Autenticazione Tomcat

Metodi di autenticazione

L'autenticazione utilizzata dalla applicazione Titulus di default è la Basic Authentication Normalmente viene utilizzato il file **“tomcat-users.xml”** reperibile nella directory conf di tomcat (per i percorsi consultare il manuale di installazione). Di seguito forniamo un esempio del file:

```
<?xml version='1.0' encoding='utf-8'?>
  <tomcat-users>
  <role rolename="aoojspuser"/>
  <role rolename="admjspuser"/>
  <role rolename="tomcat"/>
  <role rolename="jspuser"/>
  <role rolename="role1"/>
  <role rolename="manager"/>
  <role rolename="admin"/>
  <user username="admin" password="67b505920ba9903f63c0277d34697cad" fullName="" roles="admin,aoojspuser,
jspuser,manager,role1,tomcat"/>
  <user username="protocollista" password="67b505920ba9903f63c0277d34697cad" fullName="Utente base" roles="
jspuser"/>
  <user username="responsabile" password="67b505920ba9903f63c0277d34697cad" fullName="Utente amministrativo"
roles="admjspuser,aoojspuser,jspuser",/>
</tomcat-users>
```

I “roles” hanno la funzione di filtro per gli accessi alle risorse:

Per la risorsa: (i link sono relativi all'utilizzo dell'applicativo in locale)

http://localhost:8080/xway/application/xdocway/engine/xdocway.jsp

Necessita almeno la presenza del role “jspuser”

Per la risorsa:

http://localhost:8080/xway/application/xdocway/engine/xdocwayadm.jsp

Necessita della presenza del role “admjspuser”

Autenticazione LDAP

Il servlet container Tomcat supporta diverse fonti di autenticazione:

oltre alla autenticazione di default, è possibile delegare l'installazione ad un altra risorsa, quale un server LDAP.

La documentazione ufficiale per reperire informazioni sulle tipologie è reperibile sul sito ufficiale del progetto Apache Tomcat.

A seguire forniremo i valori da inserire sui campi interrogati da Tomcat per utilizzare la fonte LDAP come metodo di autenticazione.

Configurazione di esempio di una struttura LDAP:

```
#Utenti.ldif

dn: ou=titulus,dc=example,dc=net
objectClass: organizationalUnit
ou: titulus


dn: uid=admin,ou=titulus,dc=example,dc=net
objectClass: inetOrgPerson
uid: admin
sn:  app
cn: Amministratore
userPassword: test


dn: uid=protocollista,ou=titulus,dc=example,dc=net
objectClass: inetOrgPerson
uid: protocollista
sn:  app
cn: Utente Base
userPassword: test

dn: uid=responsabile,ou=titulus,dc=example,dc=net
objectClass: inetOrgPerson
uid: responsabile
sn:  app
cn: Utente Amministrativo
userPassword: test
```

```
#roles.ldif questa sezione inserisce il gruppo titulus
# e i profili ( roles ) utilizzati per limitare gli accessi
```

```
dn: cn=admin,ou=titulus,dc=example,dc=net
objectClass: groupOfUniqueNames
cn: admin
uniqueMember: uid=admin,ou=titulus,dc=example,dc=net

dn: cn=manager,ou=titulus,dc=example,dc=net
objectClass: groupOfUniqueNames
cn: manager
uniqueMember: uid=tomcat,ou=titulus,dc=example,dc=net
uniqueMember: uid=admin,ou=titulus,dc=example,dc=net

dn: cn=admjspuser,ou=titulus,dc=example,dc=net
objectClass: groupOfUniqueNames
cn: admjspuser
uniqueMember: uid=responsabile,ou=titulus,dc=example,dc=net
uniqueMember: uid=admin,ou=titulus,dc=example,dc=net
```

```
dn: cn=jspuser,ou=titulus,dc=example,dc=net
objectClass: groupOfUniqueNames
cn: jspuser
uniqueMember: uid=protocollista,ou=titulus,dc=example,dc=net
uniqueMember: uid=admin,ou=titulus,dc=example,dc=net
```

Questa Semplice configurazione associa i ad ogni utente determinati roles:

admin: **jspuser, admin, manager, aooadmjspuser, admjspuser**

responsabile: **aooadmjspuser, admjspuser, jspuser**

protocollista: **jspuser**

tutti raccolti nel gruppo **docway**

La configurazione della applicazione docway è la seguente:

all'interno della directory conf/Catalina/localhost/ di apache-tomcat

sostituire il file xway.xml con il seguente:

