DocWay3 - Metodi di Autenticazione

Il sistema di autenticazione di tomcat prevede l'utilizzo di moduli aggiuntivi per permettere diversi tipi di autenticazione. La struttura modulare di questo sistema permette di utilizzare diversi sottosistemi. Viene a questo punto definito un Realm a cui è possibile assegnare il modulo desiderato: da quelli compresi nell'installazione di Tomcat, a quelli che possono essere scaricati dal web o addirittura implementati per soluzioni personalizzate. I moduli di autenticazione attualmente utilizzati da noi sono:

- Autenticazione di base, tramite db xml su disco (tomcat-users.xml)
- Autenticazione LDAP, tramite directory su protocollo Idap
- Autenticazione mysql, autenticazione SQL (manuale in elaborazione)

In alternativa è possibile disattivare il sistema di autenticazione di Tomcat e utilizzare un proxy come Apache Web Server o IIS per fornire il servizio di autenticazione. Questa pratica è poco utilizzata poiché Tomcat ha già molti moduli equivalenti a quelli per Apache WS e generalmente si decide di risparmiare risorse non impiegando IIS come proxy. Tuttavia viene ancora utilizzato per integrazioni con ambienti Microsoft il seguente sistema:

• Autenticazione Active Directory, tramite un isapi per IIS

Autenticazione di base

L'autenticazione di base di Apache Tomcat è un sistema proprietario di controllo delle credenziali tramite un database interno. Questo database è contenuto all'interno del file xml tomcat-users.xml nella cartella conf di Tomcat (ad es. /opt/apachetomcat-6.0.26/conf).

L'autenticazione base di Tomcat riassume in modo molto semplice ed essenziale la politica di ACL di Tomcat che prevede tre campi:

- Utente
- Password
- Ruolo

La limitazione dei diritti di ogni ruolo viene poi definita all'interno del file web.xml di ogni singola applicazione. Un esempio di tomcat-users.xml può essere il seguente:

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="admjspuser"/>
<role rolename="jspuser"/>
<role rolename="manager"/>
<role rolename="admin"/>
<user username="admin" password="37c93139d9fb08245b0eb90874912bf0" fullName=""
roles="admin, admjspuser, jspuser, manager"/>
<user username="protocollista" password="37c93139d9fb08245b0eb90874912bf0" fullName="Utente
base" roles="jspuser"/>
<user username="responsabile" password="37c93139d9fb08245b0eb90874912bf0" fullName="Utente
amministrativo" roles="admjspuser,jspuser",/>
</tomcat-users>
```

Come si può notare dall'esempio si tratta di un semplice DB in xml:

- tomcat-users elemento radice, deve essere presente e tutti i dati devono essere contenuti all'interno.
- role indica una dichiarazione di un ruolo, l'elemento è facoltativo in quanto tomcat crea questi elementi automaticamente dopo la prima lettura del file
- **user** elemento che definisce un utente
- username si tratta del nome utente per effettuare l'accesso
- password password di accesso con cifratura MD5
- roles ruolo assegnato all'utente

I ruoli preimpostati per un installazione di docway sono i seguenti:

- admin ruolo generico amministratore docway/tomcat
- manager ruolo per l'accesso all'applicazione manager di tomcat
- admjspuser ruolo per l'accesso all'interfaccia amministratore di docway (docwayadm)
- jspuser ruolo per l'accesso semplice a tomcat.

×

Nonostante alcuni ruoli possano intersecarsi, è importante specificare esplicitamente nell'utente tutti i ruoli di cui si ha bisogno. In pratica l'amministratore avrà tutti i ruoli, il protocollista solo jspuser. E' inoltre consigliato l'utilizzo dei soli ruoli admjspuser e jspuser per gli utenti che non hanno formazione/mansioni tecniche.

Per la maggior parte degli ambienti è sufficiente specificare jspuser per tutti gli utenti, admjspuser per il responsabile del protocollo e admin,manager,admjspuser per i tecnici.

Creazione del file tomcat-users.xml tramite script

E' possibile creare un nuovo file tomcat-user.xml in qualsiasi modo, basta seguire le specifiche precedenti. Un possibile modo di creazione, che non prevede login con spazi e usa password iniziali da cambiare al primo accesso o per ambienti di test, potrebbe essere il seguente script bash:

```
#!/bin/bash
export nomefile="${1}"
echo "<tomcat-users>
  <role rolename=\"manager\"/>
  <role rolename=\"admjspuser\"/>
  <role rolename=\"admin\"/>
  <role rolename=\"jspuser\"/> "
# Rimuovere la riga seguente nel caso si voglia rimuovere l'utente admin 3di
echo "<user username=\"admin\" password=\"21232f297a57a5a743894a0e4a801fc3\"
roles=\"manager,admin,admjspuser,jspuser\"/>"
for i in `cat $nomefile`; do
   export $i
   password=`echo -n "${i}12345"|md5sum`
   echo "<user username=\"${i}\" password=\"${password}" roles=\"jspuser\"/>"
done
echo "</tomcat-users>"
```

Lo script prevede come parametro un file di testo che comprende tutti gli utenti uno per riga. Un esempio di esecuzione potrebbe essere:

```
nomescript fileutenti.txt > tomcat-users.xml
```

E' necessario ora aggiungere i ruoli per gli utenti amministratori con un editor e assicurarsi che le password vengano modificate. E' possibile anche impostare l'applicativo per fare in modo che al primo accesso venga richiesta la modifica delle password automaticamente.

Caricamento dei nuovi utenti

Prima di caricare il nuovo file è necessario fermare il servizio tomcat:

/etc/init.d/tomcat6 stop

Sovrascrivere il file esistente con quello appena creato:

```
cp ~/tomcat-users.xml /opt/apache-tomcat-6.0.20/conf
```

Riavviare tomcat:

```
/etc/init.d/tomcat6 start
```

Nello stesso modo è possibile effettuare le modifiche direttamente sul file nel caso di variazioni.

Autenticazione LDAP

Il servlet container Tomcat supporta diverse fonti di autenticazione: oltre alla autenticazione di default, è possibile delegare l'autenticazione ad un altra risorsa, quale un server LDAP. La documentazione ufficiale sul sito di Apache Tomcat contiene una panoramica generale delle opzioni di collegamento, mentre a questa pagina sono riportati alcuni esempi pratici di utilizzo.

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: uid=admin,ou=docway,dc=net objectClass: inetOrgPerson uid: admin sn: app cn: Amministratore userPassword: test dn: uid=protocollista,ou=docway,dc=net objectClass: inetOrgPerson uid: protocollista sn: app cn: Utente Base userPassword: test dn: uid=responsabile,ou=docway,dc=net objectClass: inetOrgPerson uid: responsabile sn: app cn: Utente Amministrativo userPassword: test roles.ldif dn: cn=admin,ou=docway,dc=net objectClass: groupOfUniqueNames cn: admin uniqueMember: uid=admin,ou=docway,dc=net dn: cn=manager,ou=docway,dc=net objectClass: groupOfUniqueNames cn: manager uniqueMember: uid=tomcat,ou=docway,dc=net uniqueMember: uid=admin,ou=docway,dc=net dn: cn=admjspuser,ou=docway,dc=net objectClass: groupOfUniqueNames cn: admjspuser uniqueMember: uid=responsabile,ou=docway,dc=net uniqueMember: uid=admin,ou=docway,dc=net dn: cn=jspuser,ou=docway,dc=net objectClass: groupOfUniqueNames cn: jspuser uniqueMember: uid=protocollista,ou=docway,dc=net uniqueMember: uid=admin,ou=docway,dc=net gruppi.ldif dn: ou=docway,dc=net objectClass: organizationalUnit ou: docway Questa Semplice configurazione associa 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

installazioni windows

