

P.I.TRE. – PROTOCOLLO INFORMATICO TRENTO

MANUALE D'INSTALLAZIONE E CONFIGURAZIONE DEI CLIENT PER L'ACCESSO A P.I.TRE.

Codice: Versione: 1.0 Prima Stesura

Data di emissione:

Firma Data

Redatto:

Maria Cinquepalmi 10/11/2018

Rivisto:

L. Luciani 15/11/2018

Approvato:

Distribuzione elettronica a:

Personale Area Tecnica

Distribuzione cartacea a:

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
07/08/2018	PiTRE3.2.12	2: Requisiti Software postazione PC Client
		3.2.4 : Configurazione Internet Explorer 11 aggiuntiva per Java applet, smart clients, ActiveX
		3.2.5.2: Configurazione del sito di P.I.Tre non in "Impostazioni Visualizzazione Compatibilità"
		4: Installazione ClientComponents
		6.5 : Installazione e configurazione di SmartClient
		7 : Acquisizione massiva

INDICE

1	INTRODUZIONE.....	1
1.1	PREMESSA	1
1.2	DEFINIZIONI E ABBREVIAZIONI.....	1
1.3	RIFERIMENTI.....	2
2	REQUISITI SOFTWARE POSTAZIONE PC CLIENT	3
3	CONFIGURAZIONE GENERALE DELLE POSTAZIONI	6
3.1	VERIFICA DELLA VERSIONE DI MS INTERNET EXPLORER UTILIZZATA.....	6
3.2	CONFIGURAZIONE INTERNET EXPLORER 11	7
3.2.1	IMPOSTAZIONI DI SICUREZZA DEL BROWSER INTERNET EXPLORER	7
3.2.1.1	Inserimento del sito di P.I.TRE. tra i siti attendibili.....	7
3.2.1.2	Configurazione del browser per l'utilizzo degli ActiveX	9
3.2.2	IMPOSTAZIONI PER L'UTILIZZO DI P.I.TRE. CON SERVER PROXY	12
3.2.3	IMPOSTAZIONI PER L'UTILIZZO DI P.I.TRE. CON PROTOCOLLO HTTPS	13
3.2.4	CONFIGURAZIONE INTERNET EXPLORER 11 AGGIUNTIVA PER JAVA APPLET, SMART CLIENTS, ACTIVE-X	19
3.2.5	CONFIGURAZIONE INTERNET EXPLORER 11 AGGIUNTIVA PER HTML5 SOCKET	19
3.2.5.1	Configurazione del sito di P.I.Tre nella Intranet Locale.....	20
3.2.5.2	Configurazione del sito di P.I.Tre non in "Impostazioni Visualizzazione Compatibilità"	21
3.2.6	CONFIGURAZIONE AREA DI MEMORIA DEI FILE TEMPORANEI DEL BROWSER	22
3.3	CONFIGURAZIONE INTERNET EXPLORER 10	24
3.4	CONFIGURAZIONE CHROME PER HTML5 SOCKET	24
3.4.1	ECCEZIONE CHROME	24
3.5	CONFIGURAZIONE FIREFOX PER HTML5 SOCKET.....	25
3.5.1	ECCEZIONE FIREFOX	25
4	INSTALLAZIONE CLIENTCOMPONENTS.....	27
5	CONFIGURAZIONE GENERALE HTML5 SOCKET	29
5.1	INSTALLAZIONE CONNETTORE WINDOWS.....	29
5.1.1	PROCEDURA STANDARD	29
5.1.1.1	Configurazione del sito di P.I.Tre non in "Impostazioni Visualizzazione Compatibilità"	32
5.2	INSTALLAZIONE CONNETTORE UBUNTU	33
5.2.1	PROCEDURA STANDARD	33
6	INSTALLAZIONE DEI DISPOSITIVI	34
6.1	CONFIGURAZIONE DELLO SCANNER.....	34
6.2	CONFIGURAZIONE DEI DISPOSITIVI DI STAMPA SU PORTA SERIALE	34

6.3	CONFIGURAZIONE STAMPANTI ZEBRA SU PORTA USB.....	34
6.3.1	PROCEDURA STANDARD.....	34
6.3.1.1	Nota su docspav2.ini	36
6.3.1.2	<i>Descrizione file docspav2.ini</i>	37
6.3.2	INSTALLAZIONE SU SISTEMI WINDOWS 7 A 32 O 64 BIT.....	39
6.4	INSTALLAZIONE E CONFIGURAZIONE DELLE STAMPANTINE DYMO	41
6.5	INSTALLAZIONE E CONFIGURAZIONE DI SMARTCLIENT.....	41
6.5.1	POST INSTALLAZIONE.....	44
6.5.2	VERIFICA SE SMARTCLIENT È STATO SCARICATO DOPO IL PRIMO UTILIZZO.	45
6.6	FIRMA DIGITALE.....	46
6.6.1	FIRMA DIGITALE SU UBUNTU PER HTML5 SOCKET	46
6.7	RISOLUZIONE DI PROBLEMI A VALLE DELL'INSTALLAZIONE DI UN DISPOSITIVO	47
7	ACQUISIZIONE MASSIVA	47
8	CONFIGURAZIONE DI ADOBE ACROBAT FULL PER L'ABILITAZIONE DELLA CONVERSIONE IN PDF DEI FILE ACQUISITI	48
8.1	INTRODUZIONE.....	48
8.1.1	PARAMETRI CONFIGURAZIONE P.I.TRE.	48
8.1.2	PARAMETRI CONFIGURAZIONE ACROBAT	49
	APPENDICE 1 - CONFIGURAZIONE STAMPANTINE DYMO (LATO SERVER).....	59

1 INTRODUZIONE

1.1 PREMESSA

Il documento illustra le procedure da eseguire per configurare le postazioni da cui viene utilizzato **P.I.TRE. 3.0 e versioni successive** e installare e configurare i dispositivi di stampa della segnatura di protocollo e di acquisizione dei documenti cartacei.

E' possibile utilizzare i seguenti dispositivi di stampa della segnatura:

- timbro Citec;
- stampante a penna (PrintPen);
- stampante di etichette.

E' possibile utilizzare i seguenti dispositivi di acquisizione dei documenti cartacei:

- qualunque scanner dotato di interfaccia TWAIN.

Nel caso di postazioni per l'acquisizione dei documenti cartacei, viene inoltre mostrato come configurare Adobe Acrobat per la conversione in PDF dei file acquisiti e per il riconoscimento ottico dei caratteri (OCR).

Tali dispositivi potranno essere gestiti, a seconda del browser utilizzato e/o delle impostazioni fatte per il singolo utente, tramite diverse tecnologie:

- ActivieX
- Smart client
- Applet Java (solo IE);
- Html5 socket

1.2 DEFINIZIONI E ABBREVIAZIONI

ActiveX

ActiveX è il nome della tecnologia sviluppata da Microsoft che rende possibile l'implementazione di particolari "controlli" in possesso di funzionalità specifiche i quali, una volta realizzati, possono essere letteralmente incorporati all'interno di altre applicazioni

Java applet

Le applet Java sono programmi scritti in linguaggio Java che possono essere eseguiti da un web browser (elaborazione lato client). Le applet sono solitamente usate per creare pagine dotate di funzioni interattive con l'utente non realizzabili con altre tecnologie per il Web statico.

Le Java applets sono eseguibili dal web browser IE che utilizza la Java virtual machine (JVM).

OCR	Acronimo di Optical Character Recognition; operazione di riconoscimento del testo contenuto in file di tipo immagine, tipicamente file in formato TIFF o PDF acquistati da scanner.
Segnatura protocollo	di Informazioni di protocollo associate o apposte al documento protocollato secondo la normativa vigente
Smart client	Gli Smart Client sono applicazioni, eseguite localmente dagli utenti, di facile distribuzione e gestione, in grado di fornire un ambiente operativo e un'interfaccia utente capace di adattarsi in modo flessibile a ogni condizione di funzionamento e di sfruttare intelligentemente le risorse del PC e le connessioni disponibili ai sistemi e ai dati aziendali
HTML5 Socket	HTML5 Socket dà la possibilità di “ stabilire e mantenere una connessione dati tra browser e server remoto ” sulla quale far transitare messaggi in entrambe le direzioni.

1.3 RIFERIMENTI

N.A.

2 REQUISITI SOFTWARE POSTAZIONE PC CLIENT

Configurazioni **Sistema Operativo/Browser** certificati:

Applet, SmartClient o Activex	
Sistema Operativo	Browser
Windows 7 32/64 bit Windows 8	Internet Explorer 9/10/ 11 (check se 32 e/o 64 bit) Chrome 44 FireFox 41
Windows 10	Internet Explorer 9/10/ 11 (check se 32 e/o 64 bit) Chrome 44 FireFox 41
Ubuntu 12.10	FireFox 22

HTML5 Socket	
Sistema Operativo	Browser
Windows 7 [32/64 bit]	Internet Explorer 10/11 Chrome 49 upgrade fino alla versione 68 FireFox 49 upgrade fino alla 61 Safari 9.3
Windows 10	Internet Explorer 10/11 Chrome 49 upgrade fino alla versione 68 FireFox 49 upgrade fino alla 61 Safari 9.3

Configurazioni **Sistema Operativo/Browser** garantiti, ma non certificati:

Applet, SmartClient o Activex	
Sistema Operativo	Browser
Apple Mac OS X Mountain Lion	Safari 5.1

HTML5 Socket	
Sistema Operativo	Browser
Ubuntu 16.04	FireFox 49
Ubuntu 15.10	
Apple Mac OS X Mountain Lion	Safari 9.3

P.I.TRE. utilizza componenti client quali **Applet**, **SmartClient (solo su IE)** , **Activex (solo su IE)**, **HTML5 Socket (tecnologia non compatibile con IE8 e IE9)** necessarie per l'interfacciamento con i *device* stessi, quali:

- stampantine di etichetta (**Zebra** serie **LP TP** e **Dymo L400**).
- lettori di smartcard per firma digitale (Aruba, Atalis, Poste.com, InfoCert).
- scanner (il sistema è compatibile con tutti i modelli di scanner di mercato che supportano **driver Twain** su Windows o **driver Sane** su Ubuntu)

oppure, necessarie per le funzionalità:

- Export smistamento
- Modelli RFT
- Export/Import Fascicoli
- Export massivo Ricerca Documenti/Fascicoli/Trasmissioni
- Export massivo Ricerca ADL Documenti/ADL Fascicoli
- Blocca e rilascia Documento
- Salvataggio in locale del documento
- Export rubrica/ Export ricerca corrispondenti
- Export documenti pregressi

In particolare, le applet sono state sviluppate con Java Virtual Machine versione 1.6_18:

	IE9	IE10	IE11	Google Chrome upgrade fino alla versione 44	Firefox upgrade fino alla 41
Windows XP SP3 (32 bit)				JVM 1.6_18(**) → ultima versione disponibile 1.8_x (!)	JVM: ultima versione disponibile 1.8_x (!)
Windows 7 (32 bit)	JVM 1.6_33 → ultima versione disponibile 1.8_x (!)	JVM 1.6_33 → ultima versione disponibile 1.8_x (!)	JVM 1.6_33 → ultima versione disponibile 1.8_x (!)	JVM 1.6_33 → ultima versione disponibile 1.8_x (!)	JVM: ultima versione disponibile 1.8_x (!)
Windows 7 (64 bit)	JVM 1.6_33(*) → → ultima versione disponibile 1.8_x (!)	JVM 1.6_33(*) → ultima versione disponibile 1.8_x (!)	JVM 1.6_33(*) → → ultima versione disponibile 1.8_x (!)	JVM 1.6_33(*) → ultima versione disponibile 1.8_x (!)	JVM: ultima versione disponibile 1.8_x (!)
UBUNTU 12.10				JVM: ultima versione disponibile 1.8_x (!)	JVM: ultima versione disponibile 1.8_x (!)
Apple Mac OS X Mountain Lion (***)				JVM: ultima versione disponibile 1.8_x (!)	JVM: ultima versione disponibile 1.8_x (!)

(*) E' necessario installare sia la versione JRE 6 versione 1.6_33 per sistemi 32 bit che JRE 6 versione 1.6_33 per sistemi 64 bit. In caso di browser Internet Explorer deve essere utilizzata la versione a 32 bit.

(**) La JVM 1.6_18 è compatibile, ma il corretto funzionamento è ostacolato dall'opzione di download automatico dell'ultima versione disponibile di JRE. Opzione presente nativamente sul browser Google Chrome 28 e successive.

(***) Il funzionamento su questo S.O. non è certificato, ma è un S.O. compatibile

(!) In caso di JVM 1.7_45 procedere comunque all'aggiornamento. Il manifest di tale versione contiene un parametro (Caller Allowable Codebase) che non è compatibile con la Trusted Library (fondamentale per tutte le versioni precedenti).

Annotazione 1:

Per le successive versioni di JVM 19_x non saranno più funzionanti le Applet , per cui chi aggiorna la JVM , non potrà più utilizzare la configurazione Applet sul PiTre.

Annotazione 2:

Per chi utilizza i browser Chrome e Firefox, il corretto funzionamento del sistema, per quanto riguarda le applet e le funzionalità ad esse associate, sono garantite per Chrome solo fino alla versione 44, mentre per FireFox fino alla 41. Le successive versioni dei due software potrebbero non attivare correttamente le applet Java, le funzionalità impattate sono:

- Acquisizione da scanner
- Stampa etichetta
- Export ricerche
- Export documenti in fascicolo
- Modelli Word
- Copia file in locale
- Firma digitale locale con smartcard

3 CONFIGURAZIONE GENERALE DELLE POSTAZIONI

3.1 VERIFICA DELLA VERSIONE DI MS INTERNET EXPLORER UTILIZZATA

Per utilizzare P.I.TRE. tramite Internet Explorer (versioni 9, 10 , 11), è necessario configurare opportunamente il browser in base a quanto indicato nei paragrafi seguenti.

Prima di procedere all'esecuzione dell'applicazione bisogna verificare la versione del browser di cui si è in possesso.

La verifica può essere fatta seguendo la seguente procedura:

1. attivare Internet Explorer
2. dalla voce di menu **? (punto interrogativo, nelle postazioni in lingua inglese *Help*)** selezionare ***Informazioni su Internet Explorer*** (About Internet Explorer)



Figura 1 – Versione di Internet Explorer

La figura sopra indica che la versione è la 11.0.

3.2 CONFIGURAZIONE INTERNET EXPLORER 11

3.2.1 IMPOSTAZIONI DI SICUREZZA DEL BROWSER INTERNET EXPLORER

Per un corretto funzionamento di P.I.TRE. sono necessarie alcune impostazioni che abbassano il livello di sicurezza del browser. Per tale motivo è fortemente consigliato inserire il sito di P.I.TRE. tra i *siti attendibili* (*trusted sites*) e abbassare i livelli di sicurezza solo su quest'area.

3.2.1.1 Inserimento del sito di P.I.TRE. tra i siti attendibili

Per inserire P.I.TRE. tra i siti attendibili procedere come segue:

1. attraverso il menu **Strumenti** (*Tools*) selezionare **Opzioni Internet...** (*Internet options...*)
2. selezionare la scheda **Sicurezza** (*Security*)

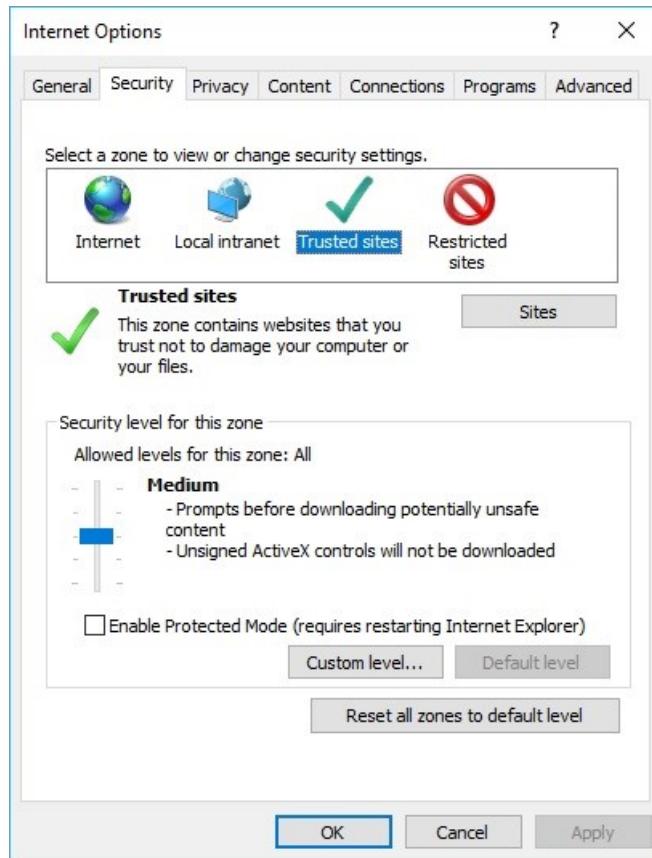


Figura 2 – Accesso alla scheda ‘Sicurezza’

3. selezionare **Siti attendibili** (*Trusted sites*)
4. selezionare il pulsante **Siti...** (*Sites...*)
5. scrivere nel campo **Aggiungi il sito Web all'area** (*Add this Web site to the zone*) l'URL relativo al server su cui è stato installato P.I.TRE. (es. <http://PITRE> o <http://10.0.2.12>)

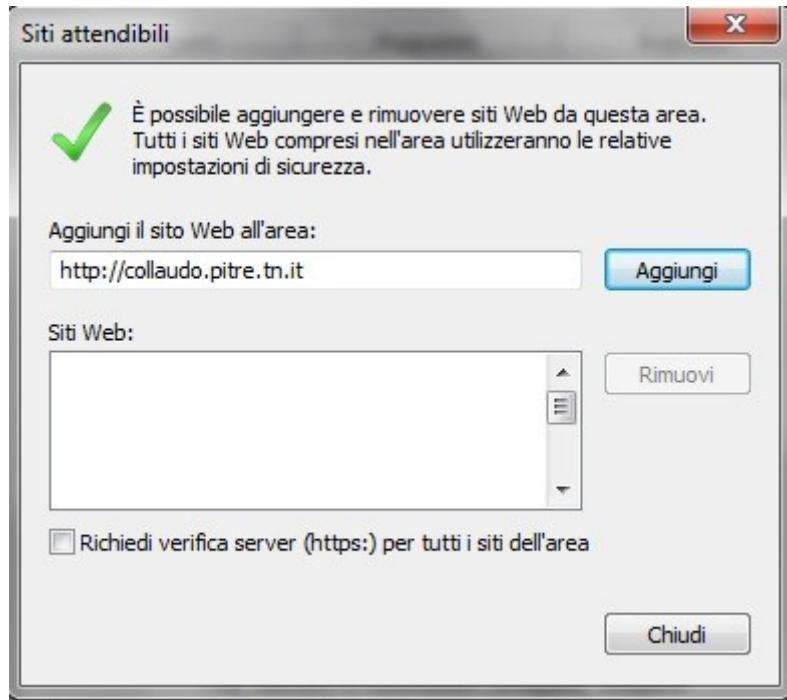


Figura 3 – Inserimento del server di P.I.TRE. tra i siti attendibili

6. selezionare il pulsante **Aggiungi** (*Add*)
7. nel caso non si utilizzi una configurazione in https assicurarsi che il campo a selezione (check box) **Richiedi verifica server (https:) per tutti i siti dell'area** (*Require server verification (https:) for all sites in this zone*) non abbia il segno di spunta.

3.2.1.2 Configurazione del browser per l'utilizzo degli ActiveX

P.I.TRE. fra gli altri, fa uso di ActiveX per pilotare gli scanner e i dispositivi di stampa della segnatura installati sulle postazioni di lavoro.

Gli ActiveX hanno accesso completo alle postazioni di lavoro e potrebbero causare problemi di sicurezza se non se ne conosce la provenienza. Internet Explorer ha dei meccanismi per proteggere le postazioni di lavoro da ActiveX maligni che possono essere scaricati inconsapevolmente dalla rete navigando in Internet.

P.I.TRE. tenta di scaricare ed seguire automaticamente sulla postazione di lavoro gli ActiveX necessari residenti sul server, il browser deve quindi essere configurato per consentirne l'uso. Per far questo, dopo aver inserito il sito di P.I.TRE. tra i siti attendibili, come descritto precedentemente, è necessario personalizzare, abbassandolo, il livello di sicurezza nell'Area dei siti attendibili (lasciando alto il livello di sicurezza nell'area Internet).