Installazioni Linux

```
<Context path="/xway" docBase="/opt/titulus/webapps/xway" debug="0" privileged="true">


<Realm   className="org.apache.catalina.realm.JNDIRealm"
        connectionURL="ldaps://[ldaphost]:636"
        userPattern="uid={0},ou=titulus,dc=example,dc=net"
        roleBase="ou=titulus,dc=example,dc=net"
        roleName="cn"
        roleSearch="(uniqueMember={0})"
/>
         <!--
          <Valve className="org.apache.catalina.valves.RemoteAddrValve"
            allow="127.0.0.1,localhost"/>
          -->

</Context>
```

installazioni windows (Active Directory)

```
<Context path="/xway" docBase="e:\Titulus\webapps\xway" debug="0" privileged="true">


<Realm   className="org.apache.catalina.realm.JNDIRealm"
        connectionURL="ldaps://ldaphost:636"
        userPattern="uid={0},ou=titulus,dc=example,dc=net"
        roleBase="ou=titulus,dc=example,dc=net"
        roleName="cn"
        roleSearch="(uniqueMember={0})"
/>
          <!--
          <Valve className="org.apache.catalina.valves.RemoteAddrValve"
            allow="127.0.0.1,localhost"/>
          -->

</Context>
```

Considerazioni

La configurazione sopra riportata è da ritenersi un esempio; in scenari con già una alberatura LDAP costituita andranno modificati i valori. Tuttavia i gruppi e le risorse sono necessari per il corretto funzionamento della applicazione.

Autenticazione tramite Active Directory

E' possibile in alternativa all'autenticazione tomcat o ldap usufruire del servizio Active Directory per gestire l'accesso al protocollo. Ovviamente è necessario inserire l'utenza anche in acl con il corrispettivo utente nella sezione “login”.

Requisiti

Per utilizzare le utenze di Active Directory di Windows sulla macchina windows che ospita l'applicativo o su una macchina windows separata [1)] (frontend) è necessario:

- Avere IIS versione 6 o superiore già installato nel sistema
- Installare Msxml
- Utilizzare una macchina Windows che sia nel dominio desiderato di Active Directory ma che non sia un Domain Controller.

Configurazione di Tomcat

E' necessario rimuovere prima l'autenticazione di tomcat nel file web.xml all'interno della cartella Titulus/webapps/xway sulla macchina che ospita l'applicativo:

```
<!-- inizio protezione dei jsp -->

     <!--
    <security-constraint>
      <web-resource-collection>
        <web-resource-name>XDocway</web-resource-name>
        <url-pattern>/application/xdocway/engine/xdocway.jsp</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>Acl</web-resource-name>
        <url-pattern>/base/acl/engine/acl.jsp</url-pattern>
      </web-resource-collection>

      <auth-constraint>
        <role-name>jspuser</role-name>
      </auth-constraint>
    </security-constraint>

    <security-constraint>
      <web-resource-collection>
        <web-resource-name>XDocway ADM</web-resource-name>
        <url-pattern>/application/xdocway/engine/xdocwayadm.jsp</url-pattern>
      </web-resource-collection>

      <auth-constraint>
        <role-name>admjspuser</role-name>
      </auth-constraint>
    </security-constraint>

    <security-constraint>
      <web-resource-collection>
        <web-resource-name>XDocway AOO ADM</web-resource-name>
        <url-pattern>/application/xdocway/engine/xdocwayaooadm.jsp</url-pattern>
      </web-resource-collection>

      <auth-constraint>
        <role-name>aooadmjspuser</role-name>
      </auth-constraint>
    </security-constraint>

    <security-constraint>
      <display-name>Extraway - Area protetta</display-name>
      <web-resource-collection>
        <web-resource-name>XDocway</web-resource-name>
        <url-pattern>/application/xdocway/engine/*</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>Acl</web-resource-name>
        <url-pattern>/base/acl/engine/*</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>XDocway ADM</web-resource-name>
        <url-pattern>/application/xdocway/engine/xdocwayadm.jsp</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>XDocway AOO ADM</web-resource-name>
        <url-pattern>/application/xdocway/engine/xdocwayaooadm.jsp</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>ACl Super User</web-resource-name>
        <url-pattern>/base/acl/engine/superuser.jsp</url-pattern>
      </web-resource-collection>

      <web-resource-collection>
        <web-resource-name>Extraway tools</web-resource-name>
```

```
      <url-pattern>/engine/*</url-pattern>
    </web-resource-collection>

    <web-resource-collection>
      <web-resource-name>Viewer</web-resource-name>
      <url-pattern>/application/generic/engine/*</url-pattern>
    </web-resource-collection>

    <auth-constraint>
      <role-name>superuser</role-name>
      <role-name>admin</role-name>
    </auth-constraint>

  </security-constraint>  -->
  <!-- fine protezione dei jsp -->
```