```
<Context path="/xway" docBase="e:\3di.it\docway3\xway" debug="0" privileged="true">
<Realm className="org.apache.catalina.realm.JNDIRealm"
    connectionURL="ldaps://ldaphost:636"
    userPattern="uid={0},ou=docway,dc=net"
    roleBase="ou=docway,dc=net"
    roleName="cn"
    roleSearch="(uniqueMember={0})"
/>
    <!--
    <Valve className="org.apache.catalina.valves.RemoteAddrValve"
        allow="127.0.0.1,localhost"/>
        -->
</Context>
```

Gli esempi sopra riportati sono adeguati ad uno scenario nel quale:

- 1. il server LDAP non richiede autorizzazione per il bind (assenza di attributi che indichino un nome utente e una password);
- il nome utente (login name) è contenuto esso stesso nel distinguished name (dn) degli elementi dell'albero della directory (esempio: uid=utente_docway,ou=docway,dc=net);
- il nome del/dei ruolo/i è contenuto nel campo cn sotto ou=docway,dc=net e riportato nell'attributo uniqueMember di un elemento di tipo utente con l'intero distinguished name ({0} in questo caso è l'intero dn).

Per una realtà nella quale le informazioni per la login degli utenti ed i loro ruoli sono più strutturati, si può utilizzare una configurazione tipo la seguente (sono omessi i dettagli relativi al context poiché irrilevanti per questo esempio):

```
<Context [...]>
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldaps://ldaphost:636"
alternateURL="ldaps://ldapsecondaryhost:636"
connectionName="cn=bindUser,ou=docway,dc=net"
connectionPassword="youllneverguessit"
userBase="ou=Utenti-docway,ou=docway,dc=net"
userSubtree="true"
userSearch="(loginName={0})"
roleBase="ou=Gruppi-docway,ou=docway,dc=net"
roleName="cn"
roleSearch="(member={0})"
/>
</Context>
```

In questo secondo esempio, la realtà delineata è la seguente:

1. Esiste un secondo server LDAP (alternateURL), al quale potersi rivolgere per l'autenticazione;

- 2. i parametri **connectionName** e **connectionPassword** indicano le credenziali (in questo caso, l'utente è specificato mediante un distinguished name) per effettuare il bind al server LDAP;
- gli elementi che contengono le informazioni degli utenti sono sotto il ramo ou=Utenti-docway,ou=docway,dc=net, anche in altre ou ivi contenute (parametro userSubtree="true");

- l'attributo nel quale ricercare la login specificata dagli utenti nella maschera di login all'interno di un elemento utente è loginName (parametro userSearch);
- 5. i ruoli sono presenti sotto il ramo ou=Gruppi-docway,ou=docway,dc=net (parametro roleBase);
- 6. il nome del ruolo è da ricercarsi nel suo common name (roleName="cn");
- infine, il nome del ruolo è anche contenuto nell'attributo member all'interno di un elemento utente (roleSearch="(member={0})"), per effettuare un controllo incrociato.

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 Idap 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 separata¹⁾ (frontend) è necessario:

- Avere IIS versione 6 o superiore già installato nel sistema
- Installare Msxml, qualora questo non sia già presente sul sistema
- 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 it-3di/docway3/xway/WEB-INF sulla macchina che ospita l'applicativo:

```
<!-- inizio protezione dei jsp -->
 <1 - -
<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>XDocwav 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 A00 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 A00 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

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 server²⁾
- Il server deve essere parte dello stesso dominio Active Directory dei client ³⁾

• 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 lato Tomcat

È necessario modificare un parametro del connettore AJP del server Tomcat che ospita l'installazione di Docway da pubblicare mediante IIS. Tale parametro indica a Tomcat di non occuparsi dell'autenticazione degli utenti, poiché se ne occuperà qualcun altro a monte (IIS nel nostro caso). Per fare ciò, aprire il file server.xml nella conf/ di Tomcat e modificare l'elemento riguardante AJP aggiungendo l'attributo **tomcatAuthentication** e impostandolo a **false**, nel seguente modo:

```
<!-- Define an AJP 1.3 Connector on port 8009 --> <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" tomcatAuthentication="false" />
```

