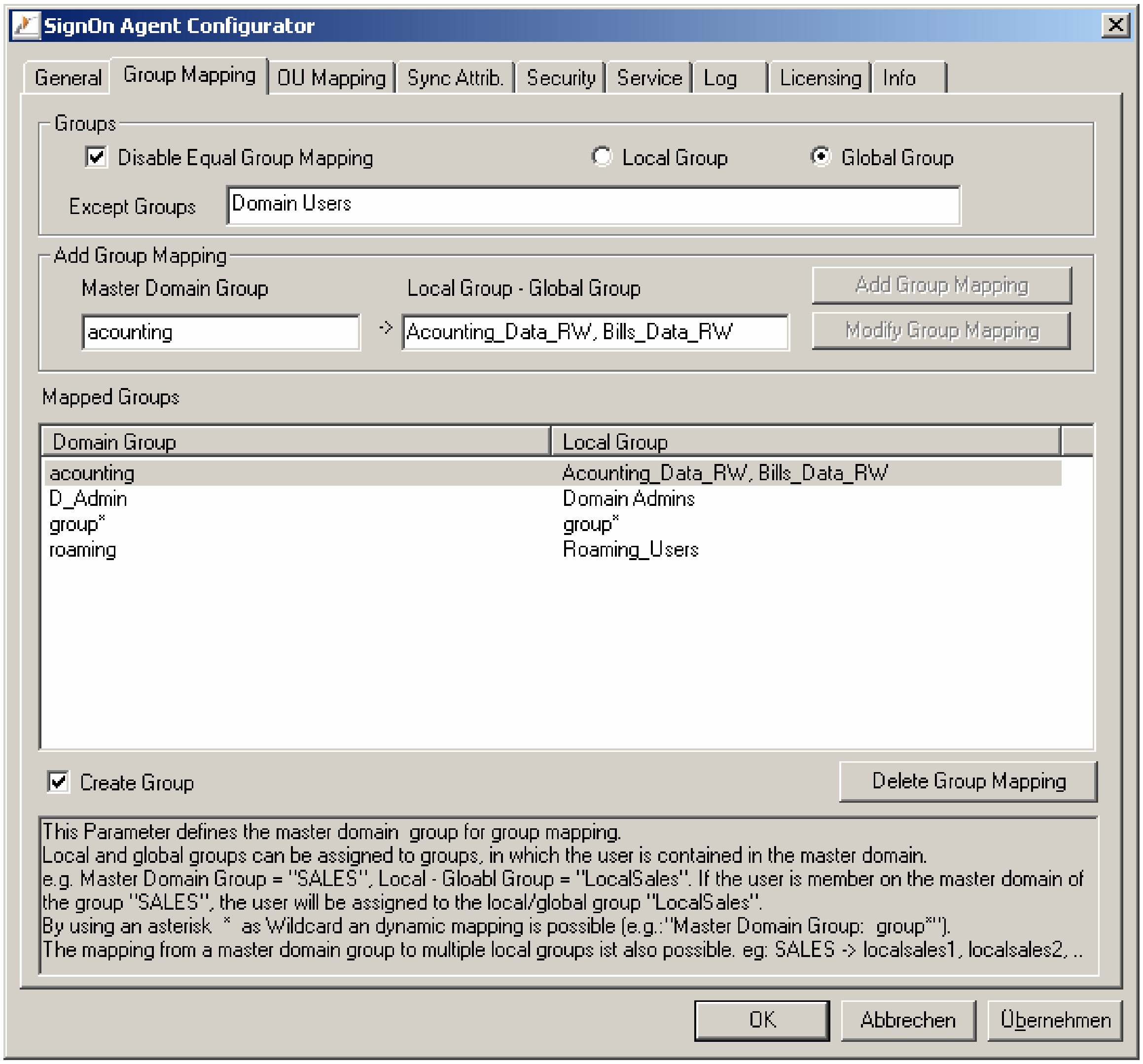
In “**ADS Options**” the support for the ADS mode can be activated with “**Enable ADS support**”. Thus it is possible to make additional ADS relevant synchronization settings.
“**Set ADS Principal Name**”: sets the principal name of the ADS user object. The principal name is composed of the UID of the LDAP user object and the Active Directory domain (UID@ADS-domain)
“**Set Given and Sur Name**”: sets the given name und the surname of the ADS user object. For this purpose the LDAP attribute SN and GivenName are used.
“**Enable OU Move**”: Thus it is possible to put users in other “Active Directory OUs” then the default OU (cn=users). “UserDNPrefix” defines the prefix of the “AD user object” (default “cn=”). Please see OU-mapping.
“**Endable Sync Attributes**”: with this “Sync Attributes” can be activated (see Sync Attributes)

Group Mapping

Group mapping **by equal group names** can be set for standalone server or domain controller: users will be member in the same groups they are in the primary user management, e.g. Sales (master domain group)-> Sales (local group). If the groups are not available on the local server, the option “Create Group” defines, whether they should be created or not.

Under "**Except Groups**" a list of groups can be excluded e.g.: Administrators, Power Users, Guests, Domain Users. The names of the “Except Groups” can be completed with wildcards, e.g. tmp*, Domain*.
This means that neither the user will be automatically assigned to these groups upon synchronization requests, nor will be the membership of the user deleted from these groups in this way.

In case of **different group names**, the checkbox “**Disable Equal Group Mapping**” has to be marked; assign to "**Master Domain Group**" the desired "**Local/Global Group**". (e.g. SALES -> LocalSales.) Wildcards are possible too, for example: group* -> group* assigns all groups which begin with group to groups which are called the same (group1 -> group1, group 1234 -> group1234, groupABCD ->groupABCD).



Groups

☑ Disable Equal Group Mapping ○ Local Group ● Global Group

Except Groups: Domain Users

Add Group Mapping

Master Domain Group: acounting -> Local Group - Global Group: Acounting_Data_RW, Bills_Data_RW

Mapped Groups

Domain Group	Local Group
acounting	Acounting_Data_RW, Bills_Data_RW
D_Admin	Domain Admins
group*	group*
roaming	Roaming_Users