- Togliere l'autenticazione di Tomcat riguardante la sezione docway, commentando la sezione security constraint nel web.xml, compresa tra i due commenti come mostrato nella tabella superiore.

Configurazione di Internet Information Services (non più usato)

Requisiti

- Windows Server con tecnologia IIS
- Comunicazione di rete diretta con il server in cui si trova tomcat (se non risiede sulla macchina stessa)
- Applicazione MSXML installata sul server (disponibile sul cd di installazione)
- Il server deve essere parte del dominio Active Directory
- Il server NON deve essere un domain controller.

Consigliati

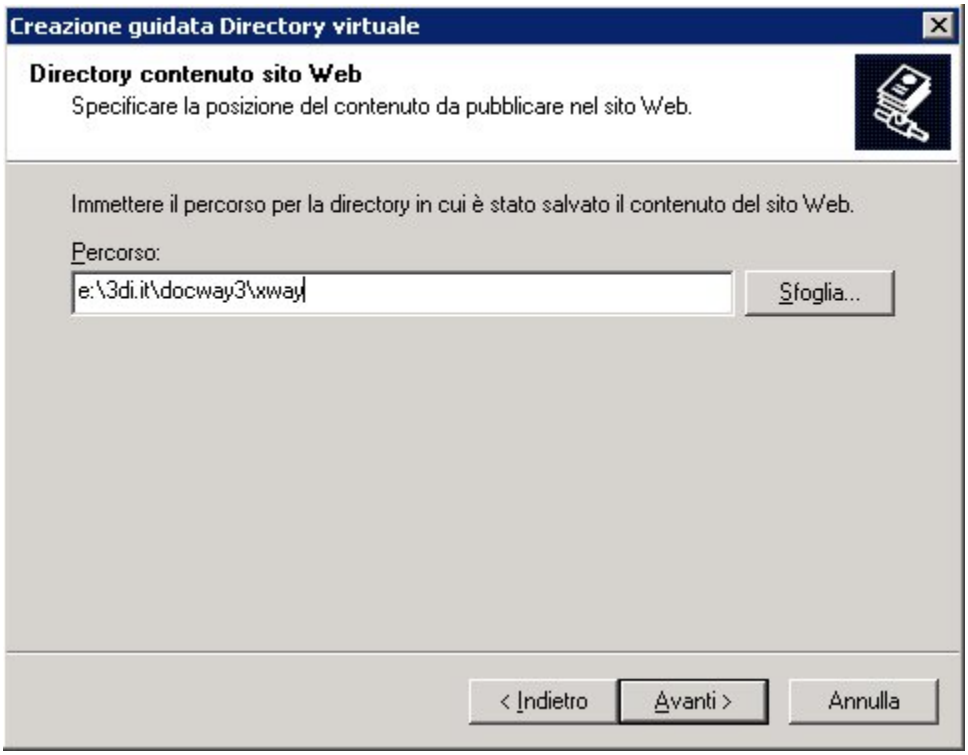
- Windows Server 2003 con IIS 6 o superiore
- Internet Explorer 7 o superiore nel lato client, per usufruire dell'autenticazione integrata di windows.

