

Comtarsia SignOn Agent for Active Directory 2008

Technische Funktionsbeschreibung



Build 5.1.5.51
21.02.2011

Inhaltsverzeichnis

1. Einleitung	3
2. Grundlegende Konfiguration	3
3. Active Directory	5
3.1. Benutzer	5
3.1.1. Benutzer-Aktionen.....	6
3.2. Benutzer-OU	7
3.3. System	8
3.4. Security Agent.....	10
4. Variablen.....	10
4.1. Variablen Regular Expressions Beispiele	14
4.2. Interne Variablen.....	14
5. Profile Forwarding	14
6. Logging.....	15
6.1. Logging in eine Datei	15
6.2. Logging in Syslog.....	17
6.3. Logfile-Format	18
7. Installation / Komponenten	19
A. Referenzen.....	19

1. Einleitung

2. Grundlegende Konfiguration

[HKLM\SOFTWARE\Comtarsia\ SignOn Solutions 2008]

REG_SZ:"path"="%ProgramFiles%\Comtarsia\SignOn Solutions 2008"

Der Installationspfad.

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\ SignOnAgent]

REG_DWORD:"listenerPort"=0x000007d3

Definiert den TCP-ListenerPort des SignOn Agent. Default ist 2002.

REG_SZ:"listenerInterface"="*"

Definiert das Listener Interface. Bei „*“ oder „“ bindet sich der SignOn Agent auf alle verfügbaren Interfaces. Wird eine IP-Adresse angegeben, lauscht der Agent ausschliesslich an dieser.

Beispiel: "listenerInterface"="192.168.1.1"

REG_DWORD:"rcvTimeout"=0x00000004

Das Socket Receive Timeout in Sekunden. Diese Zeit gilt für das Empfangen des Client-Pakets. Anschliessend wird die TTL des Clients verwendet.

REG_DWORD:"connectTimeout"=0x00000005

Definiert das maximale Socket Connect Timeout in Sekunden. Ist die TTL des Client-Pakets kleiner als das connectTimeout so wird die TTL verwendet.

REG_SZ:"tlsCAdir"=""

Definiert den Pfad zu einem absoluten Verzeichnis, in welchem sich ein oder mehrere vertrauenswürdige CA-Zertifikate befinden. Nach jeder Änderung in diesem Verzeichnis muss OpenSSL-„c_rehash“ aufgerufen werden. Diese Zertifikate dienen zur Verifizierung des Proxy Zertifikates.

Es darf nur entweder CAdir oder CAFile gesetzt werden.

REG_SZ:"tlsCAFile"="%ProgramFiles%\Comtarsia\SignOn Solutions 2008\cert\ca.pem"

Definiert einen absoluten Pfad zu einer Datei, welche ein oder mehrere vertrauenswürdige CA- Zertifikate enthält. Sollen mehrere Zertifikate in dieser Datei gespeichert werden, so werden diese einfach hintereinander kopiert. Diese Zertifikate dienen zur Verifizierung des Proxy Zertifikates.

Es darf nur entweder CAdir oder CAFile gesetzt werden.

REG_SZ:"tlsKeyFile"="%ProgramFiles%\Comtarsia\SignOn Solutions 2008\cert\proxy.pem"

Ein absoluter Pfad zu einer Private Key-Datei, welche für die Kommunikation mit den anderen SignOn Gate-Komponenten verwendet wird.

REG_SZ:"tlsCertFile"="%ProgramFiles%\\Comtarsia\\SignOn Solutions 2008\\cert\\agent.pem"

Ein absoluter Pfad zu einem Zertifikat, welches für die Kommunikation mit den anderen SignOn Gate-Komponenten verwendet wird.

REG_DWORD:"tlsOptions"=0x00000000

Wird derzeit nicht verwendet.

REG_DWORD:"trustOptionsServer"=0x00000000

Definiert die SSL Verifizierungsoptionen für die Kommunikation zwischen dem SignOn Proxy und den SignOn Agents.

Flag	Bezeichnung	Beschreibung
0	No Check	Keine Überprüfung
1	Accept List	Überprüfung mittels Accept List (Liste von IP-Adressen)
2	Certificate OIDs	Es wird auf das Vorhandensein der Comtarsia OIDs geprüft. Für Details hierzu siehe das Dokument „SignOnGate Certificates“.
0x100	Certificate FQDN	Es wird der FQDN des Zertifikates überprüft. Dieser FQDN muss mit dem vom DNS gelieferten Reverse Lookup-Ergebnis übereinstimmen.