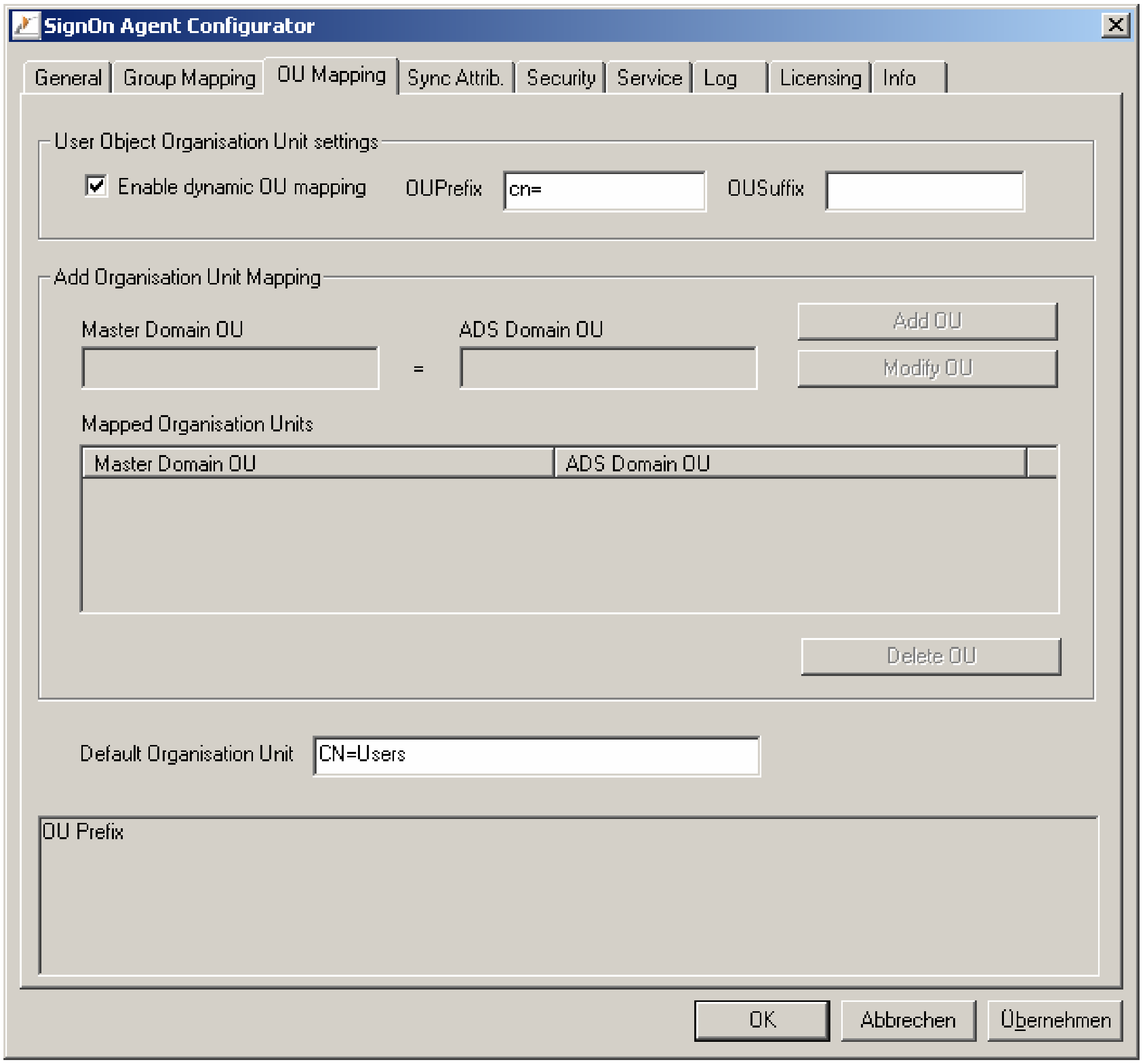
☑ Create Group

This Parameter defines the master domain group for group mapping.
Local and global groups can be assigned to groups, in which the user is contained in the master domain.
e.g. Master Domain Group = "SALES", Local - Gloabl Group = "LocalSales". If the user is member on the master domain of the group "SALES", the user will be assigned to the local/global group "LocalSales".
By using an asterisk * as Wildcard an dynamic mapping is possible (e.g.:"Master Domain Group: group*").
The mapping from a master domain group to multiple local groups ist also possible. eg: SALES -> localsales1, localsales2, ..

If the “**Create Group**” option activated, the not yet existent groups will be automatically created by the Comtarsia SignOn Agent.

OU-Mapping

The OU-Mapping effects, that the user object which the SignOn Proxy has forwarded can be placed in another than the Standard-OU in the “Active Directory” (cn=users). The user objects hereby only can be put into already existing OU’s.



