**Elanor – EGJE**

**Provozní dokumentace**

[Index dokumentací](index.htm) **(html)**

[Index dokumentací](index.docx) **(docx)**

1. **Obsah**

[**1** **Obsah** 1](#_Toc198146772)

[2 Úvod - technologie 3](#_Toc198146773)

[2.1 Nasazení aplikačního serveru 3](#_Toc198146774)

[2.1.1 Aplikační server 4](#_Toc198146775)

[2.2 Nasazení serveru pro modul EGJEWeb2, HR Portál 4](#_Toc198146776)

[2.3 Provoz přes terminálové servery 5](#_Toc198146777)

[3 HW a SW požadavky 6](#_Toc198146778)

[3.1 Shrnutí 6](#_Toc198146779)

[3.2 Databázový server 8](#_Toc198146780)

[3.3 Stanice uživatele pro standardního klienta 9](#_Toc198146781)

[**3.4** **Stanice uživatele pro EGJEWeb2 klienta** 10](#_Toc198146782)

[3.5 Přístup EGJE na internet 10](#_Toc198146783)

[3.6 Spouštěcí parametry EGJEWeb2 11](#_Toc198146784)

[3.6.1 Referentské rozhraní 11](#_Toc198146785)

[3.6.2 Rozhraní HR Portál 11](#_Toc198146786)

[3.6.3 Společná syntaxe 11](#_Toc198146787)

[3.6.4 HR Portál volaný jako portlet 12](#_Toc198146788)

[**3.7** **Konfigurace připojení k poštovnímu serveru** 13](#_Toc198146789)

[**4** **Instalace a dimenzování parametrů** 14](#_Toc198146790)

[**5** **Režim správy databáze - datového schematu Elanor EGJE** 14](#_Toc198146791)

[5.1 Objekty BLOB - uložení dokumentů 15](#_Toc198146792)

[**6** **Správa aplikace - změnové řízení** 15](#_Toc198146793)

[**6.1** **Nastavení a změna parametrů pomocí utility configurator\_egje** 15](#_Toc198146794)

[**6.1.1** **Adresa EWS** 16](#_Toc198146795)

[**6.1.2** **AS - aplikační server** 17](#_Toc198146796)

[**6.1.3** **Připojení k databázi - DB** 21](#_Toc198146797)

[**6.1.4** **Obecné** 23](#_Toc198146798)

[**6.1.5** **Ověření** 25](#_Toc198146799)

[**6.1.6** **Atributy instalace** 37](#_Toc198146800)

[6.1.7 Logování 38](#_Toc198146801)

[6.1.8 Proxy 38](#_Toc198146802)

[6.2 Nastavení a změna parametrů pomocí utility „MultiConfigurator“ 38](#_Toc198146803)

[**6.3** **Adm51 - Změnové řízení databáze** 40](#_Toc198146804)

[**6.4** **Pomocné utility** 43](#_Toc198146805)

[**6.4.1** **Utilita anonymizace** 43](#_Toc198146806)

[6.4.2 Uživatelská sestava Ela01vxc dříve validateXML - validateClobs 44](#_Toc198146807)

[6.5 Využití SuperKonfigurátoru k vytvoření reportu nad více DB pro možnosti porovnání a nalezení položek v různých DB 45](#_Toc198146808)

[**7** **Správa uživatelů aplikace** 45](#_Toc198146809)

[**7.1** **Založení uživatele – stručné shrnutí** 45](#_Toc198146810)

[**7.2** **Práva k objektům a k řádkům, role a profily** 45](#_Toc198146811)

[**7.2.1** **Pojmy a základní otázky** 45](#_Toc198146812)

[**7.2.2** **Nastavení přístupových práv v aplikaci** 48](#_Toc198146813)

[**7.2.3** **Objekty práv konfigurace** 57](#_Toc198146814)

[**7.2.4** **Zastupování uživatele na profilu** 58](#_Toc198146815)

[**7.2.5** **Dílčí (limitovaný) správce** 58](#_Toc198146816)

[**7.2.6** **Příloha – model přístupových práv EGJE** 59](#_Toc198146817)

[**7.2.7** **Speciální objekty přístupových práv** 59](#_Toc198146818)

[**8** **Hromadná korespondence** 70](#_Toc198146819)

[**8.1** **Použití MS Office** 70](#_Toc198146820)

[**8.2** **Použití OpenOffice** 71](#_Toc198146821)

[**8.3** **Rtf sestavy a uživatelské sestavy - přímé volání MS Office** 71](#_Toc198146822)

[**8.3.1** **Technologický předpoklad** 71](#_Toc198146823)

[**8.3.2** **Použití** 71](#_Toc198146824)

[**8.4** **Hromadná korespondence – Dokumenty DOCX ELA** 72](#_Toc198146825)

[**9** **Uživatelské sestavy** 72](#_Toc198146826)

[**9.1** **Schema** 72](#_Toc198146827)

[**9.2** **Popis aparátu** 72](#_Toc198146828)

[**9.3** **Vlastní vytvoření a editace sestavy** 73](#_Toc198146829)

[**9.3.1** **Přenesení uživatelské sestavy na jinou db** 73](#_Toc198146830)

[9.4 Distribuce uživatelské sestavy Elanor 73](#_Toc198146831)

[**9.5** **Předchozí verze sestavy** 74](#_Toc198146832)

[**10** **Instalace patch a výdejů pomocí utility SuperConfigurator** 75](#_Toc198146833)

[**10.1** **Instalace patche - výdeje:** 75](#_Toc198146834)

[**10.2** **Vlastní instalace utility** 75](#_Toc198146835)

[**10.2.1** **SuperConfigurator - restrikce spuštění pomocí Adm51** 76](#_Toc198146836)

[**10.2.2** **Spuštění SuperConfiguratoru bez parametru** 76](#_Toc198146837)

[**10.3** **Další funkčnost** 76](#_Toc198146838)

[11 Výčet povolených formátů pro nahrání do systému 78](#_Toc198146839)

[**Příloha A1. Instalace verze Oracle** 79](#_Toc198146840)

[**Příloha A2. Instalace verze MS SQL** 79](#_Toc198146841)

[**Příloha B. Instalace programového vybavení (std. klient)** 80](#_Toc198146842)

[**Instalace předlohy pro spouštění std. klienta pomocí EWS** 80](#_Toc198146843)

[**Instalace - přímé a dávkové spouštění std. klienta EGJE** 81](#_Toc198146844)

[**Instalace - možnost společného programového vybavení pro více databází** 82](#_Toc198146845)

[**Instalace - možnost spouštění standardního klienta** 82](#_Toc198146846)

[**Příloha C1. Instalace EGJEWeb2** 84](#_Toc198146847)

[11.1.1 Rozdíly v instalaci Tomcat 9 a Tomcat 10 86](#_Toc198146848)

[11.1.2 Tomcat a SSL/TLS 86](#_Toc198146849)

[11.1.3 Tomcat a cookie - atribut SameSite 86](#_Toc198146850)

[**Provoz EGJEWeb2 přes loadbalancer** 87](#_Toc198146851)

[**Bezpečnostní filtr** 87](#_Toc198146852)

[**Nastavení hlaviček Apache httpd (Apache Hypertext Transfer Protocol Server)** 88](#_Toc198146853)

[**Příloha D. Instalace Aplikačního serveru EGJE** 89](#_Toc198146854)

[**Příloha E. Logování - AS, EGJEWEB2** 91](#_Toc198146855)

[**Příloha F1. Nastavení JRE pro servery - AS, EGJEWEB2** 93](#_Toc198146856)

[**Příloha G. Monitorování AS pomocí JMX** 93](#_Toc198146857)

[**Příloha H. Monitorování serverových procesů na AS z java klienta resp. EGJEWEB2** 94](#_Toc198146858)

[**Příloha I. Monitorování databáze** 94](#_Toc198146859)

[**Příloha J. Monitorování EGJEWeb2(HR portál), AS pomocí Java Melody** 96](#_Toc198146860)

[**Příloha J1. Monitorování pomocí JavaFlightRecorder** 98](#_Toc198146861)

[**Příloha K. EGJE a webové služby** 98](#_Toc198146862)

[**Příloha L. Více hlášek v některých protokolech** 99](#_Toc198146863)

[**Příloha M. Základní popis databázových zámků** 99](#_Toc198146864)

[**Příloha N. Další Security opatření** 100](#_Toc198146865)

[12 Upozornění 101](#_Toc198146866)

# Úvod - technologie

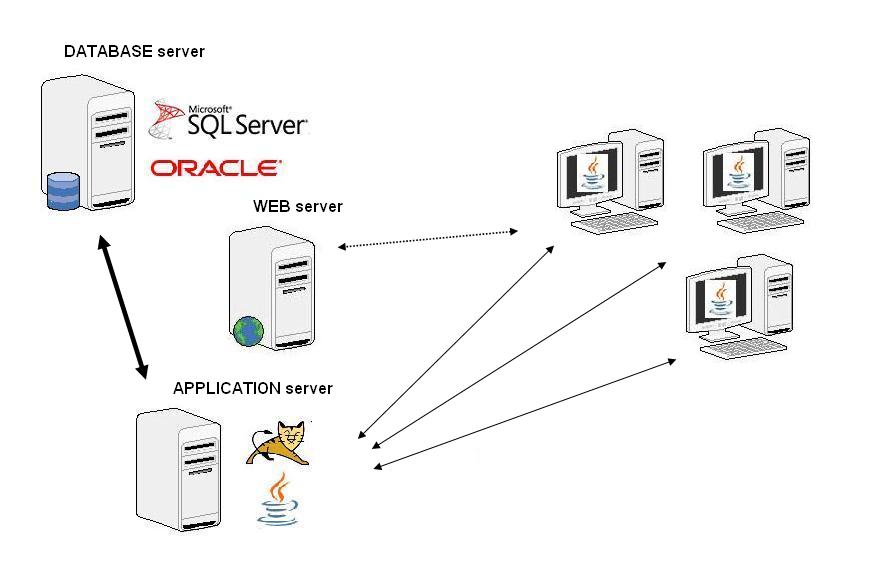
Elanor Global Java Edition (EGJE) je systémem pro práci s lidskými zdroji (HR), jinými slovy personální a mzdovou agendu.

Technologicky se skládá z SQL databáze, stanic uživatele a případně také aplikačního serveru resp. serveru pro EGJEWeb2. Systém je realizován pomocí programovacího jazyka java, pouze velmi malé části jsou naprogramované přímo v SQL databázi v jejím nativním jazyce, resp. části EGJEWeb2 v javascriptu.

Aplikační server používá java prostředí. Je možné použít i OpenJDK javu i javu z Oracle SE subscription.

EGJEWeb2 používá servlet kontejner Tomcat.

Distribuce aplikace se provádí pomocí jejího uložení na interním web serveru organizace (resp. v horším případě souborovému serveru) a následným zpřístupněním pro stanice pomocí EGJE Web Start.



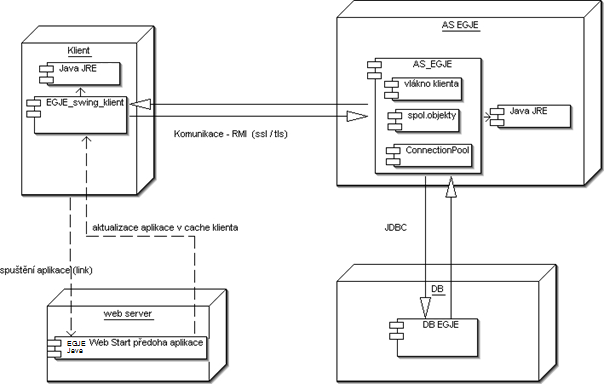
Mobilní přístup je řešen pomocí webovských technologií (EGJEWeb2). Aplikace je vystavěna v duchu "Responsive web design" a přizpůsobuje se prostředí, ve kterém je spuštěna.

K dispozici je také možnost speciální autentizace pro mobilní zařízení resp. možnost zadání určitých restrikcí pro mobilní přístup.

## Nasazení aplikačního serveru

Otázka nasazení, resp. nenasazení aplikačního serveru závisí především na síťových a paměťových požadavcích a na distribuci zatížení. Aplikační server komunikuje s aplikací pomocí technologie RMI.

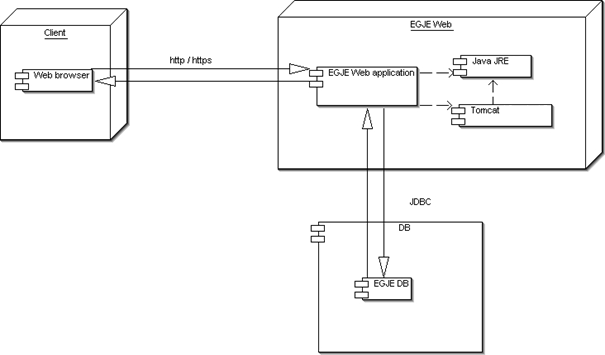
### Aplikační server



* aplikační server je volitelná komponenta
* od e201905 může jako AS sloužit i EGJEWeb (instalován na Tomcat)
* veškerá klientova komunikace probíhá přes AS pomocí RMI (implicitně šifrováno)
* komunikace je komprimována, to umožňuje výrazné snížení síťového provozu
* oproti provozu bez aplikačního serveru se liší v těchto aspektech:
  + stanice klienta nemusí mít nakonfigurováno připojení k databázi, nemusí mít ani přístup k databázovému serveru
  + stanice klienta nikdy není vlastníkem ani zprostředkovaného ani přímého databázového připojení (zabezpečení)
  + autentizace uživatele probíhá na aplikačním serveru
  + veškerá komunikace je šifrována (šifrování ssl / tls)
  + klientská aplikace je paměťově úspornější a řadě akcí rychlejší (záleží na konkrétní konfiguraci);  
    na druhou stranu je potřeba mít dostatečně dimenzovaný server
  + server poskytne řadu údajů aplikaci rychleji, neboť používá kešování informací
  + správce má možnost monitorovat a spravovat úlohy a klienty (Adm51)

## Nasazení serveru pro modul EGJEWeb2, HR Portál

Modul EGJEWeb2 slouží jako uživatelské rozhraní pro zaměstnance, resp. manažera. Je však otázkou implementace, zdali manažer (a případně který manažer) bude používat jednoduchého web klienta HR Portál nebo funkčně bohatšího, ale složitějšího "referentského" klienta EGJEWeb2, nebo jemu analogického klienta standardního. Aplikace poskytuje i většinu referentské funkčnosti.  
Rozhraní HR Portál je samostatnou obchodní položkou.



* EGJEWeb2 je Java Servlet aplikace, která používá framework GWT a komponenty ExtJs. Tato aplikace používá a zpřístupňuje kromě sestav i formuláře ze standardního EGJE java klienta.
* Aplikace používá shodnou technologii pro práci s databází (elanor datasource resp. JDBC) a stejnou technologii tvorby sestav (Jasper Reports) jako standardní EGJE, přičemž sestavy ze standardní aplikace jsou plně přenositelné do web řešení, přenositelnost formulářů je asi 90%.

## Provoz přes terminálové servery

Obecně lze aplikaci provozovat přes terminálové servery (Citrix). Je však třeba server dostatečně výkonově a paměťově dimenzovat.

Také integrace s prostředím uživatele je o něco složitější (hromadná korespondence, exporty XLS, e-mailová komunikace) neboť SW, který výstupy z EGJE přebírá a dále zpracovává je obvykle na stanici uživatele.

Doporučujeme v této konfiguraci umístit pracovní adresář (Nastavení / Uživatelská nastavení / Adresář pro export) na citrixový diskový svazek (a případné kopírování na stanici uživatele provádět pomocí kopírování souboru na zpřístupněný lokální disk nebo analogicky Adobe Reader / Soubor / Uložit kopii).

Pro práci s html položkami vyplňovanými přes schránku (např. Zpu01 / Obsah kurzu) je zapotřebí zpřístupnit v citrix html schránku - viz <http://support.citrix.com/article/CTX112063>

Pro spouštění EGJE na citrix instalace jsou tyto možnosti:

* přímé spouštění přes javaw resp. spouštění dávkou ze souborového serveru   
  – doporučená varianta!  
  (obzvlášť, je-li více Citrix serverů)  
  viz Příloha B: Instalace - alternativní dávkové spouštění EGJE
* spouštění přes EWS - nevýhodou je cache aplikace zvyšující velikost domovského adresáře uživatele, je však možné využít tzv. systémovou cache.

# HW a SW požadavky

## Shrnutí

**Databáze:**

* + Oracle:
    - Oracle 12c R2, 18c, 19c
  + MS-SQL Server
    - Microsoft SQL Server 2014
    - Microsoft SQL Server 2016
    - Microsoft SQL Server 2017
    - Microsoft SQL Server 2019
    - Microsoft SQL Server 2022

**Stanice uživatele Java klienta**

* Obecně libovolná dostatečně dimenzovaná stanice - na které je podporována Java 11, Java 17 nebo Java 21 (pouze LTS verze, jiné nejsou ze strany Elanor podporovány)**,** s prohlížečem PDF, a přístupem na tiskárnu, resp. lokální tiskárnou
* Doporučené rozlišení od 1366 x 768
* Doporučujeme též instalaci SW na práci s exportními soubory XLSX, CSV, XLS  
  (Microsoft Office, resp. Microsoft Excel viewer, resp. OpenOffice/LibreOffice)

**Aplikační server**

* + Obecně libovolný server, na kterém je podporována Java 11, Java 17 nebo Java 21 (pouze LTS verze, jiné nejsou ze strany Elanor podporovány).  
    Nemusí to nutně být samostatný server, pro menší instalace je možné společné umístění s databázovým serverem
  + Aplikační server není povinnou komponentou, resp. může běžet i na EGJEWeb2 serveru
  + Úloha aplikačního serveru spočívá v optimalizaci provozu po linkách a poskytuje také daleko větší zabezpečení než provoz bez něj
  + Instalace AS používá wrapper Tanuki  
    **Upozornění** - jeho verze pro 64-bitové Windows je placená, pro ostatní postačí neplacená verze.  
    Nastavení parametrů je stručně zmíněno v Příloze D.

