



# Comtarsia SignOn Agent für Linux 2006

## Handbuch

Version: 1.2.10.11, 04-Jul-2006

# Inhaltsverzeichnis

1.	SignOn Agent für Linux .....	3
1.1	Einführung .....	3
1.2	Systemanforderungen.....	4
1.3	Installation des SignOn Agent .....	4
1.4	Starten und Stoppen des SignOn Agent .....	4
1.5	Deinstallation des SignOn Agent .....	5
1.6	Konfiguration – Parameterbeschreibung .....	5



# 1. SignOn Agent für Linux

## 1.1 Einführung

Der SignOn Agent für Linux ist ein Produkt aus der Comtarsia SignOn Gate Familie.

Der SignOn Agent besteht aus zwei Modulen: dem System-Modul und dem Samba-Modul.

- Das System-Modul  
Dieses Modul ist für die Linux System-Benutzerkonten zuständig.  
Die Funktionen im Detail:
  - Erzeugen von neuen Benutzerkonten inklusive Benutzerverzeichnis sowie Vergabe der benötigten Dateisystem-Berechtigungen
  - Steuern der Gruppenzugehörigkeit der einzelnen Benutzer inklusive der Möglichkeit einer GroupMapping-Liste
  - Synchronisation des Benutzer-Paßwortes
  
- Das Samba-Modul  
Dieses Modul ist für die Samba-Benutzerkonten zuständig.  
Die Funktionen im Detail:
  - Erzeugen von neuen Benutzer-Einträgen im Samba
  - Synchronisation des Benutzer-Paßwortes

Der SignOn Agent für Linux bietet umfangreiche Konfigurationsmöglichkeiten, wodurch sich die einzelnen Arbeitsschritte des Agents genau auf die jeweiligen Anforderungen abstimmen lassen.

Die Synchronisation der Linux System-Benutzerkonten kann für Terminal-Benutzer verwendet werden, die direkt auf dem jeweiligem System arbeiten (z.B. über Telnet oder SSH) und auch für Benutzer, die mit speziellen Applikationen auf dem Linux-System arbeiten, welche System-Benutzerkonten verwenden (z.B. POP/IMAP-Server, Webserver).

Der Servolution SignOn Agent ist neben der Linux-Version auch noch für viele weitere Plattformen sowie Applikationen erhältlich. Weitere Informationen hierzu finden Sie auf der Servolution-Webseite unter <http://signon.comtarsia.com/>

## 1.2 Systemanforderungen

Die Systemanforderungen für die Installation des Sync Agent Daemons:

- SUSE Linux Version 8.1 oder 9.0 / SCO Linux Server Release 4.0
- RedHat Linux auf Anfrage

Bitte beachten Sie, daß sich die verschiedenen Linux-Distributionen in den mitgelieferten Programm-Bibliotheken zum Teil stark unterscheiden und es deshalb erforderlich ist, die jeweilige SignOn Agent für Linux Version zu verwenden, die genau für Ihre Distribution zusammengestellt wurde.

Anforderungen für den Betrieb des SignOn Agent für Linux:

- Protokoll TCP/IP mit einer statischen IP-Konfiguration.
- Für die automatische Erzeugung von Samba-Accounts ist Samba 2.2.X erforderlich.

## 1.3 Installation des SignOn Agent

Extrahieren Sie die Datei `soa_linux_1.1.X.tar.gz` in einem eigenen Verzeichnis mit dem Befehl:

`„tar zxvf soa_linux_1.1.X.tar.gz“`. Wechseln Sie daraufhin in das Verzeichnis `soa_linux` und führen Sie das Installationsprogramm mit dem Befehl `„./sainstall“` aus. Zur Installation des SignOn Agent werden `„root“`-Berechtigungen benötigt.

Während des Installationsvorganges wird das Programmverzeichnis des SignOn Agents sowie die IP-Adresse des SignOn Proxy-Servers abgefragt.