REG_MULTI_SZ:acceptList=[]

Dieser Wert definiert eine Liste von IP-Adressen möglicher Proxy-Server. Ist bei den „trustOptionsServer“ das Flag „Accept List“ gesetzt, so wird ein TCP-Connect nur von in der Accept-List definierten IPs zugelassen.

REG_DWORD:"nrOfWorkersThreads"=0x4

Definiert die Anzahl der Client-Bearbeitungs-Threads

REG_SZ:"profileName"=""

Der Name des Profils.

REG_SZ:"profileComment"=""

Ein Kommentar für das Profil.

3. Active Directory

3.1. Benutzer

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\Modules\System\User]

REG_DWORD:"createUser"=00000001

Definiert, ob der Agent nicht existierende Benutzer anlegen soll.

REG_DWORD:"recreateUserOnError"=00000000

Definiert, ob der Agent im Falle einer nicht erfolgreichen Benutzersynchronisation (d.h. eines Fehlers, welchen der Agent nicht autonom beheben konnte), den Benutzer löschen und neu anlegen soll.

REG_DWORD:"enableAllUsers"=00000000

Hiermit kann definiert werden, ob der Agent auch Benutzer, welche nicht durch den Agent verwaltet werden (description=SRV_TEMP_USER), aktivieren soll, wenn der Account deaktiviert ist.

REG_DWORD:"alwaysCheckACL"=00000000

Hiermit kann festgelegt werden, ob der Agent die ACL des Benutzerverzeichnisses bei jeder Synchronisation überprüfen soll, oder ob er dies nur im Zuge des Anlegen des Verzeichnisses durchführt.

REG_DWORD:"forceSetPassword"=00000000

Mit dieser Option kann konfiguriert werden, dass der Agent das Benutzerpasswort immer setzt. Ist diese Option deaktiviert, so wird das Passwort nur dann gesetzt, wenn zuvor ein LogonUser Aufruf mit falschem Benutzer/Passwort fehlschlägt.

REG_SZ:"createHomeDirPath"="%homeDirectory%"

Definiert den Pfad des Benutzerverzeichnisses. Per Default wird hierfür die Variable „%homeDirectory%“ verwendet, z.B.: %homeDirectory%="c:\homes\%USERNAME%".

REG_SZ:"createProfilePath"="%profilePath%"

Definiert den Pfad des Benutzerprofiles. Per Default wird hierfür die Variable „%profilePath%“ verwendet, z.B.: %homeDirectory%="c:\profiles\%USERNAME%".

REG_DWORD:"disableUserOnSyncError"=00000001

Ist diese Option aktiviert, so wird der Benutzer im Fall eines Fehlers während der Synchronisation deaktiviert. Dies dient um sicherzustellen, dass keine nur teilweise synchronisierten Benutzer sich anmelden können.

REG_DWORD:"syncErrorPolicy"=00000001

Diese Option definiert, in welchem Fall der Agent eine Benutzersynchronisation als fehlerhaft ansehen soll.

Per default wird jeder einzelne Fehler als kompletter Synchronisationsfehler gewertet (d.h. wenn z.B. die Anmeldung des Benutzers funktioniert hat und das Entfernen des Benutzers aus einer Gruppe aber nicht), wird dieser Wert auf „0“ gesetzt, so ist die Synchronisation nur dann fehlerhaft, wenn die Anmeldung des Benutzers nicht funktioniert hat.

REG_DWORD:"daysUserAccountExpires"=00000007

Definiert die Anzzahl an Tagen, nach welchen ein inaktiver Benutzeraccount deaktiviert wird. Dieser Wert wird direkt als AD Account Expire gesetzt.

REG_DWORD:"acctExpPercent"=0x00000064

Definiert einen Prozentsatz, nach welchem das Account Expire weiter gesetzt werden soll.

Diese Option dient hauptsaechlich zum Verringern von Active Direcotory Replicationen.