**Server EGJEWeb2**

* Server, na kterém je podporována Java 11, Java 17 nebo Java 21 se servlet kontejnerem Apache Tomcat verze 9.0.x nebo 10.1.x. (testováno na OS Windows a Linux).
* Pro verzi Tomcat 9.0.x doporučujeme použít minimální verzi 9.0.102 a pro verzi 10.1.x minimálně verzi 10.1.39.
* Z důvodu bezpečnostních zranitelností se nedoporučuje používat starší verze.
* Podpora řad Apache Tomcat 7.x a 8.x byla UKONČENA. (https://endoflife.date/tomcat)
* Instalace je popsána v Příloze C1.

**Stanice uživatele EGJEWeb2**

* Web browser (Google Chrome, EDGE, Firefox. Browsery IE a Safari nejsou podporovány.)
* Doporučené rozlišení od 1366 x 768
* Stanice by měla disponovat prohlížečem PDF a přístupem na tiskárnu, resp. lokální tiskárnou
* Doporučujeme též instalaci SW na práci s exportními soubory XLSX, CSV, XLS  
  (Microsoft Office, resp. Microsoft Excel viewer, resp. OpenOffice/LibreOffice)  
  resp. DOCX, RTF, ODT (Microsoft Word resp. OpenOffice/LibreOffice)

**Web server (resp. souborový server) s EWS předlohou**

* + Obecně libovolný intranetový web server (hůře souborový server) přístupný koncovým uživatelům.
  + Na server je umístěna aplikační předloha formou aplikačního balíku EGJE Web Start, resp. Java Web Start
  + Opět to nemusí být samostatný server, jde o vysdílení jednoho adresáře.

**Autentizační server**

* + Aplikace nevyžaduje vyhrazený autentizační server. Je možné použití již existující v organizaci používaný.
  + Typickým autentizačním serverem je doménový server Windows Active directory resp. nějaký LDAP server.

**Poštovní server**

* + Některé části systému (typicky workflow) používají e-mailovou komunikaci. Ta je realizována pomocí připojení na SMTP server pro odesílání pošty.
  + V oblasti uchazečů může být použito i POP3 rozhraní pro příjem pošty. Je vhodné, je-li poštovní server vybaven nějakým antispamovým a antivirovým řešením, není to však nezbytnou podmínkou. Aplikace rozezná "svoje" e-maily a odpovědi na ně a zpracovává přednostně tyto.
  + Konfigurace připojení k poštovnímu serveru - viz dále

## Databázový server

**Podporované databáze:**

* + **Oracle 12c R2** (Standard Edition, Enterprise Edition) - verze >= 12.1.0.1
  + **Oracle 18c** (Standard Edition, Enterprise Edition)
  + **Oracle 19c** (Standard Edition, Enterprise Edition)
  + Microsoft SQL Server 2014
  + Microsoft SQL Server 2016
  + Microsoft SQL Server 2017
  + Microsoft SQL Server 2019
  + Microsoft SQL Server 2022

Databáze může být provozována na HW s různým OS (unix, linux, windows)

Charakter aplikace je převážně transakční zpracování (OLTP).

**Databázovou instanci oracle vytváříme s unicode charset a musí být nainstalována s XML DB.**

Instalace s Oracle podporují plné využití znaků unicode, zatímco instalace s SQL Serverem jsou směrovány pro data ve znakové sadě 1250. (unicode znaky jsou dovoleny jen u některých textů a jsou k dispozici jen ve vybraných zobrazeních).

Náročnost na výkon a velikost databáze je přibližně stejná jako u Elanor Global.

U zvlášť rozsáhlých instalací ( > 5000 zaměstnanců) je možné i nasazení Oracle RAC.

## Stanice uživatele pro standardního klienta

* Obecně libovolná dostatečně dimenzovaná stanice se Oracle Java JRE 11 nebo 17, s prohlížečem PDF a přístupem na tiskárnu, resp. lokální tiskárnou.
* Testován je provoz na Windows 10 Enterprise a Windows 11 Enterprise,
* Doporučené rozlišení od 1366 x 768
* Jako prohlížeč PDF doporučujeme a testujeme Adobe Reader verze 7 a vyšších verzí.  
  (je-li systém provozován na Citrix je zapotřebí kompatibilita PDF prohlížeče s příslušnou Citrix verzí).
* Doporučujeme též instalaci SW na práci s exportními soubory CSV, XLS, XLSX  
  (Microsoft Office, resp. Microsoft Excel viewer, resp. OpenOffice / LibreOffice)
* U stanic Windows doporučujeme >= 4 GB paměti.
* Nároky na diskový prostor nejsou velké. Programové vybavení do 500 MB (%USERPROFILE%\Data aplikací\Sun\Java\Deployment).
* Požadovaný prostor pro pracovní soubory, protokoly a tiskové sestavy (%USERPROFILE%\Dokumenty\EMAN) je závislý na typu práce uživatele a řádově se pohybuje okolo 100 MB.
* Textový tisk (Vyp12, Vyp32 aj.). Textový tisk je realizován tak, že uživatel si v dialogu volí textový port LPT1/LPT2/LPT3. V operačním systému uživatele tedy musí být tiskárna připojena na jeden z těchto portů.
* **přístup na internet I.** (viz též následující kapitola Přístup EGJE na internet)

Sestava Kon04 - Kontrola insolvenčního řízení osob [CZ] používá volání webové služby

Získává data z webové služby poskytované serverem justice.cz

(viz popis https://isir.justice.cz/isir/common/stat.do?kodStranky=SLEDOVANIWS)

Provoz sestavy vyžaduje:

* nastavení http, https (proxy)

Je nutné nastavit správnou konfiguraci připojení k proxy serveru, pokud daný zákazník používá proxy server ve své firemní síťové infrastruktuře, případně povolit volání adres začínajících https://isir.justice.cz:8443/

Ze samotného nastavení spojení k proxy serveru je nutná korektní konfigurace připojení pro protokoly HTTP a HTTPS.

Testování můžete také provádět přímo v prohlížeči – můžete zkoušet, zdali se načte xml popis webové služby z adresy https://isir.justice.cz:8443/isir\_cuzk\_ws/IsirWsCuzkService?wsdl

U spouštění EGJE přes **dávkové soubory** \*.bat a u konfigurace webového serveru nesmí administrátor opomenout nastavit/použít následující proměnné prostředí:

Pro protokoly HTTP i HTTPS:

* do proměnné proxyHost zadat konkrétní (doménovou) adresu proxy serveru.
* v proměnné proxyPort nastavit port, na kterém proxy server na daném serveru poskytuje své služby.

Tedy -DproxyHost=proxy.*firma*.cz -DproxyPort=*nnnn*

* pokud daný proxy server vyžaduje autentizaci, je zapotřebí nastavit také proměnné:

- proxyUser uživatelské jméno pro autentizaci na proxy serveru.

- proxyPassword heslo pro autentizaci na proxy serveru.

Pozn.: pokud chcete mít jinak nastavené http a https, je možné použít před uváděné

proměnné prefixy:

http.

https.

Př.: http.proxyHost, https.proxyHost ...

Při spouštění přes **EWS** si správce vyzkouší, zdali je proxy nastavení potřeba a pokud to v daném prostředí nutné je, doplní předlohový .egje soubor

Pozn.: u instalací s AS se nastavení týká klienta EGJE,

pouze pokud správce zvolí spouštění na AS (přes Adm53), musí zajistit přístup z AS. Parametry týkající se proxy se potom píší do wrapper.conf AS jako wrapper.java.additional parametry -D.

Př.

wrapper.java.additional.3=-DproxyHost=xxx

wrapper.java.additional.4=-DproxyPort=ppp

Případně též -DproxyUser a -DproxyPassword

* **přístup na internet II.**

přímý přístup na internet používá formulář Adm24 - Kurzovní lístek / Import z Webu  
Situace je obdobná jako u webové služby.Tedy pro dávkové spouštění:

**-DproxyHost=pr**oxy.*firma*.cz -DproxyPort=*nnnn*

(dávkové spouštění je popsáno v kap. Instalace - přímé a dávkové spouštění std. klienta EGJE Instalace - přímé a dávkové spouštění std. klienta EGJE)

Nastavení proxy v Ovládacích panelech / Java resp.přímo v .jnlp, .egje (element property v <resources> př. <property name="proxyHost" value="proxy.firma.cz"> )

Pro stahování kurzovního lístku na AS (Adm53) je určena analogická zákaznická sestava Adm24f.

* 1. **Stanice uživatele pro EGJEWeb2 klienta**
* HW a SW nároky u Web klienta jsou podobné jako u standardního klienta, místo java JRE se používají Web prohlížeče
* Web browser (Google Chrome, EDGE (nový EDGE chromium), Firefox). U Chrome a Firefox testujeme v poslední verzi prohlížeče.  
  Doporučené rozlišení od 1366 x 768
* Stanice by měla disponovat prohlížečem PDF včetně browseru pracujícím s PDF, a přístupem na tiskárnu, resp. lokální tiskárnou
* Doporučujeme též instalaci SW na práci s exportními soubory XLSX, CSV, XLS  
  (Microsoft Office, resp. Microsoft Excel viewer, resp. OpenOffice/LibreOffice)  
  resp. DOCX, RTF, ODT (Microsoft Word, resp. OpenOffice/LibreOffice)
* Nastavení browseru
  + je třeba mít povolená popup okna   
    (jsou použita hlavně pro zobrazení protokolů viz též [nastavení práv](EGJE_provdoc.docx))
  + server s aplikací zařaďte do Local Internet, resp. Trusted sites
  + aplikace vyžaduje povolení File downloadu a to s "automatic prompting"
  + pokud chcete u browseru Firefox použít automatický single sign on je třeba jej pro konkrétní server s aplikací povolit (příkazová řádka / about:config / Filtr Ntlm / parametr network.automatic-ntlm-auth.trusted-uris vyplnit adresou serveru (serverů)
  + dtto u browseru Chrome - parametr spouštění (doplnit k zástupci)

--auth-server-whitelist  
př. --auth-server-whitelist="\*aaaa.cz,\*aaaa.corp"

* + povolit cookies
  + pokud použijete https připojení je zapotřebí povolit tzv. mixed contents  
    tj. např. IE 10/11 takto : Internet options / Security settings / Local Intranet zone / Custom level / Miscellaneous / Display mixed contents = Enable  
    tj. Možnosti internetu / Zabezpečení / Místní intranet / Vlastní úroveň / Různé / Zobrazit smíšený obsah = Povolit

## Přístup EGJE na internet

Přístup na internet je v standardním EGJE potřeba u objektů Kon04, Adm24 (viz předcházející kapitoly) a také pro přístup na obory vzdělání (Trexima CZ).

K otestování přístupu můžete použít menu O aplikaci / tlačítko Test připojení k internetu.  
Jsou testovány konkrétní adresy, přičemž vliv na přístupnost může mít nastavení proxy serveru.

Nastavení proxy pro standardního klienta i pro AS je popsané v předchozí kapitole "Stanice uživatele pro standardního klienta".

Pozn.: u EGJEWeb2 jde o připojení web serveru, u standardního klienta s AS o připojení AS i klienta.

## Spouštěcí parametry EGJEWeb2

### Referentské rozhraní

Parametry příkazové řádky prohlížeče píšeme tak, že za startovací adresu končící / přidáme ještě znak ?

Automatická volba profilu

parametr p=*kód\_profilu*

např. /?p=ZAME\_DOCH

Pozn.: Nepoužívejte kódy profilů s diakritikou - prohlížeče s tím mají problém a automatická volba profilu nemusí fungovat.

Formulář - automatické otevření

f=*kód\_formuláře* tedy např. https.…/egjeweb/?f=Dca02

Vzhled

theme=styl\_bez\_mezer

tedy např. /?theme=crisp nebo /?style=crisp-touch atp.

Standardně je tento parametr nastavován uživatelem v menu Nastavení / Změna vzhledu.

Šířka / zobrazení levého menu

parametr lmenu=0 resp. lmenu=1 resp. lmenu=x kde x>150,

který levé menu při otevření potlačí (0) resp. otevře (1), nehledě na to, jak to měl uživatel minule při opouštění aplikace.

Volba lmenu=x pak umožní správci přímo nastavit šířku levého menu v pixelech (minimálně 150).

Př.: https://.../egjeweb2\_prod/ref/?lmenu=1

Parametry spojujeme znakem &

např. https.…/egjeweb2/ref/?f=Dca02&p=ZAME\_DOCH

### Rozhraní HR Portál

Spouštěcí parametry příkazové řádky EGJEWEB2 / HR portál jsou jiné

Formulář se zde spouští pomocí přidání

#form=*kodFormulare*

na konec url adresy aplikace, která může, ale nemusí, obsahovat volbu rozhraní (tedy /mana/ či /emp/ )

Některé formuláře pak akceptují ještě další pokyn pro jejich otevření - např. id prvku v navigaci.

Př. ve worklow předlohách (Adm14) je možné používat makro %ID\_SWORKFLOW2% - ID workflow

a následně adresovat aplikaci s formulářem Wflow a tímto parametrem.

Př.

%WEB2URL%/#form=Wflow&formParams=%ID\_SWORKFLOW2%

vede na [https://xxxxx.cz/#form=Wflow&formParams=15929388](https://xxxxx.cz/portal/#form=Wflow&formParams=15929388)

### Společná syntaxe

Od e201609 je možné i v referentském rozhraní spouštěcí parametry ? zadávat i jako parametry # (tedy referentské rozhraní umí zpracovat i parametry dosud používané jen v HR portálu).

Přičemž synonymy jsou:

f form

p prof

Nově také umí obě rozhraní volat přímo záložku formuláře a případně OSCPV v navigačním seznamu Pv (Osb02, Opv01...) resp. PvDoch (Dcu01, Dcd01...).

Používá se syntaxe v části #:

tab=*kód\_záložky*

otevření formuláře s konkrétní záložkou

kód záložky je možné zjistit z Adm04 / Struktura práv objektu / Podobjekt (pro typ Záložka)

oscpv=*osobní číslo PV*

osobní číslo PV pro formulář, který má navigaci Pv, PvDoch

Kód navigačního seznamu je možné zjistit při zavolání funkce Výběr – kód je v hlavičce tohoto dialogu

Pozn. kalendářové formuláře Dov16, Dcu06 tuto navigaci nemají.

Aplikace generuje upozornění pro situace, které při spuštění mohou nastat:

"Uživatel nemá právo na formulář (%kod\_form%)"

"Uživatel nemá právo na záložku (%kod\_tab%)" (pouze když je zvolena v příkazové řádce)

"Navigační seznam – nepodařilo se nalistovat požadovaný záznam OSČPV (%OSČPV%)"

Příklad:

https.…/egjeweb2/ref/?p=MANA&f=Pkz01&tab=Komunikace&oscpv=131.01

resp.

https.…/egjeweb2/ref/#p=MANA&f=Pkz01&tab=Komunikace&oscpv=131.01

Tip:

Tyto parametry jsou také zobrazovány v příkazové řádce při pohybu v aplikaci. Je tedy možné je odsud přebírat.

Pozn.:

Pokud má uživatel jeden profil vícekrát (např. s jiným jazykem, nebo jinou organizací, nebo svůj a zastupování), tak systém i při zadání profilu dává profil vybrat ze seznamu.

Pozn.2:

I s parametry profil, formulář je možné spouštění bez udání rozhraní (tedy ref či mana či emp).

### HR Portál volaný jako portlet

Toto rozhraní je určené pro integraci do různých intranetů.

Aplikace zde poskytuje portlet, tj. řečí EGJE formulář nebo sestavu, ale není obklopena horním ani dolním pásem aplikace a často bývá zobrazení fixováno na jeden prvek (typicky osobu/PV).

Zobrazení formuláře/sestavy je odvozeno ze grafiky HR Portál.

Volat tak lze typicky např. Pkz01, Vyp11 apod.

Řešit se tak dá např. zobrazení výplatních lístků na intranetu, ten se tak vyhne existenci PDF souborů s výplatním lístkem přímo v intranetové aplikaci.

Podmínkou je SSO autentizace (tedy přebírání autentizace z operačního systému, bez zadávání jména a hesla). U interaktivní autentizace by to bylo pro uživatele dost nepraktické.

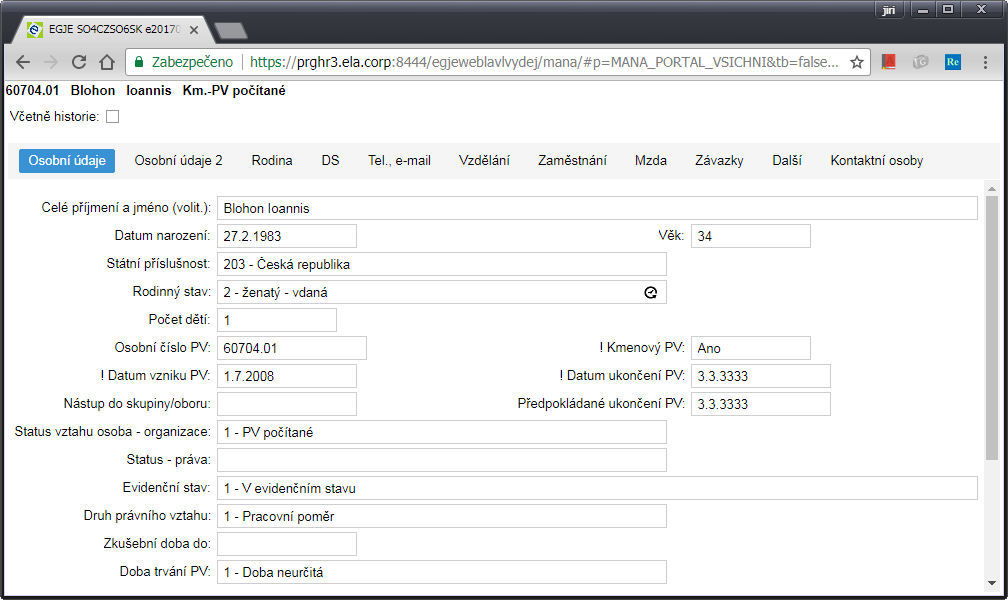
Realizace je taková, že se za volání EGJEWEB2 přidávají ještě další parametry:

**&tb=false** zobrazení bez horního a spodního pruhu EGJE HR Portálu

**&ns=fixed** zobrazení bez navigačního seznamu s fixovaným parametrem zadaným v navigaci (typicky oscpv)

Parametry jsou použitelné pro příkazovou řádku HR Portálu.

př. .../mana/#p=SPR\_MAXWP&form=Pkz01&tab= OsobaPanel&oscpv=109.02&tb=false&ns=fixed



* 1. **Konfigurace připojení k poštovnímu serveru**

se provádí na formuláři Adm21 / Parametry mailu.