Per permettere l'installazione e l'uso degli ActiveX sulla postazione locale bisogna seguire la seguente procedura (i passi 1-3 sono identici a quelli descritti per l'inserimento di P.I.TRE. tra i siti attendibili):

1. attraverso il menu **Strumenti** (*Tools*) selezionare **Opzioni Internet...** (*Internet Options*)
2. selezionare la scheda **Sicurezza** (*Security*)



Figura 4 – Accesso alla scheda 'Sicurezza'

3. selezionare **Siti attendibili** (*Trusted sites*)
4. selezionare il pulsante **Livello Personalizzato...** (*Custom Level...*)
5. scorrere la lista presentata fino a raggiungere la voce **Controlli ActiveX e plug-in** (*ActiveX controls and plug-ins*)
6. abilitare gli ActiveX selezionando il bottone **Attiva** (*Enable*) sulle seguenti sotto voci:
 - **Esegui controlli e plug-in ActiveX** (*Run ActiveX controls and plug-ins*)
 - **Esegui script controlli ActiveX contrassegnati come sicuri** (*Script ActiveX controls marked safe for scripting*)
 - **Inizializza e esegui script controlli ActiveX non contrassegnati come sicuri** (*Initialize and script ActiveX controls not marked as safe*)
 - **Richiesta di conferma automatica per controlli ActiveX** (*Automatic prompting for ActiveX controls*)
 - **Scarica controlli ActiveX con firma elettronica** (*Download signed ActiveX controls*)

- **Scarica controlli ActiveX senza firma elettronica** (*Download unsigned ActiveX controls*)

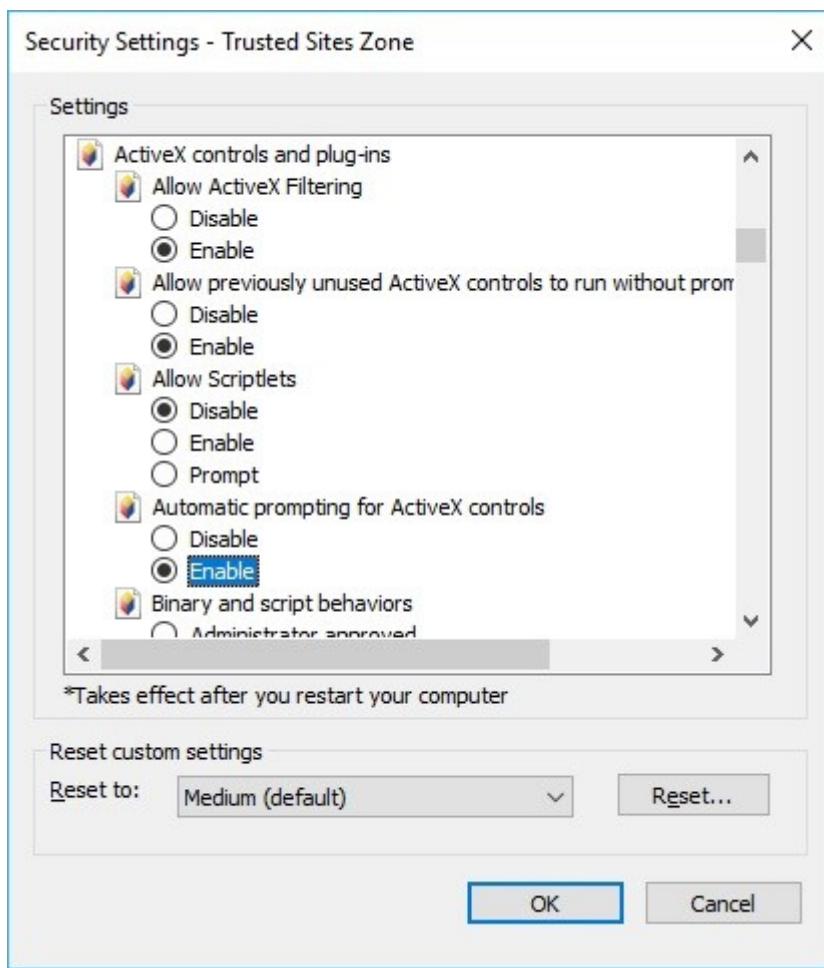


Figura 5 – Abilitazione all'uso degli ActiveX

7. sempre nella sezione **Controlli ActiveX e plug-in** (*ActiveX controls and plug-ins*), selezionare **Disattiva** (*Disable*) per la seguente sottovoce:
 - **Consenti solo ai domini approvati di utilizzare Activex senza chiedere conferma** (*Only allow approved domains to use ActiveX without prompt*)
8. scorrere la lista presentata fino a raggiungere la voce **Download** (*Download*)
9. abilitare, selezionando il bottone **Attiva** (*Enable*) la sottovoce:
 - **Richiesta di conferma automatica per il download del file** (*Automatic prompting for file downloads*)
10. scorrere la lista presentata fino a raggiungere la voce **Varie** (*Miscellaneous*)
11. abilitare, selezionando il bottone **Attiva** (*Enable*) le seguenti sottovoci:
 - **Accesso all'origine dei dati a livello di dominio** (*Access data sources across domains*)

- **Non richiedere la selezione del certificato client quando non esiste** (*Don't prompt for client certificate selection when no certificates or only one certificate exists*)
- **Visualizza contenuto misto** (*Display mixed content*).

3.2.2 IMPOSTAZIONI PER L'UTILIZZO DI P.I.TRE. CON SERVER PROXY

Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client.

Se l'ambiente in cui si opera prevede un proxy, è possibile che alcune pagine web del sistema di gestione documentale non siano visualizzate. In tal caso è necessario impostare le proprietà del browser come segue:

1. attivare il browser Internet Explorer
2. attraverso il menu **Strumenti** (*Tools*), selezionare **Opzioni Internet...** (*Internet Options...*)
3. selezionare la scheda **Avanzate** (*Advanced*)
4. scorrere la lista presentata fino a raggiungere la voce **Impostazioni HTTP 1.1** (*HTTP 1.1 settings*)
5. selezionare la sottovoce **Usa HTTP 1.1 con connessioni tramite proxy** (*Use HTTP 1.1 through proxy connections*).

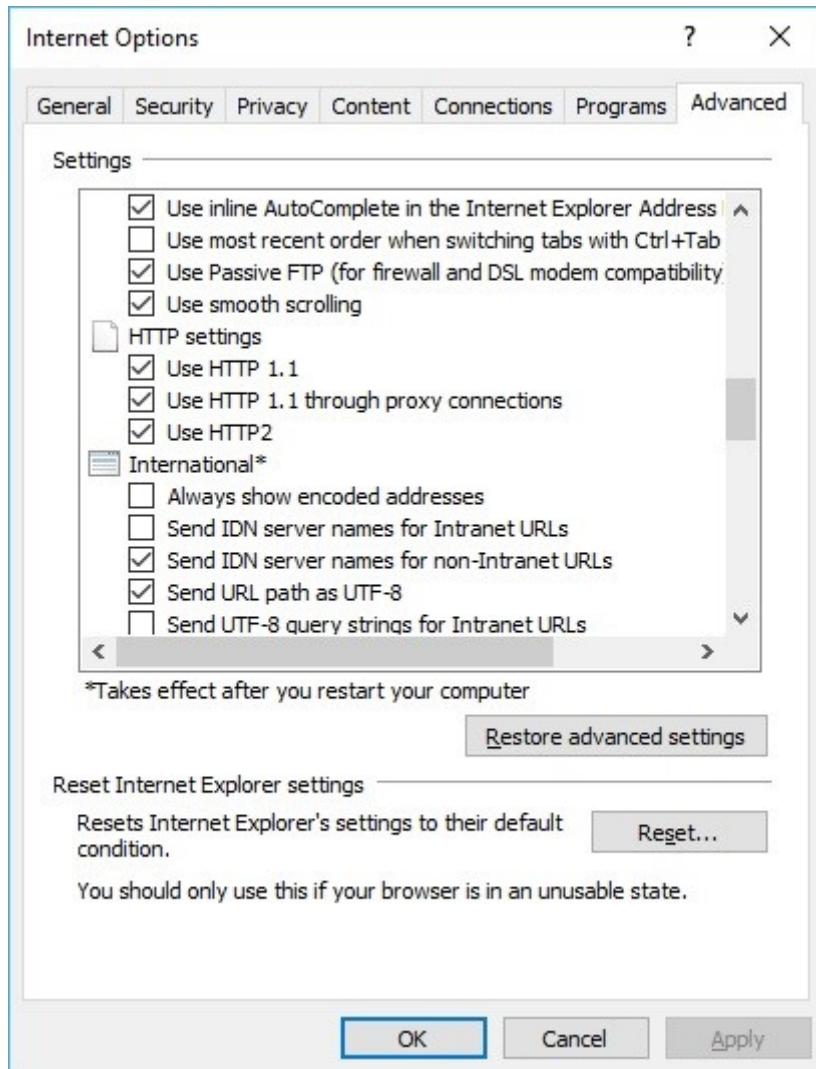


Figura 6 – Impostazioni HTTP 1.1

3.2.3 IMPOSTAZIONI PER L'UTILIZZO DI P.I.TRE. CON PROTOCOLLO HTTPS

1. attraverso il menu **Strumenti** (Tools) selezionare **Opzioni Internet...** (Internet Options...)
2. selezionare la scheda **Sicurezza** (Security)

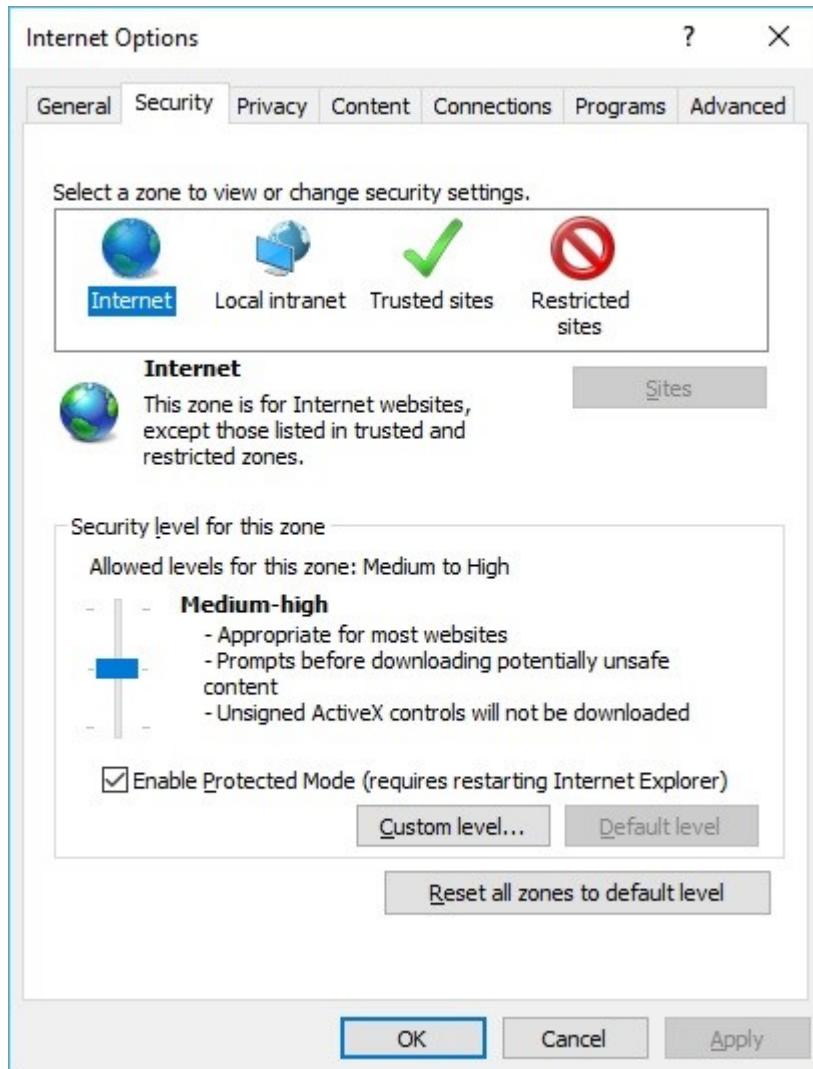


Figura 7 – Accesso alla scheda ‘Sicurezza’

3. selezionare **Siti attendibili** (*Trusted sites*)
4. selezionare il bottone **Livello personalizzato...** (*Custom Level...*)
5. scorrere la lista presentata fino a raggiungere la voce **Visualizza contenuto misto** (*Display mixed content*) nella sezione **Varie** (*Miscellaneous*)
6. abilitare la voce selezionando il bottone **Attiva** (*Enable*)

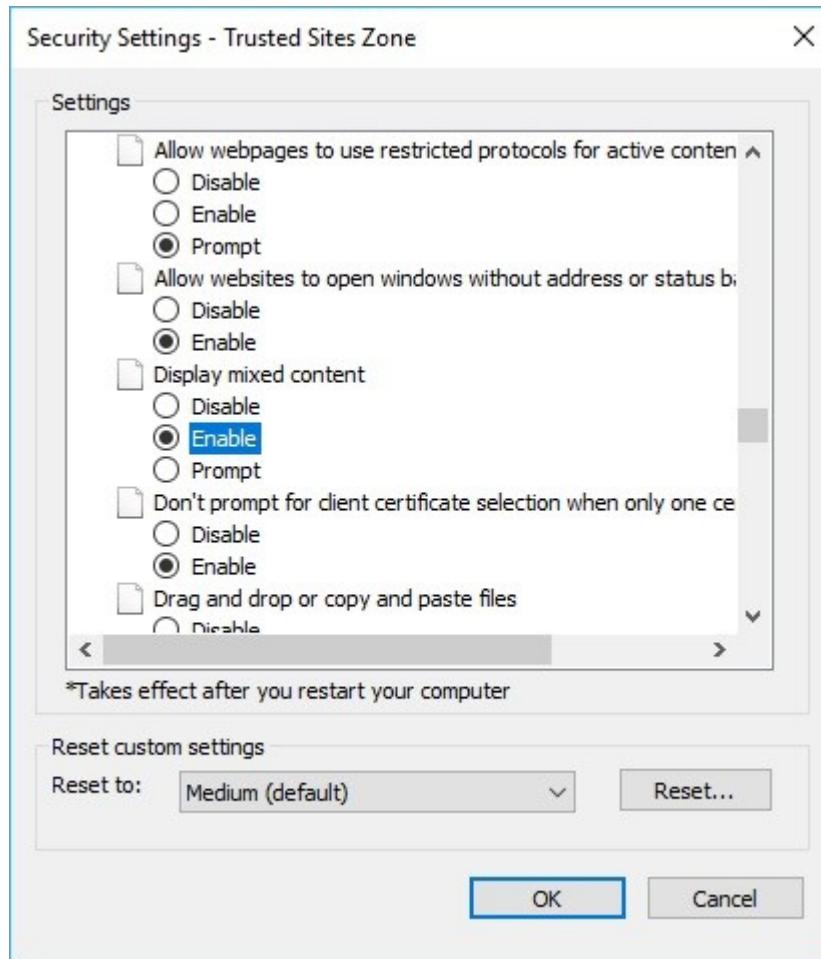


Figura 8 – Abilitazione visualizzazione contenuto misto per installazioni con HTTPS

7. confermare tramite il pulsante OK

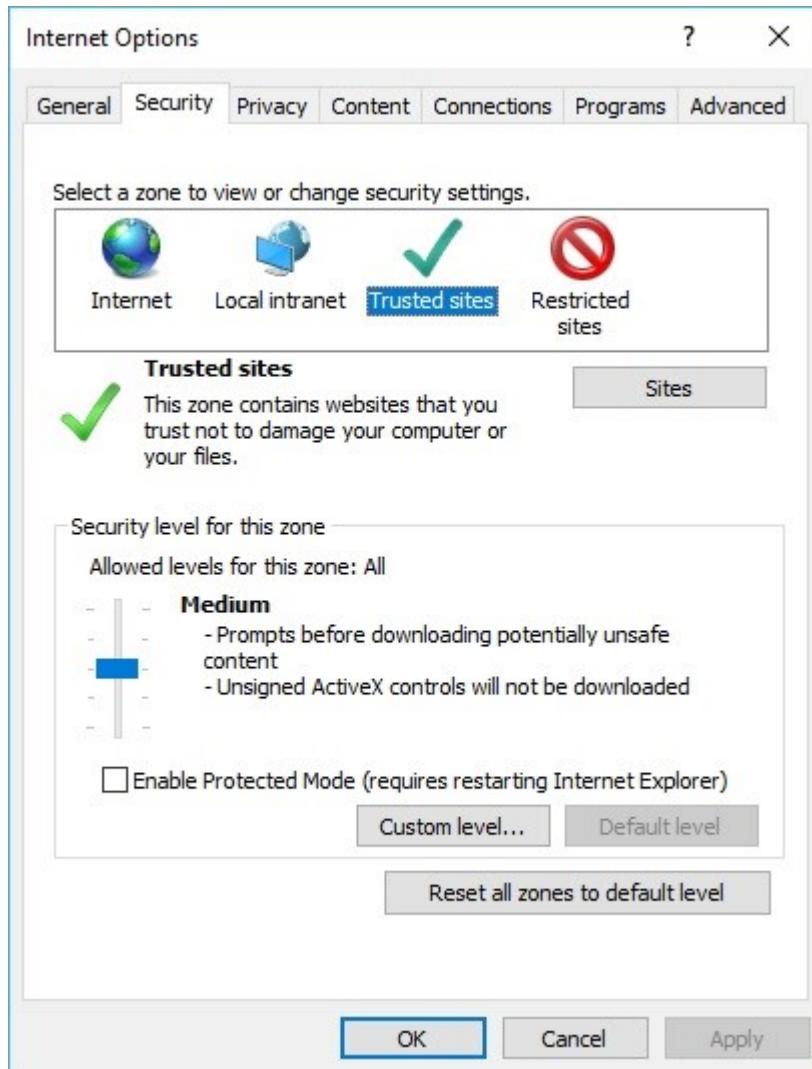


Figura 9 – Personalizzazione del livello di sicurezza Siti attendibili

8. selezionare la scheda **Avanzate** (*Advanced*)
9. scorrere la lista presentata fino a raggiungere la voce **Avvisa se si passa da modalità protetta a non protetta** (*Warn if changing between secure and not secure mode*) nella sezione **Sicurezza** (*Security*)
10. togliere, se presente, il segno di spunta.

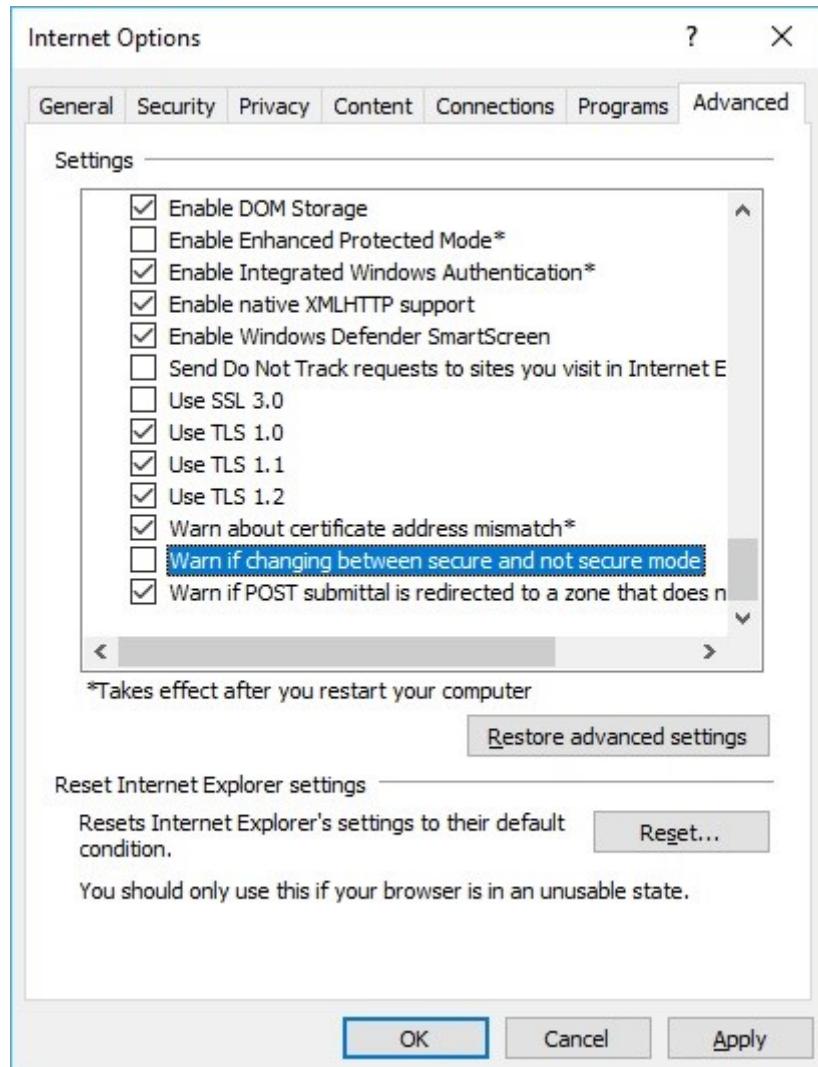


Figura 10 – Impostazione per non avvisare del passaggio da modo protetto a modo non protetto

Lasciare attivato l'avviso non comporta errori nell'applicazione, ma l'utente riceverà la seguente segnalazione ogni qualvolta si passa da un modo protetto ad un modo non protetto e viceversa.