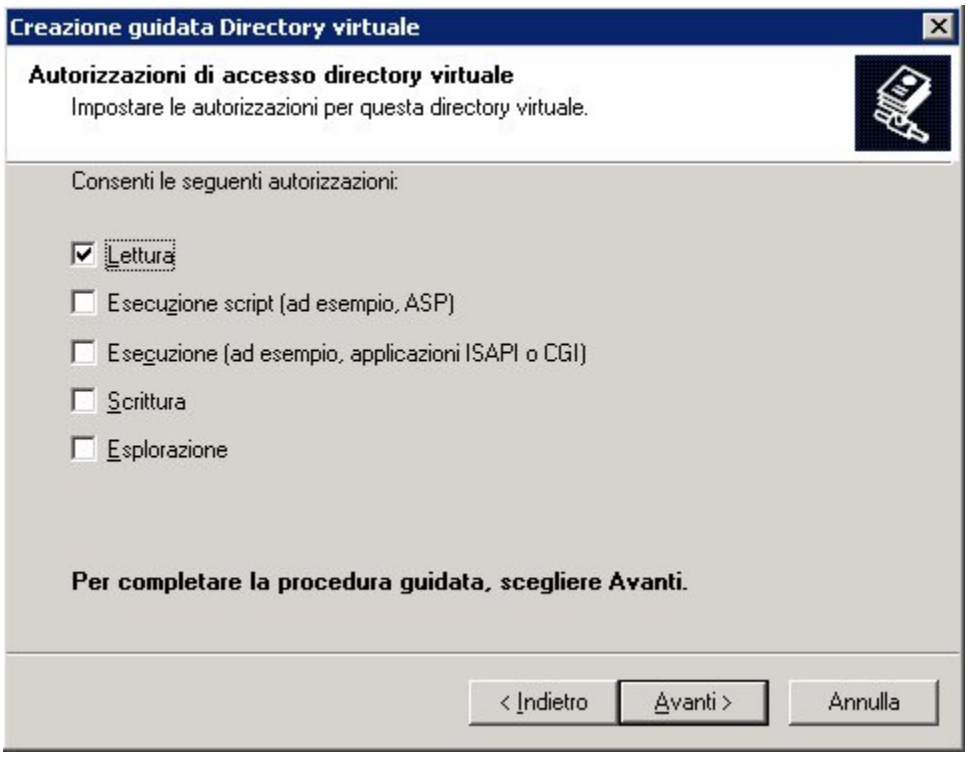
Configurazione

E' possibile accedere alla configurazione di IIS tramite il pannello *Strumenti di Amministrazione*.

Nella sezione siti web sotto *Sito predefinito* creare una nuova directory virtuale dandogli il nome *xway*, e farla puntare all'omonima directory in e:\Titulus\webapps\:


Creazione guidata Directory virtuale
Alias directory virtuale
Specificare un nome breve o alias per la directory virtuale.
Digitare l'alias che si desidera utilizzare per accedere alla directory virtuale Web.
Utilizzare le stesse convenzioni di denominazione adottate per i nomi di directory.
Alias:
xway
< Indietro
Avanti >
Annulla


Creazione guidata Directory virtuale
Directory contenuto sito Web
Specificare la posizione del contenuto da pubblicare nel sito Web.
Immettere il percorso per la directory in cui è stato salvato il contenuto del sito Web.
Percorso:
e:\3di.it\docway3\xway
Sfoglia...
< Indietro
Avanti >
Annulla



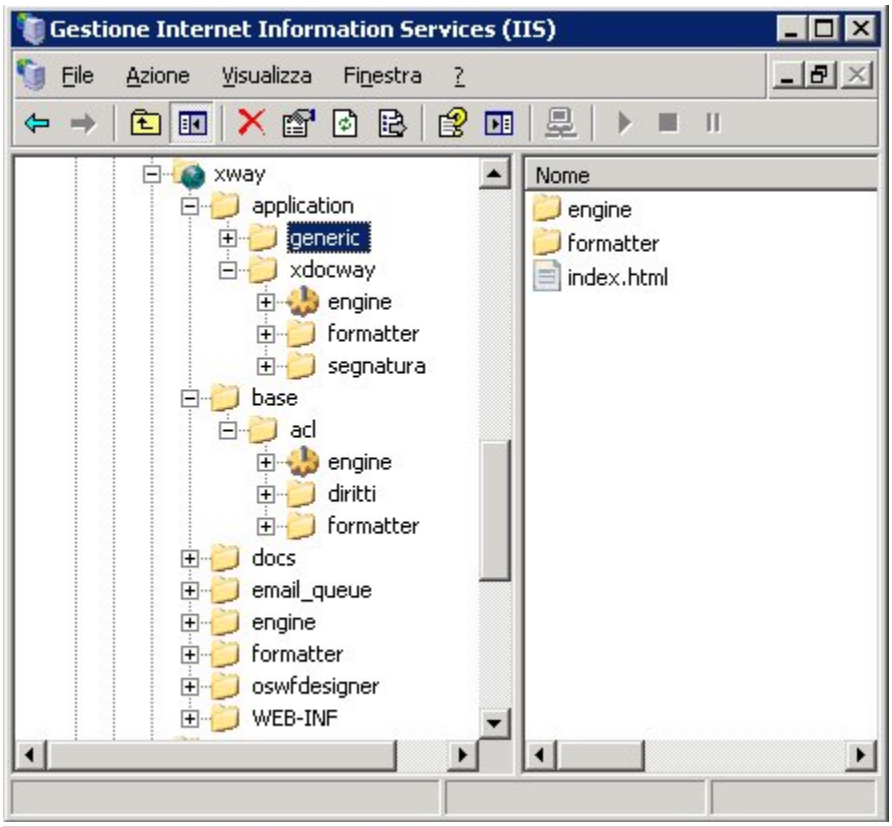
Attenzione: è possibile utilizzare una condivisione di rete alla risorsa xway, nel caso si trovi su un altro server