Parametry SMTP Host, Port slouží pro odesílání e-mailů a používají se v aplikaci na mnoha místech.

Naproti tomu parametry POP3 slouží pouze konfiguraci příjmu odpovědí uchazečů v tomto modulu.

V části Adm21 / Parametry komunikace / Odesílání pošty, jsou také 3 parametry, které umožní TLS připojení k e-mailovému serveru a autentizaci EGJE jako uživatele e-mailového serveru:

Zabezpečení připojení:

* + nevyplněno – běžné nezabezpečené připojení k SMTP,
  + SSL/TLS – zabezpečené připojení, je třeba uživatel a heslo   
    (obvykle používáno s portem 465),
  + STARTTLS – způsob, jak zabezpečit existující nezabezpečené připojení   
    (port 25 resp. 587)

SMTP Uživatel: uživatel použitý pro připojení k SMTP serveru

SMTP Heslo: heslo tohoto uživatele

Více o SSL/TLS, resp. STARTTLS zde  
 <https://www.fastmail.com/help/technical/ssltlsstarttls.html>

Při práci přes AS je v Configuratoru parametr AS / Odesílání a příjem elektronické pošty. Parametr

umožňuje veškerou mailovou korespondenci, kterou systém provádí, provozovat prostřednictvím aplikačního serveru.

Odesílání mailu se také týká parametr Configuratoru:

Nekontrolovat e-mailovou adresu odesilatele

Nastavení, zdali provádět kontrolu formální správnosti adresy odesílatele mailu (obvykle firemní mail osoby uživatele – Osb02)

**Adresa odesilatele všech e-mailů z EGJE (nepov.): -** týká se hlavně outsourcingu, resp. přísně nakonfigurovaných e-mailových serverů.

U některých instalací je problém s odesílání e-mailů s doménou zákazníka z e-mailového serveru v jiné doméně. Správné řešení je uvedení tohoto serveru na tzv. whitelist a toto odesílání tak umožnit.

Pokud to z důvodů schvalování bezpečnosti u zákazníka není možné, systém nyní umožňuje si na úrovni organizace v Adm21/Parametry mailu / Adresa odesilatele e-mailů z EGJE náhradního odesilatele. Takové e-maily projdou zabezpečením. Nicméně musíme upozornit, že takovéto e-maily např. mezi vedoucím a zaměstnancem ale i všechny ostatní jsou posílány právě a pouze tímto odesílatelem. Ztrácí se tak přehlednost komunikace a možnost přímé odpovědi v e-mailovém klientovi. Takže pokud to není technicky nutné, tak vyplňování tohoto parametru nedoporučujeme.

**Režim přidávání skut. odesilatele do předmětu e-mailu:**

1 - Standard (přidávání, pokud je vyplněna adresa odes. všech e-mailů)

2 - Nepřidávat skutečného odesilatele nikdy

3 - Přidávat pouze příjmení a jméno (tj. bez titulů a bez Od/From)

4 - Skutečný odesilatel ve tvaru Příjmení jméno (OSCPV), tj. bez titulů

Zatímco režimy 1-3 jsou určeny pro jednotného odesílatele, tj. vyplněn předchozí parametr Adresa odesilatele všech e-mailů z EGJE, tak režim 4 slouží k změně formátování doprovodného textu u odesílatele v režimu, kdy je do e-mailů dáván skutečný odesílatel.

Režim 4 umožňuje zbavit se titulů v odesílateli. Některé druhy e-mailových klientů totiž špatně odhadují co je titul, co jméno a co příjmení.

Pokud máte problémy s odesíláním e-mailu z EGJE (typicky worklow - chyby typu

cz.elanor.eman.datasource.remoteCompute.MailinatorException: Chyba odesílání e-mailu ...

Caused by: javax.mail.MessagingException: Could not connect to SMTP host: .... Permission denied: connect)

může pomoci nastavení parametru prostředí -Djava.net.preferIPv4Stack=true

(bat resp. jnlp soubor)

viz <http://stackoverflow.com/questions/8360913/weird-java-net-socketexception-permission-denied-connect-error-when-running-groo>

1. **Instalace a dimenzování parametrů**

Instalaci a konzultaci HW a SW provádí pracovník Elanor podle interní metodiky.

Některé základní body tohoto postupu jsou uvedeny na konci dokumentu v přílohách.

1. **Režim správy databáze - datového schematu Elanor EGJE**

Databázové schema EGJE je plně ve správě změnového řízení Elanor.

Změny ve schematu aplikace EGJE jsou povoleny jen firmě Elanor. Firma si vyhrazuje právo na jejich realizaci. Schematem se v Oracle rozumí nosný a pracovní uživatel (schema), v MS SQL pak celá konkrétní databáze s egje objekty.

Výjimky:

zákazník smí v db schematu/databázi aplikace EGJE vytvářet tabulky/pohledy po domluvě s implementačním týmem Elanor, resp. helpdesk,  
tyto tabulky nesmí začínat "ce"

Zvláště není dovoleno vytvářet / měnit objekty, které mohou ovlivnit průběh změnového řízení a funkčnost / dostupnost aplikace.

Sem patří především triggery a indexy nad objekty EGJE, a přidávání vlastních položek do tabulek, pohledů EGJE.

Měnit obsah databáze EGJE je povoleno pouze pomocí aplikace EGJE, případně pomocí interface vytvořených ve spolupráci s implementačním týmem, resp. akceptované prostřednictvím služby helpdesk.

Pokud zákazník s db Oracle používá ke sběru statistik jinou funkci než standardní sběrovou proceduru EGJE (instalovanou z Adm51), sdělí její obsah implementačnímu týmu / prostřednictvím helpdesk.

Standardní proceduru sběru statistik, ale zákazník spustí v případě, že je o to požádán helpdesk v rámci řešení nějakého výkonového problému. Může to být doprovázeno i žádostí o smazání jinak sebraných statistik.

Pokud potřebuje změnit zákazník ve vlastní režii interface objekt vytvořený (resp. zčásti vytvořený) firmou Elanor, sdělí to zákazník implementačnímu týmu / prostřednictvím helpdesk včetně obsahu změny.

## Objekty BLOB - uložení dokumentů

U řady zákazníků je populární ukládání dokumentů o zaměstnanci do databáze (Opv31) a jsou i další aparáty EGJE, které ukládají, resp. budou ukládat různé dokumenty do db.

Použití databází Oracle, resp. MS SQL Server pak dává možnosti ukládat tyto dokumenty na jiné diskové místo než ostatní běžná relační data.

Můžeme Vám nabídnout poradenské služby pro tento přesun. Na Oracle jde o použití mechanismů jejich přímého přesunu do jiného tablespace, datafile.

U MS SQL Serveru je to komplikovanější, vyžaduje to odstávku db, přesun dat, znovuvytvoření db tabulky a zpětný přesun dat.

V těchto variantách zůstávají dokumenty součástí relační databáze, je tak zaručena konzistence a běžné mechanismy zálohování zálohují obojí (tedy relační data i dokumenty).

V rámci racionalizace a dalšího rozvoje EGJE dochází od verze e202211 k postupnému přesunu BLOB objektů typu dokument/soubor z dílčích tabulek do jednoho společného uložiště, a tím je DB tabulka CETDOK.

Přesun dokumentů/souborů se týká v tuto chvíli pouze nově přidaných či zeditovaných záznamů, dříve přidané dokumenty/soubory zůstávají v původních tabulkách (prozatím). Přesunutý dokument/soubor je nahrazen vazbou (odkazem) na centrální uložiště, kam byl dokument/soubor přemístěn. Tuto vazbu zajišťuje vazební tabulka CETDOKVAZBA.

V tuto chvíli se tedy jedná o hybridní řešení uložení dokumentů. Interfejsy, které spadají pod maintenance, byly na tento mechanismus připraveny. V případě interfejsů, které si spravuje klient sám, je potřeba na toto myslet a upravit propojení tak, aby splňoval toto hybridní řešení. I zde Vám jsme k dispozici ke konzultaci řešení.

Po dokončení implementace vazby u všech odpovídajících tabulek obsahující BLOB objekty do nového uložiště, proběhne případný hromadný přesun původních objektů. **O této skutečnosti budete předem informováni.**

1. **Správa aplikace - změnové řízení**

Obecně se správa EGJE skládá z :

* + Nastavení a změna parametrů pomocí utility configurator\_egje - viz následující kap.
  + **Instalace změnového řízení aplikace** (patch resp. výdejové verze).  
    Postup se provádí podle popisu, který verzi provází, Standardem je provedení pomocí utility superconfigurator. Obsahem však je zkopírování dodaných souborů (typicky eman.jar resp. egjelib.jar) do příslušného adresáře deployment Web serveru (pro testovací a pro ostrou verzi) a případně na aplikační server.  
    Je-li instalován i EGJEWeb2 je třeba zaktualizovat i tomcat web aplikaci.
  + **Změnové řízení databáze**  
    Jde o spuštění změnového skriptu, který je součástí verze (patche) pomocí vlastní aplikace EGJE. Akce se provádí na formuláři Adm51 přístupném správci systému. Spuštění je potřeba provést na Testovací i Ostré databázi.

Pozn. Je možné nejprve programy instalovat a skript spustit pouze na testovací databázi, vše otestovat a až následně provést to samé na ostré instalaci/databázi.

* + Databázové statistiky (pouze db Oracle - Adm51)
  + Správa uživatelů
  1. **Nastavení a změna parametrů pomocí utility configurator\_egje**

Utilita configurator\_egje (ve windows jako dávka configurator\_egje.bat) se nachází ve složce configurator instalačního adresáře resp. následně jej správce má kořenovém adresáři instalace EGJE.

Jazyk programu je možné nastavit pomocí parametru EGJELANG uvnitř spouštěcí dávky

př. -DEGJELANG=en způsobí spuštění v angličtině.

Spouští se konfigurační program s tímto obsahem:

java -Xmx128M -DEGJELANG=cs -cp ../EGJE/egjelib/eman.jar;../EGJE/egjelib/egjelib.jar cz.elanor.eman.sgui.configurator.Configurator ./config\_egje.jar

exit

Předpokladem je cesta na program java. U OS Windows jde o java.exe, který standardní instalace java JRE nahrává do Windows\System32/ SysWOW64 adresáře. Resp. je potřeba mít v Proměnné prostředí / Path nastavenou cestu do adresáře *javaJRE*\bin resp. *javaJDK*\bin.

Spouštěnou verzi java zjistíte z příkazového řádku OS, příkazem java -version.

Každá předloha klienta resp. každý server EGJE (AS či EGJWEB2) má svůj konfigurační soubor config\_egje.jar a je vhodné si na každý udělat editační dávku (nebo je všechny namapovat do jednoho SuperConfiguratoru).

* + 1. **Adresa EWS**

Uvádíme cestu do kořenového složky distribuce EWS (EGJE Web Start)

Cestu vyplňujeme buď v podobě

http(s)://...

př.: https://prghr1/egje\_vzor

nebo v podobě

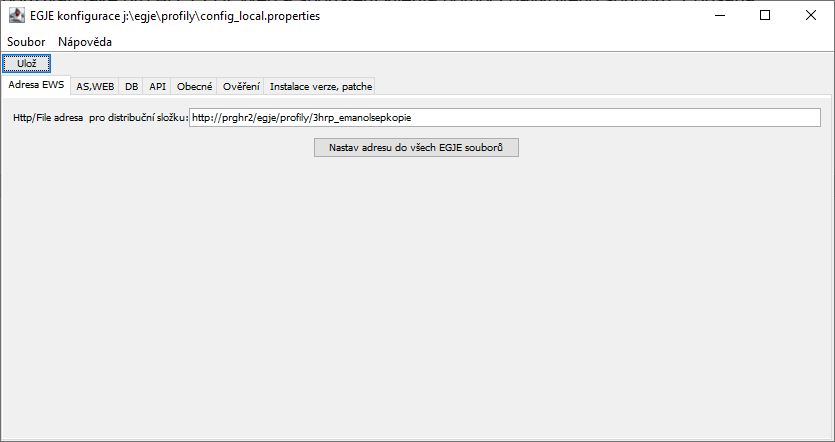
file:/...

př. file:/J:/egje\_install\_vzor/egje

Preferujte http(s) formát.

**Java 11 již mechanismus JWS nepodporuje, náhradou je EWS vytvořený firmou Elanor, proto doporučujeme nevyužívat funkcí spojených s JWS jako je například ve zvýrazněném rámečku na obrázku**

**Mechanismus EWS je vydáván jako samostatná distribuce a jeho funkčnost je popsána v dokumentu „EWS – dokumentace.pdf“ v distribuční sadě EWS** **a zde v příloze B.**



Pozn. Datový soubor config\_egje.jar, ale zůstává hlavním nositelem konfiguračních informací. Je používán také pro AS, EGJEWeb a spouštění klienta pomocí dávkového souboru. Popsaná alternativa není použitelná pro kerberos autentizace (vyžadují přenos souboru config\*.jar/krb5.conf).

Poznámka: Alternativou spouštění klienta pomocí EWS je spouštění pomocí dávkových souborů z rychlého souborového serveru viz [Příloha B](EGJE_provdoc.docx#_Instalace_-_přímé). Zde je také popsán rozdíl při použití java 9, 11.

Poznámka 2: Instalace EWS s vestavěnou Java 11 už žádný Control panel nevytváří.

* + 1. **AS - aplikační server**

Upozornění - všechny změny ukládáme společným tlačítkem Ulož.

Pro konfiguraci bez aplikačního serveru slouží nastavení

**Klient bez AS**

Pro konfiguraci s aplikačním serverem pak hodnota

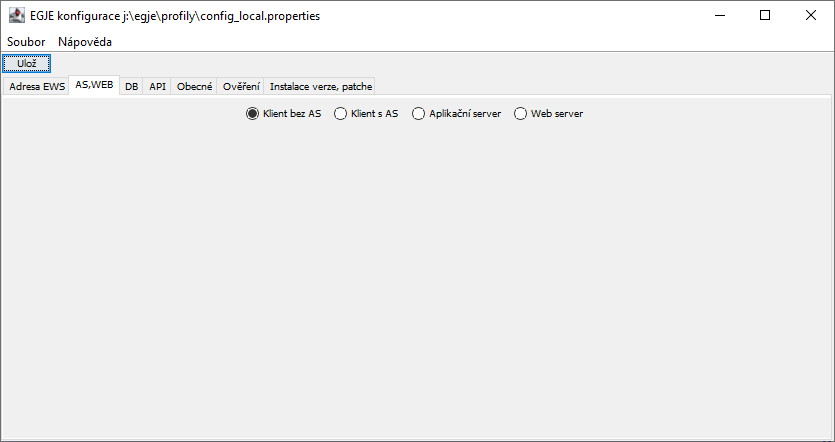
**Klient s AS**

Pro konfigurační soubor aplikačního serveru (je odlišný od Klienta AS) pak hodnota

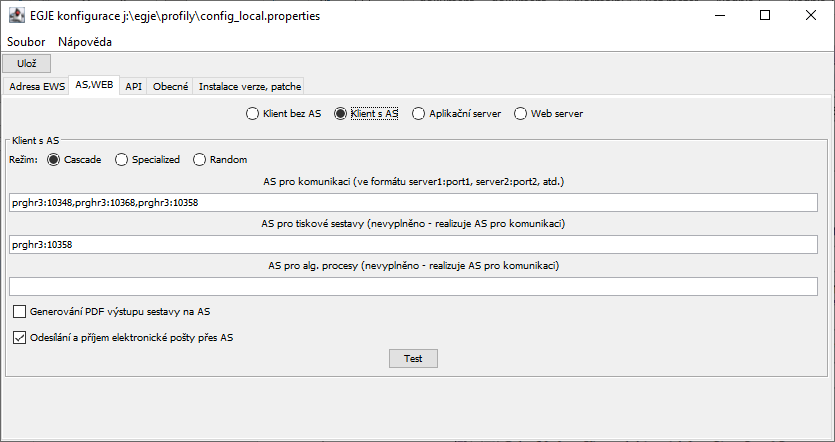
**Aplikační server**

Pro konfiguraci serveru, který slouží jako server EGJEWeb slouží volba

**Web server**



kde v režimu **Klient s AS**



je nejprve třeba zvolit režim, je-li aplikačních serverů více  
(zápis formou opakovaných dvojic server:port s oddělovačem středník nebo čárka):

* Cascade - klient se postupně pokouší připojit na AS uvedeným v AS pro komunikaci dle pořadí, v jakém jsou uvedeny.  
  Tyto servery jsou použity také jako aditivní k AS pro tiskové sestavy a AS pro alg.procesy
* Specialized - klient se postupně pokouší připojit na AS uvedeným v AS pro komunikaci dle pořadí, v jakém jsou uvedeny. Pokud ale chce vytvořit tiskovou sestavu nebo volat algoritmický proces, hledá se dostupný AS z položky AS pro tiskové sestavy resp. AS pro alg.procesy a není-li dostupný, vezme AS pro komunikaci, ale v opačném pořadí, tj. od konce
* Random - klient dostane přidělen AS vybraný ze všech AS pro komunikaci dle náhodného výběru.  
  Tyto servery jsou použity také jako aditivní k AS pro tiskové sestavy a AS pro alg.procesy

Poznámka: pro autentizace mswin\_ntlm a mswin\_kerberos musí být server uveden názvem a nikoliv IP adresou.