Figura 11 – Messaggio della Security se il settaggio non è effettuato adeguatamente.

Attenzione, in virtù delle impostazioni effettuate il messaggio di cui alla Figura 12, verrà visualizzato solo al primo accesso al server di P.I.TRE. (questo in quanto i livelli di sicurezza sono stati abbassati) .

Il browser collegandosi ad un web server HTTPS, cercherà di validare il certificato ricevuto dal web server, se ci sono problemi di validità sarà visualizzato il messaggio di Figura 12

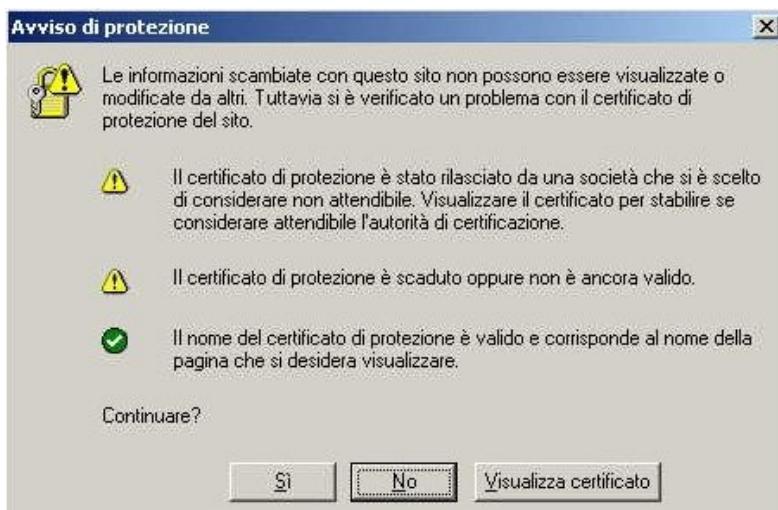


Figura 12 – Messaggio del Browser se il certificato del web server non è valido.

3.2.4 CONFIGURAZIONE INTERNET EXPLORER 11 AGGIUNTIVA PER JAVA APPLET, SMART CLIENTS, ACTIVE-X

Inoltre, il sito di amministrazione di P.I.TRE., va aggiunto fra i siti in “Configurazione visualizzazione compatibilità”. Dal menu Strumenti, selezionare la voce “Impostazioni di visualizzazione compatibilità” ed aggiungere il sito all’elenco.

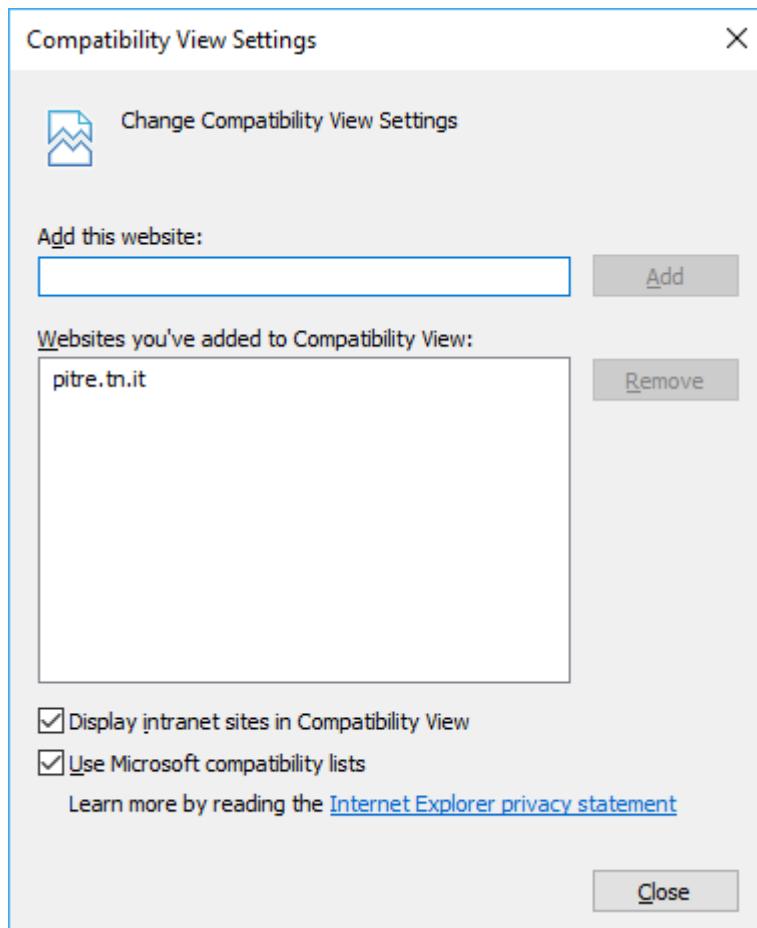


Figura 13 – Configurazione visualizzazione compatibilità (IE11)

3.2.5 CONFIGURAZIONE INTERNET EXPLORER 11 AGGIUNTIVA PER HTML5 SOCKET

Per un corretto funzionamento di P.I.Tre con questa configurazione necessita l'impostazione nella sezione **Sicurezza** (*Security*).

3.2.5.1 Configurazione del sito di P.I.Tre nella Intranet Locale

Per un corretto funzionamento di **P.I.Tre** necessita l'impostazione nella parte riguardante “Intranet locale”(/Local Intranet). Bisogna procedere come segue:

1. attraverso il menu **Strumenti** (Tools) selezionare **Opzioni Internet...**(*Internet options...*)
2. selezionare la scheda **Sicurezza** (*Security*)

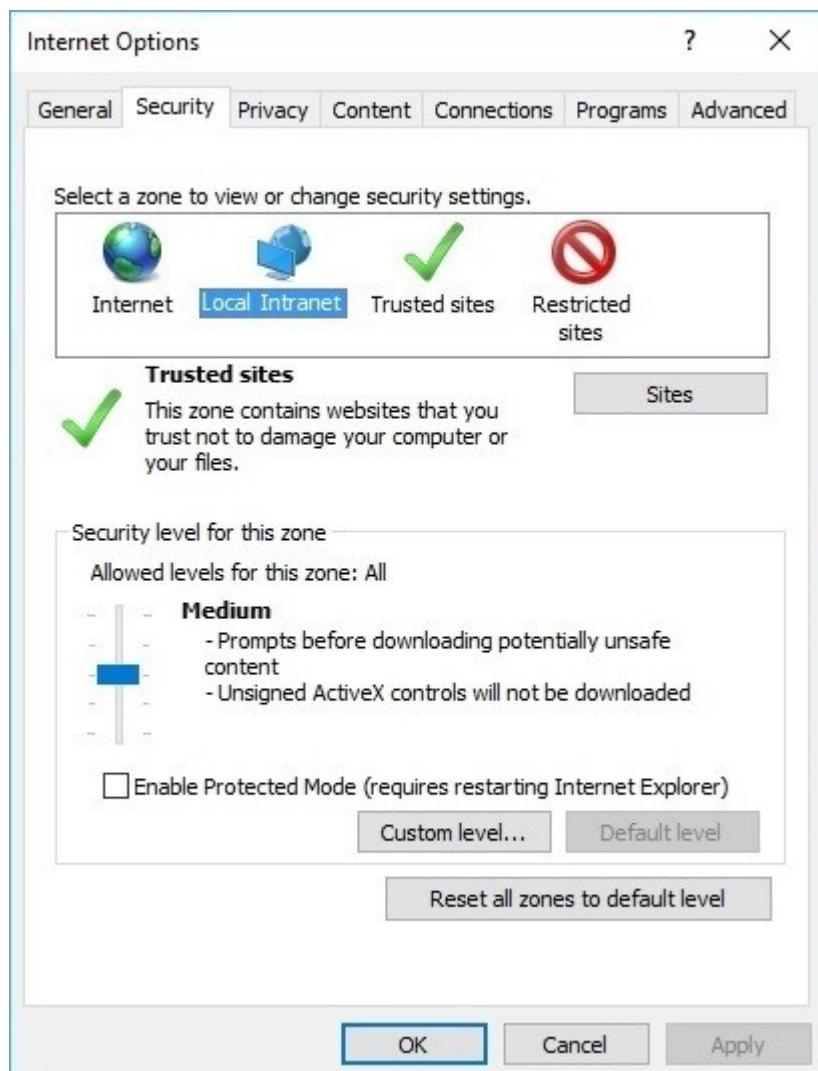


Figura 14 – Accesso alla scheda ‘Sicurezza’

3. selezionare **Intranet locale** (Local Intranet)
4. selezionare il pulsante **Siti...** (*Sites...*)
5. bisogna deselezionare la voce **Rileva Automaticamente rete Intranet** (*Automatically detect intranet network*)

6. a questo punto si abilitano le tre opzioni legate a **Rileva Automaticamente rete Intranet** (*Automatically detect intranet network*) bisogna deselectare il segno di spunta solo alla voce **Includi tutti i siti locali (Intranet) non elencati in altre aree** (*Include all local(intranet)sites not listed in other zones*)

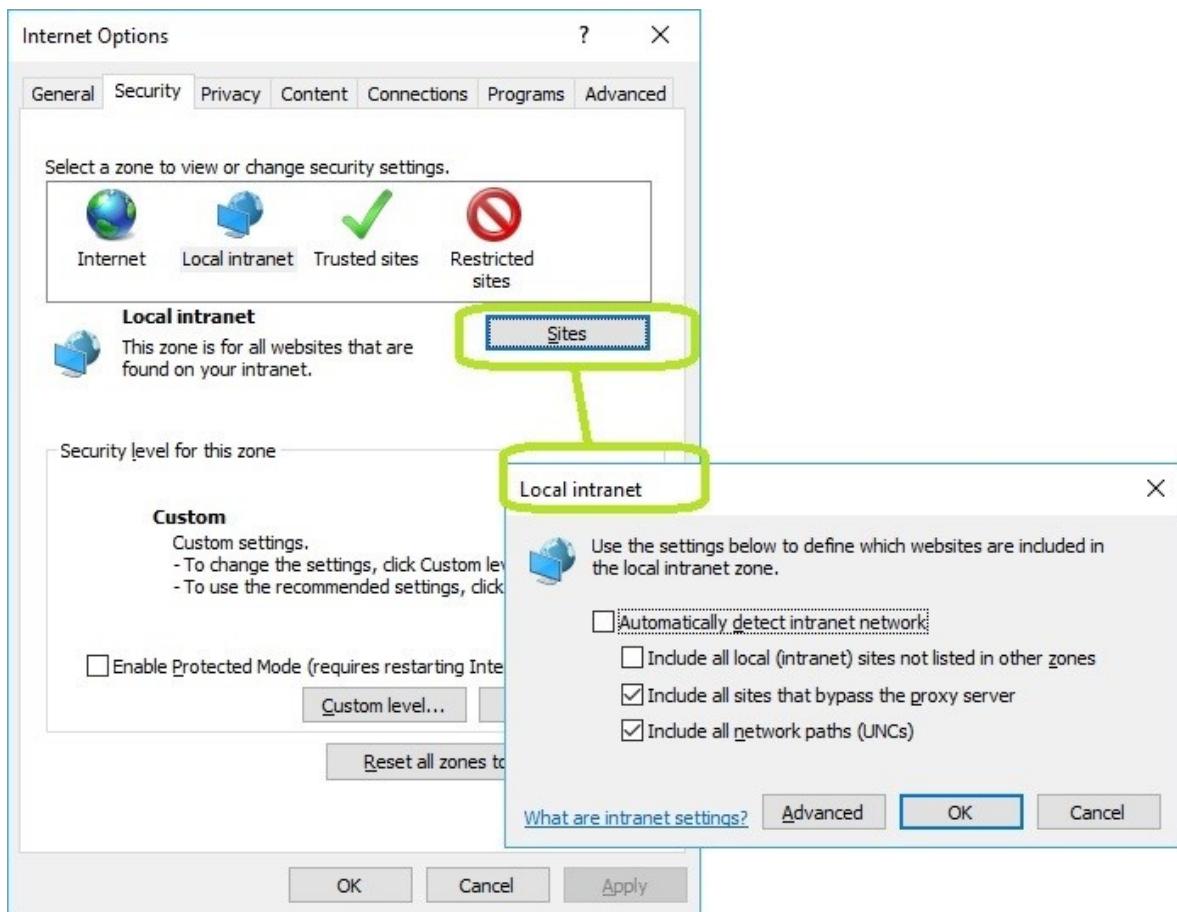


Figura 15 – Inserimento del server di P.I.Tre tra i siti attendibili

3.2.5.2 Configurazione del sito di P.I.Tre non in “Impostazioni Visualizzazione Compatibilità”

E' necessario che il sito del PiTre non sia in modalità di Visualizzazione compatibilità. Questo in quanto il browser funziona come fosse IE9, e sappiamo essere un browser obsoleto rispetto alla tecnologia d'utilizzo con “HTML5 Socket”.

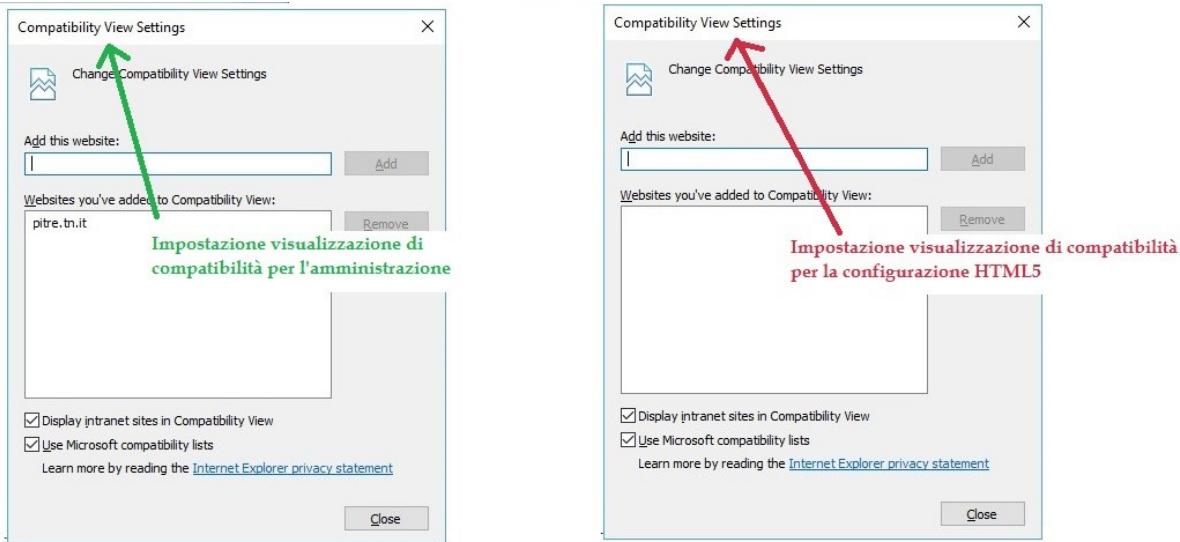


Figura 16 – Impostazioni Visualizzazione Compatibilità - come deve essere per HTML5

NOTA: Per la visualizzazione ed utilizzo corretto dell'amministrazione continua ad essere necessaria l'impostazione di visualizzazione in compatibilità

3.2.6 CONFIGURAZIONE AREA DI MEMORIA DEI FILE TEMPORANEI DEL BROWSER

Per un corretto funzionamento dell'applicativo P.I.TRE., si consiglia di impostare l'area di memoria dei File temporanei nel seguente modo.

1. attivare il browser Internet Explorer
2. attraverso il menu **Strumenti** (Tools), selezionare **Opzioni Internet...** (Internet Options...)
3. selezionare la scheda **Generale** (General)
4. cancellare tutto il contenuto dell'area come mostrato in Figura 17
5. impostare la gestione dell'area di memoria dei file temporanei come mostrato in Figura 18

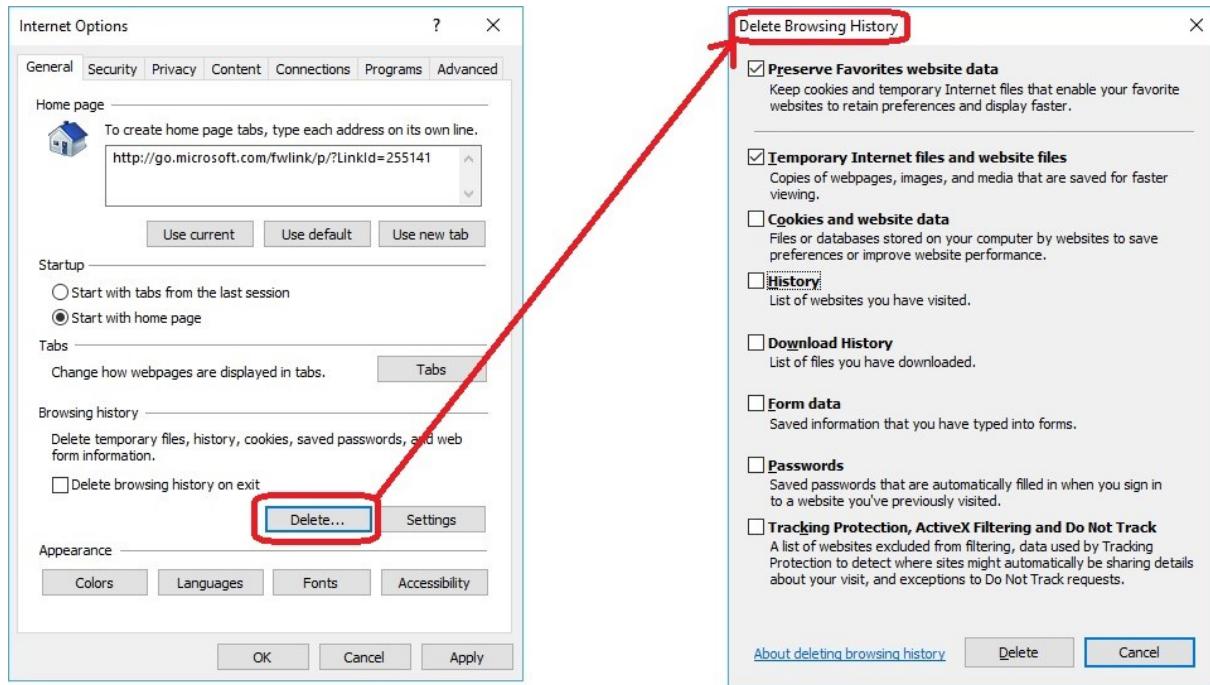


Figura 17 – Eliminazione file temporanei del browser

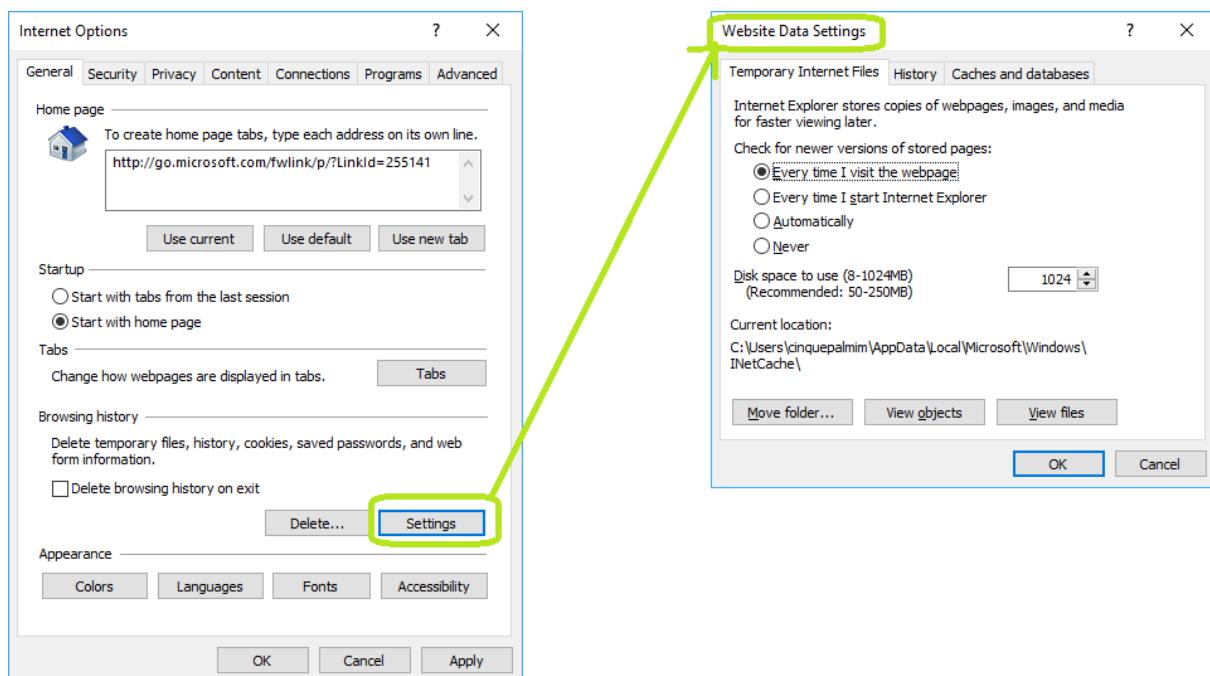


Figura 18 – Impostazione gestione area di memoria dei file temporanei del Browser

3.3 CONFIGURAZIONE INTERNET EXPLORER 10

Per il browser Internet Explorer 10, valgono le indicazioni illustrate per Internet Explorer 11.