<u>Link utili</u>

• Documentazione su AJP

Configurazione IIS versione 6

Docway3

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:\3di.it\docway3\:

Creazione guidata Directory virtuale		×
Alias directory virtuale Specificare un nome breve o alias per la d	irectory virtuale.	
Digitare l'alias che si desidera utilizzare per Utilizzare le stesse convenzioni di denomir	r accedere alla directory virtuale Web. nazione adottate per i nomi di directory.	
Alia <u>s</u> :	_	
	< Indietro Avanti >	Annulla

Γ	×	
L		l

tione guidata Directory virtuale				×	
ctory contenuto sito Web Specificare la posizione del contenuto do	pubblicare pal a	ito Web		(I)	
specificale la posizione dei contenuto da	pubblicare ner s	ito wed.		AS A	
mmettere il percorso per la directoru in cui	i è stato salvato.	il contenuto de	l sito Web		
Percorso:			1 51(0 17 00.		
e:\3di.it\docway3\xway			Sfoglia		
		J <u>_</u>	<u>_</u> g		
	a success		1		
	< <u>I</u> ndietro	<u>A</u> vanti >	Ann	iulla	
iope quidata Directory virtuale					
prizzazioni di accesso directory virt Impostare le autorizzazioni per questa dire	uale ctorv virtuale.				
5.3				200	
Consenti le seguenti autorizzazioni:					
 Lettura 					
Esecuzione script (ad esempio, ASP)					
🗌 Ese <u>c</u> uzione (ad esempio, applicazioni	ISAPLo CGI)				
🗖 <u>S</u> crittura					
Esplorazione					
Per completare la procedura quidat	ta, scenliere i	Avanti			
e e estipletare la procedura guida	a, oogioio i				
	< Indietro	(Avanti)	Ann	ulla	
	< Turgero	Oldina V		ionica	

• 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:

The setione Internet Information Services (IIS)	_ 🗆 🗙	
钉 Eile Azione Visualizza Fi <u>n</u> estra <u>?</u>	_ ð ×	
Nome Nome		
xdocway		
B → D base		
🔁 🥠 engine		
in the second s		
⊕-joinaccer ⊕-jj docs		
⊕ formatter		
	F	
Creazione guidata Directory virtuale		X
Autorizzazioni di accesso directory virtuale Impostare le autorizzazioni per questa directory virtuale.	Citty	No.
Consenti le seguenti autorizzazioni:		
F 1		
I✓ Lettura		
I <u>issec</u> uzione (ad esempio, applicazioni ISAPI o Ual)		
I scrittura		
I <u>E</u> spiorazione		
Per completare la procedura quidata, scegliere Avanti,		
		. 1
< Indietro <u>Avanti ></u>	Annul	a

Devono essere create nella sezione xway\application\xdocway con il percorso e:\3di.it\docway3\www\isapi\docway3\bin e nella sezione xway\base\acl con il percorso e:\it-3di\docway3\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

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: docway) 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.

• Proseguire con il capitolo Configurazioni aggiuntive

Configurazione IIS versione 7

Windows Server 2008 ha una gestione modulare dei componenti e di base le funzioni necessarie non sono installate. Per attivarle accedere all'interfaccia di gestione del server e selezionare il ruolo "WEB SERVER". Quando viene richiesto quali componenti attivare, aggiungere cgi, isapi, autenticazione integrata e autenticazione di base.