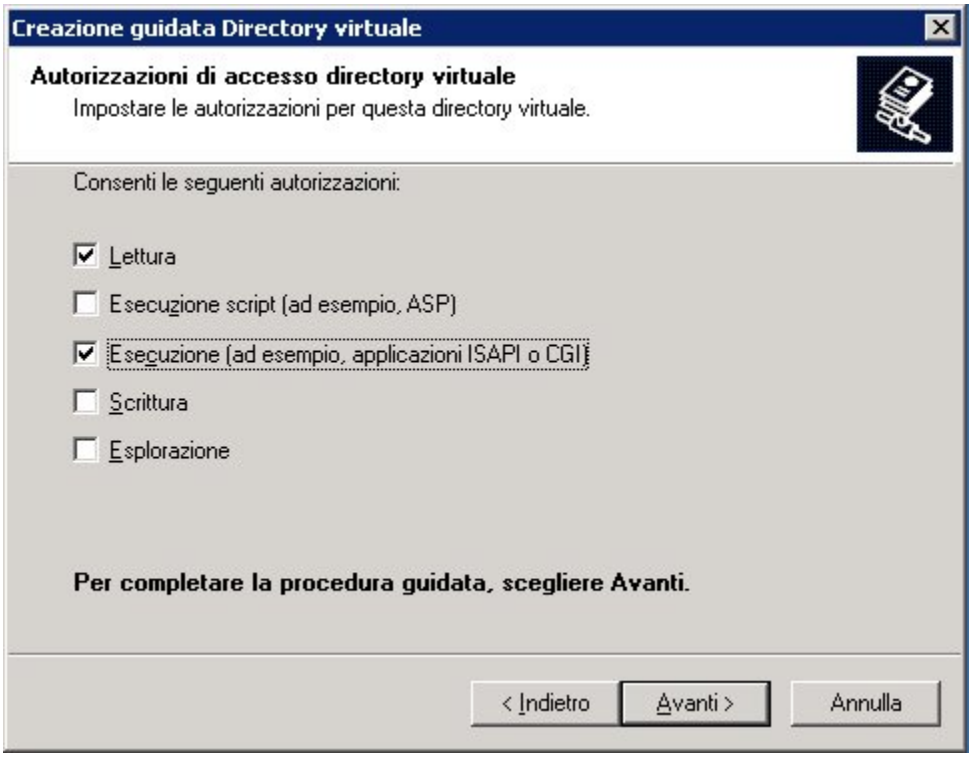
- **Creare la directory virtuale xway**

Inoltre è necessario configurare nelle proprietà:

- **Impostare livello di protezione: “bassa” (in inglese “MSSharePointAppPool”)**
- **Togliere accesso all'utente anonimo**
- **Abilitare nel campo autenticazione solo questi due campi: *Autenticazione integrata di Windows* e *Autenticazione di base (password non crittografata)***

Successivamente è necessario creare le directory virtuali *engine* con diritti di esecuzione ISAPI:





Devono essere create nella sezione xway\application\xdocway con il percorso e:\Titulus\webapps\www\isapi\docway3\bin e nella sezione xway\base\acl con il percorso e:\Titulus\webapps\www\isapi\acl\bin