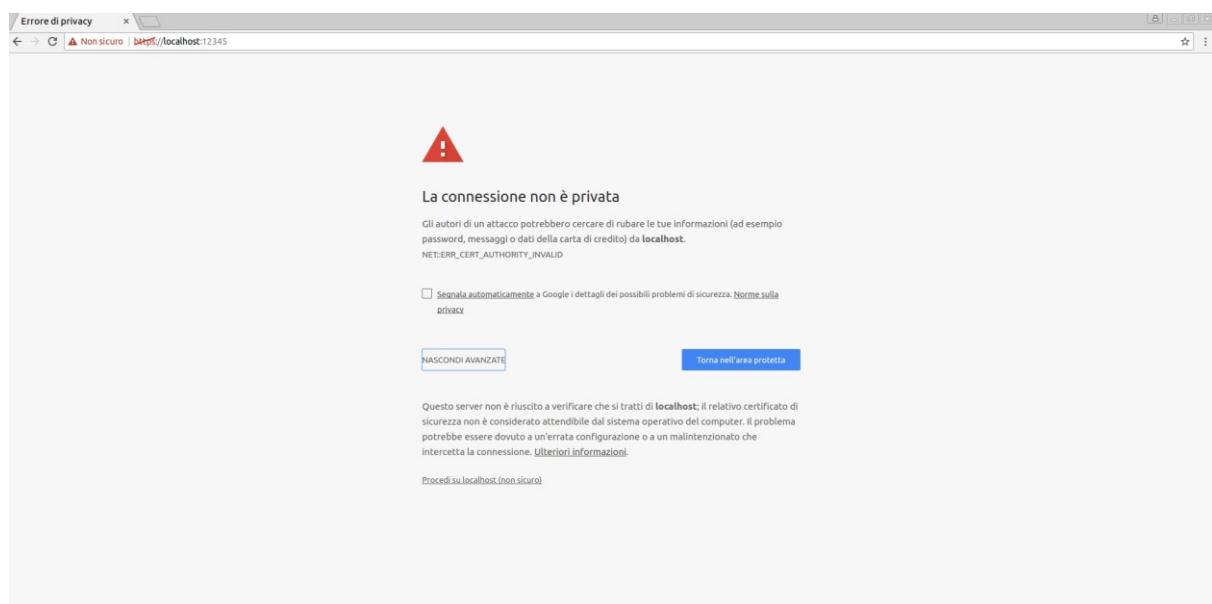
3.4 CONFIGURAZIONE CHROME PER HTML5 SOCKET

Il browser Chrome ha necessità dell'aggiunta di un'eccezione per il certificato sull'indirizzo **https://localhost:12345/**.

3.4.1 ECCEZIONE CHROME

Per il Browser Chrome, è necessario aggiungere nel seguente modo un'eccezione. Vediamo nello specifico i passaggi necessari per conseguire l'aggiunta di questa:

- Nel browser si inserisce nella barra di navigazione l'indirizzo **https://localhost:12345/** (vedi Figura 19).
- Nella pagina che si visualizza è presente un link **Procedi su localhost (non sicuro)** (Vedi Figura 20), bisogna selezionare tale tasto. A questo punto si visualizza una finestra in cui è presente un tasto “**Aggiungi Eccezione..**”, premere su di esso .



- *Figura 19 – Chrome - Connessione non sicura*

Se il browser Chrome subisce un aggiornamento manuale o automatico è necessario rifare la configurazione appena descritta

3.5 CONFIGURAZIONE FIREFOX PER HTML5 SOCKET

Il browser Firefox ha necessità dell'aggiunta di un'eccezione per il certificato sull'indirizzo **https://localhost:12345/**.

3.5.1 ECCEZIONE FIREFOX

Per il Browser FireFox, è necessario aggiungere nel seguente modo un'eccezione. Vediamo nello specifico i passaggi necessari per conseguire l'aggiunta di questa:

- Nel browser si inserisce nella barra di navigazione l'indirizzo **https://localhost:12345/** (vedi Figura 20).
- Nella pagina che si visualizza è presente un tasto **Avanzate** (Vedi Figura 20), bisogna selezionare tale tasto. A questo punto si visualizza una finestra in cui è presente un tasto “**Aggiungi Eccezione..**”, premere su di esso (Vedi Figura 21).
- Il browser visualizza una nuova finestra “**Aggiungi eccezione di sicurezza**”, si seleziona il tasto Conferma eccezione di sicurezza (Vedi Figura 22).

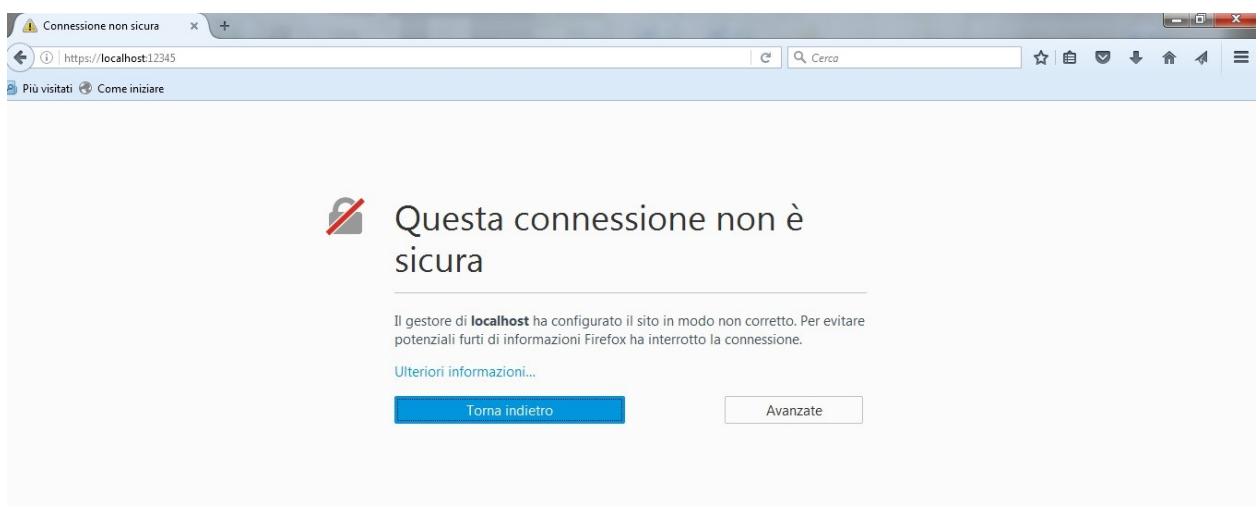


Figura 20 – FireFox - Connessione non sicura

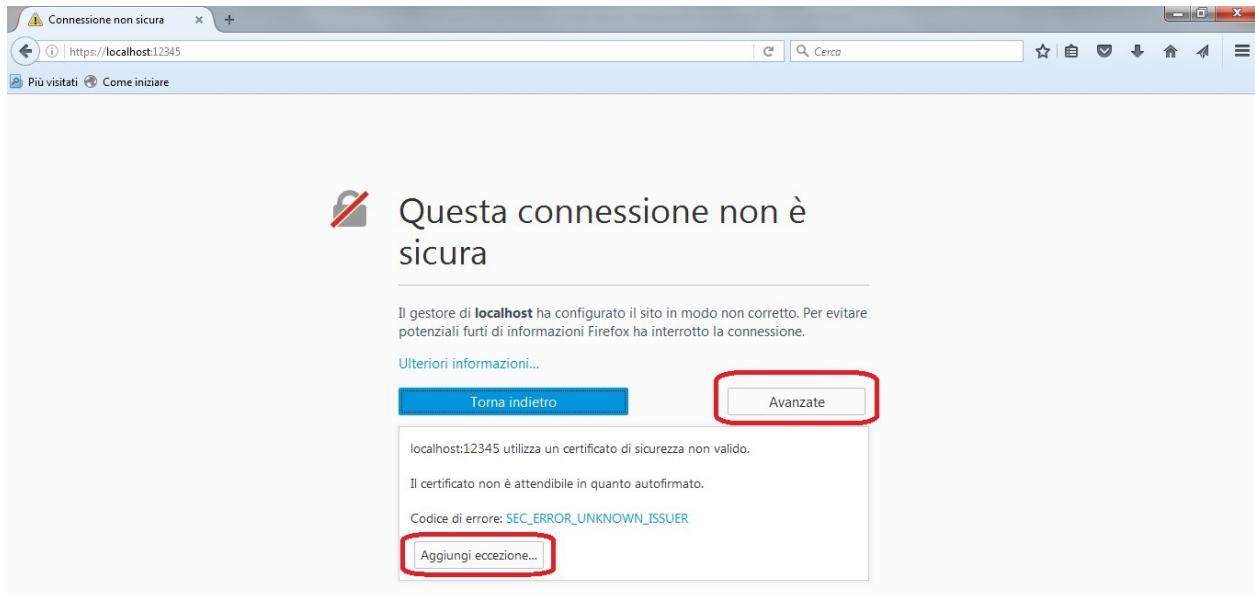


Figura 21 – FireFox - Impostazioni Avanzate

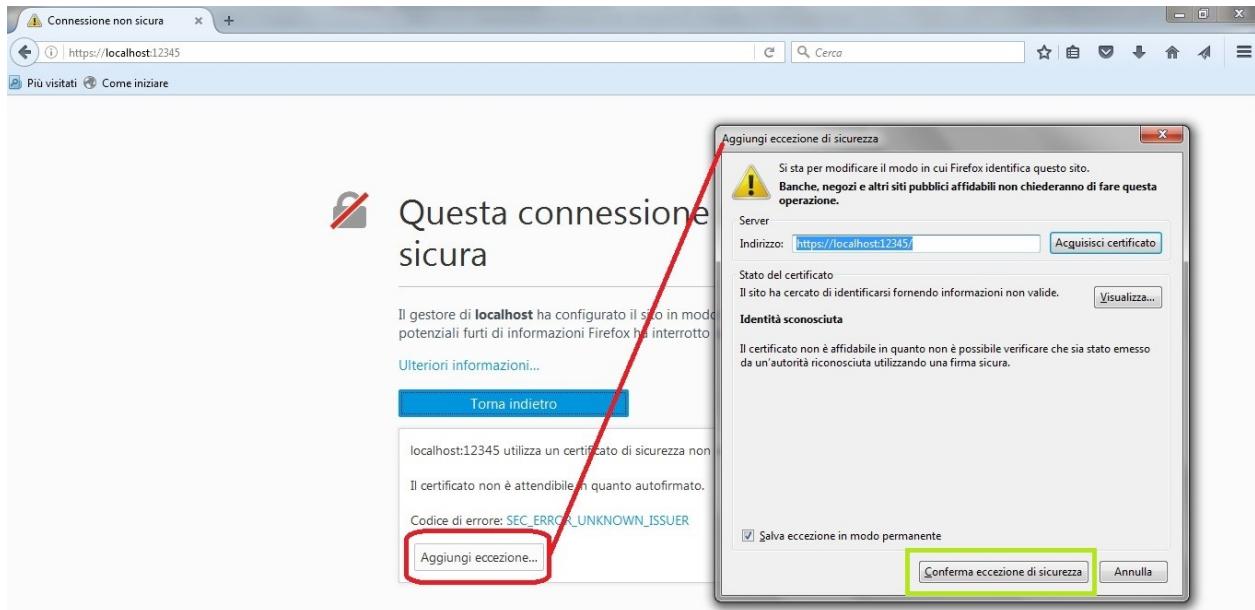


Figura 22 – FireFox - Conferma Eccezione

Anche se dal browser si dovesse visualizzare il messaggio di *connessione sicura non riuscita*, il browser riuscirà a gestire l'eccezione (vedi Figura 23).

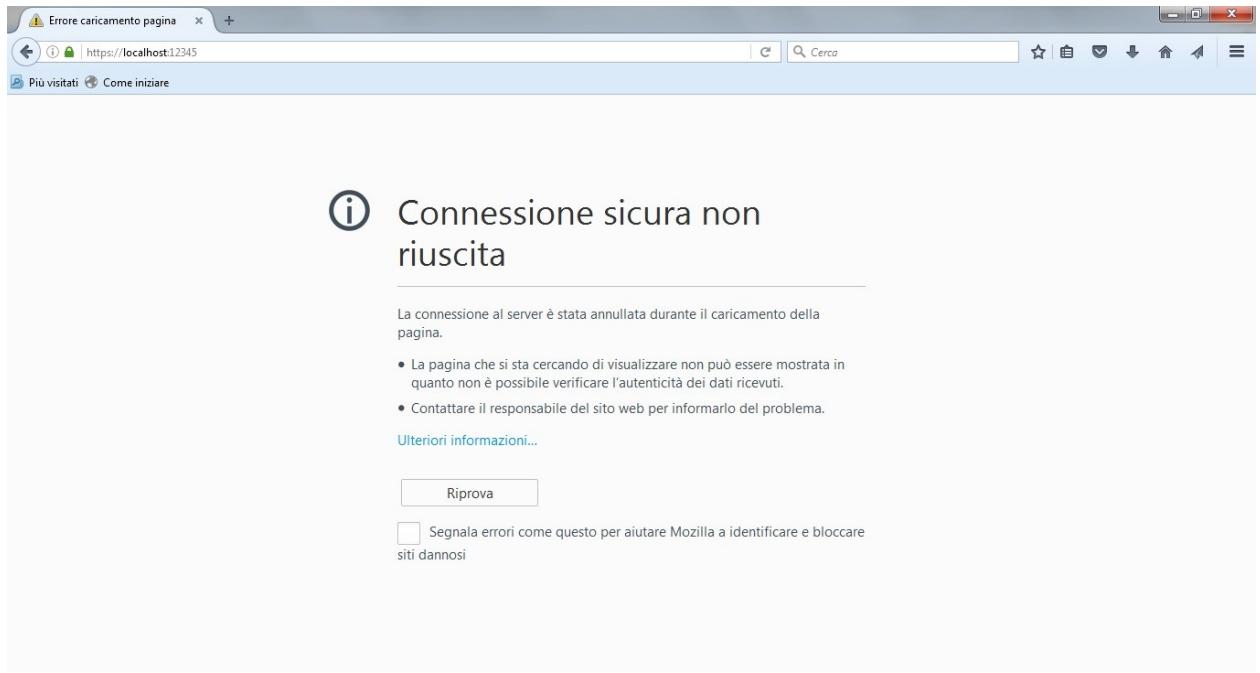


Figura 23 – FireFox - Errore caricamento pagina

Se il browser Chrome subisce un aggiornamento manuale o automatico è necessario rifare la configurazione appena descritta

4 INSTALLAZIONE CLIENTCOMPONENTS

Per eseguire l'installazione dei Client Components, copiare dalla cartella <pathWa>\frontend\activex\SETUP_EXE il file ClientComponents.exe ed eseguirlo in locale.

Su sistema Windows 7 è necessario eseguire manualmente il comando attraverso un prompt dei comandi in modalità Amministratore (Clic destro -> Esegui come Amministratore) (Figura 34) e scrivendo il percorso completo del file.

Il sistema apre una maschera di comando dos, indicazione che l'installazione si è avviata. Quando la maschera si chiude l'installazione è terminata, verificare se l'installazione è avvenuta con successo controllando che nel seguente percorso siano presenti le cartelle riportate in Figura 24 ciascuna contenente l'omonimo file .dll o .ocx¹:

C:\Program Files(o programmi)\ValueTeam S.p.A\ DocsPa_ClientComponents2.6

Affinchè i clientcomponents possano funzionare correttamente con Microsoft .NET Framework4.5, è necessario installare il file PatchFramework4.5.reg.

¹ Nella cartella DocsPa_AcquisisciDoc sarà presente anche il file Settings.ini

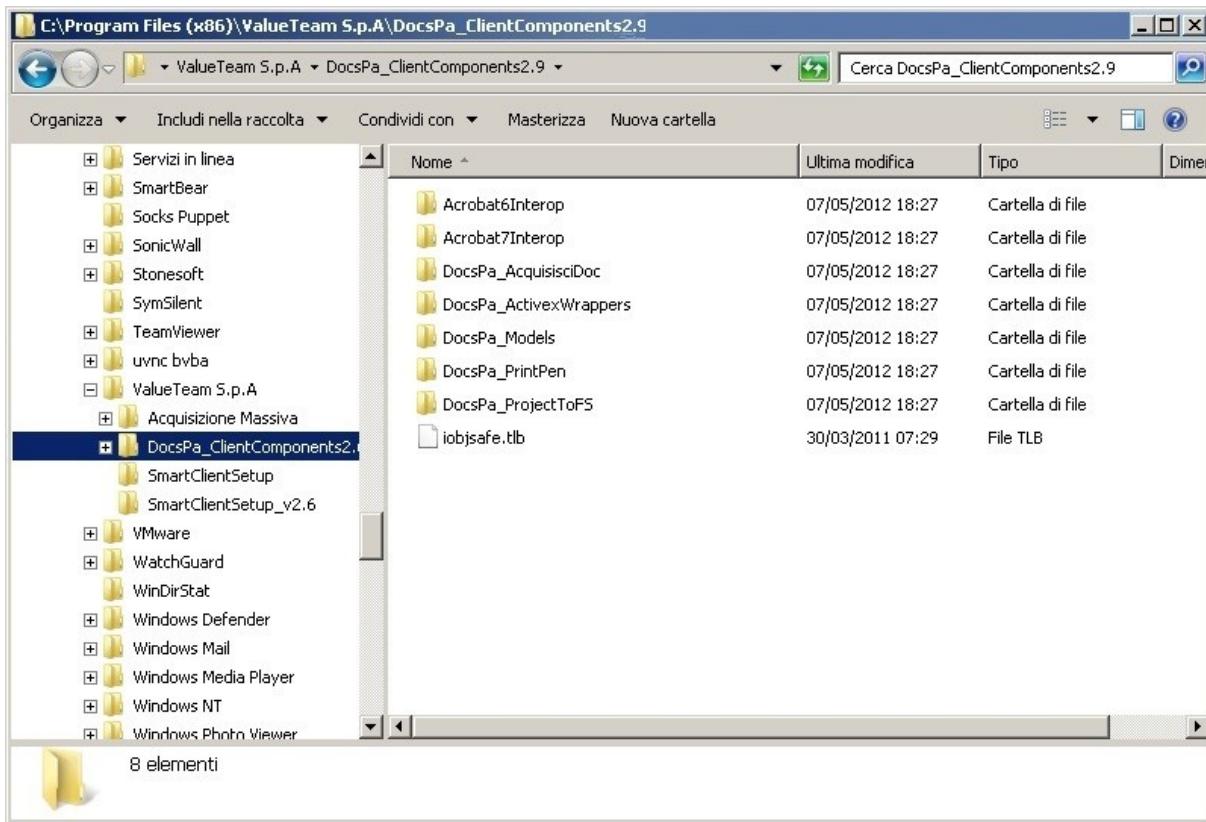


Figura 24 – Verifica installazione ClientComponents

5 CONFIGURAZIONE GENERALE HTML5 SOCKET

5.1 INSTALLAZIONE CONNETTORE WINDOWS

Nota: le procedure di seguito descritte vanno eseguite da utente amministratore della postazione.