Una volta installato IIS creare una nuova directory virtuale dandogli il nome *xway*, e farla puntare all'omonima directory in e:\3di.it\docway3\:

Connections			C11
छेन 🗟 🖄 😸			Sites
📲 Start Page		Filter	
E-1 (Contraction Pool		Marso	
Sites	,		ault Web Site
Default	Explore Edit Permissions Add Application Add Virtual Directory Edit Bindings Manage Web Site Refresh Refresh Remove Rename Switch to Content Vie	····	
Add Virtual Directory			2 X
ad Arted Directory			
Site name: Default We Path: / Alias:	b Site		
xway			
Example: images			
Physical path:			
E:\3di.it\docway3\xway			
Pass-through authenticat	ion		
Connect as Test 9	Settings		
	ОК		Cancel

• Creare la directory virtuale xway

Successivamente è necessario creare le applicazioni *engine*:

Connections			-
🔍 - 🔒 🖄 🔗		Der Der	ra
Start Page			
		Filter:	
- 者 Application Pools		IIS	
🖻 🐻 Sites			
🖻 🌍 Default Web Site		0	
🚽 🔁 tomcat			
E 🔁 xway		Authentication	
en e			
		37	
	Explore		
L. L			
	Edit Permissio	ns	
	Convert to Ap	plication	
	Add Applicatio	n	enl
	Add Virtual Dir	rectory	
±… <mark>⊆</mark> term ⊆ docs	Manage Folde	r 🕨	
🖭 🛄 email_ 🔯	Refresh		
🖽 🛁 engine 🕀 🚞 format 🖾	Switch to Con	tent View	
🕀 🧮 oswfdesigne	r		
🕀 🧮 WEB-INF			
Add Application			? ×
Site name: Default Web Site			
Path: /xway/application/:	(docway		
Alias:	Application po	ol:	
engine	DefaultAppPo	ol	Select
, Example: sales			
Physical path:			
E:\3di.it\docway3\www\isapi\docv	way3\bin		
Pass-through authentication			
Connect as Test Settings.			
	100		
		ОК	Cancel

I	×	
1		

Site name:	Default Web Site		
Path:	/xway/base/acl		
Alias:		Application pool:	
enaine		DefaultAppPool	Select.
angune -		(1 1 .) (22.3)	
:xample: sal	es	1	
:xample: sali hysical path	es II		
:xample: sal hysical path :\3di.it\docv	es 1: way3\www\isapi\acl\	bin	
Example: sal Nysical path N3di.it\docu Nass-through	es 1: way3\www\isapi\acl\ 1 authentication	bin	
Example: sal Physical path C:\3di.it\docv Pass-through	es 1: way3\www\isapi\acl\ 1 authentication	bin	

Devono essere create nella sezione xway\application\xdocway con il percorso e:\3di.it\docway3\www\isapi\docway3\bin e nella sezione xway\base\acl con il percorso e:\it-3di\docway3\www\isapi\acl\bin

• Creare le applicazioni engine per xdocway e acl

Di base IIS 7 non consente l'esecuzione di isapi a 32 bit (come hcprot.dll). Questa funzionalità deve essere attivata nel seguente modo: Accedere a Application Pools apparirà la seguente finestra:

3	(General)		-
	.NET Framework Version	No Managed Code	
	Enable 32-Bit Applications	True	•
	Managed Pipeline Mode	Integrated	
	Name	DefaultAppPool	
	Queue Length	1000	
	Start Automatically	True	
Ξ	СРО		
	Limit	0	
	Limit Action	NoAction	
	Limit Interval (minutes)	5	
	Processor Affinity Enabled	False	-
	Processor Affinity Mask	4294967295	
Ξ	Process Model		
	Identity	ApplicationPoolIdentity	
	Idle Time-out (minutes)	20	
	Load User Profile	False	
	Maximum Worker Processes	1	
	Ping Enabled	True	
	Ping Maximum Response Time (second	90	
	Ping Period (seconds)	30	
	Shutdown Time Limit (seconds)	90	
	Startup Time Limit (seconds)	90	- 0

In questa tabella modificare il valore *Enable 32-bit Applications* in TRUE.

• Abilitare le isapi a 32 bit

Attenzione: se si abilita questa impostazione del pool di applicazioni di default le isagi a 32 bit funzioneranno, tuttavia non sarà comunque possibile mischiare applicazioni a 32 bit e applicazioni a 64 nello stesso pool. Se avete già altre applicazioni a 64 bit installate è necessario creare un'altro pool altrimenti smetteranno di funzionare.

