

A large, semi-transparent magnifying glass icon is centered on the page. To its left is a semi-transparent icon of a computer monitor displaying a line graph. The background is a gradient of red and pink colors.

Guida Installazione

ACGE-K01 ACG Enterprise
Kit Adeguamento GDPR

Guida Installazione

ACGE-K01 ACG Enterprise Kit Adeguamento GDPR

Seconda Edizione (Luglio 2018)

© Copyright TeamSystem SpA 2018. Tutti i diritti riservati

Nota: Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione “Note e Trade-marks” a pagina 4.

Indice

Indice	3
Note e Trademarks	4
1. Introduzione	6
2. Prerequisiti software	7
3. Installazione prodotti.....	8
3.1 Aggiornamento programmi ACG Versione 3.8.0	8
3.2 Aggiornamento web-application agent	10
3.3 Impostazione protocollo SSL_TLSv2	11
3.4 Importazione certificato di sicurezza su WebSphere	13
3.5 Setup dei dati	15
6. Avviamento dell'applicazione.....	16
4.1 Impostazione codice di autorizzazione all'uso del prodotto	16
4.2 Rigenerazione albero dei menu.....	16

Note e Trademarks

ACG e ACG Enterprise sono marchi di ACG S.r.l., con socio unico e soggetta all'attività di direzione e coordinamento di TeamSystem S.p.A., sede legale in via Yuri Gagarin, 205 – 61122 Pesaro (PU), Cap. Soc. € 100.000 i.v., codice fiscale e iscrizione al Registro delle Imprese di Milano n. 08419500965 (di seguito "ACG") - Tutti i diritti riservati.

I marchi e loghi riportati nel presente documento diversi da ACG e ACG Enterprise (ivi inclusi, a mero titolo esemplificativo e non esaustivo, IBM, il logo IBM, Adobe, il logo Adobe, PostScript, il logo PostScript, Intel, il logo Intel, Intel Inside, il logo Intel Inside, Intel Centrino, il logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium e Pentium, Linux, Microsoft, Windows, Windows NT e il logo di Windows, UNIX, Java, Novell, il logo Novell, openSUSE e il logo openSUSE, AS/400, BladeCenter, Cognos, DB2, DB2 Universal Database, eServer, i5/OS, iSeries, OpenPower, OS/400, POWER, Power Systems, pSeries, Rational, System i, System i5, System p, System p5, System Storage, System x, WebSphere, etc.) sono di titolarità di soggetti terzi. ACG rispetta i diritti di proprietà intellettuale di terzi.

Tutti i contenuti del presente documento e i diritti ad essi correlati sono riservati. Tali contenuti pertanto possono essere consultati esclusivamente per finalità d'informazione personale, essendo espressamente vietato ogni diverso utilizzo senza il preventivo consenso scritto di ACG.

Sebbene sia stata usata ogni ragionevole cura nel raccogliere e presentare le informazioni contenute nel presente documento, nessuna garanzia è prestata in ordine alla loro esattezza, completezza, utilità, né ai loro possibili impieghi da parte degli utenti; è pertanto esclusa ogni responsabilità di ACG per errori, inesattezze od omissioni relative a dette informazioni. I contenuti del presente documento sono soggetti a continuo aggiornamento e sono da ritenersi puramente indicativi e suscettibili di eventuali errori e/o imprecisioni.

ACG può introdurre miglioramenti e/o variazioni ai prodotti e/o programmi descritti nel presente documento in qualsiasi momento e senza preavviso.

Il presente documento può contenere informazioni che riguardano programmi e propositi futuri, che vengono descritti di volta in volta mediante l'utilizzo di termini come "attendarsi", "stimare", "prevedere", "prospettare" e "programmare". Tali dichiarazioni per loro natura non comportano alcun impegno a carico di ACG, che pertanto non assume in relazione ad essi alcuna responsabilità di realizzazione.

Qualunque riferimento a siti web diversi da www.acginfo.it è fornito a solo titolo esemplificativo e non costituisce invito all'utilizzo e/o navigazione. I contenuti dei siti web referenziati non sono parte dei prodotti ACG e il loro eventuale utilizzo da parte dell'utente è effettuato a suo esclusivo rischio. Le informazioni relative a prodotti non ACG contenute nel presente documento sono fornite dai rispettivi fornitori, dagli annunci pubblicitari e da informazioni liberamente disponibili. ACG non ha collaudato tali prodotti e non può confermarne l'accuratezza delle prestazioni, la compatibilità con i prodotti ACG o qualunque altra caratteristica. Qualunque richiesta sulle caratteristiche operative dei prodotti non ACG deve essere rivolta direttamente ai rispettivi fornitori.