User Object Organisation Unit settings

☑ Enable dynamic OU mapping OUPrefix cn= OUSuffix

Add Organisation Unit Mapping

Master Domain OU = ADS Domain OU

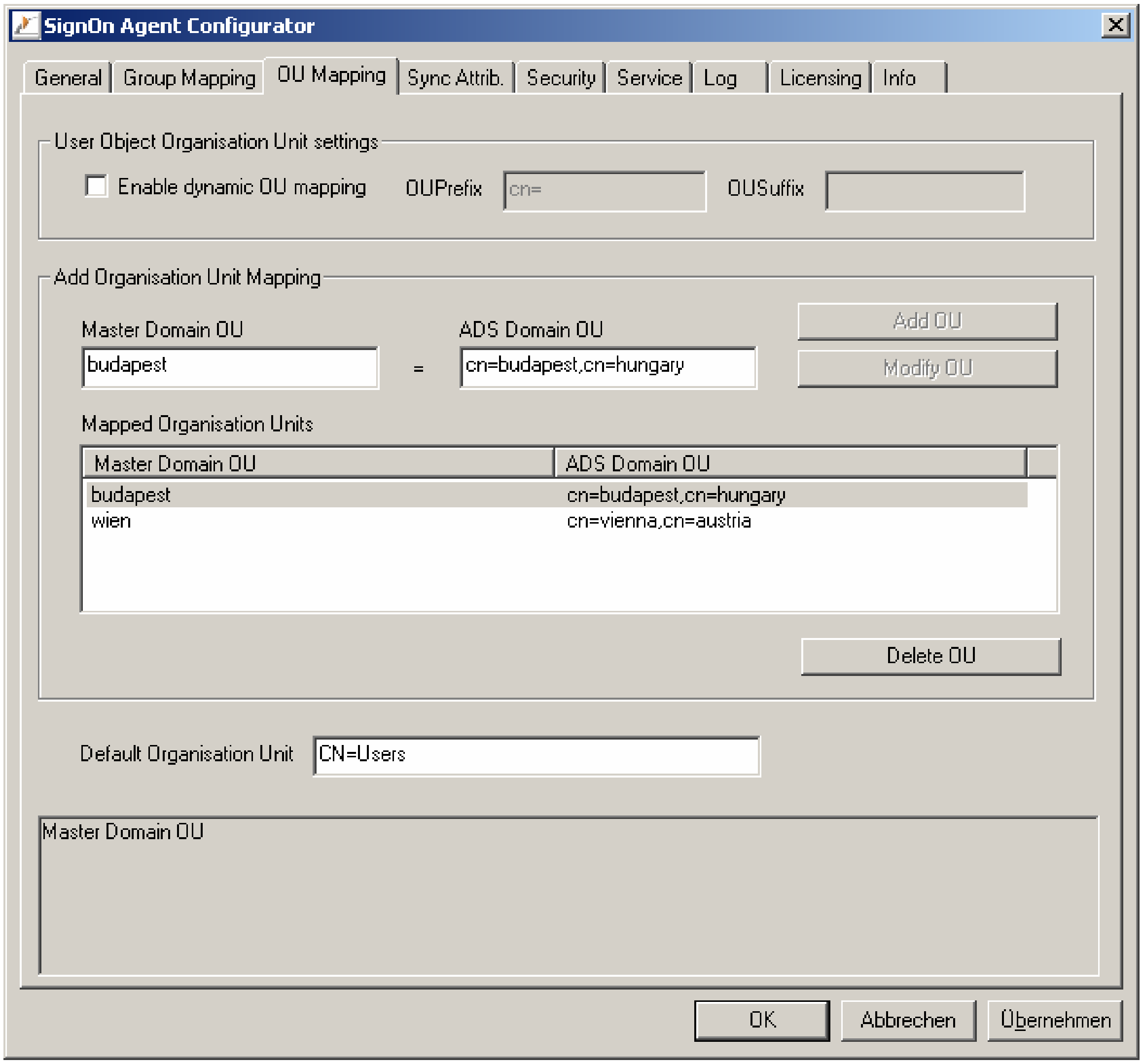
Mapped Organisation Units

Master Domain OU	ADS Domain OU

Default Organisation Unit CN=Users

OU Prefix

If “**Enable dynamic OU mapping**” is active, the final “UserDN” is created as follows:
UserDNPrefix + USERNAME + UserDNSuffix + “,” + OUPrefix + OU + OUSuffix + “,” + ADS-BaseDN
Whereas “OU” is replaced by the OU the SignOn Proxy has sent. If “**Enable dynamic OU mapping**” is not active, the OU which is transmitted from the SignOn Proxy is replaced according to the “OU-mapping-list” (Mapped Organisation Units)
Therefore the “UserDN” is created as follows:
UserDNPrefix + USERNAME + UserDNsuffix + “,” + Mapped-OU + “,” + ADS BaseDN
If an OU which is sent from SignOn Proxy does not occur in the “OU-mapping-list”, the “Default Organisation Unit” is set in.



User Object Organisation Unit settings

☐ Enable dynamic OU mapping OUPrefix: cn= OUSuffix:

Add Organisation Unit Mapping

Master Domain OU: budapest = ADS Domain OU: cn=budapest,cn=hungary

Mapped Organisation Units

Master Domain OU	ADS Domain OU
budapest	cn=budapest,cn=hungary
wien	cn=vienna,cn=austria

Default Organisation Unit: CN=Users

Master Domain OU

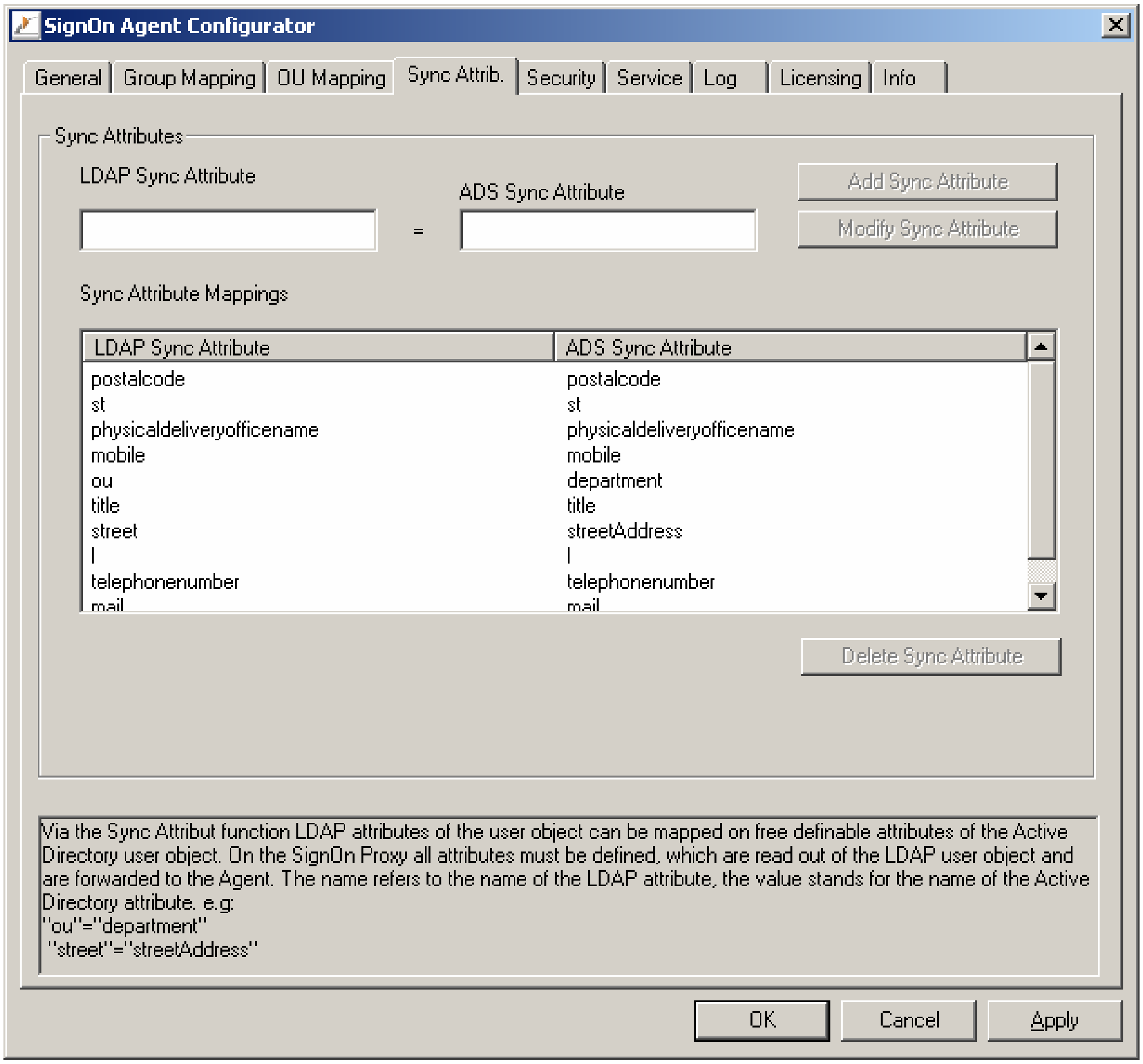
Sync Attributes

Via the **“Sync Attributes”** the attributes of the LDAP user object can be assigned to the attributes of the ADS user object. The attributes are read out from the LDAP directory by the SignOn proxy and are forwarded to the SignOn Agent. On the SignOn Agent the mapping of the configured “Sync Attribute Mappings” is carried out.
Example

postalcode	->	postalcode
ou	->	department
street	->	streetAddress
mail	->	mail

“Sync Attributes” can be activated in the “General-Tab” of the SignOn Agent under ADS-Options.