Sempre nel 🕼 DefaultAppPool	disabilitare l'esecuzione di codice .NET, poiché interferisce in alcuni casi con l'esecuzione delle
isapi, Selezionare 🛅 Basic Sett	ngs , apparirà la finestra:

it Application Pool	?
Name:	
DefaultAppPool	
NET Framework version:	
No Managed Code	•
Managed pipeline mode:	
Integrated 🗾	

Nella tendina con etichetta .NET Framework Version selezionare No Managed Code

Disablitare .NET Framework



Mappings Spostarsi su 😌 Default Web Site nel menu a sinistra e selezionare il pulsante , nel menu a destra aprire la voce Edit Feature Permissions... . Comparirà una finestra:

Edit Feature Permissions	? ×
Permissions:	
🔽 Read	
🔽 Script	
Execute	
ОК	Cancel

Selezionare come nella foto tutti i diritti di esecuzione.

Authentication

• Attivare i diritti di esecuzione delle isapi



Tornare su 😌 Default Web Site e selezionare il pulsante ^{Authentication} , si accederà alla sezione relativa:

Group by: No Grouping	•		
Name 🔺	Status	Response Type	Ī
Anonymous Authentication	Disabled		
Basic Authentication	Enabled	HTTP 401 Challenge	
Windows Authentication	Enabled	HTTP 401 Challenge	

Disabilitare l'autenticazione anonima e abilitare l'autenticazione di base e l'autenticazione Windows come da immagine.

• Abilitare l'autenticazione integrata

Spostarsi nella sezione superiore nel menu a sinistra dove compare il nome del server e selezionare il pulsante Isapi and CGI



restrictions.

Comparirà una finestra con un elenco delle isapi consentite. Inserire i seguenti percorsi come da immagine:

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

d ISAPI or CGI Restriction		? ×
ISAPI or CGI path:		
E:\3di.it\docway3\www\isapi\acl\bin	i\hcprot.dll	
Description:		
Allow extension path to execute	é.	
<u>.</u>		

Assicurarsi che la casella di spunta sia selezionata.

- Consentire le isapi di Docway
- Proseguire con il capitolo Configurazioni aggiuntive

Configurazioni aggiuntive

E' necessario configurare i file hc.ini nelle cartelle e:\3di.it\docway3\www\isapi\docway3\bin e e:\it-3di\docway3\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"

E' necessario impostare i diritti sul filesystem nelle cartelle delle isapi e:\3di.it\docway3\www, in modo che siano leggibili dagli utenti che utilizzeranno l'autenticazione IIS. Per farlo solitamente si aggiungono 2 gruppi di utenti locali nel server:

- docwayusers in cui dovranno essere inseriti i protocollisti
- docwayadm in cui dovranno essere inseriti gli utenti con possibilità di accedere all'applicativo con credenziali degli altri utenti

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

Aggiungere inoltre nell'intero albero www gli utenti locali di servizio di IIS (solo per la versione 6) 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 docwayadm e docwayprot. 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

Configurare i limiti di download (e upload)

Nel caso non si riescano a scaricare allegati superiori ai 25MB, è necessario effettuare l'override della proprietà "maxRequestLength" a valori più alti. Per fare ciò, modificare il file web.config relativo al sito di docway aggiungendo i seguenti elementi:

```
<configuration>
[...]
<system.web>
<httpRuntime maxRequestLength="XXXXX" executionTimeout="600" />
</system.web>
[...]
<system.webServer>
<security>
<requestFiltering>
<requestLimits maxAllowedContentLength="YYYYYY" />
</requestFiltering>
</security>
</system.webServer>
[...]
</configuration>
```

dove XXXXXX e YYYYYY sono, rispettivamente, la massima dimensione di download ed upload consentiti (in byte).