5.1.1 PROCEDURA STANDARD

E' possibile prendere il pacchetto di istallazione necessario al corretto funzionamento del sistema P.I.Tre con la configurazione *html5 socket*, tramite:

- PiTre al primo accesso dell'utente html5 socket (al primo accesso dalla configurazione o se la versione istallata del connettore è differente da quella attualmente in uso vedi Figura 25);
- scaricando direttamente dal link che verrà successivamente comunicato



Figura 25 – scarico connettore da PiTre

Il sistema provvederà a scaricare l'istallazione guidata del Web Client Connector, mentre l'utente dovrà procedere all'istallazione così come mostrato dalla Figura 26, Figura 27, Figura 28, Figura 29

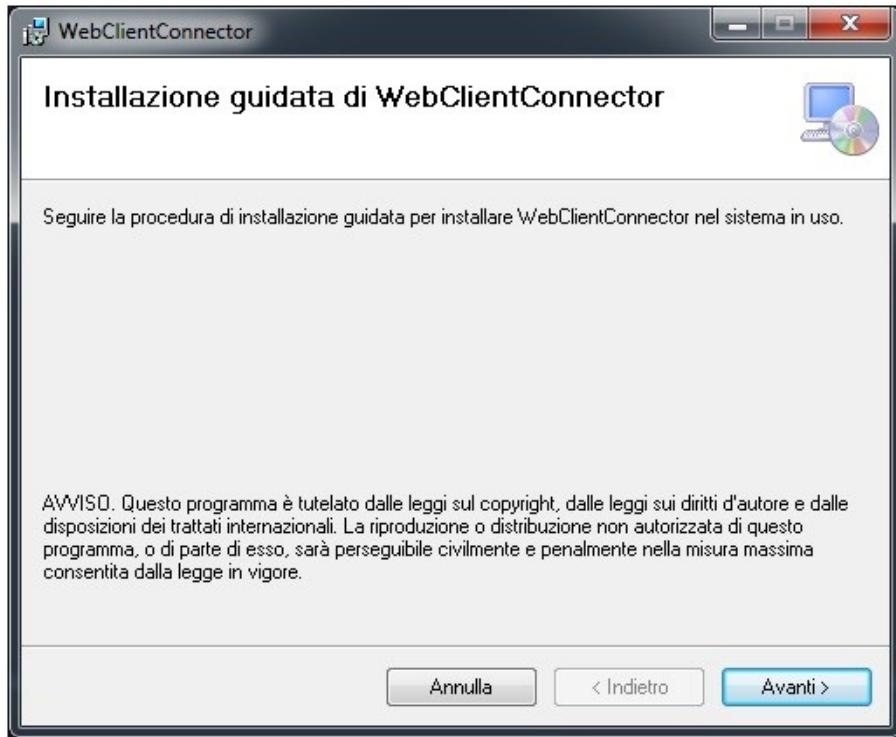


Figura 26 – Installazione Guidata connettore: step 1



Figura 27 – Installazione Guidata connettore: step2

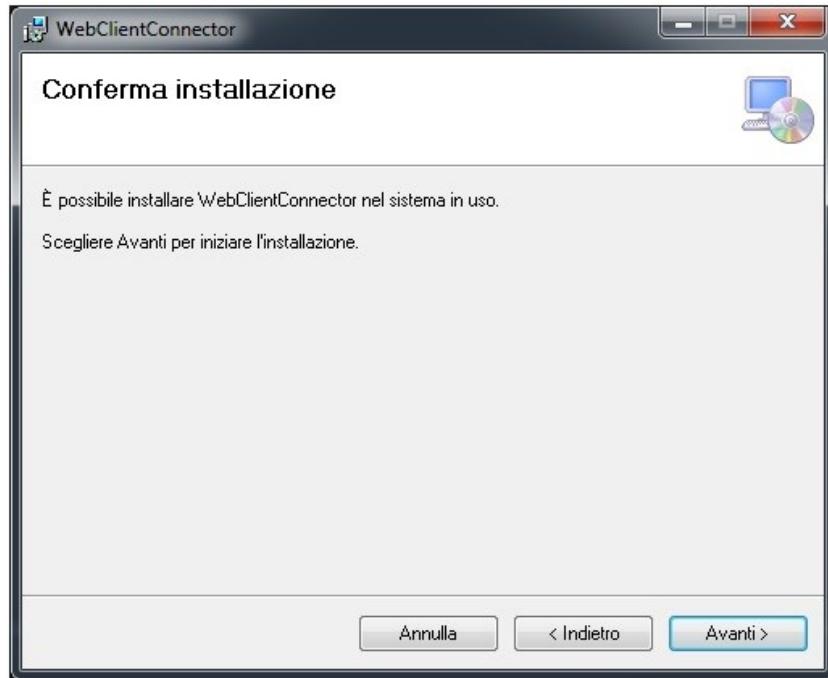


Figura 28 – Installazione Guidata connettore: step3

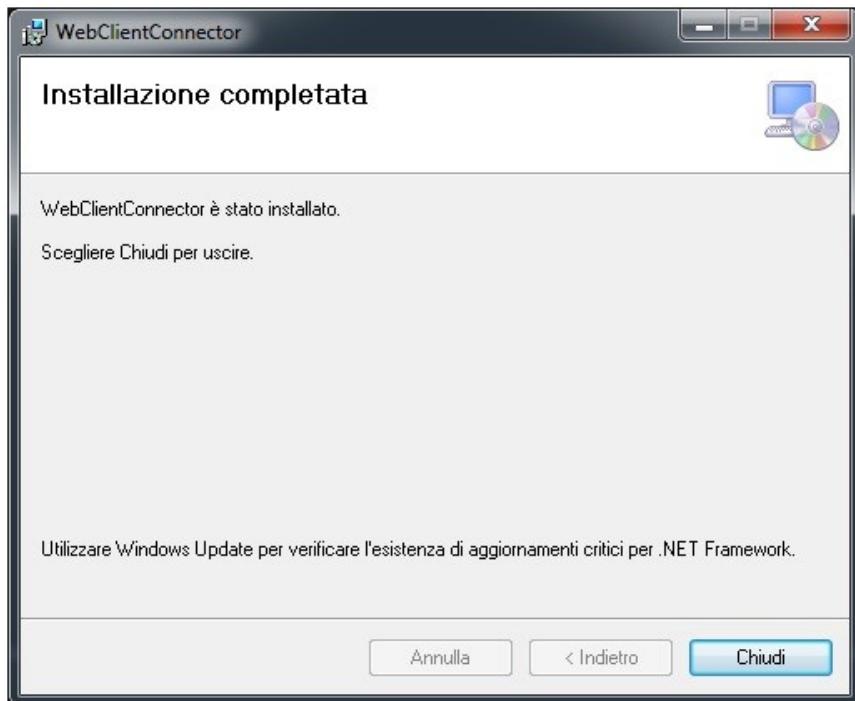


Figura 29 – Installazione Guidata connettore: step4

Al termine dell'installazione si deve effettuare il riavvio della macchina e la configurazione necessaria in base al browser d'utilizzo.

5.1.1.1 Configurazione del sito di P.I.Tre non in “Impostazioni Visualizzazione Compatibilità”

E' necessario che il sito del PiTre non sia in modalità di Visualizzazione compatibilità. Questo in quanto il browser funziona come fosse IE8, e sappiamo essere un browser obsoleto rispetto alla tecnologia d'utilizzo con “HTML5 Socket”.

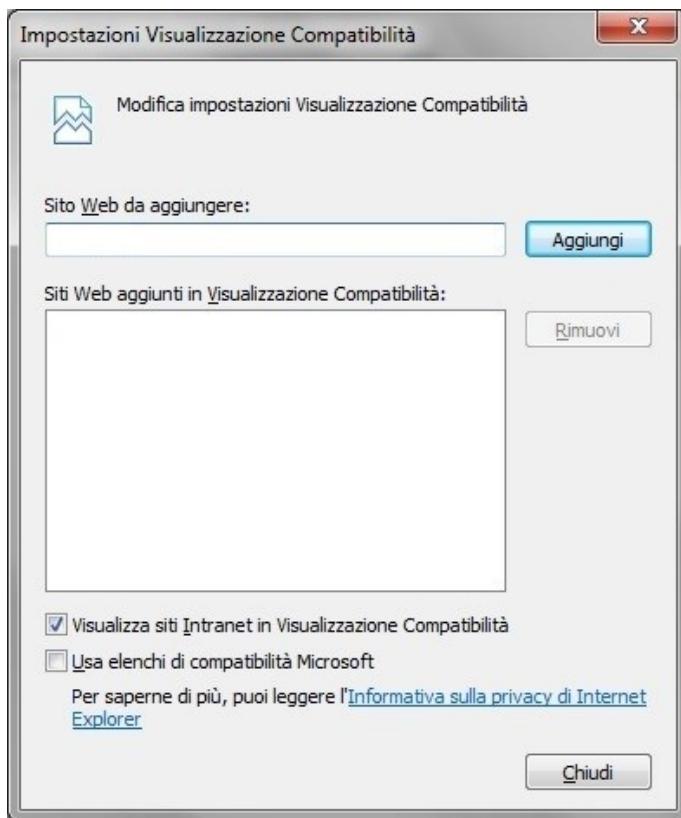


Figura 30 – Impostazioni Visualizzazione Compatibilità - come deve essere

NOTA: Per la visualizzazione ed utilizzo corretto dell'amministrazione continua ad essere necessaria l'impostazione di visualizzazione in compatibilità

5.2 INSTALLAZIONE CONNETTORE UBUNTU

Nota: le procedure di seguito descritte vanno eseguite da utente amministratore della postazione.

5.2.1 PROCEDURA STANDARD

E' possibile prendere il pacchetto di istallazione necessario al corretto funzionamento del sistema P.I.Tre con la configurazione *html5 socket*, tramite:

- PiTre al primo accesso dell'utente html5 socket (al primo accesso dalla configurazione o se la versione istallata del connettore è differente da quella attualmente in uso vedi Figura 31);
- scaricando direttamente dal link che verrà successivamente comunicato



Figura 31 – scarico connettore da PiTre

Il pacchetto che si chiama : “ **WebClientConnector.tar.gz**” si compone di una cartella (WebClientConnector) e di un file affiancato alla cartella che si chiama: “**setup.sh**”.

L'installazione si lancia da terminale.

- Da terminale si digita il comando cd nella cartella dove sono presenti i due componenti (cartella e file affiancati altrimenti non funziona).
- Poi si lancia /bin/sh setup.sh

- A questo punto è necessario riavviare il pc.
- Sempre da terminale si digita : "ps aux | grep WebClientConnector" per controllare se è partito il componente, se si visualizza più di una riga l'installazione è andata a buon fine.

Una volta che la procedura d'installazione è terminata con esito positivo occorre configurare il browser Firefox così come descritto nel paragrafo: 3.5 .

6 INSTALLAZIONE DEI DISPOSITIVI

Nota: le procedure di seguito descritte vanno eseguite da utente amministratore della postazione cui si vuole collegare il dispositivo.

6.1 CONFIGURAZIONE DELLO SCANNER

Per l'utilizzo dello scanner è necessaria l'installazione di SmartClient. Per i dettagli relativi si veda oltre il paragrafo “6.5 - Installazione e configurazione di SmartClient”.

6.2 CONFIGURAZIONE DEI DISPOSITIVI DI STAMPA SU PORTA SERIALE

Posto che su una data postazione può essere installato soltanto un tipo di dispositivo di stampa (ossia uno solo fra timbro, stampante a penna, stampante di etichette), è sufficiente che sulla postazione siano stati installati i ClientComponents (si veda par. 4).

6.3 CONFIGURAZIONE STAMPANTI ZEBRA SU PORTA USB

Posto che su una data postazione può essere installato soltanto un tipo di dispositivo di stampa (ossia uno solo fra timbro, stampante a penna, stampante di etichette), di seguito sono riportati i passi da effettuare sulla postazione client cui viene collegato il dispositivo in esame.

6.3.1 PROCEDURA STANDARD

Per installare una stampante di etichette Zebra collegata ad una porta USB installare i driver della stampante forniti dal costruttore (i driver possono essere scaricati da internet dal sito www.zebra.com).

Se la postazione utilizza gli ActiveX occorre inoltre eseguire le seguenti operazioni:

1. al termine dell'installazione dei driver da **Avvio (Start)**, selezionare la voce **Pannello di controllo (Control panel)** e **stampanti e fax (Printers)** selezionare le proprietà della stampante Zebra;

2. dalla scheda **Avanzate** (*Advanced*), accanto alla descrizione ‘Driver’ è presente un menu a tendina da cui si deve selezionare la voce “Generic / Text Only”;

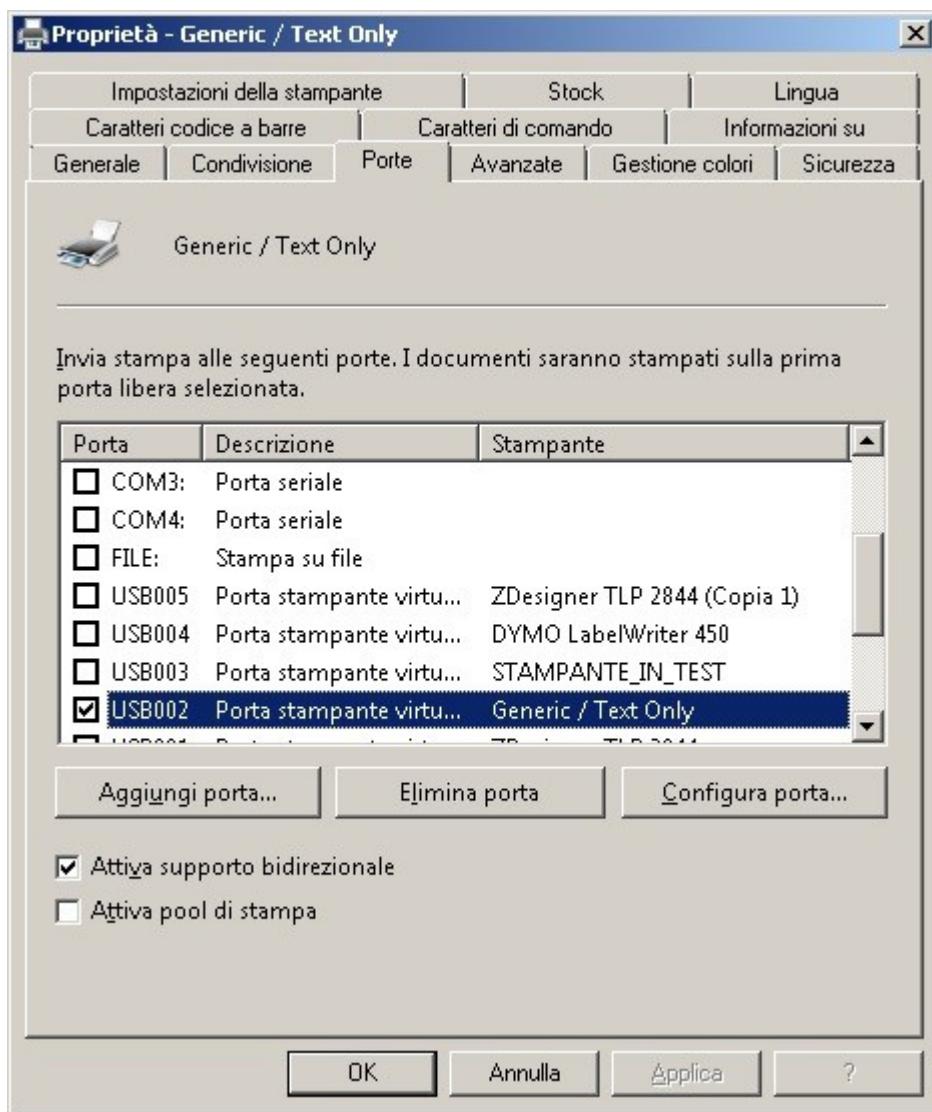


Figura 32 – Configurazione della porta USB per la stampante Zebra

3. salvare le impostazioni effettuate e chiudere la schermata con il Bottone **OK**;
4. nel caso in cui la voce “Generic / Text Only”, non compaia nel menu a tendina di cui al punto 3, premere il pulsante **Nuovo Driver** (*New driver ...*), avviare l’installazione del driver tramite il programma wizard, selezionare come:
 - **Produttore (Manufacturer)** → ‘Generale’ (*Generic*);
 - **Stampanti (Printers)** → ‘Generic / Text Only’. Procedere poi come descritto nel punto 4;
5. attivare P.I.TRE., e richiedere la stampa dell’etichetta di un documento. Al momento in cui si utilizza la funzionalità di stampa il file cab viene

automaticamente scaricato, questo contiene le librerie (riconoscibili con i file di estensione dll) da registrare. Inoltre, sotto la directory WINNT viene copiato il file docspav2.ini (a tal proposito vedi paragrafo 6.3.1.1);

6. in caso di malfunzionamenti o di messaggi di errore verificare:
 - a. Le impostazioni di sicurezza sugli ActiveX come descritto precedentemente;
 - a. l'esistenza del file DocsPa_PrintPen.Timbro nella directory **C:\WINNT\Downloaded Program Files** [oppure da internet Explorer attraverso Strumenti → Opzioni Internet... → Generale → Impostazioni... → Visualizza Oggetti... (Tools → Internet Options... → General → Settings... → View Objects...)]
7. nel file docspav2.ini bisogna controllare il punto 2 e verificare le seguenti impostazioni:
 - b. USB_PRINT_MODE=S
 - c. USB_PRINTER_DEVICE_NAME=Generic / Text Only
8. se viene rinominato il dispositivo ‘Generic / Text Only’, modificare di conseguenza la stringa indicata al punto b del passo precedente.

6.3.1.1 Nota su docspav2.ini

Il file Web.config relativo al front end contiene due righe simili a quelle riportate qui di seguito:

```
<add key="DISPOSITIVO_STAMPA" value=""/>
<!--aggiunto url del file ini di configurazione del dispositivo -->

<add key="URL_INIFILE_DISPOSITIVO_STAMPA" value="http://<host>/DocsPaWA/activex/ini/<tip>/DocsPA.INI">
```

tali righe stabiliscono quale file .ini viene scaricato sulle postazioni client al momento in cui su queste viene configurato un dispositivo di stampa.

Settare il <tip> ad uno dei seguenti valori a seconda del dispositivo da installare:

Penna, Timbro, Etichette

Se durante l'esecuzione delle procedure indicate nei paragrafi precedenti non viene copiato il file docspav2.ini sotto C:\<directory_di_sistema_di_windows> (winnt o windows) occorre:

- prelevare dalla opportuna sottodirectory (Penna, Timbro, Etichette⁽¹⁾, BarCode⁽²⁾) di DocsPaWA\activex\INI il file **DocsPA.ini**;
- copiarlo sulla macchina su cui è installato il dispositivo, in C:\WINNT o C:\WINDOWS rinominandolo docspav2.ini.

Per le stampanti di etichette possono essere previsti vari tipi di configurazione all'interno del file .ini a seconda ad esempio delle dimensioni delle etichette o simili.

6.3.1.2 Descrizione file docspav2.ini

Il file docspav2.ini si compone di una serie di comandi che vengono inviati ad ogni stampa al dispositivo con cui si interfaccia P.I.TRE.. In particolare, si divide in due sezioni di comandi:

- la sezione [DISPOSITIVO]
- la sezione [SCRIPT]

Nella prima sezione sono contenuti i comandi, che regolano il protocollo di comunicazione con il dispositivo stesso.

Nella seconda sezione sono contenuti i comandi per configurare il formato dell'etichetta, di seguito viene illustrata una descrizione nel caso di uso di stampanti Zebre della famiglia TPL..