Beispiel: "daysUserAccountExpires"=10, „acctExpPercent“=90: Dies bedeutet, dass das Accoutn Expire erst dann vom Agent weitergesetzt wird, wenn weniger als 90% Restzeit (10 Tage = 100%, 1 Tag = 10%) vorhanden sind, d.h. das Account Expire wird taeglich maximal einmal gesetzt.

3.1.1. Benutzer-Aktionen

Die folgenden Konfigurationswerte beschreiben eine Bitmaske, mit welcher fuer die jeweilige grundlegende Benutzer-Aktion festgelegt wird, ob diese beim Anlegen des Benutzer (Bit 0) und/oder beim Update des Benutzers (Bit 1) durchgeführt werden soll.

Wert	Aktion
0	Aktion wird nicht ausgeführt
1	Aktion wird nur bei „Create User“ ausgeführt
2	Aktion wird nur bei „Update User“ ausgeführt
3	Aktion wird bei „Create User“ und bei „Update User“ ausgeführt

D.h. soll eine Aktion nur beim Anlegen des Benutzers ausgeführt werden, so wird der Wert auf „1“ gesetzt, soll die Aktion nur beim Update des Benutzers ausgeführt werden, so wird der Wert auf „2“ gesetzt. Soll die Aktion in beiden Fällen durchgeführt werden, wird der Wert auf „3“ gesetzt.

REG_DWORD:"setPassword"=00000003

Definiert, ob der Agent das Benutzerpasswort setzen soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"addUserToGroup"=00000003

Definiert, ob der Agent einen Benutzer zu Gruppen hinzufügen soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"removeUserFromGroup"=00000003

Definiert, ob der Agent einen Benutzer aus einer Gruppe entfernen soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"createHomeDir"=00000000

Definiert, ob das Homedirectory des Benutzer angelegt werden soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"createProfile"=00000000

Definiert, ob das Profilverzeichnis des Benutzer angelegt werden soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"setExpireTime"=00000000

Definiert, ob das Account Expire des Benutzerobjektes gesetzt werden soll.

Bit0=on create user, Bit1=on update user

REG_DWORD:"setLastLogonTime"=00000003

Definiert, ob der SignOn Agent die Last Logon Time des Benutzers setzen soll.

Dies erfolgt als Teil der Description in der Form: SERV_TMP_USER_<date-time>

REG_DWORD:"enableUserOU"=00000000

Definiert, ob die OU des Benutzers durch den Agent verwaltet werden soll.

3.2. Benutzer-OU

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\Modules\System\ADS\UserOU]

Die resultierende Benutzer-OU setzt sich folgendermassen zusammen:

Ist die %OU%-Variable nicht gesetzt, wird der Benutzer mit folgender DN angelegt:

CN=<UserName>,<defaultUserContainer>,<directoryRoot>

Ist die %OU%-Variable gesetzt, wird %OU%, wenn "equalOUMapping=0" mittels der OUMAPPING-Einträge ersetzt, andernfalls direkt für folgende resultierende User-DN verwendet:

CN=<UserName>,<OUPrefix>%OU%<OUSuffix>,<directoryRoot>

REG_DWORD:"equalOUMapping"=dword:00000001

Ist diese Funktion aktiv, so werden OU-Werte, welche vom SignOn Proxy kommen, 1:1 übernommen, d.h. die OUMapping-Liste wird nicht verwendet.

REG_SZ:"OUPrefix"="ou="

Das OUPrefix wird vom Agent vor die eigentlichen OU-Wert gestellt.

REG_SZ:"OUSuffix"=""

Das OUPrefix wird vom Agent nach den eigentlichen OU-Wert gestellt.

[.\SOSProfile *\SignOnAgent\Modules\System\ADS\UserOU\OUMAPPING]

Hier befinden sich die Mapping-Einträge als REG_SZ, wobei der Name fuer die OU steht, welche vom SignOnProxy kommt und der Wert für die ActiveDirectory Ziel-OU.

3.3. System

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\Modules\System\ADS]

REG_DWORD:"adsDiscoverServerRefreshTime"=0x000012c

Definiert das Intervall in Sekunden, in welchem der Agent im Active Directory nach Änderungen der Domain-Infrastruktur nachschau hält.

REG_DWORD:"enableWkstOUMove"=00000000

Mit diesem Parameter kann die „Workstation OU Move“-Funktion aktiviert oder deaktiviert werden.