Attenzione: la cartella www e il suo contenuto deve necessariamente trovarsi sullo stesso server in cui si trova IIS, nel caso sarà necessario copiarle in locale

- **Creare le directory virtuali engine con i diritti di esecuzione ISAPI**

E' necessario impostare i diritti sul filesystem in quelle cartelle, in modo che siano leggibili dagli utenti che utilizzeranno l'autenticazione IIS. Per farlo solitamente si aggiungono 2 gruppi di utenti locali nel server:

• **titulusprot** in cui dovranno essere inseriti i protocollisti

• **titulusadmin** in cui dovranno essere inseriti gli utenti con possibilità di accedere all'applicativo con credenziali degli altri utenti

Il gruppo titulusadmin dovrà avere accesso in lettura e in esecuzione a entrambe le cartelle e a tutti i files contenuti, il gruppo titulusprot a tutti i file tranne hcadm.dll.

Aggiungere inoltre nell'intero albero www gli utenti locali di servizio di IIS con diritto *Controllo completo*:

- utente IWAM_<nomemacchina>
- gruppo IIS_WPG

ATTENZIONE: Per abilitare il logging all'interno del file hc.log sia nella cartella isapi\docway3 sia nella cartella isapi\acl è necessario impostare i diritti di scrittura sui file hc.log e hc.loc per entrambi i gruppi titulusadmin e titulusprot. Il file hc.log non è soggetto a restrizioni di dimensione, per questo motivo per evitare di saturare il disco nel tempo, si sconsiglia di attivare il logging se non per motivi di debug.

- **Impostare i diritti del filesystem sulle cartelle isapi**

Successivamente è necessario aggiungere alla sezione Estensioni servizio web le librerie dll utilizzate:

- www\isapi\acl\bin\hcprot.dll
- www\isapi\acl\bin\hcadm.dll
- www\isapi\docway3\bin\hcadm.dll
- www\isapi\docway3\bin\hcprot.dll

utilizzando un nome indicativo del servizio formito (es: titulus) e abilitare il checkbox finale "*consenti….*".

- **Inserire le librerie nelle estensioni consentite**

Attenzione: il server che ospita IIS non deve essere un domain controller. Esiste qualche policy di base (o bug) che blocca l'accesso agli utenti ad IIS sul domain controller a meno che non si utilizzi l'utente fittizio AUTHENTICATED USERS. Questo genera buchi nella sicurezza.

E' necessario configurare i file hc.ini nelle cartelle e:\Titulus\webapps\www\isapi\docway3\bin e e:\Titulus\webapps\www\isapi\acl\bin, modificando il valore *host* nel caso il server che ospita tomcat non sia lo stesso su cui si trova IIS.

- **Configurare opportunamente hc.ini**

E' necessario riavviare il servizio di IIS per applicare la configurazione.

- **Riavviare il "Servizio di pubblicazione sul World Wide Web"**

Accorgimenti lato client

Per poter utilizzare l'autenticazione integrata di Windows, è necessario che all'interno dell'area di sicurezza in cui si trova il sito del protocollo, sia abilitata la voce: *accedi automaticamente con nome utente e password correnti*. Questa impostazione solitamente è attivata nell'area “Intranet”, ma non nelle altre aree. Si sconsiglia in questo caso di attivare l'opzione per l'area “internet” (per motivi di sicurezza), ma di collocare manualmente il sito in un altra area tramite la tabella “Protezione” nella configurazione di Internet Explorer.

Attenzione: di base, se il protocollo si trova all'interno della stessa rete fisica della macchina client si troverà nell'area “Intranet”, altrimenti si troverà nell'area “Internet”. E' possibile verificare in quale aree di sicurezza si trova il sito del protocollo rispetto al client osservando quanto scritto nella barra di stato di Internet Explorer (icona in basso a destra)

Il link differirà da quello base di tomcat in questo modo:

```
http://[host]/xway/application/xdocway/engine/hcprot.dll
```

oppure

```
http://[host]/xway/base/acl/engine/hcprot.dll
```

E' possibile comunque indicare le variabili aggiungendo “?variable=valore” al termine dell'indirizzo.

[1)] questo è necessario nel caso la macchina che ospita l'applicativo abbia un sistema operativo differente