Per una descrizione completa dei comandi del linguaggio di comando per le stampanti Zebra, denominato, "EPL", si rimanda alla documentazione fornita dal produttore stesso.

6.3.1.2.1 Comando di tipo A

Questo comando permette di stampare una stringa di caratteri ASCII su una singola linea

Sintassi: **Ap1,p2,p3,p4,p5,p6,p7,"DATA"**

Descrizione: stampa la stringa "**DATA**".

Parametri:

p1 = punto di partenza orizzontale (X).

p2 = punto di partenza verticale (Y).

p3 = angolo di rotazione

valore	descrizione
0	Nessuna rotazione
1	90 gradi
2	180 gradi
3	270 gradi

p4 = dimensione del Font

valore	Descrizione	
	203 dpi	300 dpi
1	20.3 cpi, 6 pts, (8 x 12 dots)	25 cpi, 4 pts, (12 x 20 dots)

2	16.9 cpi, 7 pts, (10 x 16 dots)	18.75 cpi, 6 pts, (16 x 28 dots)
3	14.5 cpi, 10 pts, (12 x 20 dots)	15 cpi, 8 pts, (20 x 36 dots)
4	12.7 cpi, 12 pts, (14 x 24 dots)	12.5 cpi, 10 pts, (24 x 44 dots)
5	5.6 cpi, 24 pts, (32 x 48 dots)	6.25 cpi, 21 pts, (48 x 80 dots)
A - Z	Valori Riservati	Valori Riservati

p5 = incrementa dimensione orizzontale del testo . Valori: 1, 2, 3, 4, 5, 6, e 8.

p6 = incrementa dimensione verticale del testo. Valori: 1, 2, 3, 4, 5, 6, 7, 8, e 9.

p7 N= testo nero su sfondo bianco o **R** testo bianco su sfondo nero

"DATA" = Testo da stampare.

6.3.1.2.2 Comando di tipo B

Questo comando permette di stampare codici a barre standard su una singola linea

Sintassi: **Bp1,p2,p3,p4,p5,p6,p7,p8,"DATA"**

Descrizione: comando per stampare codici a barre standard.

Parametri:

p1 = punto di partenza orizzontale (X).

p2 = punto di partenza verticale (Y).

p3 = angolo di rotazione

valore	descrizione
0	Nessuna rotazione
1	90 gradi
2	180 gradi
3	270 gradi

p4 = tipo di codice a barre

p5 = distanza tra due single righe del codice a barre, maggiore è il valore più le righe sono vicine.

Tipo di codice a barre	P4	P5
Code 39 std. or extended	3	1-10
Code 39 with check digit	3C	1-10
Code 93	9	1-10
Code 128 UCC Serial Shipping Container Code	0	1-10
Code 128 auto A, B, C modes	1	1-10
Code 128 mode A	1A	1-10
Code 128 mode B	1B	1-10

Code 128 mode C	1C	1-10
Codabar	K	1-10
EAN8	E80	2-4
EAN8 2 digit add-on	E82	2-4
EAN8 5 digit add-on	E85	2-4
EAN13	E30	2-4
EAN13 2 digit add-on	E32	2-4
EAN13 5 digit add-on	E35	2-4
German Post Code	2G	3-4
Interleaved 2 of 5	2	1-10
Interleaved 2 of 5 with mod 10 check digit	2C	1-10
Interleaved 2 of 5 with human readable check digit	2D	1-10
Postnet 5, 9, 11 & 13 digit1	P	—
Planet 11 & 13 digit1	PL	—
Japanese Postnet	J	—
UCC/EAN 1282	1E	1-10
UPC A	UA0	2-4
UPC A 2 digit add-on	UA2	2-4
UPC A 5 digit add-on	UA5	2-4
UPC E	UE0	2-4
UPC E 2 digit add-on	UE2	2-4
UPC E 5 digit add-on	UE5	2-4
UPC Interleaved 2 of 5	2U	1-10
Plessey (MSI-1) with mod. 10 check digit	L	—
MSI-3 with mod. 10 check digit	M	—

p6 = larghezza di una singola barra del codice a barre, valori da 2 a 30.

p7 = altezza di una singola barra del codice a barre.

p8 = stampa di un codice a barre leggibile dall'uomo o no, valori: **B**=yes or **N**=no.

"DATA" = stringa contenente i valori da stampare codificati nel codice.

6.3.2 INSTALLAZIONE SU SISTEMI WINDOWS 7 A 32 O 64 BIT

Per questi nuovi sistemi è innanzitutto necessario installare il nuovo driver “Zebra Designer Driver (32 bit/64 bit, Windows Certified)” reperibili sul sito [www.zebra.com](http://www.zebra.com/id/zebra-na/en/index/drivers_downloads/drivers/results.html?productType=7)

Il file “MSCOMM32.OCX” va copiato nella cartella “c:\windows\system32\” se il sistema è a **32bit** oppure nella cartella “c:\windows\sysWow64\” se il sistema è a **64bit**
Avviare quindi il prompt dei comandi in modalità amministratore:

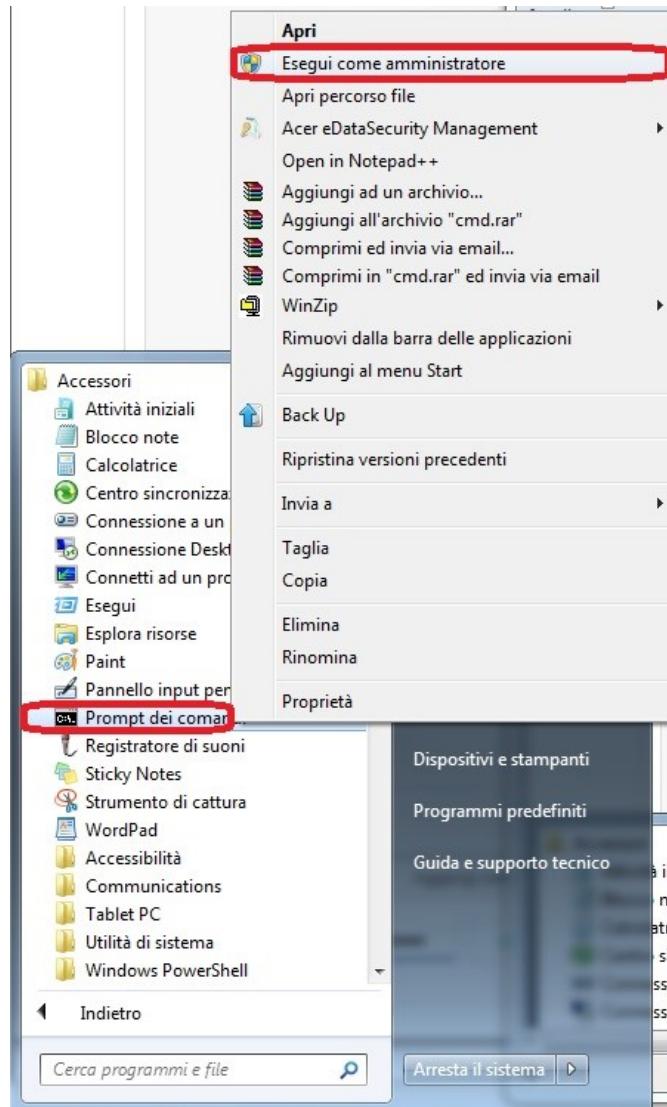


Figura 33 – Prompt dei comandi richiamato come Amministratore

Dal prompt registrare la libreria con il comando:

Regsvr32 c:\windows\system32\mscomm32.ocx
Regsvr32 c:\windows\sysWow64\mscomm32.ocx

per sistemi a 32bit
per sistemi a 64bit

Il file docspav2.ini va messo sempre nella cartella “c:\windows\”

6.4 INSTALLAZIONE E CONFIGURAZIONE DELLE STAMPANTINE DYMO

Per installare una stampante di etichette Dymo occorre installare i driver forniti dal costruttore. La configurazione viene invece eseguita lato server (si veda Appendice 1).

6.5 INSTALLAZIONE E CONFIGURAZIONE DI SMARTCLIENT

Il componente SmartClient è necessario per l'interfacciamento con le periferiche accessibili dalle postazioni client (con il software twain dello scanner, con i dispositivi di firma digitale,). È installabile su tutti i sistemi operativi da Windows XP SP3 in poi. È necessario per i sistemi Windows 7.

Tale componente non è certificata su Windows VISTA.

Come **prerequisito** richiede l'installazione sulla macchina del framework .NET 4.5 (disponibile eventualmente sul sito Microsoft).

E' inoltre necessario che sulla macchina siano installati i driver forniti dalla casa costruttrice dello scanner secondo le procedure del fornitore.

Per installare il componente Smart Client utilizzare il pacchetto contenente il setup fornito da NTTDATA (SmartClientSetup).

E' necessario eseguire manualmente il comando *install.bat* attraverso un prompt dei comandi in modalità Amministratore (Clic destro -> Esegui come Amministratore) e scrivendo il percorso completo del file install (ad esempio C:\Users\<utentexyz>\SmartClient\install.bat).

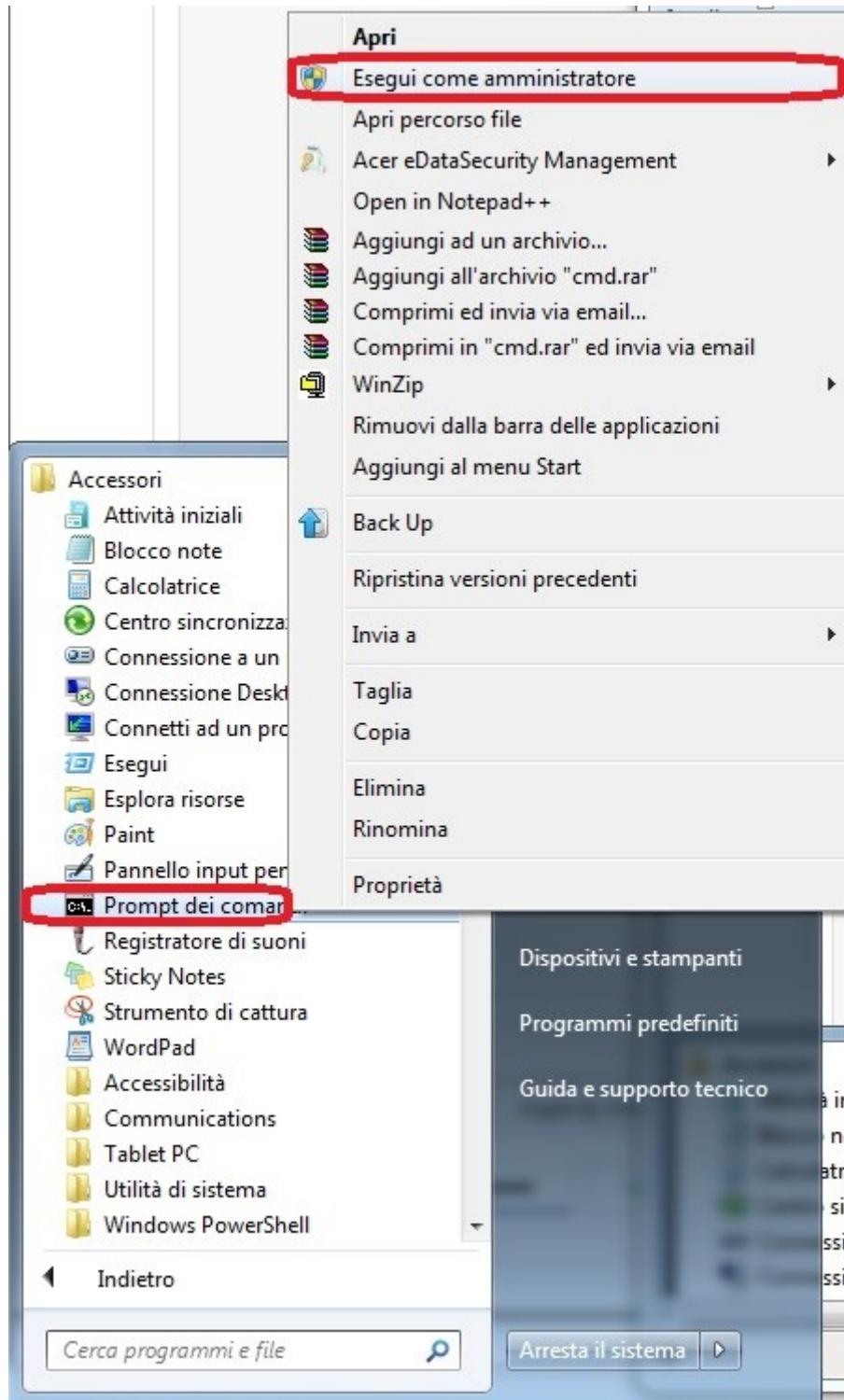


Figura 34 – Installazione SmartClient (Windows 7)

Il sistema apre una maschera di comando dos, indicazione che l'installazione è stata avviata.

Quando la maschera si chiude l'installazione è terminata, verificare se l'installazione è avvenuta con successo eseguendo i seguenti controlli:

1. Controllare il file *install.log* contenuto nella medesima cartella del file *install.bat* e verificare che nelle ultime righe vi sia scritto -- installazione completata --.

Nota: se sul sistema è già installata una precedente versione, eseguire prima *l'uninstall.bat*, così da disinstallarlo e poi ripetere il passo 1.

2. Controllare che nel seguente percorso siano presenti i files indicati nella figura sottostante:

C:\Program Files(o programmi)\ValueTeam S.p.A\SmartClientSetup

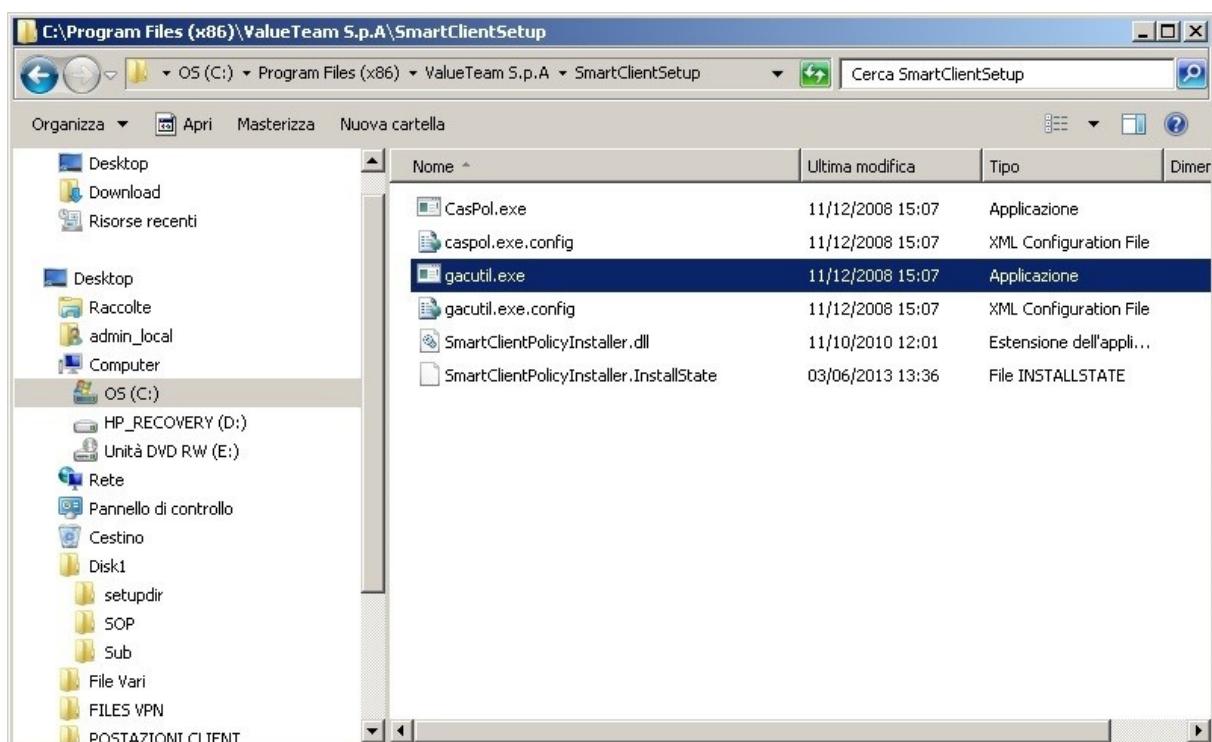


Figura 35 – Verifiche installazione SmartClient

3. Verificare che i seguenti files siano presenti nella cartella \windows\system32\ (per sistemi a 32bit) o nella cartella \windows\SysWOW64 (per sistemi a 64bit)

Eztwain3.dll

EZTiff.dll

EZSymbol.dll

EZPng.dll

EZPdf.dll

EZOcr.dll

EZJpeg.dll

EZGif.dll

EZDcx.dll

EZCurl.dll.

Per verificare se Smart Client è stato scaricato dal server dopo il primo utilizzo (per esempio dopo l'apertura della pagina di scansione dei documenti), è necessario aprire la seguente cartella del file system *c:\windows\assembly\Download*.

Attenzione: essendo una cartella di sistema non è accessibile direttamente dalla barra degli indirizzi, è necessario accedervi navigando l'albero, come mostrato nella figura successiva.

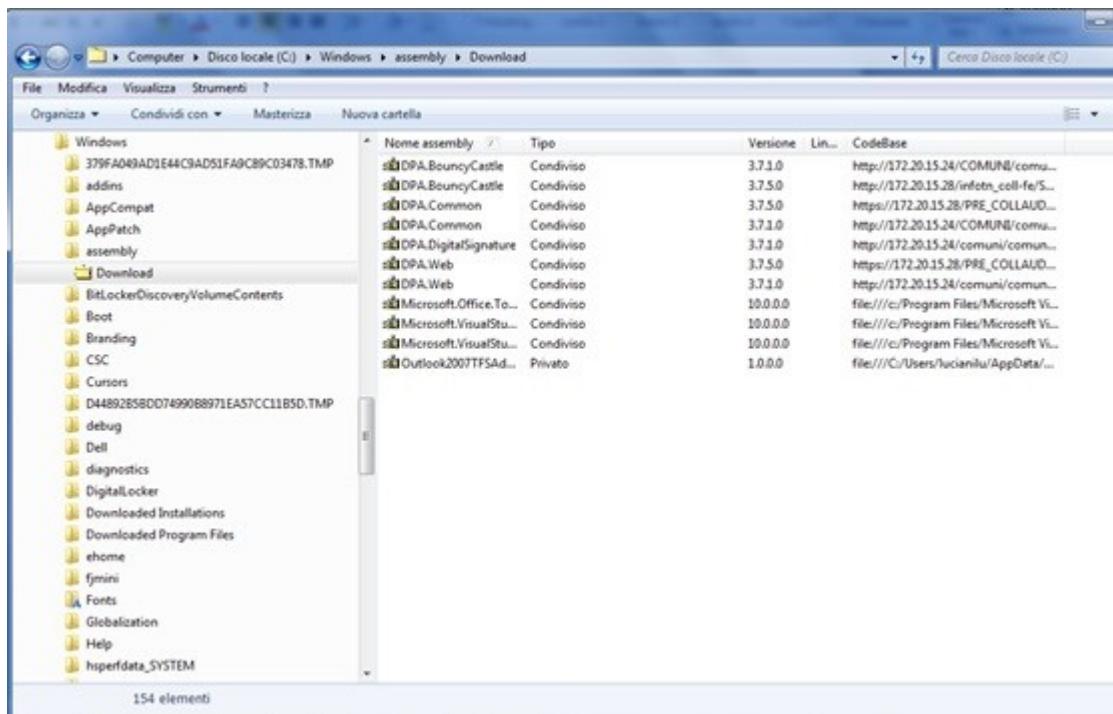


Figura 36 – Verifica download dll smart client nella cartella *c:\windows\assembly\download*

Affinchè il componente SmartClient possa funzionare correttamente con Microsoft .NET Framework4.5, è necessario installare il file PatchFramework4.5.reg.

6.5.1 POST INSTALLAZIONE

Per poter acquisire da scanner tramite SmartClient è obbligatorio abilitare espressamente il singolo utente (flag “Utilizza componenti Smart Client”) tramite il tool di amministrazione (Figura 37). Tramite il flag “Acquisisci in formato PDF” è inoltre possibile attivare la conversione in PDF al momento dell'acquisizione.