Details hierzu siehe im Logon Client 2006 bzw. Logon Client 2008 Handbuch.

REG_SZ:"defaultUserContainer"="CN=Users"

Definiert den LDAP Container, in welchem per Default alle neuen Benutzer angelegt werden.

REG_SZ:"defaultGroupContainer"="CN=Users"

Definiert den LDAP Container, in welchem per Default alle neuen Gruppen angelegt werden.

REG_MULTI_SZ:"dcHostnames"=[]

Mit diesem Parameter können ein oder mehrere Domain Controller angegeben werden, auf welchen der Agent dann Remote die Benutzersynchronisation durchführt. Dieser Modus ist dann sinnvoll, wenn der Agent nicht selbst auf einem Domain Controller installiert werden kann. Es wird nur der hostname, nicht der FQDN eingegeben.

REG_SZ:"signOnGateUserPasswordTemplate"="URRRRRLR9RSRRRRR"

Folgende Zeichen sind moeglich:

Wert	Bedeutung
L	Ein Kleinbuchstabe (a-z)
U	Ein Großbuchstabe (A-Z)
9	Eine Zahl zwischen 0-9
S	Ein Symbolzeichen (ASCII: 33-47, 58-64, 91-96, 123-126)

R	Ein zufälliges Zeichen (L, U, 9 oder S)
---	---

Beispiel: Das Passwort-Template "RLU9R9LRR" kann dieses Passwort ergeben: „qaY6_9b*Q“.

REG_DWORD:"signOnGateUserTokenTTL"=86400 (60 * 60 * 24 = 86400)

Definiert ein Zeitintervall in Sekunden, in welchem der Token des Agent-Benutzers refreshed wird.

REG_DWORD:"signOnGateUserPasswordTTL"=86400 (60 * 60 * 24 = 86400)

Definiert ein Zeitintervall in Sekunden, in welchem das Passwort des Agent-Benutzers geändert wird. Ob dieses Intervall bereits abgelaufen ist wird nur überprüft, wenn das „signOnGateUserTokenTTL“ abgelaufen ist, somit sollte der Wert PasswortTTL immer grösser als die TokenTTL gesetzt werden.

REG_DWORD:"enableDomainServers"=00000000

Hiermit kann eine spezielle Funktion aktiviert werden, wodurch der Agent auch Remote Home Directories oder Profile Paths setzen kann, z.B. auf NAS-Dateien.

REG_DWORD:"domainServersListType"=00000000

Definiert den Listen-Typ

Wert	Bedeutung
0	„DomainServers“ spezifiziert eine Deny-List, d.h. all Server, welche nicht in der Liste sind, sind erlaubt.
1	„DomainServers“ spezifiziert eine Allow-List, d.h. es sind nur Server erlaubt, welche in der Liste eingetragen sind

REG_DWORD:"domainServersAutoDiscover"=00000000

Hiermit wird definiert, ob alle Domain Member automatisch in die DomainServer Liste aufgenommen werden sollen.

REG_MULTI_SZ:"domainServers"=[]

Definiert eine Liste von Domain Controllern.

REG_DWORD:"syncAllDomainControllerOnDiscover"=00000000

Ist diese Funktion aktiv, so wird fuer jeden vom Agent gefundene Active Directory Domain Controller in der selben Site wie der Agent (bzw. Remote-Server, siehe dcHostnames) einmalig am Anfang eine volle Replizierung angestoßen.

REG_DWORD:"disableADSReplicate"=00000000

Ist dieser Wert auf „1“, so wird keine AD-Replizierung durch den Agent angestoßen als auch kein AD-Discover durchgeführt.

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\Modules\System]

REG_DWORD:"LDRFilter"=00000001

Über diesen Parameter kann das Verhalten des SignOn Agent bei einem LDR-SyncRequest gesteuert. Der Wert „LDRFilter“ ist ein Bitfeld.

Wert	Bedeutung
0x1	Deny ADS Replication
0x2	Deny Set Expire Time
0x4	Deny Set Last Logon Time on create
0x8	Deny Set Last Logon Time on update

3.4. Security Agent

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\Modules\Security]

REG_DWORD:"enableSecurityAgent"=00000000

Mit diesem Parameter kann der „Security Agent“-Modues aktiviert (=1) bzw. deaktiviert (=0) werden.