Fatti salvi i danni causati da dolo o colpa grave, ACG non assume nessuna responsabilità circa i contenuti del presente documento. In particolare, tali contenuti non rappresentano una promessa o garanzia relativa all'idoneità a determinati scopi dei prodotti ACG oppure alla non violazione, da parte dei prodotti ACG stessi, di leggi di qualsivoglia natura.

Aggiornamenti

Data	Nr PTF	Descrizione aggiornamenti
04/05/2018		Primo Rilascio
17/05/2018		Aggiornati paragrafi 3.1 e 3.5

1. Introduzione

Lo scopo di questa guida è descrivere i passi di installazione del prodotto **ACG Enterprise Kit Adeguamento GDPR Versione 1 Rilascio 1 livello di modifica 0** destinato ad ambienti con installazione dei prodotti **ACG Enterprise** e **ACG Versione 3.8.0**.

Il prodotto consta di due componenti:

- componente AS/400, rilasciata come libreria di programmi da installare sul server IBM i
- componente web da installare come aggiornamento dell'applicazione web ACG Enterprise (nel seguito referenziata anche come web-app *agent*)

2. Prerequisiti software

Il prodotto ACG Enterprise Kit Adguamento GDPR ha come prerequisito:

- per la componente AS/400 il prodotto Modulo Base V3 a livello di PTF **GA380015**
- per la componente web ACG Enterprise Hub a livello di aggiornamento **ENT1100016D**

3. Installazione prodotti

L'installazione della componente AS/400 richiede l'aggiornamento dell'installazione ACG Versione 3.8.0, mentre l'installazione della componente web richiede l'aggiornamento dell'applicazione web *acgent*.

3.1 Aggiornamento programmi ACG Versione 3.8.0

Questo passo di aggiornamento richiede il download del file **PBD11000.zip** pubblicato in TeamUpdate in data 04/05/2018 col titolo "ACGE-K01 ACG Enterprise Kit Adeguamento GDPR V1R1M0 - Package installazione" nella categoria *ACG Enterprise*.

L'installazione del prodotto può essere eseguita in duplice modalità:

- installazione AUTOMATICA (con l'uso del comando KAPYPTF)
- installazione MANUALE.

In entrambi i casi, prima di procedere con l'installazione, è necessario eseguire le seguenti operazioni:

1. Aprire una sessione di lavoro con utente QPGMR ed immettere il comando:

```
CALL PBD11000/DEPACK1 ('PBD11000' 'PBD110000')
```

una volta scaricata la libreria della PTF sul proprio sistema

2. Da riga comandi immettere

```
CRTDUPOBJ OBJ(IPROD00F) FROMLIB(ACGGAA) OBJTYPE(*FILE)  
TOLIB(PBD11000) NEWOBJ(INDICE)
```

3. Dal prompt SQL immettere

```
INSERT INTO PBD11000/INDICE  
(AVFLG, CDPRO, DEPRO, DTINS, AREAD, ACRON) VALUES( '0',  
'ACGE-K01', 'Kit Adeguamento GDPR', 240418, 'IACGEK01', 'PBD')
```

4. Immettere il comando:

```
CALL PGM(PBD11000/PBD000PI)
```

5. Immettere il codice di autorizzazione all'uso del prodotto con il comando:

```
KPWACQ CDPRO ('ACGE-K01')
```

Se non si è ancora in possesso della password è comunque possibile procedere con l'installazione della PTF. Verrà emesso un messaggio di avvertimento che ne segnalerà la mancanza.

Installazione AUTOMATICA (con utilizzo del comando KAPYPTF)

Aprire una sessione di lavoro con utente QPGMR ed immettere il comando:

```
KAPYPTF PTFNAME(PBD11000) OBJLIB(ACGGAA) PGMSRCLIB(*NO)
```

Installazione MANUALE (senza utilizzo del comando KAPYPTF)

Nel caso non si voglia utilizzare il comando KAPYPTF eseguire invece tutti i passi che seguono.

a) Copia oggetti

In funzione del proprio ambiente, fare in modo che i seguenti oggetti:

```
C RTPBDJOBQ *PGM
KCB30 *PGM
KCB50 *PGM
KCB51 *PGM
KCB61 *PGM
KCB65 *PGM
KCB65V *PGM
KCB80 *PGM
KCB81 *PGM
KCB82 *PGM
KRB31 *PGM
KRB31V *PGM
KRB50 *PGM
KRB52 *PGM
KRB53 *PGM
KRB54 *PGM
KRB56 *PGM
KRB60 *PGM
KRB61 *PGM
KRB65 *PGM
KRB71 *PGM
KRB72 *PGM
KRB73 *PGM
```

KRB74 *PGM
KRB80 *PGM
KRB81 *PGM
KRB6500V *FILE
KRB8000V *FILE
PBD1D *FILE

siano copiati dalla libreria di PTF alla libreria ACGGAA.

b) Adeguamento librerie dati

Per ogni libreria dati aziendale già presente sul sistema eseguire da QPGMR i seguenti comandi:

```
ADDLIBLE PBD11000
UPDPBD000
LIBAZI(libreria dati azienda)
LIBCOM(libreria dati comune)
LIBGRP(libreria dati di gruppo)
LIBOBJ(ACGGAA)
LIBSRC(ACGFBASV3)
```

c) Sorgenti

Non è previsto il rilascio di alcun modulo in formato sorgente.