Attention: “Sync Attributes” must be configurated on the SignOn proxy as well as on the SignOn Agent (See also “Sync Attributes” under “Setting up the SignOn Proxy”→ LDAP)



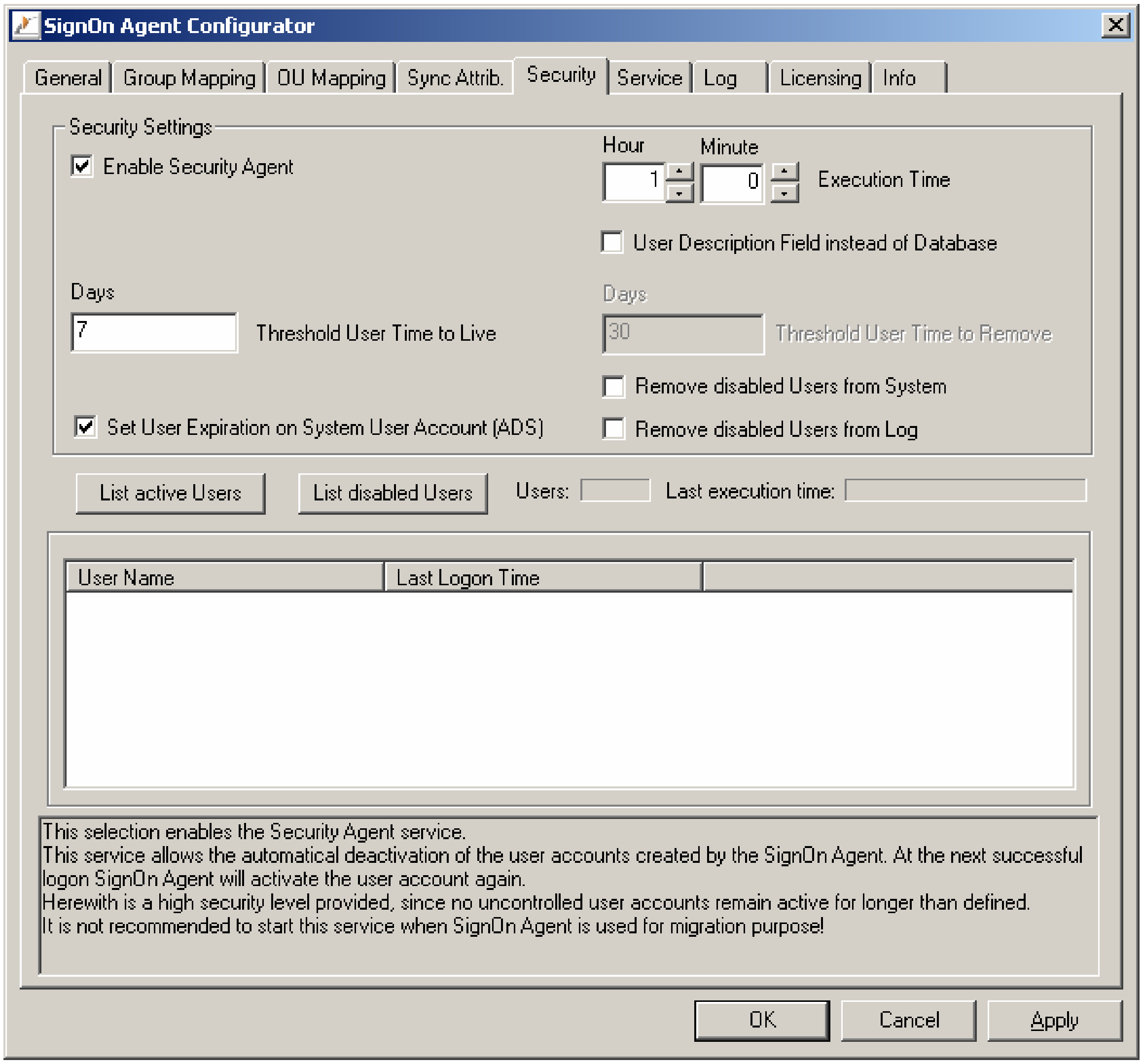
LDAP Sync Attribute	ADS Sync Attribute
postalcode	postalcode
st	st
physicaldeliveryofficename	physicaldeliveryofficename
mobile	mobile
ou	department
title	title
street	streetAddress
l	l
telephonenumber	telephonenumber
mail	mail

Via the Sync Attribut function LDAP attributes of the user object can be mapped on free definable attributes of the Active Directory user object. On the SignOn Proxy all attributes must be defined, which are read out of the LDAP user object and are forwarded to the Agent. The name refers to the name of the LDAP attribute, the value stands for the name of the Active Directory attribute. e.g:
"ou"="department"
"street"="streetAddress"

Security Agent

This feature provides a high security level: no uncontrolled user accounts remain active longer than defined, since Security Agent automatically deactivates these. The execution time is precisely configurable.

"**Threshold Time to Live**" defines how many days after the last login the user account shall be deactivated. After the numbers of days (set in the "**Threshold User Time to Remove**") are up, the user will be finally deleted from the Comtarsia user database.
With a new user logon the account will be automatically activated again, provided that the account is still valid in the primary user management.
Both active and disabled users are to be listed up by "**List active Users**"/"**List disabled users**".



Security Settings

☑ Enable Security Agent

Hour: 1 Minute: 0 Execution Time

□ User Description Field instead of Database

Days: 7 Threshold User Time to Live

Days: 30 Threshold User Time to Remove

□ Remove disabled Users from System

☑ Set User Expiration on System User Account (ADS)