REG_SZ:"startTime"="01:00"

Definiert den Startzeitpunkt des Security Agent. Der Durchlauf des Security Agents erfolgt einmal täglich und sollte nach Möglichkeit zu einem Zeitpunkt stattfinden, an welchem das Synchronisationsaufkommen nicht so hoch ist, da der Security Agent Durchlauf selbst kurzfristig für eine gewisse Systembeanspruchung sorgen kann.

REG_DWORD:"disableUserPeriod"=00000007

Definiert eine Anzahl an Tagen, nach welcher Benutzer, welche sich in dieser Zeitspanne nicht angemeldet haben, deaktiviert werden.

REG_DWORD:"deleteDisabledUsers"=00000000

Ist diese Funktion aktiviert, so werden inaktive Benutzer nach „deleteUsrPeriod“ Tagen vom System gelöscht.

REG_DWORD:"deleteUserPeriod"=00000007

Definiert eine Zeitspanne, nach welcher inaktive Benutzer aus dem System gelöscht werden.

4. Variablen

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\Variables\<VariableEffectivePoint>\<VariableName>]

<VariableEffectivePoint> = "BeforeSync" oder "AfterSync"

Der „VariableEffectivePoint“ bestimmt den Zeitpunkt, an welchem das jeweilige Variablen-Mapping durchgeführt werden soll.

Der Comtarsia SignOn Agent bearbeitet jeden empfangenen Synchronisationsrequest in der folgenden Reihenfolge:

- 1) Empfang eines Datenpaketes vom SignOn Proxy

VariableEffectivePoint: BeforeSync

- 2) Synchronisation des Benutzers

- 3) Rücksenden eines Datenpaketes an den SignOn Proxy

<VariableName> muss in der Form „NNN_VARIABLENAME“ sein, wobei „NNN“ für eine dreistellige Zahl steht, die die Reihenfolge des Mappings angibt, d.h. die Variable „001_Var1“ wird vor der Variable „002_Var2“ gemappt. „VARIABLENAME“ ist der Name der Variable.

REG_SZ:"displayName"=""

Definiert einen Anzeigenamen für die Variable, hat keine technische Funktion und kann als Art Kommentarfeld verwendet werden.

REG_SZ:"source"=""

Definiert die Quelle des Variablenmappings. Dies ist ein String, der ein oder mehrere Variablen (vordefinierte oder benutzerdefinierte) enthalten kann.

REG_DWORD:"mappingType"=0

Wert	Mapping Type
0	1:1 Mapping
1	Regular Expression Mapping

REG_SZ:"expression"=""

Eine Regular expression

REG_SZ:"formatter"=""

Der Formatter für das Ergebniss, z.B. „\$1“

REG_DWORD:"index"=0

Wenn die Regular expression mehrfach matched, so kann hier angegeben werden, das wievielte Ergebniss genommen werden soll. Ist der Wert „0xffffffff“ gesetzt, so werden alle Ergebnisse als Array uebernommen.

REG_DWORD:"flags"=0x2000000

Match Flags:

Flag	Name	Beschreibung
0x00000000	match_default	
0x00000001	match_not_bol	first is not start of line
0x00000002	match_not_eol	last is not end of line
0x00000004	match_not_bob	first is not start of buffer
0x00000008	match_not_eob	last is not end of buffer
0x00000010	match_not_bow	first is not start of word
0x00000020	match_not_eow	last is not end of word
0x00000040	match_not_dot_newline	\n is not matched by '.'
0x00000080	match_not_dot_null	'\0' is not matched by '.'
0x00000100	match_prev_avail	*--first is a valid expression
0x00000200	match_init	internal use
0x00000400	match_any	don't care what we match
0x00000800	match_not_null	string can't be null
0x00001000	match_continuous	each grep match must continue uninterrupted from the previous one
0x00002000	match_partial	find partial matches
0x00004000	match_not_initial_null	don't match initial null
0x00008000	match_all	must find the whole of input even if match_any is set
0x00010000	match_perl	Use perl matching rules
0x00020000	match_posix	Use POSIX matching rules
0x00040000	match_nosubs	don't trap marked subs
0x00080000	match_extra	include full capture information for repeated captures
0x00100000	match_single_line	treat text as single line and ignor any \n's when matching ^ and \$.
0x00200000	match_unused1	Unused

