

Title: Zintegrowane logowanie SSO za pomocą NTLM

Subject: eDokumenty - elektroniczny system obiegu dokumentów, workflow i CRM - AdminGuide/SSOAuth

Version: 16

Date: 07/03/24 09:17:16

Table of Contents

<i>Zintegrowane logowanie SSO za pomocą NTLM</i>	3
<i>Konfiguracja logowania automatycznego</i>	3
<i>Konfiguracja serwera IIS</i>	3
<i>Konfiguracja systemu eDokumenty</i>	3
<i>Konfiguracja pliku sso.aspx</i>	3
<i>Uruchomienie funkcjonalności</i>	4
<i>Konfiguracja funkcji logowania automatycznego w popularnych przeglądarkach</i>	4
<i>Firefox</i>	4
<i>Google Chrome i Internet Explorer</i>	4
<i>Wymagane pakiety</i>	4

Zintegrowane logowanie SSO za pomocą NTLM

Konfiguracja logowania automatycznego

Przed przystąpieniem do konfiguracji należy upewnić się, że spełnione zostały wszystkie wymagania. Aby automatyczne logowanie działało poprawnie:

Użytkownicy muszą logować się do systemu operacyjnego dzięki autoryzacji domenowej, czyli **Active Directory**.

Użytkownicy logują się do swoich stacji roboczych wykorzystując domenę.

Na kontrolerze domeny musi być uruchomiony serwer **IIS**, port jest dowolny.

Kontroler domeny oraz serwer eDokumentów **muszą** mieć dostęp do siebie nawzajem.

Konfiguracja serwera IIS

Z katalogu **/var/tpl** (Panel sterowania > Szablony systemowe) należy skopiować plik **sso.aspx.tpl** do katalogu na serwerze IIS, zmieniając mu nazwę na **sso.aspx** lub inną (nazwa **sso.aspx** zostanie użyta w dalsze części instrukcji). Plik ten musi być dostępny z zewnątrz poprzez protokół **HTTP** lub **HTTPS**.

Następnie należy wyłączyć anonimowy dostęp do pliku **sso.aspx** i wymusić autoryzację NTLM podczas dostępu do niego.

<http://technet.microsoft.com/pl-pl/library/cc754628%28v=ws.10%29.aspx>

Aby dodać Windows Authentication w IIS posłużmy nam poniższy artykuł

<https://www.iis.net/configreference/system.webserver/security/authentication/windowsauthentication/providers/add>

Należy sprawdzić instalację ASP.NET do poprawnego przetworzenia pliku **sso.aspx** [https://technet.microsoft.com/pl-pl/library/hh831475\(v=ws.11\).aspx](https://technet.microsoft.com/pl-pl/library/hh831475(v=ws.11).aspx)

Konfiguracja systemu eDokumenty

W pliku **config.inc** należy ustawić pewne stałe.

EXT_ACTIONS_ENGINE_URL - Adres główny systemu eDokumenty z kończącym slashem, np. <http://edokumenty.companyname.com/>

SSO_REMOTE_SERVICE - Pełny adres do pliku **sso.aspx**, np. <http://domena.firma/sso.aspx>

SSO_SALT - Losowy ciąg znaków który dodatkowo zabezpieczy system logowania, np. **abcd1234**

SSO_LOGIN_ENABLED - Na tym etapie konfiguracji należy zostawić wartość **FALSE** aby nie zaburzyć działania systemu.

EDOK_API_LOGIN - Login, który umożliwi zalogowanie do API, dowolny.

EDOK_API_PASSWORD - Hasło do API, dowolne.

Konfiguracja pliku sso.aspx

Należy otworzyć plik **sso.aspx** w edytorze tekstu w trybie **UTF-8 bez BOM** - np. w darmowym Notepad++.

Następnie znajdujemy deklarację zmiennych **api_user**, **api_pass**, **api_host**, **entity** oraz **salt** i ustawiamy je na poprawne wartości. Opis zmiennych:

api_host - Pełny adres do pliku **eDokumentyApi.php**, np. <http://edokumenty.companyname.com/eDokumentyApi.php>

api_user - użytkownik API, taki sam jak w **config.inc**

api_pass - Suma md5 hasła **EDOK_API_PASSWORD** generowanego przy pomocy md5 oraz solenie jej i ponowne liczenie sumy. Pseudokod generujący sumę: dla PHP

```
md5(md5('<HASŁO DO API>').'_SOAP_eDok_api');
```

dla PostgreSQL

```
SELECT md5(md5('<HASŁO DO API>' || '_SOAP_eDok_api');
```

Powyższa definicja jest konkatencją md5 z hasła do API oraz ciągu znaków o treści: `_SOAP_eDok_api`.

entity - Symbol jednostki organizacyjnej, np. beta

salt - Wartość soli, czyli wartość `SSO_SALT` z `config.inc`

Uruchomienie funkcjonalności

Aby uruchomić logowanie automatyczne należy w pliku **config.inc** systemu eDokumenty zmienić wartość stałej `SSO_LOGIN_ENABLED` na **TRUE**.

Aby wyłączyć - wystarczy ustawić na **FALSE**.

Uwaga: zmiany są natychmiastowe.

Konfiguracja funkcji logowania automatycznego w popularnych przeglądarkach

Firefox

Należy otworzyć stronę `about:config`, w wyszukiwarce wpisać **ntlm-auth.trust**, następnie podwójnie kliknąć na **network.automatic-ntlm-auth.trusted-uris** i po przecinku wpisać adres zarówno systemu eDokumenty jak i serwera IIS. Przykład:

<http://moja.firma.biz>,<http://kontroler.firma>

Google Chrome i Internet Explorer

W systemie Windows należy otworzyć **komponent Opcje internetowe**, przejść na zakładkę **Zabezpieczenia**, kliknąć przycisk **Poziom niestandardowy** i na dole listy, w sekcji **Uwierzalnianie użytkownika** wybrać opcję **Zaloguj automatycznie z bieżącą nazwą użytkownika i hasłem** i zaakceptować przyciskiem OK. Następnie kliknąć na **Zaufane witryny** w górnej części okna, następnie na przycisk **Witryny**, a następnie dodać do listy adres serwera eDokumenty jak i serwera IIS.

Wymagane pakiety

Do poprawnego działa usługi wymagany jest pakiet `php-curl`

```
apt-get install php5-curl
```

w pliku `php.ini` dodajemy dla Linux

```
extension=curl.so
```

dla Windows

```
extension=php_curl.dll
```

Następnie wykonujemy restart Apache2

```
/etc/init.d/apache2 restart
```