Der SignOn Agent wird so installiert, daß er sich bei einem Neustart des Linux-Systems automatisch startet. Dieses Verhalten könne Sie bei Bedarf durch Veränderung der Runlevel-Links an Ihre Erfordernisse anpassen.

## 1.4 Starten und Stoppen des SignOn Agent

Der Starten sowie Stoppen des SignOn Agent erfolgt über das Skript `„/etc/comtsoa_sys/comtsoa_sysctl“`.

Zum Starten führen Sie den folgenden Befehl als `„root“` aus:  
`„/etc/comtsoa_sys/comtsoa_sysctl start“`

Das Stoppen erfolgt analog zum Starten:  
`„/etc/comtsoa_sys/comtsoa_sysctl stop“`

Wenn Sie Konfigurationsänderungen durchführen, während der SignOn Agent aktiv ist, müssen Sie den Agent beenden und neu starten, um die Konfigurationsänderungen zu aktivieren:

`„/etc/comtsoa_sys/comtsoa_sysctl restart“`

## 1.5 Deinstallation des SignOn Agent

Die Deinstallation des SignOn Agent für Linux muß manuell erfolgen.  
Löschen Sie die folgenden Dateien/Verzeichnisse:

/etc/comtsoa\_sys

Das SignOn Agent bin-Verzeichnis z.B.: /usr/local/comtsoa\_sys

Die Symbolischen-Links in den Runlevel-Verzeichnisse (/etc/init.d/,  
/etc/init.d/rc3.d, /etc/init.d/rc5.d)

## 1.6 Konfiguration – Parameterbeschreibung

Die SignOn Agent für Linux Konfigurationsdatei befindet sich unter  
/etc/comtsoa\_sys/comtsoa\_sys.conf.

Nachfolgend findet sich die Standard-Konfigurationsdatei mit deutscher  
Parameterbeschreibung:

```

#####
###
# comtsoa_sys.conf
# /etc/comtsoa_sys.conf is the configuration file for the
# === Comtarsia SignOn Agent 2003 ===
# (comtsoa_sys) daemon
# Copyright (c) 2003 Comtarsia IT Services GmbH
#
#####
##

# Configuration settings for the CORE module
#
[SA_CORE]

# Defines if sync request message is encrypted. Must be ALWAYS 1, if this
# parameter is set to 0 severe problems can occur.
# Default: 1
cryptMessage=1

# Defines the installation directory for the comtsoa_sys daemon
# Default: /usr/local/comtsoa_sys
workingDirectory=/usr/local/comtsoa_sys

# Specifies the listener port for incoming sync requests coming from
# the sync proxy. If changing this parameter be sure that the selected port
# number is not used by other services.
# Default: 2000
listenerPort=2000

# Specifies the maintenance listener port for the maintenance interface. You
# can connect yourself to the maintenance interface with a TELNET client. When
# connected HELP can be invoked by pressing "? ENTER". If changing this
# parameter be sure that the selected port number is not used by other services.
# This is not supported in the current version.
# Default: 3000
maintenancePort=3000

# Defines the standard socket receive timeout for PROXY communication in
seconds.
# On expiration of this value the socket connection will be closed by the
# syncagent. This case is shown in the logfile (if logging is activated) as
# "receive error". If this error accumulates contact your network administrator.
# Default: 4
rcvTimeout=4

# Configuration settings for the LOG module
#
[SA_LOG]

# Defines if logging is activated without a maintenance connection, must be 1 if
# you want to log to file.
# Example cases when file logging is activated:
# 1) logToFile=1 AND a maintenance connection is established AND the
maintenance
# command "log start" is performed.
# 2) logAlways=1 and logToFile=1
# Default: 1