0x00400000	match_unused2	Unused
0x00800000	match_unused3	Unused
0x00800000	match_max	

Format Flags:

Flag	Name	Beschreibung
0x00000000	format_perl	perl style replacement
0x01000000	format_sed	sed style replacement.
0x02000000	format_all	enable all extentions to syntax.
0x04000000	format_no_copy	don't copy non-matching segments.
0x08000000	format_first_only	Only replace first occurrence.
0x10000000	format_is_if	internal use only.
0x20000000	format_literal	treat string as a literal

REG_DWORD:"multivalueAction"=0

Wert	Action
0	Override
1	Delete
2	DeleteValue
3	AddValue

REG_DWORD:"hold"=0

Ist dieser Wert aktiv, so wird das Variablenmapping nicht ausgefuehrt, und ist fuer den Agent praktisch nicht existent. Diese Option dient hauptsaechlich zum Testen von Mappings, um einzelne Mappings schnell aktivieren oder deaktivieren zu koennen.

4.1. Variablen Regular Expressions Beispiele

Expression	Formatter	Beschreibung	Beispiel Werte	Beispiel Resultate
..(*)	\$1	Schneidet 2 Zeichen vom Anfang des Wertes ab	\\servername	servername
...(*)	\$1	Schneidet 3 Zeichen vom Anfang des Wertes ab	ADS001	001
ab(*)	\$1	Alle entfernen die nicht mit "ab" anfangen, von jenen die mit "ab" anfangen wird dieses weggeschnitten	ab001 cd002	001 // gelöscht
(ab)*(*)	\$2	Alle "ab"-Folgen von vorne abschneiden	ababab123 ab123 123	123 123 123
(ab)?(*)	\$2	Nur die Erste „ab“-Folge von vorne abschneiden	ababab123 ab123 123	abab123 123 123

4.2. Interne Variablen

%USERNAME%

Enthält den Benutzernamen.

%__GROUP__%

Diese interne Variable enthält alle Gruppen des Benutzers. Diese Gruppenvariable kann über die Variablenfunktionen bearbeitet werden.

5. Profile Forwarding

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\SignOnAgent\ProfileForwarding\<ProfileForwardingName>]

REG_SZ:"profile"=""

REG_SZ:"source"=""

REG_SZ:"expression"=""

6. Logging

Die SignOn Produkte unterstützt derzeit zwei verschiedene Log-Ziele, welche unabhängig voneinander konfiguriert und aktiviert werden können. Grundsätzlich ist zu beachten, dass speziell beim Loglevel „Detail MSG“ eventuell noch in Kombination mit ein oder mehreren „Detail Log Flags“ zum Teil pro Logon Reuquest bis zu hundert Zeilen in das Log geschrieben werden.

6.1. Logging in eine Datei

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\Log]

REG_DWORD:"enable"=00000001

Mit diesem Parameter kann diese Loggingmethode aktiviert/deaktiviert werden.

REG_SZ:"logFileName"="%ProgramFiles%\Comtarsia\SignOn Solutions 2008\log\Comt%COMT_MODULE%.log"

Definiert den vollen Pfad der Log-Datei. Es können Environment-Variablen verwendet werden, wenn Sie im Kontext des jeweiligen Service-Benutzer zur Verfügung stehen, sowie die folgenden SignOn Proxy internen Variablen:

- %COMT_MODULE%

Ist im Fall des SignOn Proxy immer „SOP“.

- %COMT_PROFILE_ID%

Ist die Profile-ID des aktuellen in Verwendung befindlichen Profiles als dreistellige Zahl, z.B. „501“.

REG_DWORD:"logLevel"=00000004

Definiert das Log-Level. Als Default fuer den Produktiv-Betrieb wird „4“ empfohlen, bei Bedarf in Kombination mit Log Transactions. Alle niedrigeren Log-Level als das Konfigurierte sind immer automatisch enthalten, d.h. wird der Log-Level auf „2“ gesetzt, so werden alle „Error“ und alle „Exception“-Meldungen ausgegeben.

Wert	Log-Level
1	Error
2	Exception
3	Warning
4	Information
5	Detail Messages

REG_DWORD:"logMask"=00000000

Definiert eine Bitmaske, mit welcher sehr detaillierte Logausgaben für bestimmte Bereiche aktiviert werden können.