AS pro komunikaci

základní AS, používají se pro běžnou online komunikaci klienta

AS pro tiskové sestavy

požadavek na vytvoření tiskové sestavy je směrován na tyto AS

dle nastavení Generování PDF výstupu sestavy pak distilace PDF probíhá na tomto serveru či na klientské stanici. Je-li specializovaný tiskový server, doporučujeme je pro tuto akci použít, jinak je lepší používat stanice

AS pro alg. procesy

je-li nakonfigurován, je prioritním pro zpracování procesů

* výpočet mzdy (Vyp01, Vyp02, Vyp51)
* měsíční a roční uzávěrky, kopie číselníků (Vyp02, Cep02)
* import mzdových vstupů (Vst06)
* exporty do účetnictví (Uct02)
* eldp (Poj13, Poj14)
* přihlášky nem.poj. (Poj18, Poj19)
* kontrolní aparát (Kon\*)

Generování PDF výstupu sestavy

viz AS pro tiskové sestavy

není-li specializovaný tiskový server, doporučujeme využívat k této úloze klientskou stanici, neboť např. hromadné tisky sestav v období mzdové uzávěrky by představovaly velké paměťové a procesorové nároky na aplikační server.

Odesílání a příjem elektronické pošty

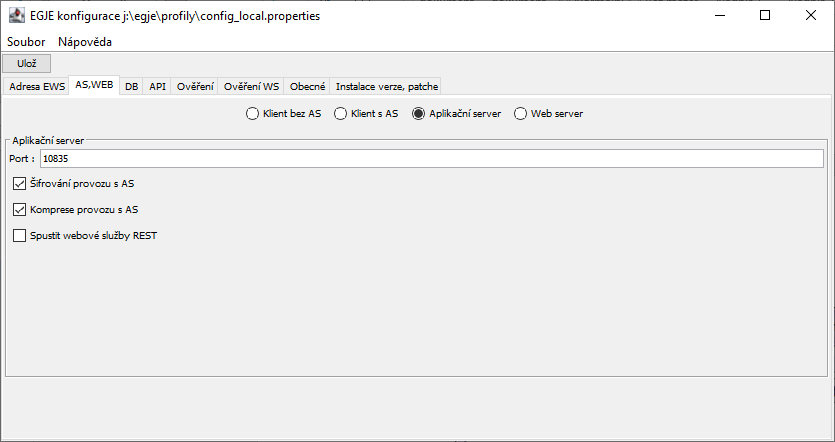
umožňuje veškerou mailovou korespondenci, kterou systém provádí, provozovat prostřednictvím aplikačního serveru. To dává možnost lepšího zabezpečení např. smtp a pop3 serveru.

**Upozornění:**

**pro klienta s AS se nevyplňuje na následující záložce DB připojení.**

**Jeho vyplnění je vážnou bezpečnostní chybou!**

a v režimu **Aplikační server**



Je-li aplikačních serverů více má každý svůj konfigurační soubor (má jiný port)

Port je IP port použitý pro RMI komunikaci s klientem.

Na tomto portu je navazováno spojení. Poté vlastní komunikace probíhá na portu přiděleném systémem.

O spojení žádá klient. V systému jsou však i komunikace navazované z druhé strany - server žádá o spojení klienta (aby mu předal vytvořenou sestavu, protokol atp.). Na toto je nutné pamatovat při případném provozu přes firewall.

Šifrování provozu s AS - implicitně šifrováno

Doporučujeme šifrování použít. Je to bezpečnější.

Používáme šifrování bez certifikátu pomocí java JRE.

Implicitním nastavení je TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA, které nabízí dostatečnou ochranu.

Dále java nabízí:

SSL\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA

SSL\_DH\_anon\_WITH\_DES\_CBC\_SHA

TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA

TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA256

TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA

TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA

Pro změnu šifrování je třeba nastavit šifrování do parametru

rmi\_cipher\_suite

v klientském i serverovém config\_local.properties

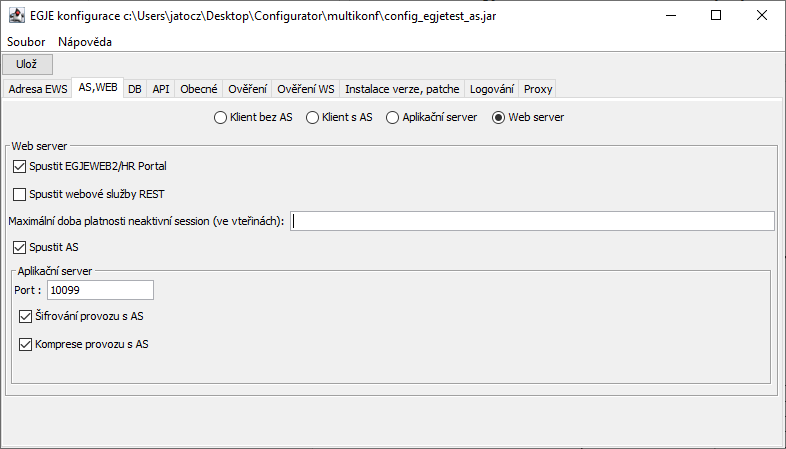
(resp. na serveru lze i pomocí wrapper.conf

wrapper.app.parameter.*n*=-Crmi\_cipher\_suite=...)

Komprese provozu s AS - implicitně zaškrtnuto.

Doporučujeme kompresi použít, významně snižuje přenášené objemy, aniž by příliš zatěžovala obě strany.

**Režim Web server**



Existují tři přístupné interfejsy:

EGJEWEB2/HR Portal

REST web services

AS EGJE (od e201905 může běžet i v EGJEWEB)

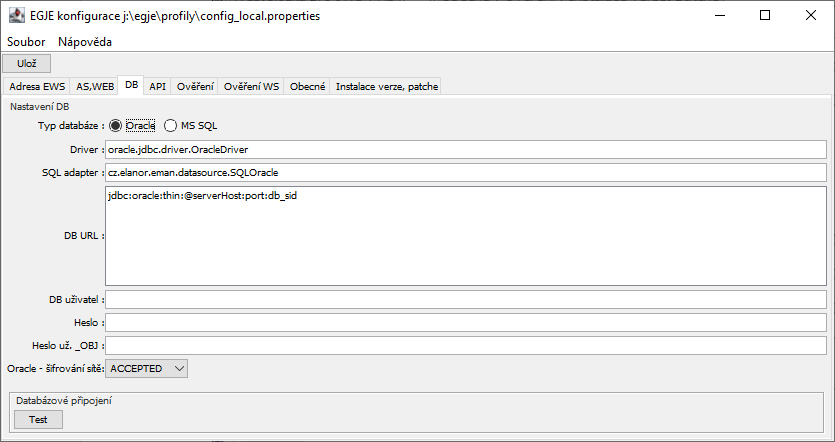
Maximální doba platnosti neaktivní session (ve vteřinách):

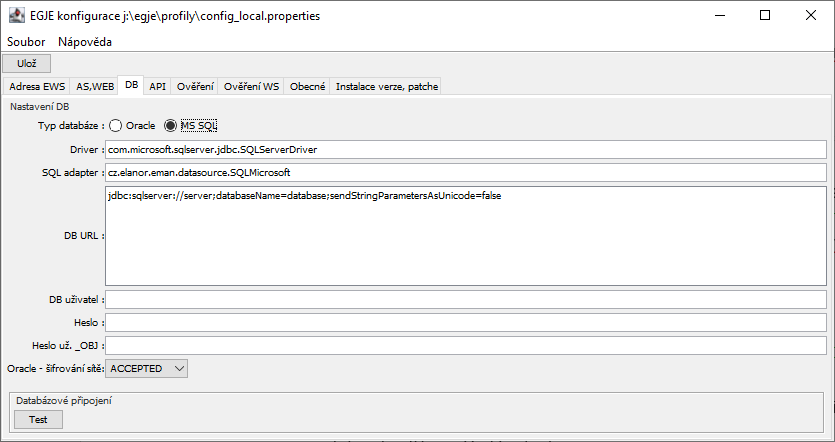
Nastavuje dobu po jaké se neaktivní session ukončí. Defaultní hodnota je 15 minut.

* + 1. **Připojení k databázi - DB**

Upozornění - všechny změny ukládáme společným tlačítkem Ulož.

**V režimu Klient s AS se nevyplňuje !**





Driver - Třída JDBC driveru

buď (pro db Oracle) oracle.jdbc.driver.OracleDriver

nebo (pro db MS SQL) com.microsoft.sqlserver.jdbc.SQLServerDriver

SQL adapter:

buď (pro db Oracle) cz.elanor.eman.datasource.SQLOracle

nebo (pro db MS SQL) cz.elanor.eman.datasource.SQLMicrosoft

DB URL

buď (pro db Oracle) jdbc:oracle:thin:@***serverHost*** **:*port* : *db\_sid***

nebo (pro db Oracle RAC

jdbc:oracle:thin:@***description z tnsnames.ora***

př.: vše v jednom řádku

jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS = (PROTOCOL = TCP)(HOST = ***host***)(PORT = ***port***))(ADDRESS = PROTOCOL = TCP)(HOST = ***host2***)(PORT = ***port2***)) (LOAD\_BALANCE = yes) (CONNECT\_DATA =(SERVER = DEDICATED)(SERVICE\_NAME = ***service\_name***)))

nebo (pro db MS SQL)

jdbc:sqlserver://***server***;databaseName=***database***;sendStringParametersAsUnicode=false

obecně:

jdbc:sqlserver://[serverName[\instanceName][:portNumber]][;property=value[;property=value]]

**Poznámka: pro SQL Server doporučujeme na konec URL uvádět ;sendStringParametersAsUnicode=false**

**Dosáhne se tak výrazně rychlejšího zpracování SQL příkazů s parametry.**

**Toto nastavení však úplně ruší možnost použití unicode znaků ve vybraných položkách.**

Jméno - db uživatel použitý pro přihlášení uživatele aplikace (na Oracle ten bez \_OBJ)

Heslo - jeho db heslo

Heslo už. \_OBJ - heslo vlastníka objektů (tj. na Oracle uživatele se suffixem \_OBJ) - uživatel je používán pouze ve změnovém řízení

Oracle - šifrování sítě.

Volba umožňuje nastavit režim pro šifrování síťového provozu Oracle. Implicitní hodnota je ACCEPTED.

Šifrování se také analogicky zpřístupní i v Oracle Listeneru na serveru Oracle.  
Viz též http://download.oracle.com/docs/cd/B28359\_01/java.111/b31224/clntsec.htm#EHAFHEIG

Položku oracleNetEnc, je možné také do konfiguračního souboru config\_local.properties přidat ručně.

Popis položky:

#oracle network encryption

# hodnoty: none, ACCEPTED,REJECTED,REQUESTED,REQUIRED

oracleNetEnc=none

Pro SQL Server existují property parametry pro nastavení šifrované komunikace.

Property encrypt=true; resp. bez nastavení serverového certifikátu společně jako ;encrypt=true;trustServerCertificate=true

V tom případě komunikuje jdbc driver přes SSL protokol, druhý parametr znamená, že není ověřován certifikát serveru.

Aplikace používá connection pool. V případě Oracle jde o Oracle UCP tj. řešení přímo pro JDBC driver, pro SQL Server se používá Apache Commons DBCP.

Pro Oracle je možné přímo v konfiguračním souboru config\_local.properties (popřípadě v konfiguračním souboru wrapperu) nastavit tyto hodnoty:

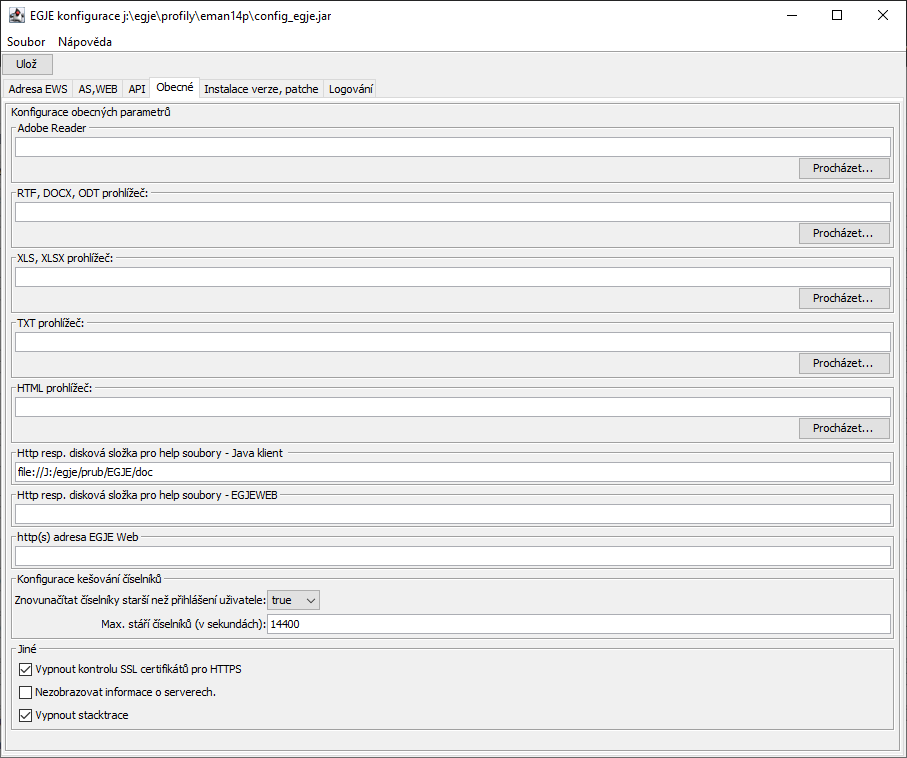
oracle.min.pool.size - minimální velikost poolu

oracle.max.pool.size - maximální velikost poolu

oracle.inactive.connection.timeout - doba neaktivního připojení

Pokud se hodnoty nevyplní, použijí se defaultní hodnoty.

* + 1. **Obecné**



Uživatelské sestavy – jen pro administrátory, kteří je vytvářejí.

(viz kapitola Uživatelské sestavy)

Adobe Reader

Standardní cesta k PDF prohlížečům je uživateli předvyplněna, ale uživatel si jí může změnit v aplikaci.

RTF, XLS, TXT, HTML prohlížeče

Analogické položky k předchozí pro další typy vytvářených souborů. Stejný princip obsluhy.

Http/file složka pro help soubory

odkaz na soubory help systému

Pro správnou identifikaci help souboru v jiném než českém jazyce je zapotřebí použít buď:

mapovaný disk př. N:/egje/doc/

http adresu (doporučeno)

Http(s) adresa EGJE Web

adresa používaná pro generované e-maily jako odkaz na aplikaci v EGJE Web MAZM

Ve standardním klientovi i v EGJE Web je nahrazena položkou Adm21 / Konf. parametry / Http(s) adresa EGJE Web

Konfigurace kešování číselníků

Konfigurace má význam pro AS resp. EGJEWEB2

**Znovunačítat číselníky starší než přihlášení uživatele**: ("cache\_cis\_od\_prihlas")

false - používat i starší načtená data - implicitní rychlý režim

true - používat pouze data, která byla načtena v době od přihlášení uživatele   
(může mít za následek pomalejší náběh start aplikace z pohledu uživatele, ale zase jistotu, že všechny číselníky jsou aktuální)

smart - speciální režim se zjišťováním datových změn

Přináší hlavně redukci objemu přenášených dat, neboť se vždy zeptá, jestli ve výsledku db dotazu pro číselník došlo k nějaké změně, a data přenačte pouze v případě, že ano.

Technicky se k tomu používá Oracle funkce ORA\_HASH a na MSS funkce CHECKSUM\_AGG.

**Max. stáří číselníků (v sekundách):** implicitně 14400 tj. 4 hodiny.

**Sekce jiné**

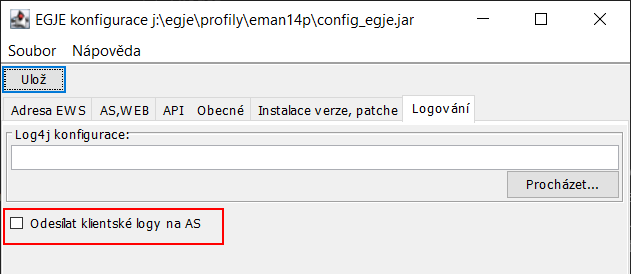
***Vypnout kontrolu SSL certifikátů pro HTTPS***

Položka má význam např. pokud firemní proxy server provádí dešifrování SSL spojení s tím, že je opět zašifruje certifikátem vydaným interní certifikační autoritou. Nemá vliv při spouštění tlustého klient EGJE přes Java Web Start.

***Vypnout stacktrace***

Tato volba vypne generování stracktrace. Pokud zákazník požaduje, aby z bezpečnostních důvodů, kdy stacktrace může obsahovat informace o interních cestách v systému nebo například cesty k serverů atd. nebyly tyto informace dostupné, zaškrtnutím této volby může generování stacktrace do konzole potlačit. Avšak stacktrace slouží k identifikaci případných chyb y systému, obsahuje informace o nastavení systému, které jsou potřebné k odhalení interních chyb.

Pokud byla tedy použita tato volba, **důrazně doporučujeme** na záložce „Logování“ také zatrhnout volbu „Odeslat klientské logy na AS“.



V případě chyby, budou dostupné alespoň logy stacktrace, které jsou uložené na aplikačním serveru. Pokud by tato volba nebyla zatrhnuta, tak veškeré logy stacktrace budou nenávratně ztraceny a nebude možné je použít pro detekci a identifikaci nastalých chyb.

* + 1. **Ověření**

Ověření neboli autentizace zjišťuje, kdo je do aplikace vstupující uživatel.

V zásadě se dělí na interaktivní (uživatele zadává jméno a heslo) a SSO (Single Sign On, aplikace se snaží převzít ověření z již provedené autentizace v OS).

Možná je i kombinace, kdy aplikace zkusí SSO a když se nepovede, nabídne uživateli interaktivní autentizaci.

Doporučujeme nepoužívat Windows účty s diakritikou.



Poznámka - pracujeme-li s aplikačním serverem, je vyplnění této záložky důležité na aplikačním serveru (na klientu je bezpředmětné).

Po provedení změn na této záložce je potřeba restartovat AS resp. WEB EGJE server.

Od verze e202405 jsou 3 nové typy NTLM autentizací, které nově umožňují použití protokolu SMB2: NTLogin3, NTLogin3Only a NTLogin3Interactive. Změnu autentizace realizujete výhradně v konfigurátoru EGJE. Dosavadní starší typy NTLM autentizací budou kvůli zpětné kompatibilitě stále dostupné a odstraněné budou až v průběhu roku 2024.