3.2 Aggiornamento web-application agent

L'aggiornamento delle funzioni dell'applicazione web ACG Enterprise Kit Adeguamento GDPR richiede l'installazione del file **agent_PBD110.zip** mediante la console di amministrazione di Websphere Application Server, selezionando l'opzione di aggiornamento multiplo dell'applicazione ("Sostituire, aggiungere o cancellare più file") e indicando nel campo "Percorso del file compresso" il percorso completo del file .zip sopra indicato.

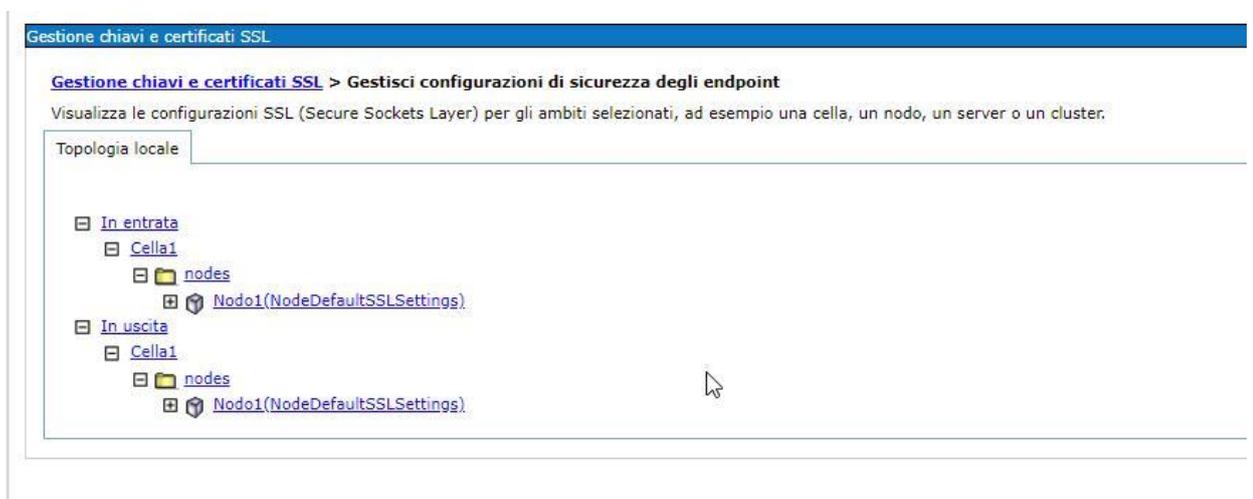
3.3 Impostazione protocollo SSL_TLSv2

Successivamente all'installazione dell'applicazione è necessario effettuare l'impostazione del protocollo SSL_TLSv2, che richiede l'esecuzione dei seguenti passi:

1. Accedere alla console di gestione di Websphere Application Server.
2. Espandere la voce *Sicurezza* nel menu di navigazione a sinistra e fare clic su *Gestione chiavi e certificati SSL*. Nella sezione *Impostazioni della configurazione*, fare clic su *Gestisci configurazioni di sicurezza dell'endpoint*.



3. Selezionare la configurazione in uscita appropriata per giungere all'ambito di gestione (cella/nodo)



4. Sotto *Elementi correlati*, fare clic su *Configurazione SSL* e selezionare la configurazione denominata *NodeDefaultSSLSettings*

5. Cliccare su *Impostazioni QoP (Quality of Protection)*
6. Selezionare nella tendina “Protocollo” la voce “SSL_TLSv2” e premere il tasto *Salva*

Gestione chiavi e certificati SSL

[Gestione chiavi e certificati SSL](#) > [Gestisci configurazioni di sicurezza degli endpoint](#) > [Nodo1](#) > [Configurazioni SSL](#) > [NodeDefaultSSLSetting](#)
Impostazioni QoP (Quality of protection)

Specifica il livello di sicurezza, le cifrature e le impostazioni di autenticazione reciproca.