□ Remove disabled Users from Log

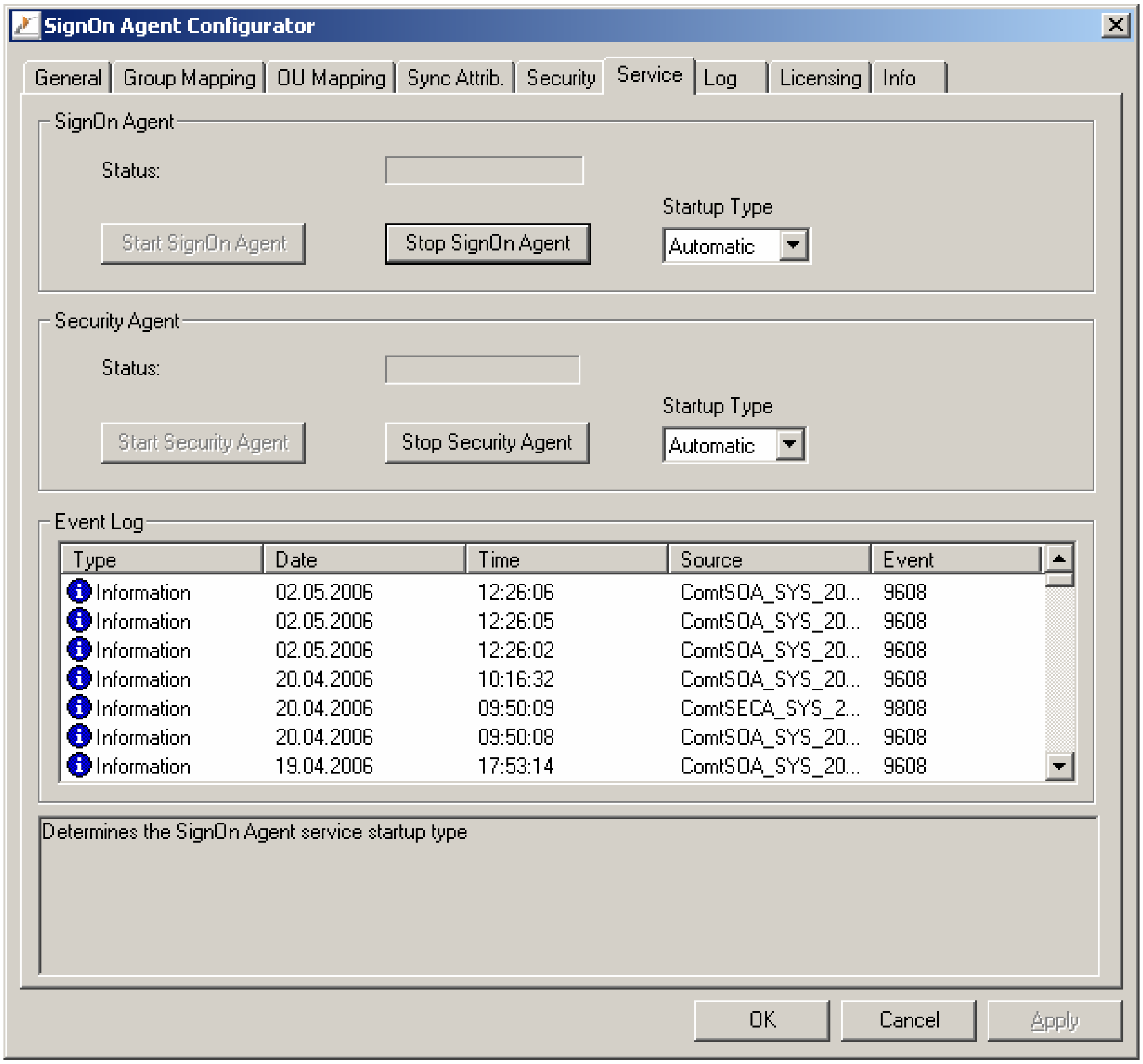
Users:

Last execution time:

This selection enables the Security Agent service.
This service allows the automatical deactivation of the user accounts created by the SignOn Agent. At the next successful logon SignOn Agent will activate the user account again.
Herewith is a high security level provided, since no uncontrolled user accounts remain active for longer than defined.
It is not recommended to start this service when SignOn Agent is used for migration purpose!

Service Control

Startup type (Autom./Manual) specifies which Comtarsia services should be automatically started at system start. Agent service can be started and stopped or disabled manually.



SignOn Agent

Status:

Startup Type: Automatic

Security Agent

Status:

Startup Type: Automatic

Event Log

Type	Date	Time	Source	Event
Information	02.05.2006	12:26:06	ComtSOA_SYS_20...	9608
Information	02.05.2006	12:26:05	ComtSOA_SYS_20...	9608
Information	02.05.2006	12:26:02	ComtSOA_SYS_20...	9608
Information	20.04.2006	10:16:32	ComtSOA_SYS_20...	9608
Information	20.04.2006	09:50:09	ComtSECA_SYS_2...	9808
Information	20.04.2006	09:50:08	ComtSOA_SYS_20...	9608
Information	19.04.2006	17:53:14	ComtSOA_SYS_20...	9608

Determines the SignOn Agent service startup type

The “Event Log” provides information, warnings or error messages. (Double cklick.)

Licensing

A license key for testing purposes is provided, validity please see on the key. Press "**Load a new licensekey**" in order to browse for purchased license key according to individual conditions.

1.3.3 Setting up SignOn Proxy

Domain Synchronization

In the field "**Add domain**" can be specified the name(s) of the domain(s) or the standalone server name, which is to be synchronized ("**Domain Name**").
Click „Add“.

Also the server, where the SignOn Agent will run and process the synchronization requests, must be defined here ("**Server**").
In case a standalone server is configured, "Failover" and "Loadbalancing" is disabled. Otherwise it is here to configure, whether secondary server (set under "**Secondary Server**") will only be contacted, if primary server stops processing inbound requests (enable "**Failover**"); or instead the requests are sent to server1 and server2 in alternation (enable "**Loadbalancing**").
In the field "**Domain Type**" is/are the domain type(s) or the standalone server configuration to set.

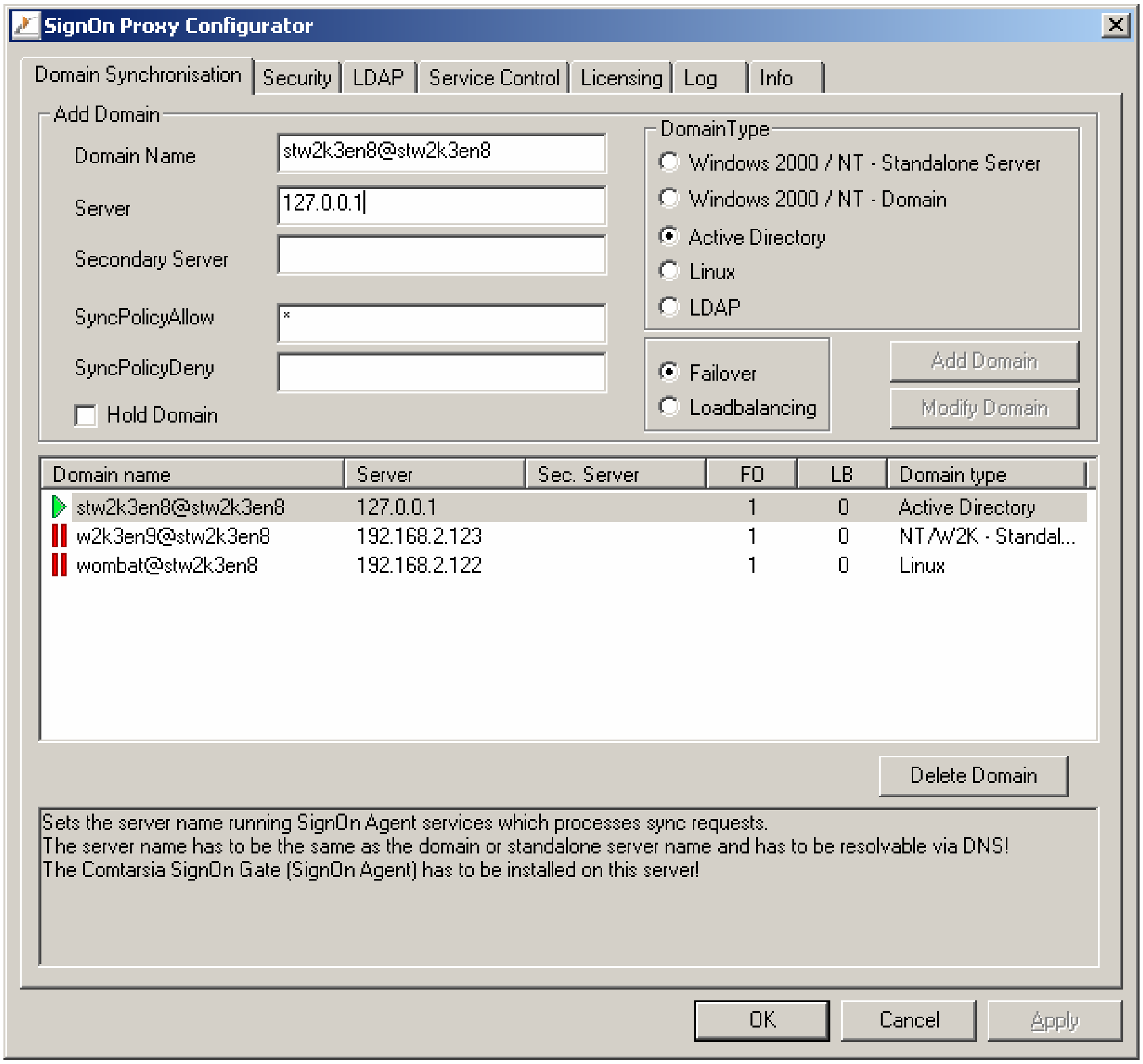
“**SyncPolicy**” makes a group dependent synchronization possible.
At “**SyncPolicyAllow**” groups can be defined, which members can be synchronized to these agents.
At “**SyncPolicyDeny**” groups can be defined, which members are not to be synchronized to these agents.
The names of the groups are separated with commas and can be completed with wildcards, e.g. group*.
“SyncPolicyDeny” overwrites “SyncPolicyAllow”, i.e. users, which are members in a “SyncPolicyAllow”-group as well as in a “SyncPolicyDeny”-Group are not going to be synchronized.
The fields “SyncPolicyAllow” and “SyncPolicyDeny” must not contain more than 1024 characters.