Sempre tramite tool di amministrazione è possibile inoltre scegliere il tipo di stampante di etichette utilizzato dall'utente (Figura 37).

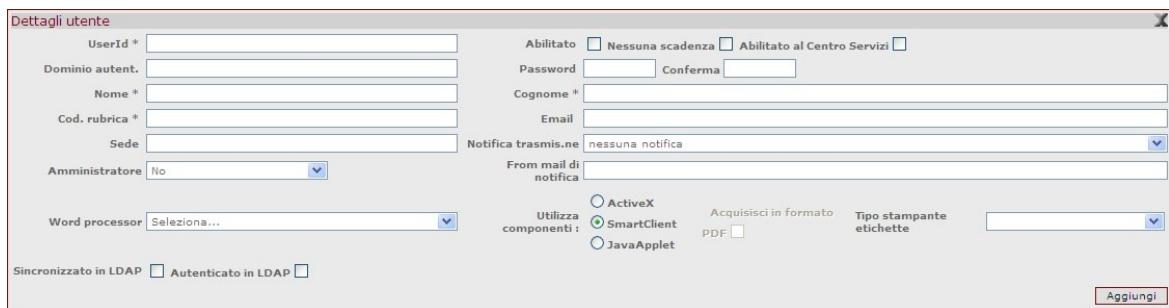


Figura 37 – Attivazione utilizzo componenti Smart Client

6.5.2 VERIFICA SE SMARTCLIENT È STATO SCARICATO DOPO IL PRIMO UTILIZZO.

In caso di non corretto funzionamento, per verificare se SmartClient è stato scaricato dal server dopo il primo utilizzo è necessario aprire in esplora risorse la cartella c:\windows\assembly\Download.

Attenzione: essendo una cartella di sistema non è accessibile direttamente dalla barra degli indirizzi, è necessario accedervi navigando l'albero come mostrato nella figura successiva.

Per la verifica, se SmartClient è stato scaricato le varie dll sue componenti sono presenti in questa cartella, se le dll non sono presenti, allora molto probabilmente il lancio della policy di cui ai paragrafi precedenti non ha avuto successo.

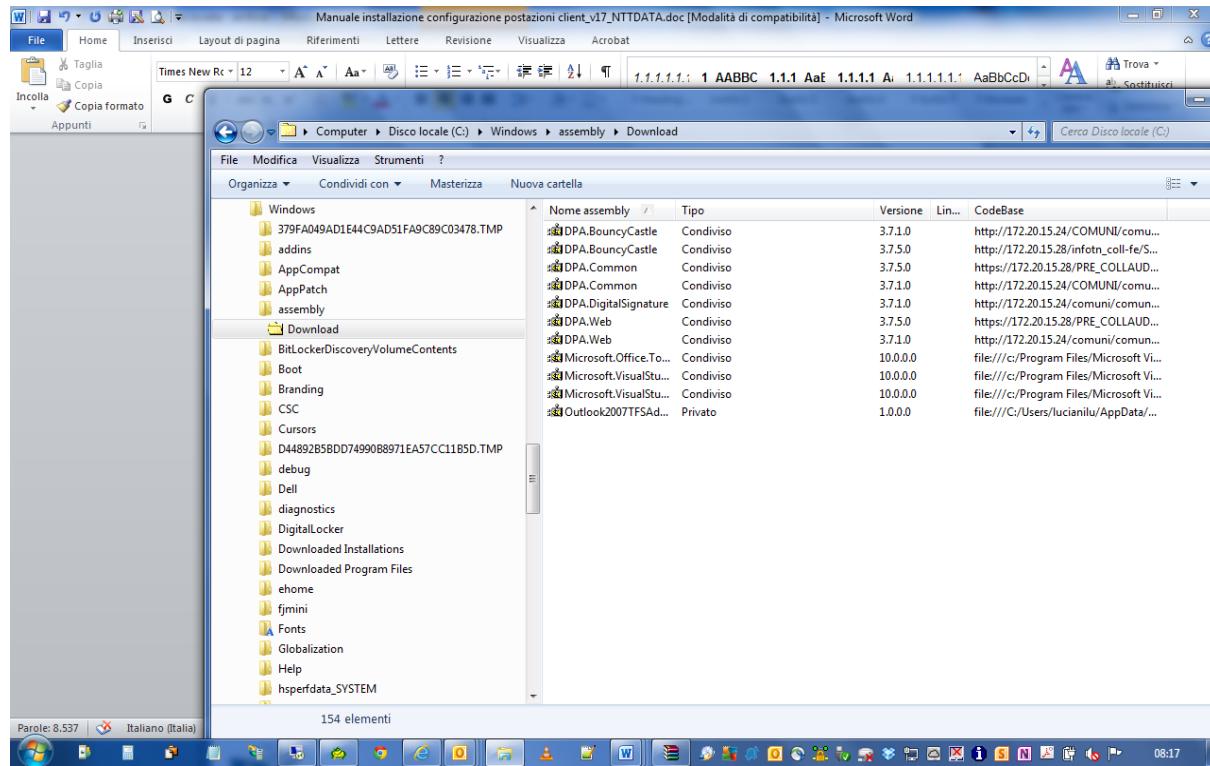


Figura 38 – Verifica download dll smartclient nella cartella c:\windows\assembly\download

6.6 FIRMA DIGITALE

In P.I.TRE. è ora possibile firmare con algoritmo SHA256 tramite la tecnologia SmartClient. Per attivare tale funzionalità sulle postazioni utente è dunque necessario installare i componenti di cui al paragrafo “6.5 - Installazione e configurazione di SmartClient”.

6.6.1 FIRMA DIGITALE SU UBUNTU PER HTML5 SOCKET

Il funzionamento corretto della firma digitale per Ubuntu è legato ai driver scaricati dal sito di appartenenza del chip (Aruba, Infocert, etc,..).

I due file scaricati vanno copiati sotto la cartella /usr/lib.

Il path dei driver viene specificato all'applicativo tramite una proprietà del file /opt/WebClientConnector/conf/pkcs11.cfg denominata library.

Nel file sono presenti alcuni percorsi dei driver possibili commentati , mentre quello di utilizzo per la mia carta non è commentato:

#library = /usr/lib/opensc-pkcs11.so

```
#library = /lib64/libASEP11.so
```

```
library = /usr/lib/libbit4xpki.so
```

Le librerie devono poter essere accessibili come permessi dall'utente che utilizza l'applicativo altrimenti la firma non funziona.

6.7 RISOLUZIONE DI PROBLEMI A VALLE DELL'INSTALLAZIONE DI UN DISPOSITIVO

Qui di seguito riportiamo i problemi che si possono manifestare a valle della configurazione di un dispositivo:

1. **Object error.** Il messaggio indica che l'applicativo non riesce ad istanziare gli oggetti definiti negli ActiveX e nelle librerie installate. Occorre utilizzare il comando regsvr32 per registrare le librerie che non vengono riconosciute (digitando semplicemente regsvr32 da Start --> Run, si ottiene un messaggio di help che illustra la sintassi del comando)

Gli errori che non consentono l'installazione di un Activex sono loggati da IE stessa in apposite pagine html. Per accedere a quest'area di log, è consigliato pulire l'area dei file temporanei come descritto nel paragrafo 3.2.6, poi accedere alla pagina che utilizza l'ActiveX non installato, quindi:

- a. aprire la maschera delle proprietà di Internet Explorer: **Strumenti(Tools) > Opzioni internet (Internet Options)**
 - b. da qui accedere dall'area **File Temporanei Internet** (Temporary Internet files) premere **Impostazioni** (Settings). Su IE7, quest'area si chiama **Cronologia esplorazioni** dove è presente il pulsante **Impostazioni** (Settings)
 - c. da qui premere su (View Files...) e si aprirà la cartella locale contenente i file temporanei
 - d. ordinare i file per data **Ultimo accesso** (last accessed) crescente
 - e. l'ultimo file è una pagina di errore che può essere editata con un editor di testo ad esempio Notepad (si consiglia di puntare il file col mouse e mantenendo premuto trascinarlo in una finestra di notepad già aperta)
 - f. il file di errore contiene il log dell'errore verificatosi durante l'installazione
 - g. si consiglia di copiare il testo di questo errore e inviarlo al supporto P.I.TRE.
2. **La configurazione del browser non permette di eseguire**: Indica la necessità di abbassare il livello di protezione per l'uso degli ActiveX.

7 ACQUISIZIONE MASSIVA

Per l'istallazione del modulo dell'Acquisizione massiva è stato scritto un documento allegato a tale manuale : Allegato1 – Istallazione Modulo Acquisizione Massiva

8 CONFIGURAZIONE DI ADOBE ACROBAT FULL PER L'ABILITAZIONE DELLA CONVERSIONE IN PDF DEI FILE ACQUISITI

8.1 INTRODUZIONE

P.I.TRE. utilizza Adobe Acrobat Full per convertire in formato PDF, quando richiesto, i file acquisiti. Adobe Acrobat versione Full deve essere installato sul client con le modalità previste dal fornitore e configurato secondo quanto descritto di seguito. La configurazione dipende dalla versione di Adobe Acrobat installata.

8.1.1 PARAMETRI CONFIGURAZIONE P.I.TRE.

Per Integrare le funzioni di Adobe Acrobat, P.I.TRE. utilizza un opportuno componente ActiveX (i cui dettagli di installazione e configurazione sono stati descritti nella sezione precedente ‘Configurazione dello scanner’ e per il quale valgono le stesse considerazioni fatte per gli altri ActiveX (par. 3.2).

Tale componente legge i parametri di configurazione relativi alla funzionalità di conversione in formato pdf dal file “**Settings.ini**” che risiede nella cartella di installazione. A seconda della procedura di setup utilizzata per installare l’ocx, il file può risiedere in:

- Cartella “**\Windows\Downloaded program files**” in caso di CAB autoinstallato (in tal caso, eventuali modifiche al file possono essere effettuate solo accedendo mediante prompt di msdos);
- Cartella scelta dall’utente in caso di setup client manuale;

Le impostazioni personalizzabili presenti nel file di configurazione sono:

- Sezione **PDFPrinters**: sezione contenente le possibili stampanti PDF presenti nel sistema, i cui nomi possono cambiare a seconda della versione di Acrobat installata. Per la conversione verrà utilizzata la prima stampante che, in base alla posizione, risulti per prima installata tra quelle in lista.
- Sezione **PDFOutputFolder**: cartella di output nella quale Acrobat crea i file PDF (corrisponde alla cartella selezionata nelle preferenze della stampante PDF) e nella quale il componente si “aspetta” siano presenti i file PDF al termine della conversione. La configurazione di default prevede la presenza della cartella “C:\AdobePDFOutput”. **NB**: eventuali file già presenti nella suddetta cartella verranno spostati automaticamente in una cartella di backup (il cui nome corrisponde a: pdfOutputFolder + “_” + DataOra) e ripristinati al termine della conversione.

- Sezione **PDFCreationTimeoutSec**: permette di impostare un tempo limite in secondi in base al quale il processo di conversione (che è un processo esterno) di un documento in PDF venga interrotto nel caso di conversione non effettuata. Ciò può essere dovuto essenzialmente ad un malfunzionamento di Acrobat oppure nel caso in cui la cartella di output impostata tra le preferenze di stampa non corrisponda esattamente a quella impostata nella sezione “PDFOutputFolder”. Default=20 sec

8.1.2 PARAMETRI CONFIGURAZIONE ACROBAT

Dopo aver installato Adobe Acrobat bisogna configurare correttamente la stampante virtuale ad esso relativa.

Innanzitutto si deve accedere alle proprietà della stampante Adobe PDF per impostare le preferenze di stampa.

Inoltre dopo aver creato sul disco C la cartella specificata nel file settings.ini (per default è presente C:\AdobePDFOutput) occorre configurare la cartella di output nella quale verranno automaticamente creati i file convertiti. A questo punto per le versioni 5 e 6 di Acrobat, l'impostazione della suddetta cartella di output deve essere effettuata aggiungendo una nuova porta di tipo “Adobe PDF” tra le porte della stampante stessa da associare alla directory creata. Per la versione 7 invece la maschera delle preferenze di stampa permette di impostare direttamente la cartella.

Nel dettaglio **per la versione 5 di Acrobat:**

1) dal **Pannello di controllo** selezionare **Stampanti**.

Selezionare la stampante relativa ad Adobe, creata durante l'installazione del prodotto. Generalmente il nome è “Adobe PDF”. Selezionare la stampante e visualizzare le proprietà.

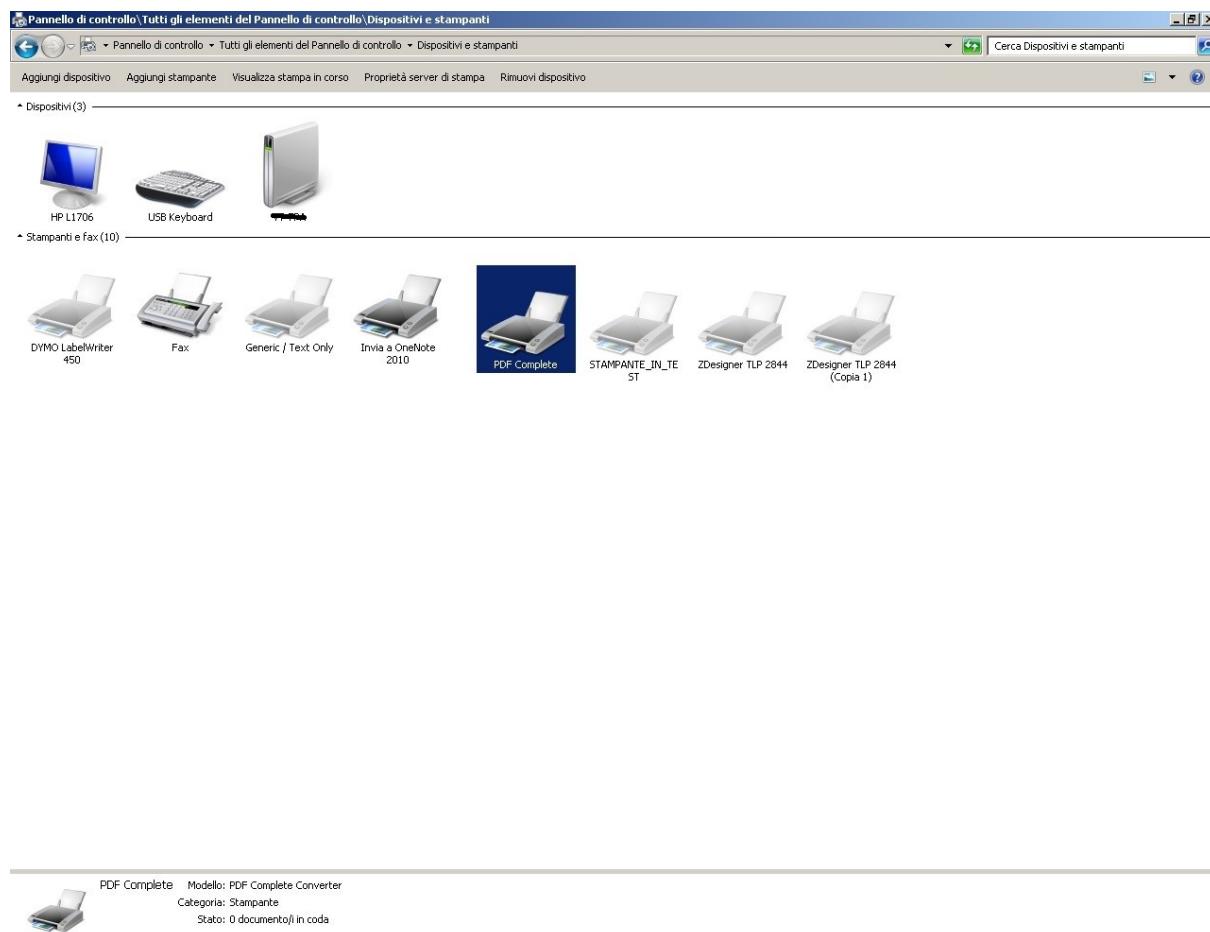


Figura 39 – Pannello delle stampanti

Verificare che il nome della stampante sia uno dei seguenti

- Adobe PDF;
- Acrobat PDFWriter;
- Acrobat Distiller;

ed eventualmente rinominarla.

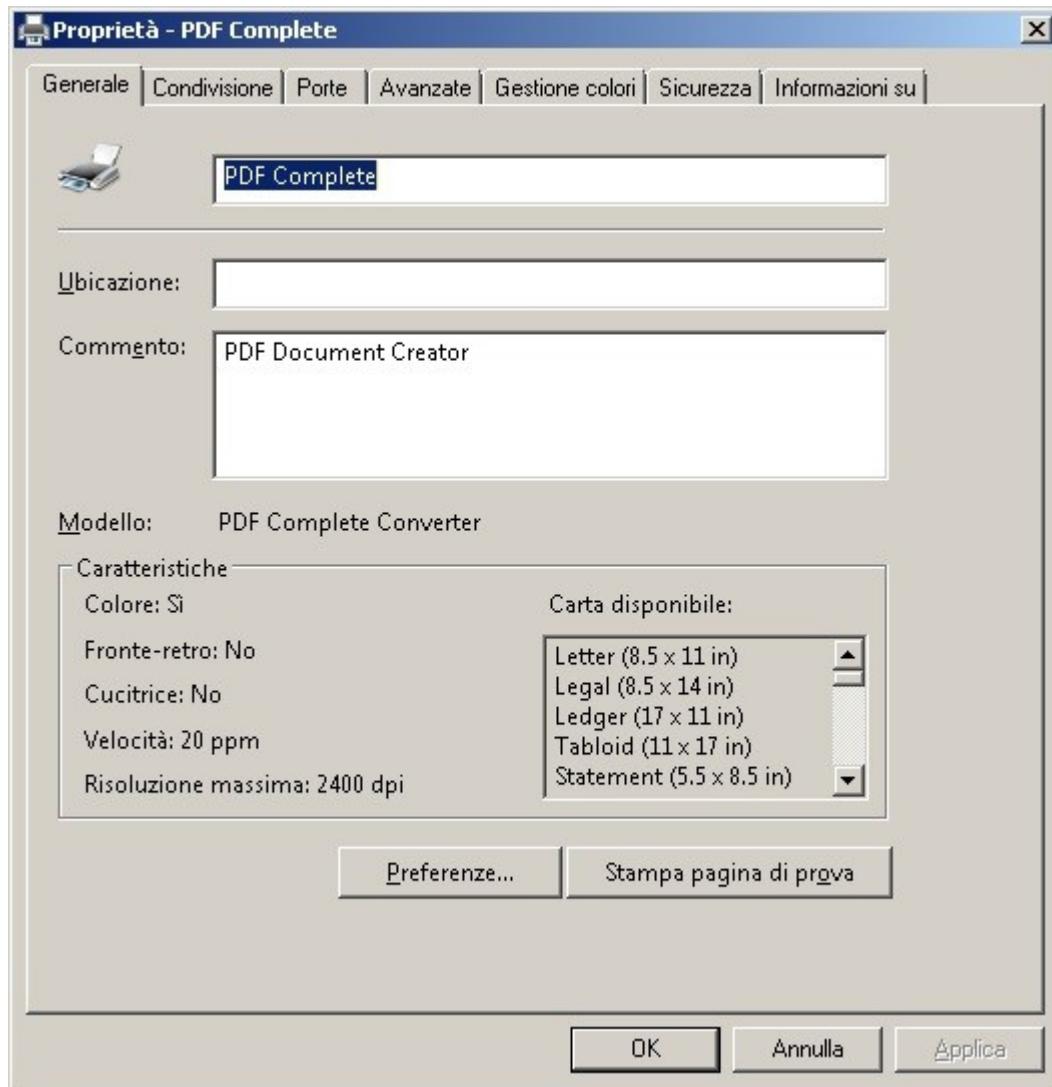


Figura 40 – Proprietà della stampante

2) Accedere alle preferenze di stampa e, sulla scheda impostazioni PDF Adobe, lasciare selezionata la sola checkbox per la cancellazione dei file di registro per i processi completati. Tornare con OK sulle proprietà.