Accorgimenti lato client

Impostazioni specifiche per Internet Explorer (IE)

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*. Dato che questa impostazione è attivata di default unicamente nell'area "Intranet Locale", si consiglia di non attivare l'opzione per le altre aree (per motivi di sicurezza), ma di collocare manualmente il sito in quest'area.

Per inserire il sito del protocollo nell'area "Intranet Locale" in Internet Explorer:

1. Aprire Internet Explorer, andare nel menù "Strumenti" e cliccare "Opzioni Internet":

- Windows Internet Explorer					
] about:blar	nk				
Visualizza	Preferiti	Strumenti	?		
		Elimina cr InPrivate Riapri ult	ronologia esplorazioni Browsing ima sessione di ricerca	CTRL+MAIUSC+CANC CTRL+MAIUSC+P	
		InPrivate Impostaz	: Filtering tioni InPrivate Filtering	CTRL+MAIUSC+F	
		Blocco po Filtro Sm Gestione	opup artScreen componenti aggiuntivi))
		Visualizza Impostaz	azione Compatibilità cioni Visualizzazione Compatibilità	i	
		Sottoscri Individua Windows	zione al feed, Izione feed I Update		×
		Strument	i di sviluppo	F12	
		Windows Diagnost	Messenger ica problemi di connessione		
		Opzioni I	nternet		

Conn General	ession	n ommi Drivoru	Avanzate
acherai	Protezioni	e privacy	
Pagina iniz	iale		
	Per creare le schede sulla riga corrisponde	della pagina iniziale nte.	, digitare ogni indirizzo
~	about:blank		<u> </u>
			-
		1	
	Pagina corrente	Pagina predefir	nita Pagina vuota
Cronologia	a esplorazioni 🛛 ———		
Ð	Consente di eliminare password salvate e le	i file temporanei, la e informazioni dei m	a cronologia, i cookie, le oduli Web.
	🔲 Elimina la cronolog	gia delle esplorazior	ni al momento di uscire
		Elimina	Impostazioni
Ricerca			
P	Consente di modificar ricerca predefinite.	e le impostazioni di	Impostazioni
Schede			
	Consente di modificar delle pagine Web.	e la visualizzazione	Impostazioni
Aspetto			
Cold	ori Lingue	Caratteri	Accesso facilitato

3. Selezionare "Intranet locale" e cliccare sul pulsante "Siti":

Opzioni Internet ? 🗙			
Connessioni Programmi Avanzate Generale Protezione Privacy Contenuto			
Selezionare l'area di cui visualizzare o modificare le impostazioni.			
Intranet locale Area riservata a tutti i siti Web sulla rete			
Livello di protezione per l'area Livelli consentiti per questa area: Tutti			
Medio-bassa - Impostazione appropriata per i siti Web sulla rete locale - (Intranet) - Esecuzione della maggior parte dei contenuti senza - -			
Livello personalizzato Livello predefinito			
Ripristina livello predefinito per tutte le aree			
OK Annulla Applica			

4. Cliccare sul bottone "Avanzate" nella finestra che viene aperta:



5. Scrivere l'URL del sito di DocWay nell'apposita casella di testo (dove è scritto http://esempio.com), assicurarsi che non sia selezionata la voce "Richiedi verifica server (https:) per tutti i siti dell'area" e cliccare sul bottone "Aggiungi":

Intranet locale	×			
È possibile aggiungere e rimuovere siti Web da o Tutti i siti Web compresi nell'area utilizzeranno la impostazioni di protezione.	questa area. e relative			
Aggiungi il sito Web all'area:				
http://esempio.com	Aggiungi			
Siti Web:				
	Rimuovi			
🔲 Richiedi verifica server (https:) per tutti i siti dell'area				
	Chiudi			

6. Il sito di DocWay dovrebbe ora comparire nell'elenco di siti web associati all'intranet locale:

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)

3)

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

Solitamente la versione corretta è già installata con IIS, viene fornita una versione compatibile con IIS 6 nel pacchetto di installazione

In alcuni casi è possibile utilizzare anche domini in trust, se vengono configurati correttamente i client