```



logAlways=1

# Specifies the logfile name (path has to be included)

# Default: /var/log/ComtSOA\_Sys.log

logFileName = /var/log/ComtSOA\_Sys.log

# Defines the desired log level. Loglevel should at least be set to 1 to log all

# error messages which will occur. For more exact system analyses set this

# parameter to a higher level (e.g. during system test phase).

# Be aware that higher log levels than 1 especially 3 (if file logging is activated)

# could consume on high syncagent load a not to neglect amount of disk space.

# 0 no log

# 1 only errors

# 2 log messages

# 3 verbose log level

# Default: 1

logLevel=1

# Specifies if the log output should be written to "logFileName".

# For more information see [SA\_LOG] -> logAlways.

# Default: 1

logToFile=1

# Defines the maximum logfile size in bytes. If this size is reached

# a backup copy of the logfile is made (naming convention is

# <logFileName>\_YEAR\_MONTH\_DAY\_HOUR\_MINUTE\_SECOND) and the logfile size is set

# to 0. If free disk space is less than 50 megabytes the oldest logfile backup

# copy will be deleted.

# Default: 1024000

maxLogFileSize=1024000

# Configuration settings for the SYSTEM module

#

[SA\_SYSTEM]

# Specifies if the SYSTEM sync module is enabled. The SYSTEM sync module is

# responsible for UNIX user AUTHENTICATION, UNIX user CREATION, UNIX

PASSWORD

# synchronization and UNIX GROUP synchronization.

# All further modules will be not processed if the SYSTEM

# module fails. Thus "syncEnabled" must be ALWAYS 1

# Default: 1

syncEnabled=1

# Specifies the policy bit field flags for syncing.

# If a previous level fails further operation is canceled.

# (e.g.)

#0x1 check password (must be ALWAYS set)

#0x2 create user (must be ALWAYS set)

#0x4 update user (update the user's supplementary groups)

# default = 7 (all bits set)

syncPolicy=7

# Specifies if the user's home directory should be created

# Default: 1

createHomeDir=1



```

# Specifies if on directory creation the users' home directory
# mask should be changed.
# Default: 1
changeHomeDirPermission=1

# Specifies the home directory mask to use (octal)
# Default: 0700
homeDirPermissionMask=0700

# Specifies if groupmapping is enabled (1 = group mapping is enabled).
# When groupmapping is disabled the supplementary group list send by the client
# is used to update the UNIX group membership.
# When group mapping is enabled (see [SA_GROUPMAPPING]) group mapping
translation
# is used.
# Default: 0 (group mapping is disabled)
disableEqualGroupMapping=0

# Specifies the except groups. These are groups which will be deleted
# from the users's supplementary group list (groups are separated by ", ").
# Example: root, audio
exceptGroups=root

# Specifies the minimum GID. All groups in the supplementary group list which
# group ID is < than minGid are deleted from the user's supplementary group
list.
# Default: 30
minGid=30

# Specifies if new groups should be created on the system
createGroups=0

# Configuration settings for the SAMBA module
#
[SA_SAMBA]

# Specifies if the SAMBA sync module is enabled (1 = enabled). The SAMBA sync
# module is responsible for SAMBA user AUTHENTICATION, SAMBA user
CREATION and
# SAMBA PASSWORD synchronization. If the SYSTEM module fails, the SAMBA
module
# will be NOT processed.
# Default: 1
syncEnabled=1

# Proxy accept list
# List of SYNC PROXY IP's form which requests will be accepted. Sync requests
# whose sender is not in this list will be REJECTED and an entry (if logging
# is activated) in the log file is made.
# Maximum list size is 10.
# PROXY1 = ...
# PROXY2 = ...
# ...
[SA_ACCEPTLIST]

PROXY1=192.168.2.209

#PROXY2=192.168.2.206

```



```
# Groupmapping list.
# The group mapping list describes group mapping translation. The left situated
# group (SOURCE group) in a group mapping entry is checked against the group
# list send by the client. If the SOURCE group is found in the client list the
# TARGET (right situated group of a group mapping entry) group(s) will be
# added to the user's supplementary group list. Groups in the client list which
# do not match to any SOURCE group will be discarded.
# Syntax: "USERLIST GROUP" = "SUPPLEMENTARY GROUP1" [ ,
"SUPPLEMENTARY GROUP2"...]
# Maximum list size is 32.
# Example: OS2GRP1=linuxgrp1, linuxgrp2
[SA_GROUPMAPPING]
```