Example:

SyncPolicyAllow: group*
SyncPolicyDeny: group5

User1 member of “group10” → is synchronized
User2 member of “group2, group5” → is not synchronized
User3 member of “group” → is synchronized
User4 member of “group5” → is not synchronized

At “**Hold Domains**” domains can be temporally deactivated. In the domain-list “Hold Domains” are marked with a red “Pause” icon.



Add Domain

Domain Name: stw2k3en8@stw2k3en8

Server: 127.0.0.1

Secondary Server:

SyncPolicyAllow: *

SyncPolicyDeny:

□ Hold Domain

DomainType

○ Windows 2000 / NT - Standalone Server

○ Windows 2000 / NT - Domain

● Active Directory

○ Linux

○ LDAP

● Failover

○ Loadbalancing

Domain name	Server	Sec. Server	FO	LB	Domain type
▶ stw2k3en8@stw2k3en8	127.0.0.1		1	0	Active Directory
‖ w2k3en9@stw2k3en8	192.168.2.123		1	0	NT/W2K - Standal...
‖ wombat@stw2k3en8	192.168.2.122		1	0	Linux

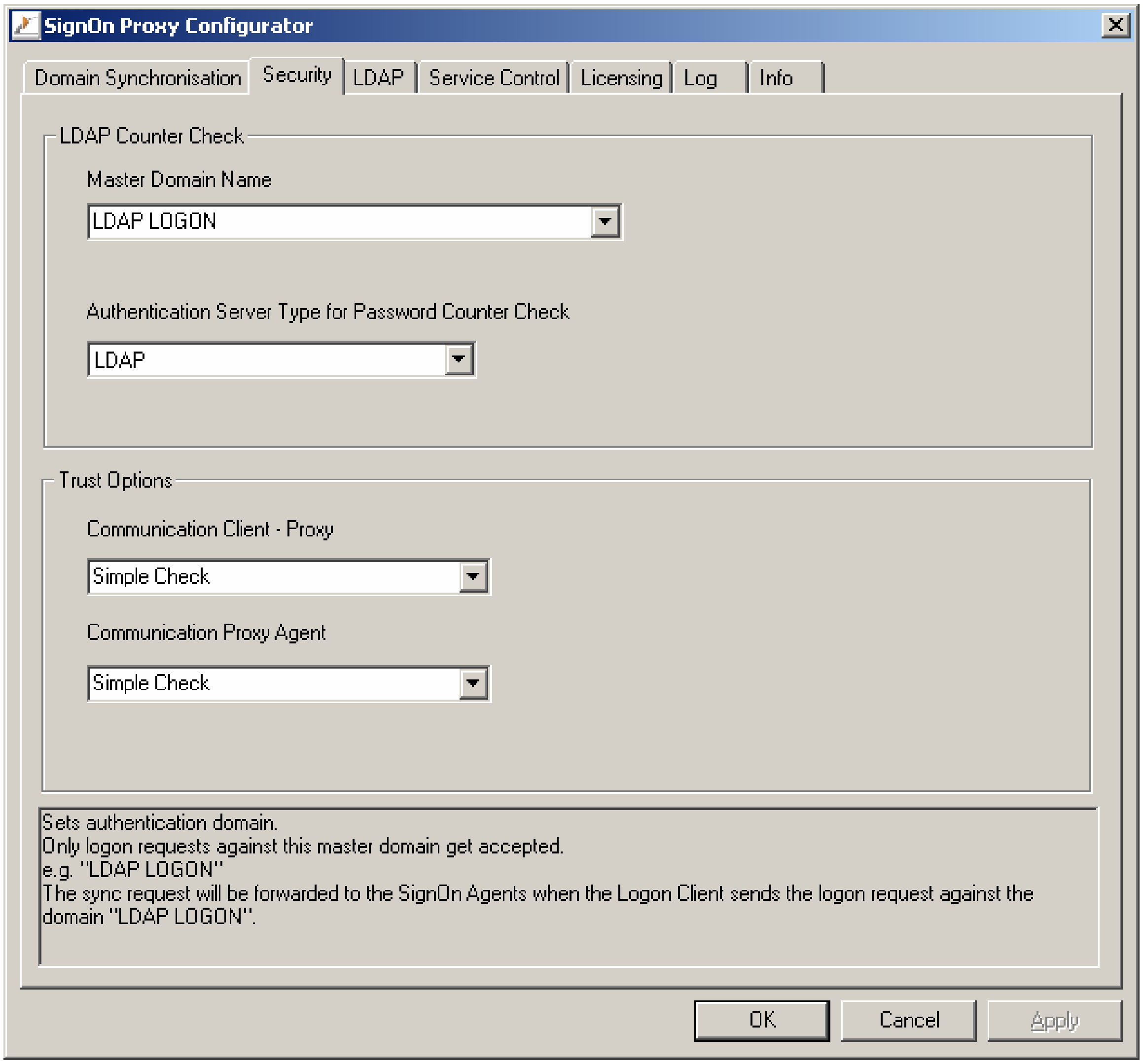
Sets the server name running SignOn Agent services which processes sync requests.
The server name has to be the same as the domain or standalone server name and has to be resolvable via DNS!
The Comtarsia SignOn Gate (SignOn Agent) has to be installed on this server!