Wert	Log-Bereich
0x00000080	LDAP
0x00000100	LDAP SSL
0x00004000	Dump Config
0x00010000	Certificate Information
0x00020000	Dump Profile
0x00080000	Dump Variables
0x00200000	Variable Mapping

REG_DWORD:"logDetails"=0xFFFFFFFF

Definiert die Log-Details:

Wert	Log-Details
0x0	Keine Log Details
0x1	Date
0x2	Time
0x4	Prozess und Thread Ids
0x8	Source Postion
0xFFFFFFFF	Alle Details

REG_DWORD:"enableLogTransactions"=00000000

Aktiviert(=1) oder Deaktiviert(=0) Log-Transaktionen.

Sind die Log-Transaktionen aktiviert, so werden alle Log-Nachrichten, welche ein Log-Level haben, das hoeher als das konfigurierte ist, in einen internen Buffer geschrieben. Tritt dann spaeter bei der Bearbeitung noch ein „Error“ oder eine „Exception“ auf, so werden alle im Buffer befindlichen Nachrichten in die Datei geschrieben. Im Falle des SignOn Proxy umfasst eine Log-Transaktion genau eine Benutzer-Synchronisationsrequest.

REG_DWORD:"maxLogFileSize"=0x00a00000

Definiert die maximale Grösse der Log-Datei in Bytes. Überschreitet die Datei die definierte Grösse, so wird eine Log-Rotation durchgeführt.

REG_DWORD:"maxLogFileHistory"=00000001

Definiert wieviele Log-Histories von Log-Rotationen aufgehoben werden sollen.

6.2. Logging in Syslog

[HKLM\SOFTWARE\Comtarsia\SOSProfile *\Log\SysLog]

Ist diese Logging-Methode aktiv, so werden alle Log-Nachrichten an einen Syslog-Server geschickt. (siehe RFC3164)

REG_DWORD:"enable"=00000000

Mit diesem Parameter kann diese Loggingmethode aktiviert/deaktiviert werden.

REG_SZ:"host"=""

Definiert den SysLog Server. Hier kann ein Hostname oder eine IP-Adresse eingetragen werden.

REG_DWORD:"facility"=00000010

Definiert die SysLog facility.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit

14	log alert
15	clock daemon
16	local use 0
17	local use 1
18	local use 2
19	local use 3
20	local use 4
21	local use 5
22	local use 6
23	local use 7

REG_DWORD:"logLevel"=00000000

Definiert den LogLevel. (siehe 6.1.)

Das Mapping des Comtarsia Log-Level auf die Syslog Severity erfolgt so:

Comtarsia Log-Level	Severity Numerical Code	Severity
1	3	Error: error conditions
2	3	Error: error conditions
3	4	Warning: warning conditions
4	5	Notice: normal but significant condition
5	6	Informational: informational messages

REG_DWORD:"logMask"=00000000

Definiert die Log-Details. (siehe Kapitel Logging in eine Datei)

REG_DWORD:"logDetails"=0x00000000

Definiert die Log-Details. (siehe Kapitel Logging in eine Datei)

6.3. Logfile-Format

A	B	C	D	E	F	G
K						

2010.10.08 11:15:59.195 1ACC:055C:00 <4:Comt::Prod::SOS2008::SOPConfig::readConfig:120:S0:C0>
Comtarsia SignOn Proxy 2008 Build 1.2.2.11

[illegible]

```
2010.10.08 11:09:28.698 09A4:0F34:00
<2:Comt::Prod::SOS2008::SOP::onServiceStart:62:S0:C0><Comt::Prod::SOS2008::SOP::onServiceStart:100>
The licence key is not valid!
```

A	Date
B	Time
C	Process ID in Hex
D	Thread ID in Hex
E	Log transaction
F	Detail Flag and Message urgency
G	Source code module
H	Source code line
I	Message source
J	Message code
K	Message text
L	Source code module performing exception handling
M	Source code line performing exception handling

7. Installation / Komponenten

Die Installation der SignOn Agent-Komponenten erfolgt durch den Installer nach „%PROGRAMFILES%\Comtarsia\SignOn Solutions 2008“.

A. Referenzen

RFC3164 - The BSD syslog Protocol <http://tools.ietf.org/html/rfc3164>