



Comtarsia SignOn Agent for Linux 2006

User Guide

Version: 1.2.10.11, 04-Jul-2006

Contents

1.	SignOn Agent for Linux.....	3
1.1	Introduction	3
1.2	System Requirements	4
1.3	SignOn Agent Installation.....	4
1.4	Starting and Stopping of SignOn Agent	4
1.5	Deinstalling SignOn Agent.....	5
1.6	Configuration Parameter Description	5



1. SignOn Agent for Linux

1.1 Introduction

SignOn Agent for Linux is a member of the Comtarsia SignOn Gate product family. SignOn Agent consists of two modules: system module and Samba module.

- System Module
This module is responsible for maintaining Linux user accounts.
It has following functions:
 - Creation of new user accounts including user directories and assigning of necessary file system permissions
 - Directing of group memberships of individual users including the possibility of a GroupMapping list; new groups can be added automatically
 - Synchronization of user passwords

- Samba Module
This module is responsible for maintaining Samba user accounts.
It has following functions:
 - Creation of new Samba user accounts
 - Synchronization of user passwords

SignOn Agent for Linux features a variety of configuration options by means of which you can individually customize individual agent functions.

Synchronization of Linux system accounts can be used for terminal users who are directly working on the system (e.g. via Telnet or SSH) as well as for users who are using Linux system applications which make use of system accounts (e.g. POP/IMAP server, web server).

Comtarsia SignOn Agent is available for a multitude of platforms and applications besides of Linux. For more information please refer to the Comtarsia SignOn homepage at <http://signon.comtarsia.com/>



1.2 System Requirements

System Requirements for installation of SignOn Agent Daemon:

- SUSE Linux Version 8.1 / SCO Linux Server Release 4.0
- RedHat Linux 8.0 (soon available)

Please note that supplied program libraries can vary widely with Linux distributions. Therefore you have to make sure you are using the SignOn Agent version that is compiled for your specific distribution.

Requirements for using Sync Agent for Linux:

- TCP/IP protocol with static IP configuration
- Samba 2.2 or 3.0 is required for automatic creation of Samba accounts.

1.3 SignOn Agent Installation

Extract the file `soa_linux_1.1.X.tar.gz` into a new directory with this command:
`„tar zxvf soa_linux_1.1.X.tar.gz“`. Now change into directory `soa_linux` and execute the installation program with command `„./sainstall“`. Permissions as root are required for installing SignOn Agent.

During installation you will be asked for the SignOn Agent program directory as well as the IP address of the SignOn Proxy server.

SignOn Agent will be installed so that it automatically starts upon rebooting of the Linux system. You can customize this behavior to your requirements by changing the Runlevel links.

1.4 Starting and Stopping of SignOn Agent

Use this script to start and stop SignOn Agent: `„/etc/comtsoa_sys/comtsoa_sysctl“`.

To start it execute the following command as root:

```
„/etc/comtsoa_sys/comtsoa_sysctl start“
```

Stopping works similar to starting:

```
„/etc/comtsoa_sys/comtsoa_sysctl stop“
```

If you change configuration parameters while SignOn Agent is active you have to restart the agent for changes to become effective.:

```
„/etc/comtsoa_sys/comtsoa_sysctl restart“
```



1.5 Deinstalling SignOn Agent

You have to deinstall SignOn Agent for Linux manually.

Delete the following files/directories:

- /etc/comtsoa_sys
- SignOn Agent bin directory e.g.: /usr/local/comtsoa_sys
- Symbolic links in the run level directories (/etc/init.d/, /etc/init.d/rc3.d, /etc/init.d/rc5.d)

1.6 Configuration Parameter Description

The configuration file for SignOn Agent for Linux can be found at /etc/comtsoa_sys/comtsoa_sys.conf.



```
#####
#
# comtsoa_sys.conf
# /etc/ comtsoa_sys/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]
```