Security

"**Master Domain Name**" - specifies the authentication domain name. In case of a LDAP-logon, the value “LDAP LOGON” can be left alone, in case of a primary OS/2-logon of the clients, the according domain name has to be put in. Logon requests are accepted ONLY against this domain!

“**Authentication Server Type for Password Counter Check**”: If enabled, the SignOn Proxy executes a counter checking, e.g. does not simply accept the user/password received from the Logon Client, processes instead a logon against the master domain to reassure password validity. Synchronization request will be forwarded to SignOn Agent **only** after successful logon.

If OS/2, configure "**Server Name**" and "**IP Address**" below, if LDAP, the next page "LDAP" will be enabled for complete setup.



Master Domain Name: LDAP LOGON

Authentication Server Type for Password Counter Check: LDAP

Communication Client - Proxy: Simple Check

Communication Proxy Agent: Simple Check

Sets authentication domain.
Only logon requests against this master domain get accepted.
e.g. "LDAP LOGON"
The sync request will be forwarded to the SignOn Agents when the Logon Client sends the logon request against the domain "LDAP LOGON".

LDAP

Here several LDAP parameters can be configured for the "Logon Client" and the "Web Sync Client" (please refer to the "Logon Client LDAP" manual).

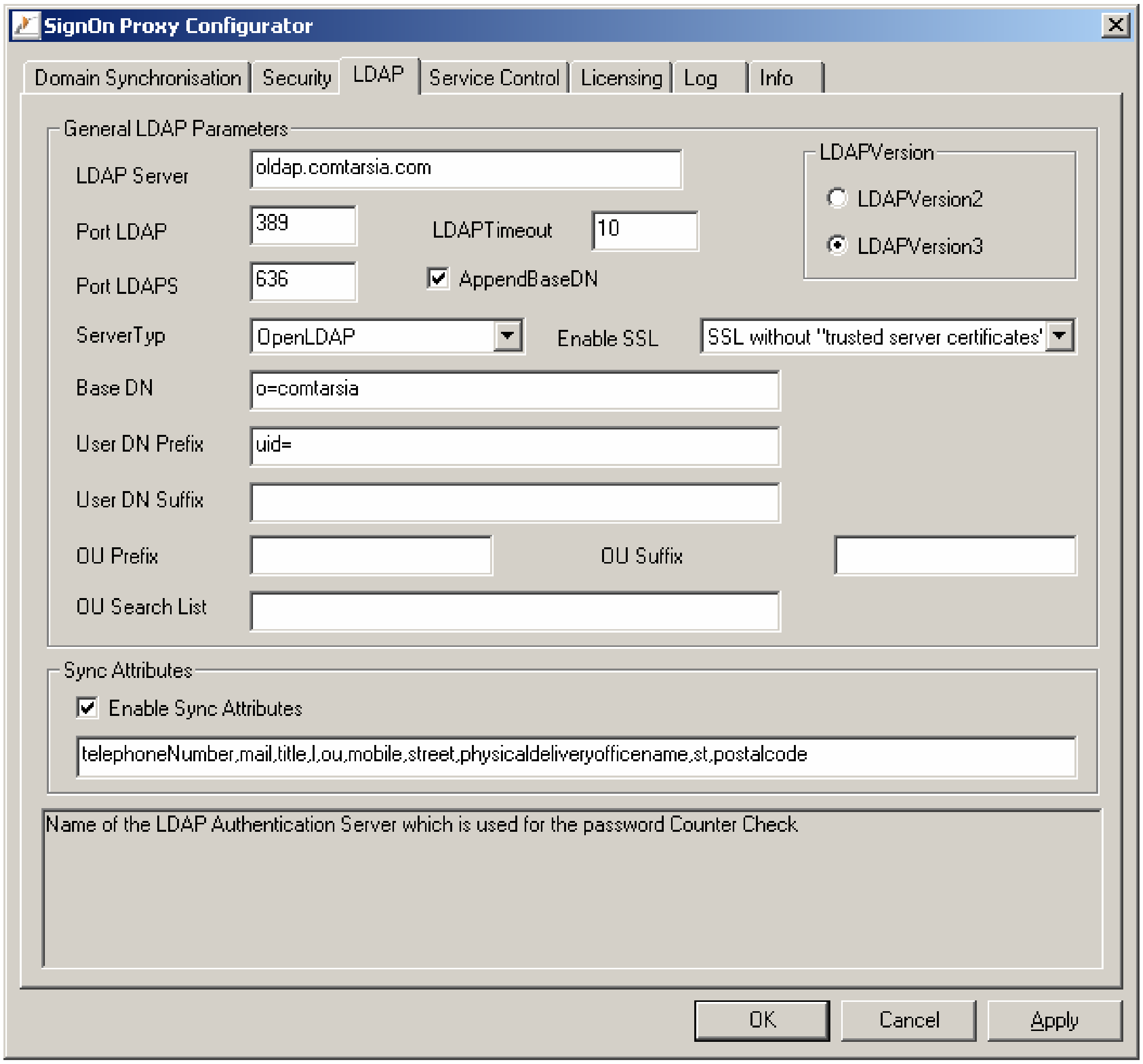
The parameter "**OU Search List**" is only implemented together with the "**Web Sync Client**".
The "OUSearchList" is a list of OU's, which are used for the automatic creation of the UserDN, instead of the OU of the Logon Panel.
The "SignOn Proxy" tries an authentication with all OUs in the defined order until a logon is successful.
The several OU strings are separated with ";", for example:
LDAPOUSearchList="at;de;uk"

Sync Attributes

Via the "Sync Attribute" the attributes of the LDAP user object can be assigned to the attribute of the ADS user object. Under "**Sync Attributes**" a comma or semicolon-separated list of LDAP attributes, which should be forwarded to the SignOn Agent, can be specified.

Example
postalcode,ou,street,title,mail

Attention: "**Sync Attributes**" must be configurated on the SignOn proxy as well as on the SignOn Agent (See also "Sync Attributes" under "Setting up the SignOn Agent")



General LDAP Parameters

LDAP Server: oldap.comtarsia.com

Port LDAP: 389

LDAPTimeout: 10

Port LDAPS: 636

☑ AppendBaseDN

ServerTyp: OpenLDAP

Enable SSL: SSL without "trusted server certificates'

Base DN: o=comtarsia

User DN Prefix: uid=

User DN Suffix:

OU Prefix:

OU Suffix:

OU Search List:

LDAPVersion

○ LDAPVersion2

● LDAPVersion3

Sync Attributes

☑ Enable Sync Attributes

telephoneNumber,mail,title,l,ou,mobile,street,physicaldeliveryofficename,st,postalcode

Name of the LDAP Authentication Server which is used for the password Counter Check

LDAPSearchForUser

Registry Entry:
HKLM\SYSTEM\CurrentControlSet\Services\ComtSOP\LDAP\
Attribute: LDAPSearchForUser
Type:REG_DWORD

If the value of this entry is set to “1”, the SignOn Proxy searches for the user object (LDAPUserDNPrefix + USERNAME) below the “LDAPBaseDN”. The LDAP directory server has to allow “Anonynmous – Search/Read-Access”.