Od verze e202409 byla ukončena podpora základních NTLM autentizací – NTLogin a NTLoginOnly. Tyto autentizace již nepůjdou v rámci Configurátoru EGJE zadat. Od verze e202411 se již pomocí této autentizace přihlásit nejde.

**Ověření** - zvolený autentizační mechanismus. Jedna z hodnot:

**mswin\_ntlm**

Realizováno pomocí Microsoft security package.

Umožňuje SSO (převzetí autentizace od OS) ale pouze pro MS Windows

(u instalace s AS/Web server platí podmínka OS Windows i pro ně)

Nevyžaduje žádné další parametry.

AS/Web server musí běžet pod uživatelem z domény.

Nastavení u klienta AS - server je nutné zadávat jménem a nikoliv IP adresou.

Lze použít pro java klienta bez AS.

Nepodaří-li se SSO přihlášení následuje autentizační dialog (s doménou).

**mswin\_ntlmOnly**

Nepodaří-li se SSO následuje ukončení aplikace

**mswin\_ntlmInteractive**

Vždy autentizační dialog.

**mswin\_kerberos**

Realizováno pomocí Microsoft security package.

Přísnější autentizace, která zkusí nejprve autentizační protokol kerberos.

SSO jako mswin\_ntlm.

Vyžaduje u domény nastavený service principal name SPN (utilita setspn) pro aplikaci a uživatele:

* + - utilita setspn (u windows serveru 2003 ji případně doinstalujte z instalačního CD)
    - setspn.exe -A *principal účet*

kde *principal* je

HTTP/ServerName pro EGJEWEB,

EGJE/ServerName pro AS

*účet*  účet pod kterým běží AS resp. EGJEWEB

AS/Web server musí běžet pod uživatelem z domény.

Nastavení u klienta AS - server je nutné zadávat jménem a nikoliv IP adresou.

Nepodaří-li se SSO přihlášení následuje autentizační dialog (s doménou).

**mswin\_kerberosOnly**

Nepodaří-li se SSO následuje ukončení aplikace

**NTLogin2** autentizace uživatele se přebírá z NT autentizace Windows.  
 pokud se nepřevezme z OS, přejde systém do režimu NTLoginInteractive

**NTLogin2Only** dtto s tím,že je umožněnopouze převzetí přihlášení z OS

**NTLoginInternactive** s autentizačním dialogem

pokud je server linux a ověření má být SSO vůči AD, je možné použít tyto autentizace, zvládají protokol NTLM2.

K jejich použití je potřeba vyplnit parametry - viz odstavec NTLogin/2 JCifs

**NTLogin3** jako NTLogin2 ale umožňuje použít novější SMB2 protokol

**NTLogin3Only** dtto s tím,že je umožněnopouze převzetí přihlášení z OS

**NTLogin3Internactive** s autentizačním dialogem

**LDAPOnly** aplikace vůči ldap serveru (obvykle MS Active directory položka userPrincipalName).  
Do položky LDAP/Web - implicitní doména uživatele se pak zadává doména (tj. to co je v userPrincipalName za znakem @ - uživatel to pak nemusí zadávat).

V tomto režimu podporujeme pouze SSL připojení.

**LDAPSearch** podobné Only s tím, že ve LDAP SSL URL je ještě navíc makro pro přihlášení se jménem tedy   
např. Ldaps://xxxxxxx/dc=yyy,dc=cz   
popis formátu viz http://docs.oracle.com/javase/jndi/tutorial/ldap/misc/url.html

Pozn. filtr zadávejte samostatně do specializované položky LDAPSearch - filter.

a navíc mohou být vyplněny položky:

LDAP - uživatel s právy na čtení

LDAP - heslo uživatele s právy na čtení

přes tohoto uživatele se pak aplikace připojí, prohledá celý podstrom a vyhledá se v něm autenizující se uživatel.  
Pokud ldap server umožňuje anonymního uživatele, je možné položky nechat prázdné.

LDAPSearch - filter - Filtr, uplatněný po přihlášení k LDAP serveru

(nutný pro Novell eDirectory)

např. uid=%username%

LDAPSearch – Atribut unikátní identity uživatele – Atribut v AD specifikující hodnotu logname přihlašovaného uživatele. V případě nevyplnění je jako logname v rámci EGJE použita hodnota DN (Distinguished Name). Hodnota tohoto atributu, v případě jeho vyplnění, musí korespondovat s makrem %username% uvedeným v rámci konfigurační položky LDAPSearch – filtr. Př. Nastavení LDAPSearch – filtr: *(&(objectClass=person)(employeeNumber=%username%))*, LDAPSearch – Atribut unikátní identity uživatele: *employeeNumber*

**kerberos** pouze kerberos autentizace - tj. při spouštění uživatel vždy zadává jméno a heslo

Vyžaduje, aby v config\_ejge.jar byl zkonfigurovaný soubor krb5.conf (konfigurace realms)

Oproti mswin\_kerberos může na AS/Web serveru být linux. U této autentizace je důležité nastavení DNS. U ověřování linux vůči Active Directory je vhodné, aby primární DNS server byl doménový řadič Active Directory.

**Příklad souboru krb5.conf:**

[logging]

default = FILE:/var/log/krb5libs.log

kdc = FILE:/var/log/krb5kdc.log

admin\_server = FILE:/var/log/kadmind.log

[libdefaults]

ticket\_lifetime = 24000

default\_realm = FIRMA.CZ

dns\_lookup\_realm = false

dns\_lookup\_kdc = true

default\_tgs\_enctypes = des-cbc-md5

default\_tkt\_enctypes = des-cbc-md5

permitted\_enctypes = des-cbc-md5 des-cbc-crc

[realms]

FIRMA.CZ = {

kdc = serverdc.firma.cz:88

admin\_server = serverdc.firma.cz:749

default\_domain = firma.cz

}

[domain\_realm]

.firma.cz = FIRMA.CZ

[kdc]

profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]

pam = {

debug = false

ticket\_lifetime = 36000

renew\_lifetime = 36000

forwardable = true

krb4\_convert = false

}

**kerberos\_sso**

dtto ale navíc je zde primární pokus o SSO autentizaci.

Nastavení u klienta AS - server je nutné zadávat jménem a nikoliv IP adresou.

Pro java klienta bez AS není režim vhodný.

Nepodaří-li se SSO přihlášení následuje autentizační dialog.

Vyžaduje vyplnění doprovodných položek odstavce "kerberos sso":

Uživatel pro preautentizaci

Heslo pro preautentizaci

**SAML**

Ověření vůči serveru splňujícímu standard SAML2. Nastavení autentizace se liší pro Java klienta a EGJEWEB2.

Slovník pojmů:

**SP** – Service provider – webová aplikace EGJE

**IdP** – Identity provider – důvěryhodný systém ověřující identitu uživatele

**Metadata** – XML soubor dodaný IdP obsahující nastavení potřebné pro výměnu SAML requestů

**SP Metadata** - XML soubor generovaný EGJE, obsahující nastavení pro dodání do IdP

**SSO** – Single Sign On – jednotné přihlášení do více SP

**SLO** – Single Logout – jednotné odhlášení i IdP a všech podporujících SP

**jks** – Java KeyStore – uložiště pro ukládání digitálních certifikátů

**EGJEWEB2:**

Ve Vašem Identity Provideru je potřeba nastavit koncový endpoint, na kterém EgjeWEB přijme SAML Token. Tvar endpointu je následující: **https://<egjewebURL>/saml/SSO** (pozor, je to case sensitive).

V Identity Provideru může být tato konfigurační položka označena jako Single-Sign-On URL, Destination URL, záleží na Vašem Identity Provideru.

Dále pak je potřeba v konfiguraci EGJE nastavit v rámci zvolené autentizace SAML následující položky:

**SP Entity ID:** Vámi zvolený identifikátor Vaší aplikace EgjeWEB. Parametr nastavujete v rámci Vašeho Identity Providera. Název položky v IdP se může lišit, např. Audience nebo Audience Restriction. Záleží na Vašem IdP. Podle hodnoty, kterou nastavíte v IdP, nastavte pak odpovídající hodnotu i v konfiguraci EgjeWEB.

**IDP SSO URL:** Adresa pro zahájení automatického přihlášení iniciovaného ze strany IdP. Položka je nepovinná, pokud nebude nastavena, pro přihlášení uživatelů bude použito přihlášení iniciované ze strany SP (Service Providera) neboli EgjeWEBu. Nastavte zde tedy adresu aplikace, kterou Vám musí dodat Váš IdP, pokud budete aplikovat SSO iniciované Vaším IdP, v opačném případě ponechte prázdné. Pozor, adresou aplikace se zde nemyslí adresa Vaší aplikace EgjeWEB, ale adresa v rámci IdP, přes kterou je možné se na aplikaci EgjeWEB prostřednictvím IdP dostat.

**Adresa Web aplikace:** Externí adresa, na které je provozována aplikace EgjeWEB, měla by se shodovat s adresou, na kterou IdP zasílá výsledek přihlášení, bez koncového /saml/SSO

**IDP metadata:** XML dokument s metadaty IdP. Dokument Vám vydá Váš IdP**.** Pro ADFS v Elanoru je tento dokument možné získat z adresy<http://fsso.domena.cz/federationmetadata/2007-06/federationmetadata.xml>

**IDP metadata – cesta:** URL adresa ke XML dokumentu s metadaty IdP. Z této adresy si EgjeWEB2 při spuštění stáhne dokument s metadaty.

**Interval pro obnovu metadat v CRON formátu:** Interval nastavující obnovu souboru s metadaty bez nutnosti restartu aplikace. V případě potřeby lze obnovu provést u ručně na Adm51/Správa AS/klienta/Web tlačítkem **Přenačíst SAML metadata.**

U parametru je tlačítko na kontrolu CRON formátu zda je zadaný správně a aplikace ho dokáže přečíst.

EGJE umožňuje uživatelům specifikovat si vlastní Java Keystore s certifikáty, které se použijí pro šifrování, resp. dešifrování SAML Tokenů. Pro manipulaci s keystorem se používá utilita keytool, která je součástí používané Javy.

Do keystoru je nutné pod nějakým aliasem vygenerovat pár klíčů, privátní a veřejný. Privátní klíč použije EgjeWEB pro dešifrování tokenu, který je zašifrován Vaším IdP, veřejný klíč je nutné předat Vašemu IdP. IdP použije veřejný klíč pro zašifrování Tokenu před odesláním tokenu do Egjewebu. Příklad použití utility keytool pro vygenerování páru klíčů:

*keytool -genkeypair -alias spring -keypass secret -validity 365 -storepass secret -keystore keystore2.jks -keyalg RSA -keysize 2048*

Výše uvedený příkaz vygeneruje pár klíčů pod aliasem spring, heslo ke klíči je secret, heslo ke store je také secret, platnost certifikátu je 365 dní, použitý šifrovací algoritmus je RSA, velikost klíče je 2048 bitů. Keystore se nachází v souboru ./keystore2.jks. Pokud takový soubor dosud neexistuje, bude vytvořen nový.

Vygenerovaný certifikát v keystoru je možné zobrazit příkazem

*keytool -keystore keystore2.jks -alias spring -list -rfc -storepass secret*

Zobrazený certifikát následně vložte do Vašeho IdP.

Dokumentace k utilitě Java Keystore Javy 11 je k nalezení zde:

<https://docs.oracle.com/en/java/javase/11/tools/keytool.html>

Na straně konfigurace EgjeWEBu je nutné pak vyplnit následující položky:

**Cesta pro uložení jks souboru:** Zadejte zde cestu k souboru, kde se nachází Java Keystore s certifikáty pro šifrování/dešifrování SAML Tokenů. Zde zadaný soubor bude pak přímo vložen do konfiguračního jaru. Pokud provedete jakoukoliv změnu v keystoru, je nutné nahrát soubor do konfigurace znovu a restartovat webový server, aby se změna v keystoru projevila v aplikaci. Podobně se manipuluje například i se souborem obsahujícím metadata IdP.

**Alias pro klíč:** Alias, pod kterým je certifikát v keystoru uložen

**Heslo ke store:** Heslo ke keystore

**Heslo ke klíči:** Heslo k privátnímu klíči, který bude sloužit pro dešifrování SAML Tokenu na straně EGJE.

Pokud si nepřejete šifrovat SAML Tokeny, můžete nechat uvedené konfigurační položky nevyplněné.

Další volitelné parametry:

**NameID format:** Lze nastavit NameID formát který se bude posílat v SAML AuthnRequest. Je potřeba nastavit přesnou hodnotu.

**Vytvořit SP metadata:** Vytvoří endpoint pro generování SP Metadat obsahující aktuální nastavení. Endpoint se skládá z **Adresa Web Aplikace/saml/metadata.**

Tlačítko **Vytvořit metadata** zobrazí aktuální metadata. Více o nastavení viz [**Generování SP Metadat**](#Generovani_sp_metadat)**.**

**Logname element:** Nastavuje atribut ze kterého se má načítat logname pro přihlášení do EGJE ze SAML Assertion.  
Defaultní hodnota je Subject/NameID.

Pokud se použije AttributeStatement, je zapotřebí vyplnit položku „Název attributu obsahujícího logname“.

**Název attributu obsahujícího logname:** Obsahuje název custom attributu obsaženého v elementu „AttributeStatement“ v SAML Assertion pro zjištění logname. Zadává se název obsažený v atributu „Name“ v elementu „Attribute“.

**Vždy při spuštění EGJE vynutit ověření:** Přidá k SAML requestu parametr forceAuthn=true. Při novém otevření EGJE se vždy vynutí u IdP nová autentizace. IdP musí tento parametr podporovat a musí být povolen. Název položky v IdP se může lišit, např. Honor Force Authnentication.

**Při odhlášení z EGJE odhlásit i z IdP:** Při odhlášení z EGJE, se zároveň odešle request pro Single Logout z IdP. Tím se uživatel odhlásí z IdP a zároveň ze všech aktuálně přihlášených SP, které tuto funkci podporují. V IdP je zapotřebí SLO povolit a nastavit pro něj URL: **https://<egjewebURL>/logout/saml2/slo** (pozor, je to case sensitive). Dále je zapotřebí nastavit SP Issuer na stejnou hodnotu jako je nastavené SP Entity ID.

**Logovat SAML:** Zapne úroveň logování pro SAML knihovny na úroveň debug. Loguje velké množství dat a log se tak stává nepřehledným. Doporučujeme zapínat pouze při řešení problémů se SAML autentizací.

**Java klient:**

Ve Vašem Identity Provideru je potřeba nastavit koncový endpoint, na kterém klient EGJE přijme SAML Token. Tvar endpointu je následující: **http://localhost:<saml\_port>/saml/SSO** (pozor, je to case sensitive).

V Identity Provideru může být tato konfigurační položka označena jako Single-Sign-On URL, Destination URL, záleží na Vašem Identity Provideru.

Dále pak je potřeba v konfiguraci EGJE nastavit v rámci zvolené autentizace SAML následující položky:

**SP Entity ID:** Vámi zvolený identifikátor Vaší aplikace EGJE AS. Parametr nastavujete v rámci Vašeho IdP. Název položky v IdP se může lišit, např. Audience nebo Audience Restriction. Záleží na Vašem IdP. Podle hodnoty, kterou nastavíte v IdP, nastavte pak odpovídající hodnotu i v konfiguraci EGJE AS.

**IDP metadata:** Xml dokument s metadaty IdP. Dokument Vám vydá Váš IdP**.** Pro ADFS v Elanoru je tento dokument možné získat z adresy<http://fsso.domena.cz/federationmetadata/2007-06/federationmetadata.xml>.

**IDP metadata – cesta:** URL adresa ke xml dokumentu s metadaty IdP. Z této adresy si EGJE AS při spuštění stáhne dokument s metadaty.

**Interval pro obnovu metadat v CRON formátu:** Interval nastavující obnovu souboru s metadaty bez nutnosti restartu AS. U parametru je tlačítko na kontrolu CRON formátu, zda je zadaný správně a aplikace ho dokáže přečíst.

Pro podepisování SAML requestů je potřeba specifikovat Java Keystore s certifikáty, které se použijí pro šifrování, resp. dešifrování SAML Tokenů. Pro manipulaci s keystorem se používá utilita keytool, která je součástí používané Javy.

Do keystoru je nutné pod nějakým aliasem vygenerovat pár klíčů, privátní a veřejný. Privátní klíč použije EGJE AS pro dešifrování tokenu, který je zašifrován Vaším IdP, veřejný klíč je nutné předat Vašemu IdP. IdP použije veřejný klíč pro zašifrování Tokenu před odesláním tokenu do EGJE AS. Příklad použití utility keytool pro vygenerování páru klíčů:

*keytool -genkeypair -alias spring -keypass secret -validity 365 -storepass secret -keystore keystore2.jks -keyalg RSA -keysize 2048*

Výše uvedený příkaz vygeneruje pár klíčů pod aliasem spring, heslo ke klíči je secret, heslo ke store je také secret, platnost certifikátu je 365 dní, použitý šifrovací algoritmus je RSA, velikost klíče je 2048 bitů. Keystore se nachází v souboru ./keystore2.jks. Pokud takový soubor dosud neexistuje, bude vytvořen nový.

Vygenerovaný certifikát v keystoru je možné zobrazit příkazem

*keytool -keystore keystore2.jks -alias spring -list -rfc -storepass secret*

Zobrazený certifikát následně vložte do Vašeho IdP.

Dokumentace k utilitě Java Keystore Javy 11 je k nalezení zde:

<https://docs.oracle.com/en/java/javase/11/tools/keytool.html>

Na straně konfigurace EGJE AS je nutné pak vyplnit následující položky:

**Cesta pro uložení jks souboru:** Zadejte zde cestu k souboru, kde se nachází Java Keystore s certifikáty pro šifrování/dešifrování SAML Tokenů. Zde zadaný soubor bude pak přímo vložen do konfiguračního jaru. Pokud provedete jakoukoliv změnu v keystoru, je nutné nahrát soubor do konfigurace znovu a restartovat AS, aby se změna v keystoru projevila v aplikaci. Podobně se manipuluje například i se souborem obsahujícím metadata IdP.