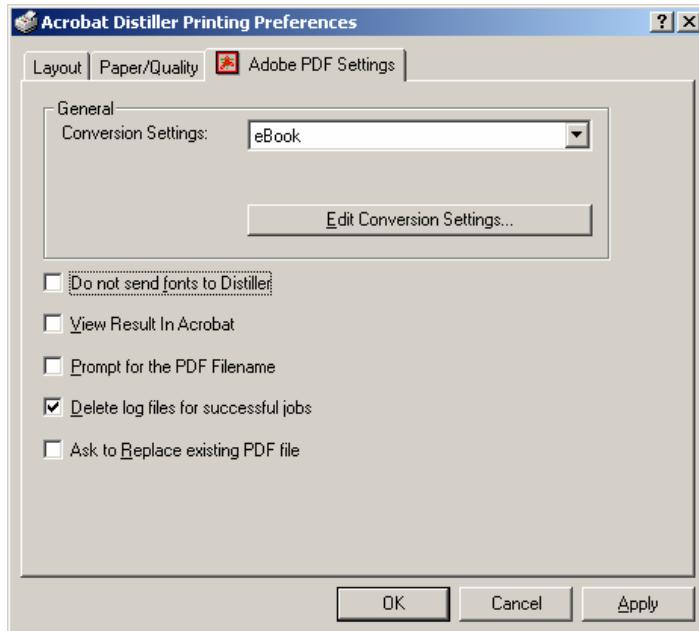


Figura 41 – Impostazioni della stampante Adobe PDF (v5)

3) Andare su porte ed aggiungere una nuova porta di tipo pdf .

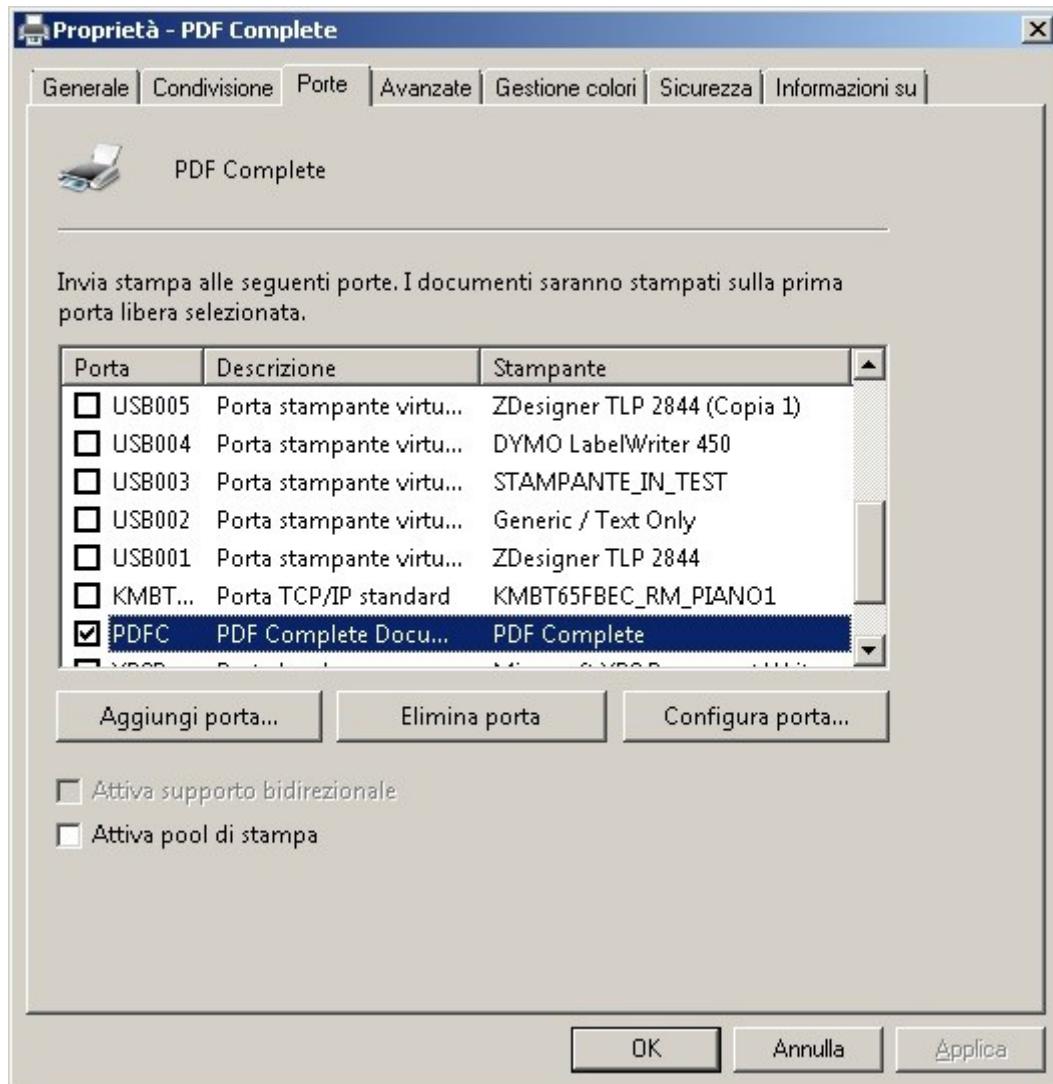


Figura 42 – Creazione nuova porta per la stampante Adobe (v5)

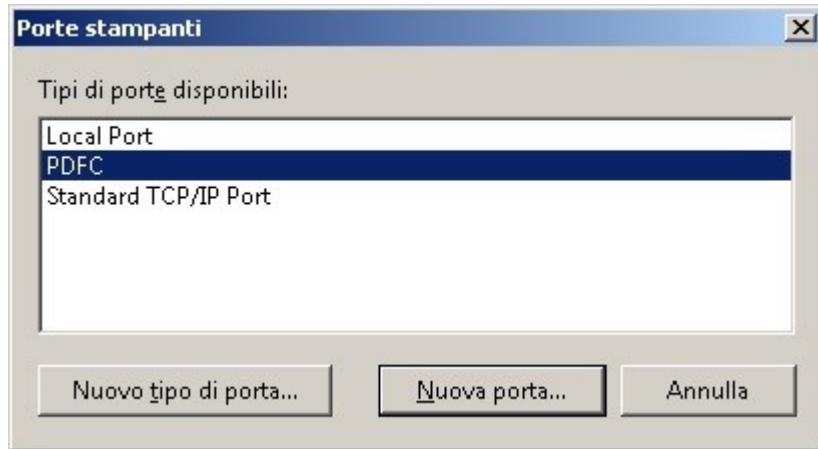


Figura 43 – Creazione nuova porta di tipo pdf per la stampante Adobe (v5)

Ciccare su new port, selezionare la directory scelta per l'appoggio dei file da convertire (default c:\AdobePdfOutput) e tornare con il tasto ok alle proprietà.

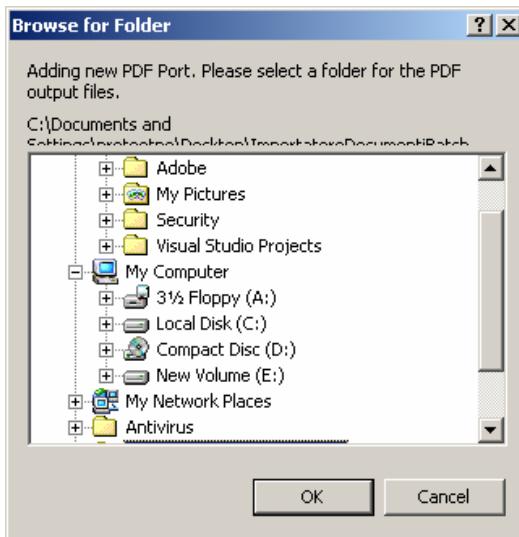


Figura 44 – Associazione directory alla nuova porta di tipo pdf per la stampante Adobe (v5)

Nel dettaglio **per la versione 6 di Acrobat:**

Impostare le preferenze di stampa deselezionando le voci:

- View Adobe PDF Results;
- Prompt for Adobe PDF filename;

Come mostrato nella figura che segue:

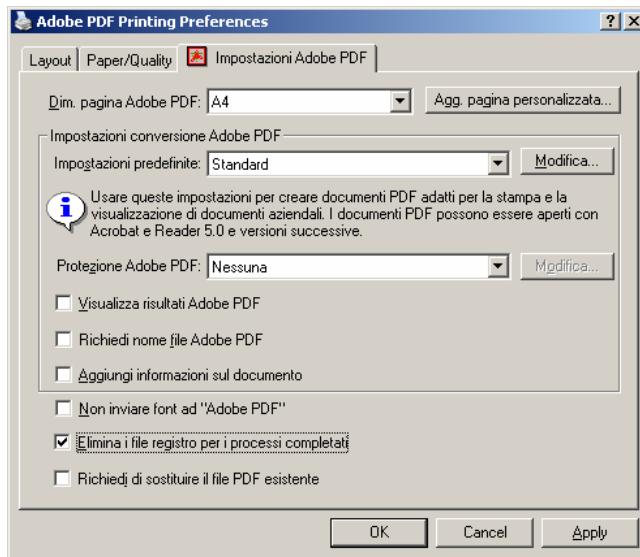


Figura 45 – Selezione maschera Ports (v.6)

Bisogna poi impostare la porta della stampante:
dal pannello iniziale delle proprietà selezionare la maschera '**Ports'** e, se non presente,
aggiungere la porta relativa alla stampante PDF indicando il percorso in cui andranno
appoggiati i file prima del salvataggio sul server come indicato nella figure seguenti.

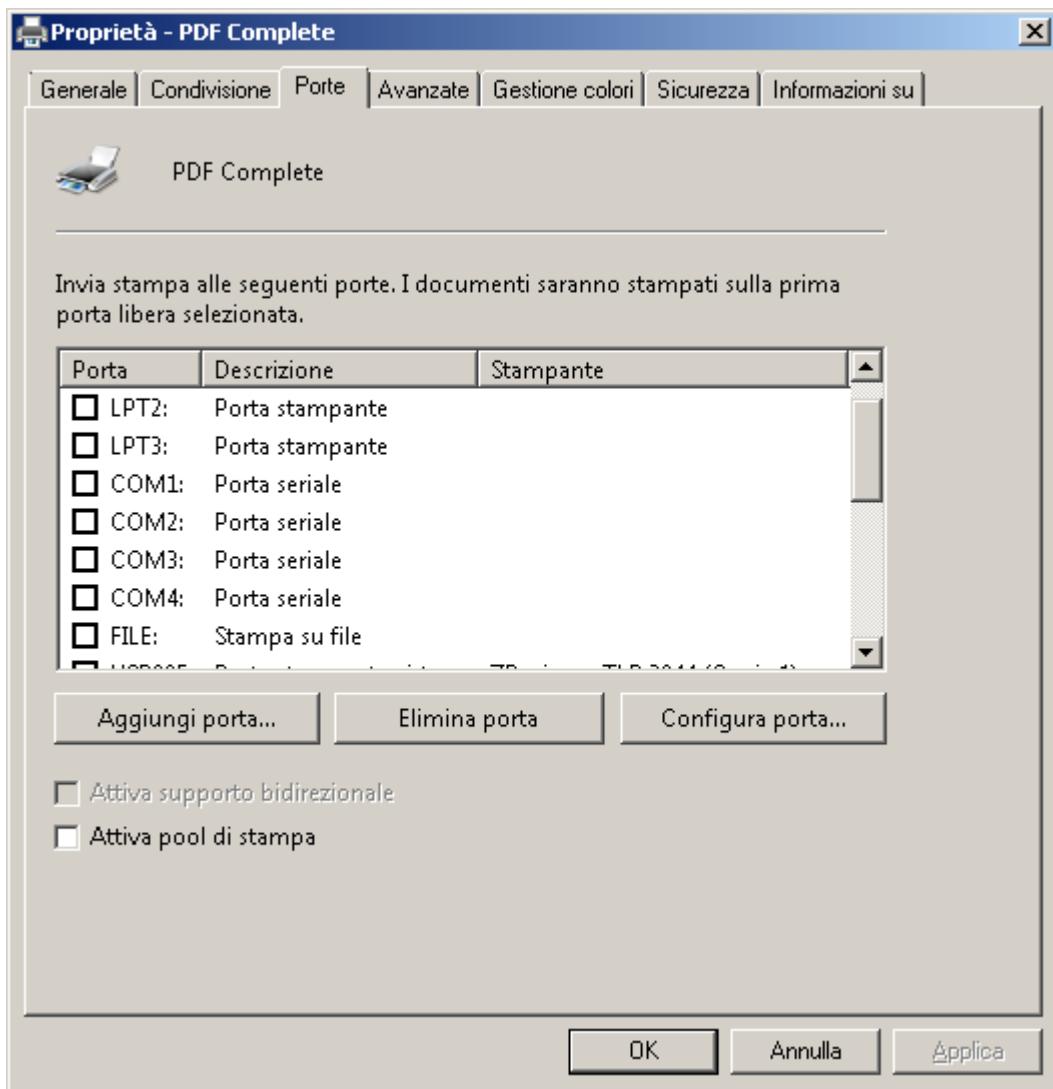


Figura 46 – Selezione maschera Ports (v.6)

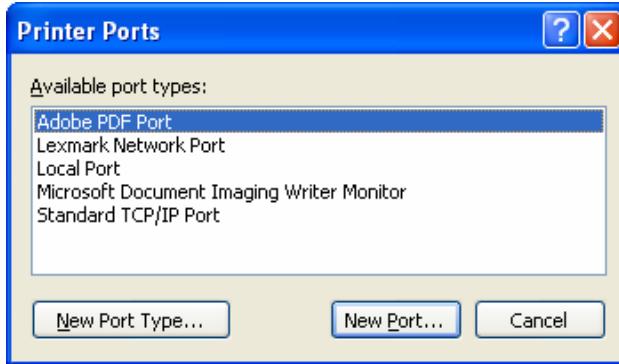


Figura 47 – Apertura popup di aggiunta nuova porta e selezione porta di tipo Adobe PDF (v.6)

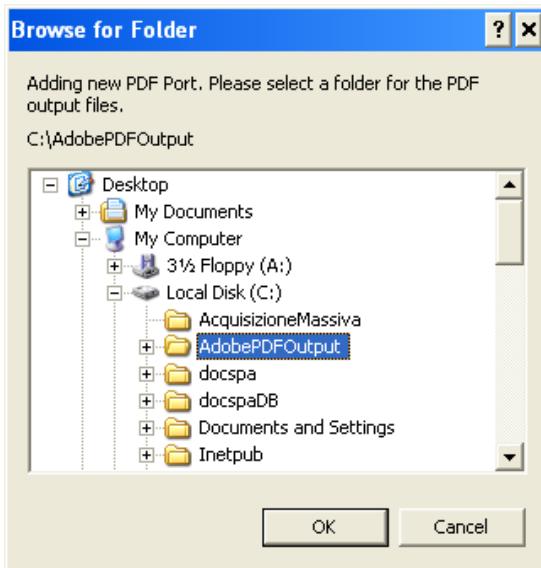


Figura 48 – Associazione directory di appoggio per nuova porta PDF (v.6)

Adobe Acrobat 7:

Impostare le preferenze di stampa dal pannello delle proprietà di Adobe PDF, in particolare:

- deselezionare la voce “View Adobe PDF Results”
- impostare la cartella di output dei file PDF (“Adobe PDF Output Folder”)

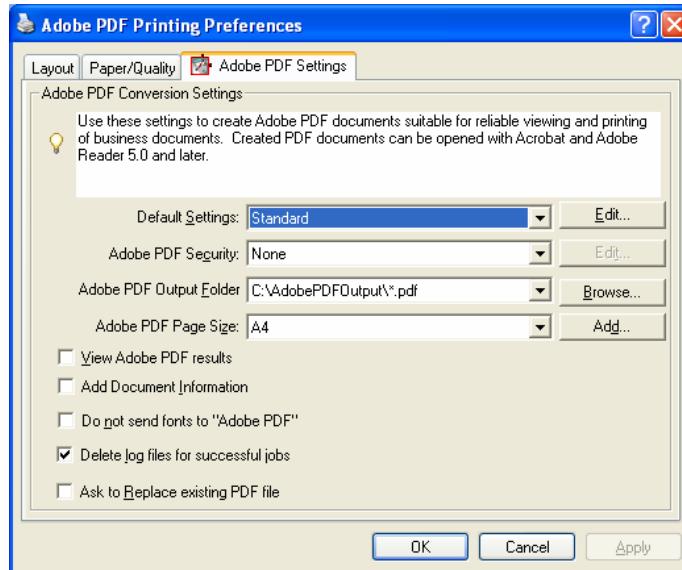


Figura 49 – Impostazioni della stampante (v.7)

APPENDICE 1 - Configurazione stampante Dymo (lato server)

Per la configurazione delle stampantine Dymo (eseguita lato server), si deve usare il programma Label 8.3 o superiore:

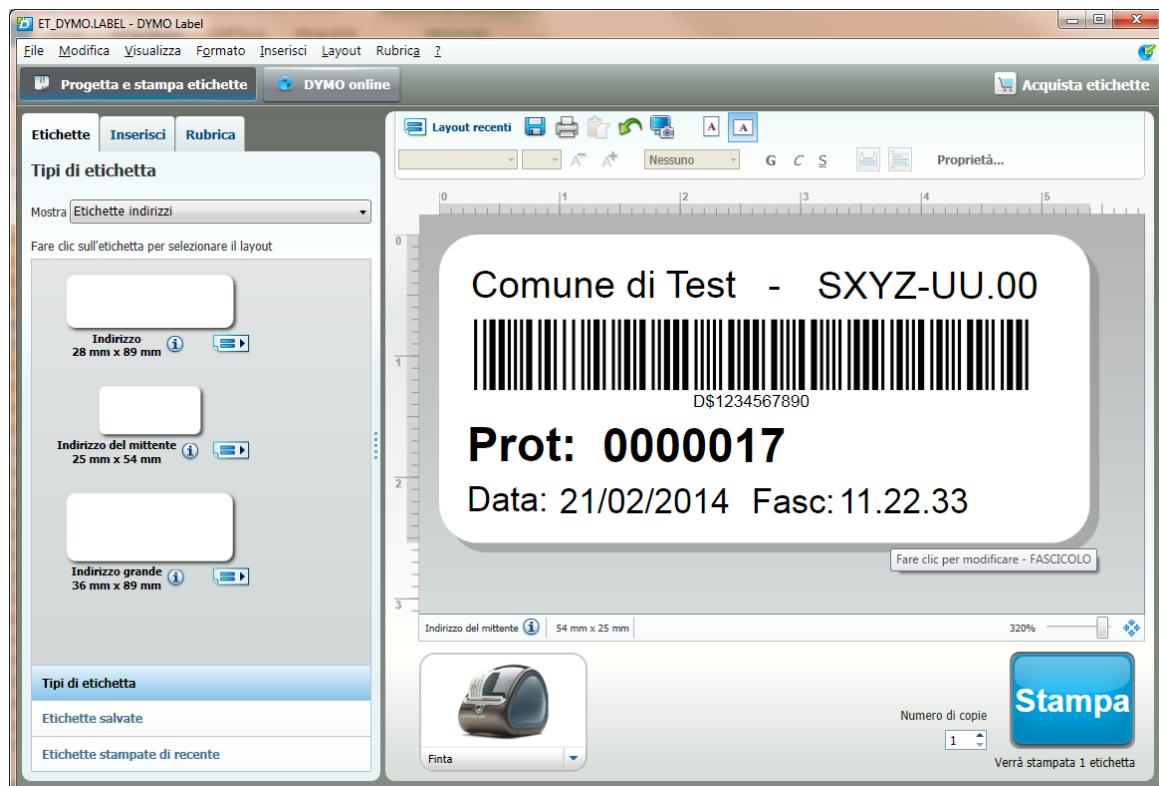


Figura 50 – Configurazione stampanti Dymo

Il file creato per l'etichetta ha estensione .label e va salvato sul server nel percorso configurato (vedi oltre chiave LABELS_PATH) oppure nella cartella di default \<pathdelfrontend>\Popup.

Per gestire installazioni multi amministrazione, nel web.config della WA vanno impostate le seguenti chiavi di configurazione:

```
<!-- path etichette per dymo e applet -->
<add key="LABELS_PATH" value="C:\Pitre\Frontend\Etichette\%COD_AMM%" />
<!-- prefisso per poter gestire il codice a barre con la massiva -->
<add key="DYMO_DOCNUMBER_PREFIX" value="D"/>
```

Per valorizzare la chiave LABELS_PATH si possono usare le variabili:

- %COD_AMM% valore dinamico per l'amministrazione
- %COD_REG% codice registro protocollo
- %COD_UO% codice UO protocollo.