AttributeBasedGroups

Registry Entry:
HKLM\SYSTEM\CurrentControlSet\Services\ComtSOP\LDAP\
Attribute: AttributeBasedGroups
Type:REG_MULTI_SZ

This entry allows adding of groups dynamically to the current user based on LDAP attributes.

Example:
AttributeBasedGroups: physicalDeliveryOfficeName=ATQA%s01_G

At logon of the user, the SignOn Proxy tries to read the LDAP-attribute “physicalDeliveryOfficeName” out of the user object and then adds a dynamic group “ATQA%s01_G” to the user. “%s” is replaced with the contents of the attribute “physicalDeliveryOfficeName”.

Multivalue LDAP attributes with up to 10 entries are being supported. There is also the possibility to cut the first character of the LDAP attribute off, by setting a “>” behind the “=”.

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

AttributeBasedOU

Registry Entry:
HKLM\SYSTEM\CurrentControlSet\Services\ComtSOP\LDAP\
Attribute: AttributeBasedOU
Type:REG_MULTI_SZ

Based on this registry entry an attribute of the LDAP-user object can be specified to use it as OU. This OU is then forwarded to the agent systems and there it is used for further purposes (depending of the configurations).

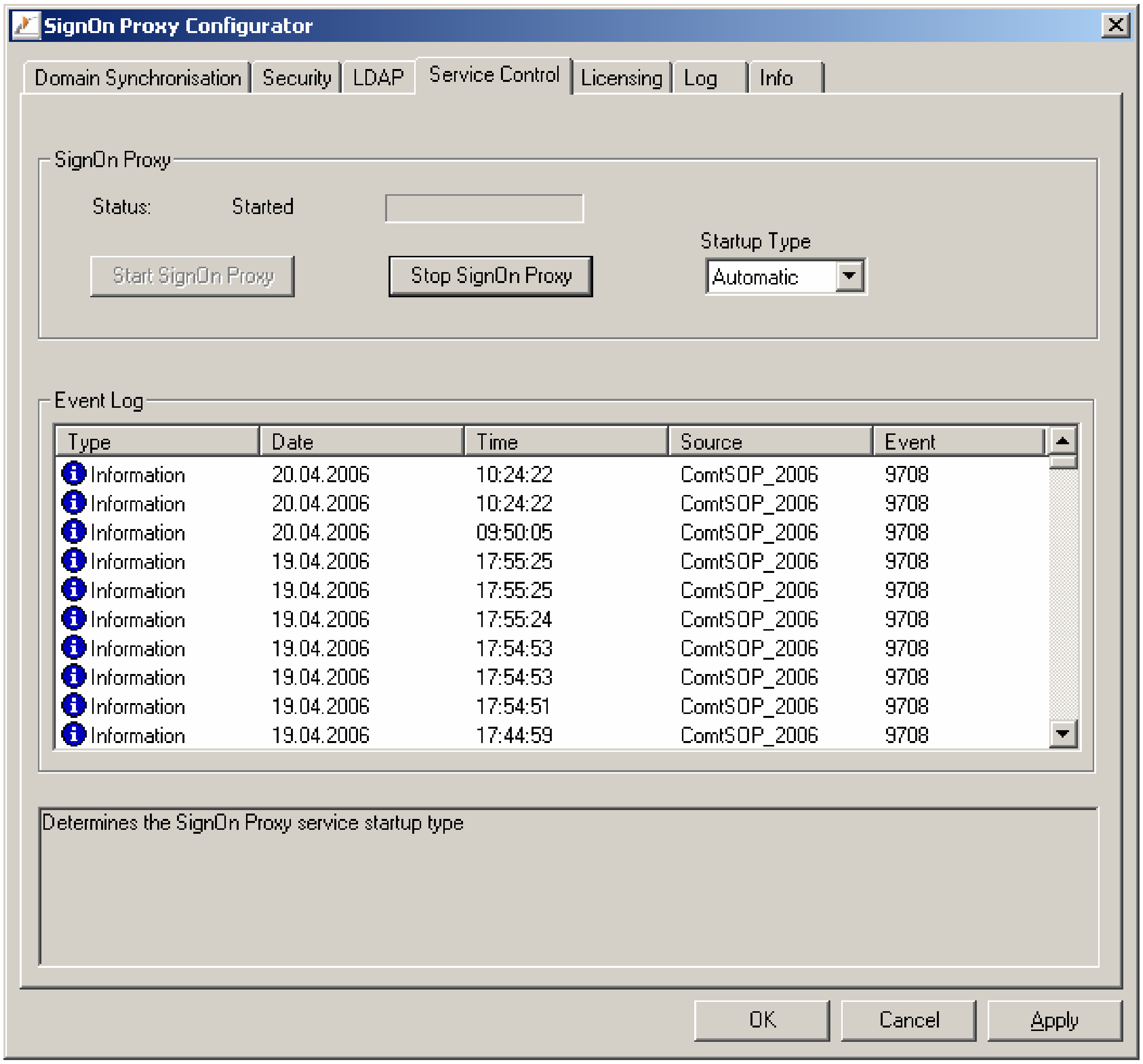
Example:
AttributeBasedOU:departmentNumber=DEP_%s
The left part of this entry defines which LDAP-attribute should be used; the right part defines how this attribute should be completed. “%s” is replaced with the contents of the attribute of the LDAP user object.

There is also the possibility to cut the first character of the LDAP attribute off, by setting a “>” behind the “=”.

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

Service Control

Startup type (Autom./Manual) defines which Comtarsia services are automatically started at system start. Furthermore these services can be stopped and started manually.



Status: Started

Startup Type: Automatic

Type	Date	Time	Source	Event
Information	20.04.2006	10:24:22	ComtSOP_2006	9708
Information	20.04.2006	10:24:22	ComtSOP_2006	9708
Information	20.04.2006	09:50:05	ComtSOP_2006	9708
Information	19.04.2006	17:55:25	ComtSOP_2006	9708
Information	19.04.2006	17:55:25	ComtSOP_2006	9708
Information	19.04.2006	17:55:24	ComtSOP_2006	9708
Information	19.04.2006	17:54:53	ComtSOP_2006	9708
Information	19.04.2006	17:54:53	ComtSOP_2006	9708
Information	19.04.2006	17:54:51	ComtSOP_2006	9708
Information	19.04.2006	17:44:59	ComtSOP_2006	9708

Determines the SignOn Proxy service startup type

Licensing

A license key for testing purposes is provided, validity please see on the key. Press "**Load a new licensekey**" in order to browse for purchased license key according to individual conditions.

Herewith installation of SignOn Proxy and SignOn Agent is successfully finished.