**Alias pro klíč:** Alias, pod kterým je certifikát v keystoru uložen

**Heslo ke store:** Heslo ke keystore

**Heslo ke klíči:** Heslo k privátnímu klíči, který bude sloužit pro dešifrování SAML Tokenu na straně EGJE.

Pokud si nepřejete šifrovat SAML Tokeny, můžete nechat uvedené konfigurační položky nevyplněné.

**Port pro SSO/SLO:** číslo portu, na kterém lokální server naslouchá pro přesměrování do IdP a zpět. Zadaný port musí být součástí URL pro SSO a SLO endpointy.

Další volitelné parametry:

**NameID format:** Lze nastavit NameID formát který se bude posílat v SAML AuthnRequest. Je potřeba nastavit přesnou hodnotu. Pokud se nevyplní použije se hodnota urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

**Vytvořit SP metadata:** Vytvoří endpoint pro generování SP Metadat obsahující aktuální nastavení. Endpoint se skládá z **http://<adresa\_as>:<saml\_metadata\_port>/saml/metadata.**

Tlačítko **Vytvořit metadata** zobrazí aktuální metadata. Více o nastavení viz [**Generování** **SP Metadat**](#Generovani_sp_metadat)**.**

**Port pro generování SP metadat:** port na kterém se spustí server pro generování SP metadat.

**Logname element:** Nastavuje atribut ze kterého se má načítat logname pro přihlášení do EGJE ze SAML Assertion.  
Defaultní hodnota je Subject/NameID.

Pokud se použije AttributeStatement, je zapotřebí vyplnit položku „Název attributu obsahujícího logname“.

**Název attributu obsahujícího logname:** Obsahuje název custom attributu obsaženého v elementu „AttributeStatement“ v SAML Assertion pro zjištění logname. Zadává se název obsažený v atributu „Name“ v elementu „Attribute“.

**Vždy při spuštění EGJE vynutit ověření:** Přidá k SAML requestu parametr forceAuthn=true. Při novém spuštění EGJE se vždy vynutí u IdP nová autentizace. IdP musí tento parametr podporovat a musí být povolen. Název položky v IdP se může lišit, např. Honor Force Authnentication.

**Při odhlášení z EGJE odhlásit i z IdP:** Při odhlášení z EGJE, se zároveň odešle request pro Single Logout z IdP. Tím se uživatel odhlásí z IdP a zároveň ze všech aktuálně přihlášených SP, které tuto funkci podporují. V IdP je zapotřebí SLO povolit a nastavit pro něj URL: **http://localhost:<saml\_port>/saml/SLO** (pozor, je to case sensitive). Dále je zapotřebí nastavit SP Issuer na stejnou hodnotu jako je nastavené SP Entity ID. Pro odhlášení z IdP je zapotřebí mít vyplněný keystore pro podepsání SAML tokenů.

**Podepsat SAML SSO Request:** Podepíše SAML request pro přihlášení. Využívá se pro IdP, které nepodporují nastavení atributu *WantAuthnRequestsSigned* v metadatech z IdP. Pro podepsání je zapotřebí mít vyplněný keystore.

**Logovat SAML:** Zapne úroveň logování pro SAML knihovny na úroveň debug. Loguje velké množství dat a log se tak stává nepřehledným. Doporučujeme zapínat pouze při řešení problémů se SAML autentizací.

**Generování SP metadat:**

Kromě základního generování metadat je možné parametricky doplnit dodatečné informace. Pro jejich doplnění je nutné ručně upravit soubor **config\_local.properties** v archivu **config\_egje.jar**. Pro tyto atributy lze obvykle nastavit více hodnot například pro každý jazyk vlastní hodnotu.

Aby se správně zobrazovala čeština, je potřeba upravovat soubor v kódování ISO-8859-1.

Doplnit lze následující oblasti:

* + **UIInfo – Element UIInfo v elementu Extensions**
    - Slouží k dodatečnému nastavení informací o spouštěné aplikaci.
    - Nastavit lze tyto elementy: *Description, DisplayName, InformationUrl*.
    - Pro každý element se nastaví atribut *lang* obsahující jazyk, pro který jsou informace vyplněny.
    - Příklad nastavení v properties:

saml\_extensions\_uiinfo[0].displayname=EGJE CZ

saml\_extensions\_uiinfo[0].description=Personálně-mzdový systém

saml\_extensions\_uiinfo[0].informationurl=https://elanor.cz

saml\_extensions\_uiinfo[0].lang=cs

* + **Organization** 
    - Slouží k dodatečnému nastavení informací o organizaci.
    - Nastavit lze tyto elementy: *name, displayname, url.*
    - Pro každý element se nastaví atribut *lang*, obsahující jazyk, pro který jsou informace vyplněny.
    - Příklad nastavení v properties:

saml\_organization[0].name=Elanor  
saml\_organization[0].displayname=Elanor  
saml\_organization[0].url=https://elanor.cz  
saml\_organization[0].lang=cs

* + **ContactPerson**
    - Slouží k zadání kontaktní osoby.
    - Nastavit lze tyto elementy: *company, given\_name, sur\_name, email\_address, telephone\_number.*
    - E-mailové adresy i telefonní čísla lze zadat pro daný kontakt vícekrát za pomoci indexů.
    - Pro daný typ kontaktu lze nastavit atribut *contactType*.
    - Příklad nastavení v properties:

saml\_sp\_contact[0].contactType=technical  
saml\_sp\_contact[0].company=Elanor  
saml\_sp\_contact[0].given\_name=Guy  
saml\_sp\_contact[0].sur\_name=Technical  
saml\_sp\_contact[0].email\_address[0]=mailto:technical@example.com  
saml\_sp\_contact[0].telephone\_number[0]=+720123456987

**NTLogin/2/3 JCifs**

Autentizace NTlogin\* bez číslovky 2 byli zrušeny v e202409 a od e202411 se pomocí nich nejde do EGJE přihlásit.

Autentizace NTlogin2\* jsou zde pouze pro zpětnou kompatibilitu. Nedoporučujeme je používat.

Autentizace NTlogin3\* však bezpečnostní kritéria splňují a pro OS linux jsou vhodné. Tyto autentizace využívají novější SMB2 protokol.

SSO autentizace (NTLogin3 a NTLogin3Only) nepoužívá zabezpečený secure channel pro NETLOGON komunikaci s doménovými controllery. Pro správnou funkčnost je pro servisní NTLM účet zapotřebí použít nezabezpečeného Netlogon připojení viz. odkaz: <https://support.microsoft.com/en-au/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e#bkmk_thegrouppolicy>

Na zprovoznění zabezpečené komunikace pracujeme a bude podporována v další verze IS EGJE.

IP adresy doménových řadičů (NT Login)  
IP adresa autentizačního serveru pro NT login (je-li jich více jsou odděleny čárkou; použit je pak první, který je spuštěn)

Není-li vyplněn, je použit řadič zjištěný z NT login implic. domény

V praxi je někdy výhodné zadat jiný server než doménový řadič, který volání zprostředkuje (SSO u Web aplikace a doménovým řadičem Windows 2003)

NT login implic.doména předvyplnění položky doména u NT login

Pro NTlogin2 je třeba vyplnit parametry:

DC hostname (NT Login2)  
Simple (non-FQDN) hostname of DC host (NT Login2) (domainControllerName)

Účet počítače pro připojení k DC (NT Login2)  
Computer account for connection to DC (NT Login2) (ntlm2ServerAccount)

Účet počítače pro připojení k DC (NT Login2) - Heslo  
Password of computer account (NT Login2) (ntlm2ServerPassword)

Více technických informací o NTlogin2 je možné získat na webu u knihoven

jespa-1.1.21 Jespa\_Operators\_Manual.pdf

Je zde dobře popsáno vytvoření computer account v AD, který je pro NTlogin2 zapotřebí.

Pozn. knihovny jespa EGJE nepoužívá, není tedy třeba jejich licence.

Stručně je postup vytvoření computer account následující:

* vytvoření účtu nějakou ze standardních utilit (Active Directory Users and Computers (ADUC) MMC Snap-In.)  
  Maximálně 15 znaků z A-Z, a-z, 0-9,“-„, „\_“
* nastavení hesla – z příkazové řádky skriptem



prvním parametrem je jméno účtu následované znaky $ a @ DNS doménovým jménem a druhým heslo  
př. C:\tmp>SetComputerPassword [elanor1$@firma.corp](mailto:elanor1$@firma.corp) *heslo*

Heslo musí být jiné než jméno účtu.  
Úspěšné provedení indikuje hláška „The password was set successfully“.

**smart\_card**

Autentizace je k dispozici od e201905 pro java klienta, od e201909 i pro web klienta.

Jde o tzv. 2-faktorovou autentizaci, kdy klient pro přihlášení potřebuje vsunout kartu do čtečky a zadat heslo, které EGJE ověří vůči certifikátu na kartě.

Systém jsme vyvinuli a testovali na čtečce a kartě prodávané firmou První certifikační autorita (https://www.ica.cz/Order-Hardware, Smart-Card Reader GemPC USB-SL, Smart Card Starcos 3.5).

Certifikát si uživatel zaeviduje pomocí formuláře Opv51 - Osobní certifikát, přičemž vlastní veřejný klíč je uložen do úložiště společného s Opv31 (jako uchaz\_dok\_typ 51 - Osobní certifikát I.).

To slouží pro tuto autentizaci místo standardního Adm10 / Logname, které používají všechny ostatní autentizace.

Pro tuto autentizaci jsou v sekci Smart Card další parametry:

* + **Zdroj certifikátů**: combo Čipová karta/Osobní certifikáty uživatele
  + **Certifikační autorita**: certifikát autority v binárním formátu. Je-li vyplněno, lze pro autentizaci použít pouze certifikáty touto autoritou vydané.
  + **Jméno v certifikátu se musí shodovat se jménem v EGJE** - checkbox

Kontrola shody Jména a Příjmení - certifikát, vs. Osb02.

V EGJEWeb je tato autentizace funkční pro tomcat + Chrome nebo EDGE.

Ve Firefoxu také funguje, ale je třeba nastavit PKCS#11 modul v konfiguraci.

Přičemž zde je hláška Firefoxu pro zadání pinu, která je trochu odtažitá: "Please enter the master password for the 9203050100050786."

Příklad konfigurace tomcatu pro tuto autentizaci:

<Connector port="8548" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

truststoreFile="${catalina.home}/conf/trust.jks" truststorePass="tomcat"

keystoreFile="${catalina.home}/conf/prghr2.pfx" keystorePass="79798796"

keystoreType="pkcs12" keyAlias="{d2046356-d048-4cac-8a82-9f195766c035}"

clientAuth="true" sslProtocol="TLS" />

**Údaje pro změnu hesla pomocí LDAP a autentizaci LDAP:**

LDAP - SSL URL

adresa a port ldap serveru

např. ldaps://xxxx:636

resp. adresa port i kořen, pod kterým jsou uživatelé systému (mohou být i v podřízených uzlech)  
např. ldaps://prgxx1:636/OU=Country.Czech,OU=ElanorUsers,DC=myorg,DC=cz

LDAPSearch - filtr

aditivní filtr

použije se typicky s Novell eDirectory resp. s Microsoft AD resp. všude tam kde filtr nejde psát přímo do přihlašovacího řetězce LDAP - SSL URL.

např. uid=%username%

resp. (&(objectclass=person)(userPrincipalName=%username%@myorg.cz))

LDAP-speciální uživatel pro práci s LDAP (+heslo)

uživatel použitý pro přihlášení a procházení LDAP serveru resp. pro činnost v rámci správy uživatelů Adm12.

uživatel je také použit při změně hesla v AD po jeho expiraci (resp.první přihlášení)

obvykle musí být uveden i s doménou

např. [ldapadmin@myorg.cz](mailto:ldapadmin@myorg.cz)

LDAP/Web - implicitní doména uživatele

doména, která se doplňuje při přihlášení za uživatelské jméno (typicky pro LDAPOnly)

např. myorg.cz

Web - ldap base s maxPwdAge (změna hesla)

ldap adresa pro ziištění maximální doby platnosti hesla

např. dc=myorg,dc=cz

Jde o varování ještě před expirací hesla.

Zjišťování se provádí pouze pro LDAPOnly a pro uživatele, kteří mají práva na Xpw01.

Pozn. v EGJE implementována i změna hesla po expiraci, viz výše.

LDAP/Web - doba (počet dní) předstihu před vypršením hesla

doba, po jejímž dosažení systém vyžaduje jeho změnu

Web - telefon na správce - zobrazen v případě, kdy vypršelo heslo

Web - e-mail na správce - zobrazen v případě, kdy vypršelo heslo

LDAP/Web - zpráva - heslo nesplňuje pravidla

zpráva, kterou systém odpoví v případě, že nové zadané heslo při změně hesla nesplňuje podmínky na heslo kladené

Pozn. Další parametry pro vytváření uživatele v LDAP repository (form. Adm12) jsou v Adm21/Konfigurační parametry/Vytváření uživatelů LDAP/AD.

Soubor s požadavky na reset hesla (úplná cesta):

EGJE Web umožňuje z adresy

http://xxxxxx/egjeweb2/ref/resetpass

generovat textový soubor s požadavky na reset hesla

Tento parametr udává plnou cestu k tomuto souboru.

(následné promítnutí souboru např. do Active Directory již aplikace neřeší)

**WEB / http adresa - přesměrování - uživ.nemá profil:**

je parametr, který použije aplikace EGJEWEB v případě, že dojde sice k ověření uživatele, ale tomu správce nepřiřadil žádný aplikační profil pro přístup do EGJE. V tomto případě aplikace přesměruje prohlížeč na tuto adresu, kde předpokládáme, že jsou uvedeny organizační informace, jak se má uživatel dále zachovat.

**Výčet profilů povolených pro WEB**.

Z této konkrétní instalace EGJEWeb2 se pak půjde přihlásit jen na uvedené zaměstnanecké, manažerské nebo referentské profily. Jde o regulární výraz. Např. MANA.\*|ZAME.\* znamená profily s kódy začínajícími MANA nebo ZAME.

**Nekontrolovat e-mailovou adresu odesilatele**

Nastavení, zdali provádět kontrolu formální správnosti adresy odesílatele mailu (obvykle firemní mail osoby uživatele - Osb02)

* + - 1. **Konfigurace pro mobilní přístup**

Pro přístup z mobilů/tabletů včetně zpřístupnění mimo intranet či doménu může být v organizaci speciální instalace EGJEWeb2.

Zde může být zadáno speciální ověření „Mobile“, ale může zde být i jiné ověření, ale pro prohlížeče mobilů / tabletů s mobilním user agentem je stejně vždy používáno ověření Mobile.

Pokud tedy správce u serveru zadá ověření Mobile, není dovoleno žádné jiné ověření. I uživatelé PC pak podléhají mobilnímu ověření. Což může být využito pro některé externí přístupy i z PC.

Zabezpečení aplikace má pak trochu jinou strukturu:

* Zde v Configuratoru / Ověření je možné zadat „Výčet profilů povolených pro WEB“.   
  Z této konkrétní instalace EGJEWeb2 se pak půjde přihlásit jen na uvedené zaměstnanecké, manažerské nebo referentské profily. Jde o regulární výraz. Např. MANA.\*|ZAME.\* znamená profily s kódy začínajícími MANA nebo ZAME.  
  Pozn. omezení platí pro celou EGJEWeb2 tedy i pro přístupy z PC tj. přes nějaké jiné ověření (např. mswin\_ntlm aj.)
* Adm02 / Povoleno pro autentizaci mobil/tablet - který profil smí dostupný být z mobilu tj. mobilní autentizací (plošně pro všechny EGJEWeb2)
* Adm10 / Povolení přístupu z mobilních zařízení - která osoba smí přistupovat do aplikace z mobilu/tabletu (tj. pomocí mobilního ověření).
* Adm16 – Správce nebo Manažer či jiný uživatel se zadaným mobilním profilem a povolením zde (tedy z ověřeného uživatele) vytvoří dočasné heslo pro vytvoření autentizace v konkrétním zařízení a konkrétním prohlížeči v něm (pozor je třeba jej mít v režimu „mobilní user agent“ tzn. nemít např. v mobilním Chrome zaškrtnuto „Verze webu pro PC“).  
  Heslo si může do mobilního zařízení (má-li jej právě v ruce) rovnou opsat, nebo jej odeslat na e-mail zadaný personalistou v Osb02 (druh komunikace 31) – tlačítko „Odešli heslo e-mailem“.  
  Pozn. pokud má uživatele více mobilních zařízení nebo jej mění je vhodné si tyto přístupy evidovat se jménem zařízení.
* Pokud má uživatel tento e-mail přístupný v mobilním zařízení, je zprovoznění nejpřímočařejší. Otevře si e-mail a klikne na link v něm. Ten již jednorázové heslo obsahuje a aplikaci v konkrétním mobilním zařízení zprovozní.  
  Pokud ne, zadá v mobilním prohlížeči adresu aplikace a do jediné v tu chvíli zobrazené položky zadá jednorázové heslo.  
  Zároveň je v obou případech vhodné si rovnou z mobilního prohlížeče odkaz na aplikaci přidat na plochu a příště ji již spouštět odsud.
* Jednorázové heslo je dočasné, při jeho generování se zadává jeho platnost (standardně 10 minut).
* Když uživatel mobilní zařízení ztratí, je potřeba z EGJE co nejrychleji v Adm16 přístup pomocí tohoto zařízení zneplatnit (tlačítko Zneplatni přístup)!   
  Případně, má-li uživatel zařízení více a není jasné, které je které, tak zneplatnit všechny resp. zrušit v Adm10 uživateli mobilní povolení úplně.
* Přímo v mobilní aplikaci má uživatel volbu „Zrušení přístup z mobilního zařízení“ (nad volbou Odhlášení). Po dotazu se pak přístup z konkrétního prohlížeče konkrétního mobilního zařízení zneplatní shodně jako výše uvedenou akcí „Zneplatni přístup“ z Adm16 resp. smazáním řádku s evidencí přístupu tamtéž.

Pozn.: v Adm21 / Parametry komunikace je parametr "http(s) adresa EGJEWeb2 pro mobilní přístup:" Tato adresa je použita v Adm16 při akci Odešli heslo e-mailem. V e-mailu je link složený z této adresy a parametru – jednorázového hesla.

