

EoleSSO - Tâche #29436

Scénario # 28809 (Terminé (Sprint)): Passer EoleSSO en TLS 1.2 sur EOLE 2.7

Utiliser le protocole par défaut

01/07/2020 03:21 PM - Joël Cuissinat

Status:	Fermé	Start date:	01/07/2020
Priority:	Normal	Due date:	
Assigned To:	Joël Cuissinat	% Done:	100%
Target version:	sprint 2019 51-03 Equipe MENSUR	Estimated time:	0.00 hour
		Spent time:	0.00 hour

Description

root@scribe:~# diff tlv1.out default.out

```
10,13c10,13
<          for TLS 1.1 (RFC4346) support... no
<          fallback from TLS 1.1 to... TLS 1.0
<          for TLS 1.2 (RFC5246) support... no
<          fallback from TLS 1.6 to... TLS1.0
---
>          for TLS 1.1 (RFC4346) support... yes
>          for TLS 1.2 (RFC5246) support... yes
>          fallback from TLS 1.6 to... TLS1.2
>          for inappropriate fallback (RFC7507) support... yes
16c16
<          for encrypt-then-MAC (RFC7366) support... yes
---
>          for encrypt-then-MAC (RFC7366) support... no
19c19
<          for version rollback bug in RSA PMS... no
---
>          for version rollback bug in RSA PMS... dunno
34c34
<          for AES-128-GCM cipher (RFC5288) support... no
---
>          for AES-128-GCM cipher (RFC5288) support... yes
42c42
<          for CHACHA20-POLY1305 cipher (RFC7905) support... no
---
>          for CHACHA20-POLY1305 cipher (RFC7905) support... yes
45c45
<          for SHA256 MAC support... no
---
>          for SHA256 MAC support... yes
```

Associated revisions

Revision 8c436cb5 - 01/07/2020 03:23 PM - Joël Cuissinat

Use default (=highest) protocol

Ref: #29436

Revision b2b674fe - 03/04/2020 04:25 PM - Joël Cuissinat

Use default (=highest) protocol

Ref: #29436

Revision f5699006 - 03/16/2020 10:44 AM - Joël Cuissinat

Use default (=highest) protocol

Ref: #29436

History

#1 - 01/07/2020 03:41 PM - Joël Cuissinat

- Status changed from *Nouveau* to *Résolu*
- Assigned To set to *Joël Cuissinat*
- % Done changed from 0 to 100

#2 - 01/22/2020 10:49 AM - Joël Cuissinat

- Status changed from *Résolu* to *Fermé*
- Remaining (hours) set to 0.0