Proprietà generali

Autenticazione client
 Nessuna ▼

Protocollo
 SSL_TLSv2 ▼

Provider

Provider JSSE predefinito
 Selezionare provider:
 IBMJSSE2 ▼

Provider JSSE personalizzato
 Personalizza provider

Impostazioni delle suite di cifratura

Gruppi di suite di cifratura
 Forte ▼

Aggiorna cifrature selezionate

Suite di cifratura

Aggiungi >>

<< Rimuovi

Cifrature selezionate

- SSL_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_AES_256_CBC_SHA
- SSL_DHE_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_AES_256_CBC_SHA
- SSL_DHE_DSS_WITH_AES_128_CBC_SHA

7. Salvare la Configurazione di Websphere
8. Riavviare il WAS.

3.4 Importazione certificato di sicurezza su WebSphere

Successivamente è necessario importare due certificati di sicurezza in WebSphere Application Server:

- 1) **agyolog-storage.agyo.io** per consentire l'invio dei log al portale Agyo Privacy
- 2) **connector.teamsystem.com** per inviare la richiesta di verifica contratto

Configurazione del primo certificato:

Attenzione: prima di effettuare i passi descritti in questo paragrafo verificare che effettuando dalla linea comandi del server dove è installato Websphere Application Server il comando descritto di seguito si ottenga un IP valido e che questo IP sia raggiungibile:

Per AS400: **NSLOOKUP HOSTNAME (agyolog-storage.agyo.io)**

Per Win/Linux: **nslookup agyolog-storage.agyo.io**

In caso negativo controllare e modificare opportunamente le impostazioni TCP/IP del server che ospita WAS per far sì che la verifica sopra indicata abbia esito positivo prima di proseguire nell'esecuzione dei passi di configurazione descritti qui di seguito.

L'importazione del certificato di sicurezza richiede l'esecuzione dei seguenti passi:

1. Seguire i primi tre passi indicati nel paragrafo precedente.
2. Sotto *Elementi correlati*, fare clic su *Keystore e certificati* e selezionare il keystore *NodeDefaultTrustStore*.
3. Nella sezione *Ulteriori proprietà* fare clic su *Certificati firmatario*
4. Cliccare sul pulsante "Richiama da porta"
5. Nella forma che si apre impostare i campi come segue:
 - Host: **agyolog-storage.agyo.io**
 - Porta: **443**
 - Alias: **agyolog-storage.agyo.io** (o altro nome di fantasia)
6. Fare clic sul pulsante *Richiama informazioni firmatario*.
7. Verificare che le informazioni sul certificato siano relative ad un certificato affidabile.
8. Fare clic su *Applica e Salva*.

Configurazione del secondo certificato:

Attenzione: prima di effettuare i passi descritti verificare che, effettuando dalla linea comandi del server dove è installato Websphere Application Server il comando descritto di seguito, si ottenga un IP valido e che questo IP sia raggiungibile:

Per AS400: **NSLOOKUP HOSTNAME (connector.teamsystem.com)**

Per Win/Linux: **nslookup connector.teamsystem.com**

In caso negativo controllare e modificare opportunamente le impostazioni TCP/IP del server che ospita WAS per far sì che la verifica sopra indicata abbia esito positivo prima di proseguire con la configurazione .

Per configurarlo, seguire gli stessi passi del primo certificato, indicando al punto 5:

- Host: **connector.teamsystem.com**
- Porta: **443**
- Alias: **connector.teamsystem.com** (o altro nome di fantasia)

Infine riavviare il WAS.

3.5 Setup dei dati

L'operazione di setup dati deve essere effettuata solo sul sistema informativo ACGGAA indicando i seguenti valori:

Acronimo	<i>PBD</i>
Versione	<i>VIR1M0</i>
PTF	
Sist. informativo	<i>ACGGAA</i>

Terminata l'operazione di setup, occorre arrestare e riavviare l'applicazione web.

6. Avviamento dell'applicazione

4.1 Impostazione codice di autorizzazione all'uso del prodotto

L'attivazione del prodotto *ACG Enterprise Kit Adempimenti GDPR* in *acgent* richiede l'immissione da parte dell'amministratore del sistema del codice di autorizzazione all'uso, secondo la procedura illustrata nella guida d'installazione del prodotto *ACG Enterprise Hub*, indicando il codice prodotto **ACGE-K01**. È possibile scaricare tale codice dal sito TeamUpdate, selezionando la licenza avente:

Sigla:	ACGE-K01
Descrizione:	ACG Enterprise Kit Adeguamento GDPR (parte web)

4.2 Rigenerazione albero dei menu

L'operazione di setup della base dati aggiunge una serie di codici operazioni e di menu, per cui si rende necessario per ciascun utente:

- rigenerare il menu ad albero lanciando l'operazione "Ricarica albero dei menu"
- attendere la visualizzazione del messaggio di completamento dell'operazione,
- premere il pulsante OK per ricaricare il desktop.

Dopo queste operazioni, nel menu *ACG Enterprise Hub* comparirà la voce di menu "Kit adeguamento GDPR" qualora ci si colleghi al sistema informativo ACGGAA.

Successivamente è necessario rieseguire il setup del menu su Polyedro.