Možnost vypnutí mobilní autentizace

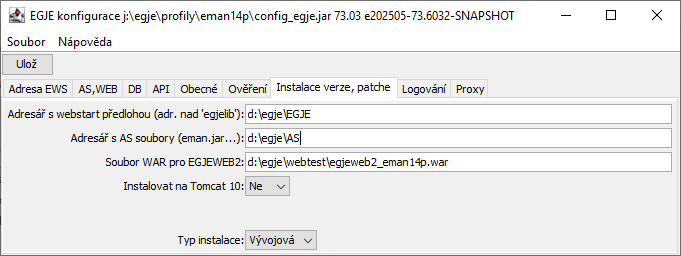
V konfiguraci zpřístupňované utilitou Configurator je na záložce Ověření parametr (v pořadí druhý)

Pro mobilní zařízení (dle user agent) použít vždy autentizaci Mobile Ano/Ne

Jeho nastavení na Ne pak způsobí, že i z mobilních zařízení, které se prohlížeči hlásí jako

user agent = mobile, se bude volat ta autentizace, která je uvedena o řádek výš v položce autentizace.

* + 1. **Atributy instalace**



Údaje využívá instalační program pro správu více instalací SuperConfigurator.

Jsou použity pro instalaci patche/výdeje z instalačního adresáře do zde uvedených adresářů konkrétní instalace EGJE.

Adresář s web.start předlohou

Celá cesta k adresáři, ve kterém je webstart předloha tj. adresář, ve kterém se nachází podadresář "egjelib". Standardně jde o adresář …\EGJE.

Soubor s WAR pro EGJEWEB2:

Souborová cesta k web aplikaci (tj. cesta k souboru v adresáři webapps servlet kontejneru Tomcat)

Vlastní instalace se skládá z

Konfigurace web aplikace - z původní se převezmou z web.xml hodnoty parametrů  
<param-name>config\_jar</param-name>

a zkonfigurovaný souboru se zkopíruje místo dosavadního.

Aplikace obsahuje i rozhraní HR portal pro manažery a zaměstnance.

Instalovat na Tomcat 10:

Pro Ano se při tvorbě waru použije war pro Tomcat 10. Viz Příloha C1.

Typ instalace:

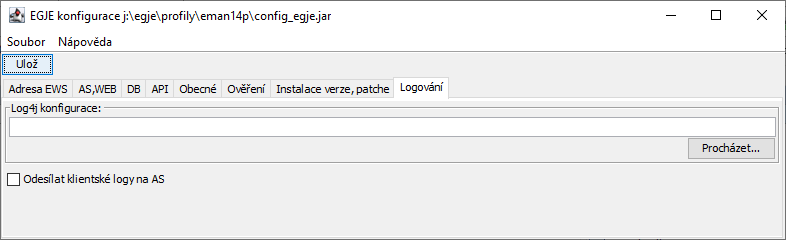
Možné hodnoty: nevyplněno = Produkční / Testovací / Vývojová

Testovací a Vývojové prostředí pak indikuje poměrně výrazně standardní i webový klient.

U web klienta se změní i ikona aplikace.

U std. klienta s AS se údaj nastavuje pro konfiguraci AS, nikoliv klienta. Po nastavení je třeba AS (EGJEWEB2) restartovat.

### Logování



Na této záložce lze nastavovat logování aplikace pomocí Log4j.

Log4j konfigurace:

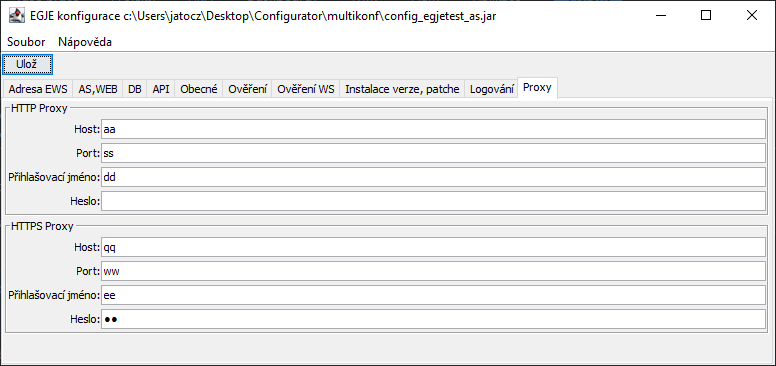
Zde lze umístit adresu externího konfiguračního souboru Log4j. Pokud se nenastaví, použije se defaultní nastavení EGJE.

Více viz [**Příloha E. Logování - AS, EGJEWEB2**](#_Toc125008396)

Odesílat klientské logy na AS:

Při zaškrtnutí se veškeré události, logované pomocí log4j, v klientské části aplikace odesílají na AS. Má význam nastavovat pouze pro Java klienta připojujícího se k AS.

### Proxy



Na této záložce lze nastavit proxy pro http a https. Součástí proxy může být v případě autentizace vyplněno i jméno a heslo. Toto nastavení má přednost před nastavením parametrů při spuštění aplikace (\*.bat, spouštění tomcatu…).

## Nastavení a změna parametrů pomocí utility „MultiConfigurator“

Tato utilita umožní výběr více configů najednou a je pro ni vytvořena třída pro spuštění \*.bat souborem.

***Upozornění***: Stará funkcionalita configuratoru zůstává zachována. Pořád je možno spustit configurator nad jedním souborem a upravovat jen tento soubor.

*Vzor pro spuštění*:

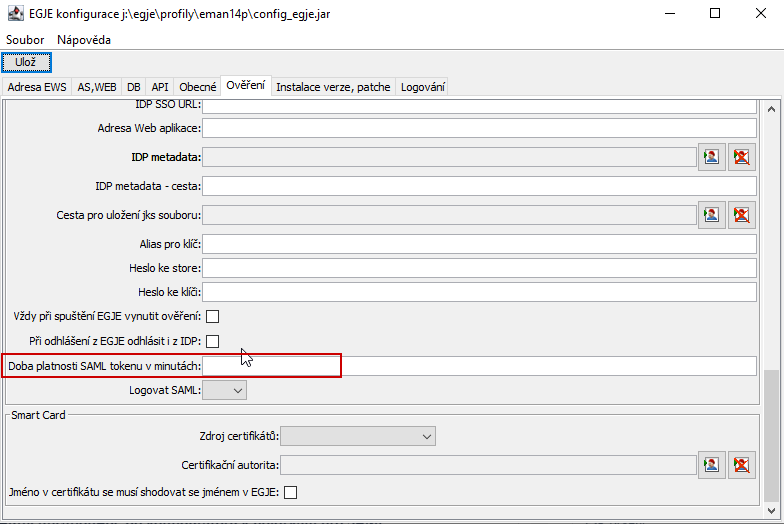
start java -Xmx512M -ea -Dlog4j.configuration=log4j.eman.properties -Djdk.jar.maxSignatureFileSize=16000000 -cp /egje/vzor/EGJE/egjelib/eman.jar;/egje/vzor/EGJE/egjelib/egjelib.jar cz.elanor.eman.sgui.configurator.MultiConfigurator %1exit

*Přidání krb5.conf*

Pokud se za %1 vloží druhý parameter %2, obsahující cestu ke krb5.conf pro konfiguraci Kerberos autentizace, tento konfigurační soubor se automaticky vloží do všech nových jar souborů.

Po spuštění se zobrazí tabulka a v ní seznam configů ze složky, ze které se bat soubor spustil. Soubory se načtou dle masky config\_egje\*.jar. Tabulka bude umožňovat výběr více configů najednou.

Pod tabulkou budou tlačítka:

* Označ vše - označí všechny záznamy v tabulce
* Zruš označení - zruší označení záznamů v tabulce
* Přidat - zobrazí dialog obsahující:
  + Jméno: text editor - zvolení jména souboru
  + Typ: combo box pro výběr typu soubouru obsaující hodnoty:
    - C - Klient bez AS
    - SC - Klient s AS
    - S - Aplikační server
    - WS - Webový server
  + Tlačítko “Přidat” - po zmáčknutí založí nový soubor se zvoleným názvem a pro daný typ
    - soubor se založí okamžitě na disk
    - do nového souboru se vloží krb5.conf
* Odebrat - po stisknutí zobrazí dialog “Vybrané konfigurační soubory budou smazány z disku. Tato akce je nevratná! Chcete pokračovat?” - Ano/Ne - Po odsouhlasení smaže soubor z tabulky i z disku
* Vygenerovat sadu - založí sadu configů, pro testovací configy nastaví r\_typ\_inst=T
  + config\_egje\_as - S
  + config\_egje\_cl - C
  + config\_egje\_web - WS
  + config\_egjetest\_as - S
  + config\_egjetest\_cl - C
  + config\_egjetest\_web - WS
* **Upravit nastavení**
  + pokud je vybrán pouze jeden config. soubor, otevřít standartní configurator.
  + provede se kontrola všech vybraných konfigů, zda se údaje ukládané do více konfigů shodují (např. nastavení DB pro AS a WEB), kontrolují se údaje, které se ukládají do více config. souborů viz “Záložky konfigurátoru”.
    - pokud se neshodují
      * vypsat do protokolu jaké položky se v jakých souborech liší a nepustit dál
    - pokud se schodují
      * otevřít std. konfigurátor s možností úprav všech souborů najednou
* v záložce Konfigurátoru „**Ověření**“ přibyl parametr pro nastavení platnosti SAML tokenu. Pole má název „Doba platnosti SAML tokenu v minutách:“. Do tohoto pole se může nastavit doba platnosti parametru (maxAutenticationAge). Pokud zde není vyplněná hodnota, je standardně nastaveno 7 dnů (10 080 minut). Viz obrázek.  
  
  1. **Adm51 - Změnové řízení databáze**

Záložka **Verze databáze** zobrazuje informace o současné verzi struktury a obsahu databáze EGJE.

Informace se skládá z:

* kódu verze
* posledního povinného patche
* nepovinné patche (může jich být více)

Záložka **Změna Db** obsahuje tlačítko "**Provedení změny Db / Instalace uživatelské sestavy**"

Následuje výběr skriptu a ihned poté (pokud je splněna kontrola na současnou verzi) dochází k jeho provádění. Protokol z provádění akcí se průběžně ukládá v uživatelském pracovním adresáři (tentýž kam se ukládají tiskové sestavy) tj. %HOME\_DIR%\Dokumenty\Eman\output pod stejným jménem jako má skript a s extenzí html. Po ukončení instalace se soubor automaticky otevře v defaultním prohlížeči.

U instalací s AS je před spuštěním skriptu vhodné informovat uživatele, k tomu je zde k dispozici tlačítko "Rozeslat požadavek na odhlášení přihlášeným uživatelům".

Informace je předávána přes databázi všem klientům, každý klient si tuto informaci čte jednou za 5 minut. Ti uživatelé, kteří jsou připojeni přes ten samý AS či EGJEWEB, přes který správce tlačítko mačká, dostávají informaci okamžitě a v protokolu je uveden jejich seznam, uživatelé připojení jinak v protokolu nejsou, zpětnou informaci systém nezasílá.

Po instalaci uživatelské sestavy, která mění repository, má správce k dispozici tlačítko "Přenačíst repository na všech AS / EGJEWEB2" pro promítnutí změn i na další servery EGJE.

Nicméně i když to neučiní, servery EGJE si periodicky (interval 5 minut) kontrolují, zdali ke změně v repository nedošlo, a když ano, přenačtou si ji.

Záložka **Změnový log**

zobrazuje informace o změnových řízeních, která proběhla v databázi. Nejjemnější jednotkou zde je blok změnového řízení.

Záložka **Konfigurace klienta**

má významu pouze při správcovském spouštění přímo na serveru pomocí egje.bat. Tlačítko Konfigurační formulář pak vyvolává to samé konfigurační okno jako v předcházející kapitole popsaná utilita configurator\_egje.

Záložka **Oracle statistiky**

má význam právě a pouze pro instalaci nad databází Oracle. Pro správnou funkci příkazů pro práci s databází je bezpodmínečně zapotřebí provádět pravidelně aktualizaci databázových statistik. Jinak dochází k pozvolnému nerovnoměrnému zpomalování některých částí aplikace. Akci doporučujeme provádět automatizovaně pomocí Oracle jobu. Ten je možné vytvořit přímo z tohoto formuláře. Vyplňte položku "Hodina" (př. 23 => v jedenáct večer; 0 - o půlnoci) a poté stiskněte tlačítko Vytvořit/Obnovit job na aktualizaci statistik. Pokud se vytvoření podaří, jsou od té chvíle také přístupná tlačítka "Spustit job" "Zrušit job".

Délka akce je závislá na velikosti db a výkonu serveru. Může být od minuty do desítek minut.

Na záložce je také tlačítko Rebuild/přesun indexů.

Umožňuje zavolat na všechny indexy db EGJE alter index rebuild.

Při spuštění také dialog umožní vybrat jiný přístupný tablespace - indexy jsou pak přesouvány do něj. To může u některých konfigurací databázi zrychlit.

Při spuštění bez vybraného tablespace se provede výše uvedený rebuild.

Funkčnost pro rebuild indexů je určena správcům malých databází. Kvalifikovaní správci velkých instalací by měli používat nástroje Oracle.

Záložka **MS SQL statistiky**

má význam právě a pouze pro instalaci nad databází MS SQL.

Obsahuje seznam indexů, informace o jejich fragmentování a informaci o poslední aktualizaci statistik indexů.

Tlačítko Rebuild indexů aktualizace statistik provádí následující:

* alter index rebuild - na všechny EGJE indexy
* update statistics na všechny EGJE tabulky

Funkčnost rebuild indexů, aktualizace statistik je určena správcům malých databází. Kvalifikovaní správci velkých instalací by měli používat nástroje MS SQL.

Záložka **Správa AS/klienta**

u instalací s aplikačním serverem poskytuje informace o všech uživatelích, kteří se systémem pracují, u instalací bez AS pak pouze o sezení a procesech současného uživatele, s výjimkou podzáložky Databázové zámky, která zobrazuje i zámky ostatních uživatelů. Více o zámcích v [příloze M](#DB_zámky).

Na Oracle je k dispozici také záložka. Kdo koho blokuje, která se snaží najít původce zámků.

Správce má možnost i jednotlivé úlohy (s AS i sezení) ukončovat.

Ukončování je ovšem na straně javy, nikoliv na straně databáze (k tomu nemá db účet, který aplikace používá dostatečná oprávnění)

Poslední podzáložkou je "DB připojení". Určena je pro zákazníky, kteří používají java klienta bez AS. U všech ostatních klientů dochází ke sdílení db připojení, a tak zde uvedené údaje mají trochu jiný, ne tak užitečný, smysl.

Pro WEB EGJE server existuje záložka Web, obsahující tlačítko na přenačtení metadat pro SAML autentizaci. Záložka je viditelná pouze pro WEB při nastavení SAML autentizace.

Záložka **Zabezpečení**

Po provedení změn na této záložce je potřeba restartovat AS resp. WEB EGJE server.

Na záložce "Zabezpečení" je možné:

* zapsat autentizace, která je jediná povolená (směrováno na java klienta bez AS)
* zabezpečení SuperConfiguratoru vůči aktuální db
  + Možnost provést změnový skript
  + Povolit export číselníků
  + Výčet IP adres, ze kterých je dovolené SuperConfigurator spustit
* "Pokoušet se o znovupřipojení k aplikačnímu serveru",

parametr určuje, zda se klient AS má v případě výpadků spojení zkoušet znovu připojit. Pokud zde nastavíte Ne, tak to klient nečiní a tudíž nemá důvod si heslo pamatovat. Pokud nastavíte Ano (= dosavadní režim), tak si klient pro tento účel heslo pamatuje, ale pamatuje si v podobě zašifrované symetrickým algoritmem.

Heslo si klient také musí pamatovat v případě, že má pracovat s více AS.

* expirace sezení

Položky

Std.klient - sezení expiruje za [min]:

EGJEWEB(2) - sezení expiruje za [min]:

U std. (java) klienta je z technických důvodů sledována aktivita uživatele v celém operačním systému, nikoliv jen v aplikaci EGJE.

Když není vyplněna položka "Std.klient - sezení expiruje za [min]:", k expiraci u standardního klienta nedochází = dosavadní stav.

Expirací u standardního klienta, což není webová aplikace, dochází tak, že je běh klienta ukončen - aplikace tedy uživateli zmizí (poznámka - může to být i považováno za trestání kuřáků). Zvažte tedy dobře, jestli to u standardního klienta nastavit, určitě lepší cestou je povinné (interní politikou vynucené) zamykání obrazovky na úrovni operačního systému.

Když není vyplněna položka "EGJEWEB(2) - sezení expiruje za [min]:", je implicitní chování následující:

Stará web aplikace - sezení neexpiruje nikdy - aplikace stále sezení prodlužuje, takže ho neukončí ani tomcat.

Nová webová aplikace (včetně WP) - expirace je dána nastavením tomcat tj. standardně 10 minut.

Pro všechny klienty platí, že při spuštěné sestavě či výpočtu aplikace čeká na výsledek a automatické odhlašování je pozastaveno. Expiraci brání také otevřený formulář Adm51, který se serverem komunikuje neustále.

Doba expirace také může být o určitý čas prodloužena díky příjmu interní pošty EGJE.

Servery si uvedené údaje přenačítají z db každých 5 minut. Klient (java či prohlížeč) si pak údaj přebírá ze serveru v okamžiku přihlášení

Záložka **Org. IT par.**

Obsahuje master-detail z organizacemi zadanými v Adm21 a vybírá z Adm21 a Ftp02 parametry, které spíš než věcnému správci aplikace přísluší IT správcům. Jde o alternativní umístění a editaci.

Záložka **Zpráva všem**

Správce může na dobu mezi dvěma datumy zadat textovou správu, která se uživatelům po přihlášení zobrazuje ve všech klientech EGJE.

Tyto zprávy se řadí nahoru.

V HR Portál jsou v pravém sloupci Zprávy a odkazy.

V ostatních rozhraních jsou pak zobrazovány pomocí interního okna Mail.

Datově zůstává zpráva společná a nerozkopírovává se tedy každému uživateli. Tudíž ji tento ani nemaže. Po uplynutí datumu do zpráva sama zmizí.

Záložka **Odstávka systému**

V podstatě podobná věc, ale definují se zde i časy a je možné ale ne nutné specifkovat server a port čímž se dá určit konkrétní AS, který bude správci odstaven.

Od určitého času při přihlašování upozorňuje, kdy odstávka bude a když už je a systém ještě běží, nedovolí uživateli přihlášení, resp. upozorňuje přihlášené a pokud nejsou správci (práva na Adm51) tak ukončí jejich sezení shodně jako při expiraci.

Kontrola probíhá jednou za 5 minut a týká se web i std klienta (s AS i bez).

Záložka **Link všem**

Umožňuje správci do EGJE přidat nějaký http(s) odkaz.

HR Portál jej zobrazuje nahoře ve sloupci Zprávy a odkazy

ostatní rozhraní vytvoří v menu nabídku Odkazy.

Také odkaz může být dočasný, také má od a do.

Odkazy se otevírají dle nastavení prohlížeče, obvykle do nové záložky.

Pozn.: není ambicí EGJE nahrazovat firemní intranet, zvlášť při používání interaktivní autentizace jsou odkazy poněkud "za rohem".

Záložka E(W)SOI

Zákazníci využívající rozšíření Egje o ESOI (Egje Standard Output Interface) mají nyní možnost nastavit parametry tohoto interface. Nová verze interface, která bude vydána po verzi e202309, bude toto nastavení využívat. Jedná se o volby:

Jazyk pro názvy

Status pro uzavření mezd

Pro připravované rozhraní EWSOI je tam i volba (bez možnosti změny):

Výstup Web rozhraní.

* 1. **Pomocné utility**
     1. **Utilita anonymizace**

Slouží k odstranění, resp. zmatení citlivých osobních dat z databáze EGJE.

Je vhodná pro různá testovací prostředí.

Ale na ostré prostředí dokáže udělat nevratné škody.

Součástí instalačního adresáře verze je i vzorová dávka anon\anomymizace.bat pro MS Windows prostředí, pro linux se dá snadno vytvořit analogická.

Dávka předpokládá existenci těchto souborů v aktuálním adresáři:

config\_egje.jar - aktuální konfigurace (s připojením k db tedy AS, egjeweb, klient bez AS)

anonymizace.jar - aktuální soubor z tohoto adresáře

eman.jar - aktuální eman.jar z výdeje

egjelib.jar - aktuální egjelib.jar z výdeje

Pozn. v patch není anonymizace vydávána. Používejte proto soubory z posledního výdeje.

S aktualizovanou eman.jar z patche není spuštění doporučeno a díky obfuskaci kódu pravděpodobně ani nepoběží.

Standardní spouštění je bez parametrů.

Anonymizační utilita od verze e202401 neobfuskuje konstantní a specifický symbol a variabilní symbol je pozměněn tak, aby odpovídal počet číslic.

Dále u částek mezd je částka pozměněna tak, aby odpovídala počtem číslic.

Přídavné parametry:

zapisují se do dávky za parametr z\_run\_test.anonymizace.Anonymizace

resp. se dají psát až při spouštění dávky anonymizace\_template.bat, neboť ta je psána tak, že parametry zvenčí předává

parametr -gidoscpv který navíc nahradí libovolným vygenerovaným kódem cetpv.gid cetoso.gid

a cetpv.oscpv - polonáhodným kódem - jde po osobách a pokud zjistí v kmenovém PV osoby znak "." tak respektuje část osc, která je společná pro osobu, pak dá tečku a dvojmístné č.PV v lib. pořadí; když v tom kmenovém PV tečku nezjistí, tak generuje nezávislá čísla pro jednotlivá PV.

parametr -updcastky

mění částky dlouhodobých plateb, průměrů, zúčtovaných mezd a částky v různých pracovních tabulkách exportů (update na náhodné hodnoty).

parametr -delmzdy

smaže úplně záznamy zúčtovaných mezd (delete)

parametr -nodelete potlačující standardní mazání itf a převodních tabulek

speciální varianta pro testování některých interface

při jeho použití se nepromažou tabulky:

"cetrlfodatask",

"cemisp",

"ceiosoz2",

"cewcscvl2" (pokud existuje)

"ceuuts",

"ceu2osvecpouc",

"ceu2osvecmoc",

"ceu2osvec",

"ceu2orgoso",

"ceu2org",

"cetoso\_v\_titul",

"cetredop",

"cedmes\_status\_over",

"cesastaskprot",

"cedavprot",

"ceswflcfg1log",

"cetrlfodatask",

"cetrlfodavkysk",

"ceteldata\_sk",

"cemisp",

"cetisosdata",

"cetnpdata",

/cemzuct.dalsi\_xml/protokol

a náhodné hodnoty se nedají do zbytku "cemzuct".

parametr -noupdjmena

nastavení způsobí, že se nebude anonymizovat Příjmení, Jméno, Celé jméno   
(Osb02, zúčt. mzdy, tj. cetoso\_prijmeni.cetoso\_jmeno, tituly, cetoso.jmeno\_cele a cemzuct.prijmeni, jmeno)

Tedy vlastně anonymizace bez anonymizace.

parametr -log *jménoSouboru*

Parametr log je následován názvem log souboru. Soubor obsahuje podrobné informace o provedené anonymizaci

Parametr log je následovaný názvem log souboru. Obsahuje podrobné informace o provedené anonymizaci.

parametr -onlylogin *login*

Parametr umožňuje v db ponechat pouze jeden zadaný login, všechny ostatní jsou pak smazány. Je vhodné login vybrat správně, abyste neztratili přístup do EGJE.

Ve verzi e202405 došlo k úpravě anonymizační utility tak, aby bylo možné následně s daty provádět výpočty mezd a bylo možno generovat bankovní soubory.

Nově byly upraveny částky tak, aby si odpovídaly řádově (nestávalo se například, že částka 700 000 se změní na 123).

Dále došlo k tomu, že se nemění hodnota těchto polí (kvůli generování bankovních příkazů):

* Bankovní cesta k příjemci
* Platnost
* Předčíslí konc. příjemce
* Č. účtu koncového příjemce
* Sm. kód banky konc. příjemce
* IBAN individuálního příjemce
* BIC kód (SWIFT)ind. příjemce
* Variabilní symbol
* Konstantní symbol
* Specifický symbol konc. příjemce

### Uživatelská sestava Ela01vxc dříve validateXML - validateClobs

Uživatelská sestava Ela01vxc bývá obvykle používána po převodech dat.

Výdejový adresář ji obsahuje jako anon\validateXML.bat.

Kontroluje hlavně formální syntaktickou správnost XML v databázi.

U XML položek kontroluje také data vůči registrovanému datovému typu.

Zobrazí také data, která již byla v repository zrušena. Pozn. EGJE standardně neruší data z XML položek při zrušení deklarace této položky, protože to není nutné.

## Využití SuperKonfigurátoru k vytvoření reportu nad více DB pro možnosti porovnání a nalezení položek v různých DB

Superkonfigurátor nyní obsahuje možnost vyexportovat z označených DB například SLM, Role, JPČ, atd.

V horním seznamu, se vyberou pomoci Ctrl+klik myši DB ze kterých se má exportovat data a na záložkách „Export číselníků“ a „Export číselníků II.“, se vyberou položky, které je potřeba exportovat. Pak po stisku tlačítka „Export XLSX“ se vytvoří soubor ve formátu XLSX, který ale neslouží k následnému importu, ale pouze k porovnání dat ve vybraných DB. Může sloužit například k porovnání, zda se daná Role s číslem 501 vyskytuje ve vybraných DB, což dá uživateli informaci o tom, jak jsou například volná čísla pro Role v jiných DB.

1. **Správa uživatelů aplikace** 
   1. **Založení uživatele – stručné shrnutí**

Typický postup:

Osoba není (ještě není) evidována jako zaměstnanec:

Adm01p - založíme osobu a uživatelské PV (status 21),   
přiřadíme Profil (a jazyk, případně organizaci)  
a vyplníme Logname pro Přihlášení-autentizaci.

Osoba je již evidována jako zaměstnanec:

Osoba zaměstnanec/manažer:

v Adm10 jí přiřadíme Profil (jazyk, organizaci) a Logname pro Přihlášení-autentizaci (dtto první bod)

Osoba referent:

buď postupujeme shodně jako u zaměstnance/manažera, nebo pomocí Adm01p založíme uživatelské PV (status 21) již existující osobě a dále přiřadíme Profil (jazyk, organizaci) a Logname pro Přihlášení-autentizaci (dtto první bod)

Pozn. referentům a manažerům často přiřazujeme více profilů, logname však bývá zpravidla pouze jeden.

Pozn. typické vyplnění logname

Autentizace NTLM

***WinDoména\uživatel*** př. MOTOR\jigecz

Autentizace kerberos, LDAP

***uživatel@doména*** př. jigecz@motor.cz

* 1. **Práva k objektům a k řádkům, role a profily**
     1. **Pojmy a základní otázky**

Pojmy přístupových práv v EGJE, jejich výskyt a použití

**Adm*nn*** – formuláře administrátora - vyvolají se buď z menu Správa systému nebo z příkazové řádky EGJE

**Uživatel** – osoba s PV se statusem 21 Systémová evidence (zobrazeno a editovatelné na formuláři Adm11)  
(PV je právní vztah osoba - organizace)

**Uživatel přiřazený na profil** – spojení uživatele a profilu přístupových práv – (Adm01)  
Uživateli může být přiřazeno více profilů, resp. vícekrát jeden profil s různým jazykem nebo jako zastupování jiného uživatele.

**Autentizace uživatele** – obecně jde o ověření, že uživatel je tím, za koho se vydává; v EGJE je tato informace buď přebírána z přihlášení do operačního systému (Windows NT), nebo je provedena vůči Kerberos serveru (mechanismem vestavěným v java JRE);  
(Adm01 – Přihlášení autentizace, Adm01p dtto.)

**Profil přístupových práv** – spojení přístupových práv k objektům a přístupových práv k řádkům. Někdy používáme také termín abstraktní uživatel. Konkrétní osoba může mít přiřazeno více profilů přístupových práv, vystupuje v systému v různých uživatelských rolích (například zaměstnanec a vedoucí nebo mzdová účetní a vedoucí mzdové účtárny). (Adm02)   
Zatímco přístupová práva k řádkům jsou uživateli definována pomocí profilu, práva k objektům se přiřazují nepřímo pomocí rolí (Adm03)

**Role přístupových práv** – sada přiřazení přístupových práv k jednotlivým objektům systému. Rozlišujeme role, které jsou ve správě Elanor (1-499) a role, které jsou ve správě uživatele (500-999) (Adm03)

**Přístupová práva k objektům -** základní stavební jednotka přístupových práv je **objekt**. Typickými objekty jsou **Formulář, Proces, Sestava, Export, Položka menu**. Objekty formulář a proces mohou být dále děleny z pohledu přístupových práv na jemnější objekty -záložka, datový zdroj, položka. (Adm04)

**Hodnoty přiřazení práv k objektu** – sada povolených hodnot přístupových práv je závislá na typu objektu, ke kterému je přiřazujeme. Přiřazení provádíme vždy na roli.

Zatímco k formuláři máme obvykle možno přiřadit práva **-2-Odnětí zápisu i čtení / -1 -Odnětí zápisu / *0-Nic / 1-Čtení / 2-Čtení i Zápis*, je u sestav,** položek menu a procesů obvykle dvojice **-1 – Odnětí / *0-Nesmí spustit / 1-Smí spustit***.

Speciálními hodnotami jsou potom hodnoty záporné, které právo omezují i když je právo profilu přiřazeno například jinou rolí. Omezení pak může být úplné (-2) nebo částečná (snížení práv pouze na čtení tj. -1). (Adm03)

**Konfigurace použití objektů přístupových práv** – jelikož EGJE je typovým projektem, obsahuje řadu objektů, které konkrétní zákazník nebude využívat. Aby takové objekty nepřekážely v přiřazování práv k objektům konkrétním rolím, a aby nedošlo k nesouladu v přiřazení, je možné informaci o úplném nepoužití objektu v organizaci zadat ve formuláři Adm04 v záložce Konfigurace použití. (Adm04)

**Přístupová práva k řádkům** – jelikož organizace bývá plošně nebo hierarchicky rozčleněna, je zapotřebí toto rozčlenění zohlednit v definici a přiřazení přístupových práv. Jinými slovy uživatel má sice právo k nějakému objektu, ale nemá v něm přístup ke všem datům, ale pouze k jejich části, která je určena jeho kompetencemi v organizaci.

Pro toto rozčlenění je možné použít **Správní jednotku, Správní oddíl,** přiřazení do **Struktur** (typicky organizační středisko nebo struktura mzdové účetní), **Status PV, Status práva** resp. **Příznak chráněné osoby(PV).** V položkách určených pro výběr SJ/SO je možné použít buď výběr konkrétní SJ/SO, nebo do těchto polí zadat výčet SJ/SO (ve formátu 1, 2, 5-8, 10), které chceme do výběru zahrnout. (Adm02)

Pozn. U instalací s více organizacemi ve smyslu jejich číselníku Adm21 se dalším prvkem přístupových práv k řádkům stává organizace. Ta se uvádí u přiřazení profilu uživateli (Adm01, Adm01p, Adm10, Adm12)

Toto řešení umožňuje používat jeden profil pro více organizací.

**Nastavení přístupových práv k řádkům**

Uvedené možnosti omezení přístupových práv k řádkům se velmi často používají v kombinaci. Typické příklady:

Uživatel má přístupné všechny osoby v rámci správního oddílu - vyplněno:

SJ pro omezení práv

SO pro omezení práv

PV způsob vyhodnocení výčtu struktur - "VSE-všechno"

Uživatel má přístupné všechny osoby v rámci správního oddílu, pouze "živí" tj. počítaní zaměstnanci- vyplněno:

SJ pro omezení práv

SO pro omezení práv

PV způsob vyhodnocení výčtu struktur - "VSE-všechno"

PV výčet povolených statusů - "1,2,3"

Na formuláři je nový řádek s názvem „Rozšíření omezení a editace dle skupin ŘP:“, který umožnuje pomocí rolldown menu rozšířit možnosti editace a omezení zobrazování skupin dle zadaných řádkových práv pro struktury.

**Základní otázky**

**Mohou dva uživatelé používat stejný profil?**

Mohou. Musí však mít shodná objektová práva. U řádkových práv je také buď musí mít shodná nebo musí používat "shodné makro". Typicky mohou být odvozena od vlastního střediska uživatele, které pak má každý uživatel jiné a tudíž mají oba uživatelé nakonec jiná přístupová práva k řádkům.

**Jak je vhodné konstruovat název profilu?**

Název by měl zohlednit roli uživatele (např. mzdová účetní, vedoucí) a základní definici práv k řádkům (např. MÚ1 SJ 1 nebo Vlastní střed.). Stejně tak by ve zkratce téhož měl být konstruován kód profilu.

**Jaký je vztah přístupových práv k řádkům k historii údajů?**

V systému rozlišujeme dvě základní úložiště údajů přiřazení do rozčlenění organizace – kmenové přiřazení (typicky Opv01) a přiřazení uložené v zúčtované mzdě (např. detail ve Vyp01). Záleží tedy na povaze objektu, ve kterém práva hrají roli. Pokud objekt čerpá z kmenových dat, jsou práva vyhodnocována k referenčnímu datu a k přiřazením platným k tomuto datu v té podobě jak jsou nyní v databázi.

U objektů čerpajících ze zúčtovaných mezd je situace složitější. Zatímco formuláře používají kmenové přiřazení u sestav je situace složitější.

Vztah sestavy ze zúčtovaných mezd k přístupovým právům k řádkům může být následující:

* + - Sestava vyhodnocuje práva co nejdetailněji, tedy vychází z toho, jak byly jednotlivé přiřazení PV do struktur, SJ a SO v okamžiku výpočtu mzdy v daném období (Rek02p, Rek05p, ...)
    - Sestava vyhodnocuje práva k řádkům sice detailně, ale z kmenové tj. současné definice přiřazení (Sra02, Sra03, Vyp09, ...)
    - Sestava vyhodnocuje přístupová práva, ale pouze na úroveň přiřazení na SJ, SO s respektováním chráněných osob. Prioritou je u takto postavené sestavy její úplnost. Je pak věcí správce jestli uživateli, který např. nemá práva na celou SJ sestavu přidělí nebo nikoliv.  
      (Evs10, Evs11, Rek01, Rek02, Rek03, Rek04, Rek05, Rek06, ...)
    - Sestava práva k řádkům nevyhodnocuje, jinými slovy sestava má smysl pouze v úplnosti nebo vůbec.

Nakonec je třeba ještě zmínit, že strana definice práv historicky sledována není. Definice řádkových práv v profilu je tedy použita taková, jakou ji zobrazuje formulář (Adm02, Adm01). Minulá nastavení se neukládají, nicméně informace o provedení změn se auditují do Adm52.

**Přístupová práva a tiskové sestavy**

Z pohledu přístupových práv k objektům je sestava jeden nedělitelný objekt, uživatel ji buď může, nebo nemůže spustit. Pokud může, vidí všechny položky sestavy. To je rozdíl oproti formulářům, kde u řady z nich lze nastavit práva i na záložku, datové formuláře a položky a to buď na úrovni role (Adm03) nebo konfigurace (Adm04).

Přístupová práva k řádkům se však v sestavách uplatňují. Většinou jde o práva na osoby a PV.

V některých případech však proti sobě jdou požadavky na úplnost sestavy oproti požadavku na detailní promítnutí přístupových práv k řádkům.

Některé sestavy jsou tedy realizovány tak, že se v nich práva k řádkům buď záměrně nepromítají vůbec, nebo se promítají třeba jen práva na SO, SJ ale nikoliv jemnější (podle struktury). Typicky sem patří rekapitulační sestavy Rekxx. V [Rek\_uzdoc](Rek_uzdoc.htm) je u každé z nich uvedeno jaký režim práv k řádkům používá.

Typické sestavy s důrazem na úplnost jsou výpisy Ban*xx* členěné podle dávek.

**Vyhodnocení přístupových práv k řádkům a referenční datum**

Přístupová práva k řádkům jsou vyhodnocována k referenčnímu datu.

Do budoucnosti je však toto datum omezeno. Dlouho jsme drželi pravidlo, že shora bylo omezeno dnešním datem. Od verze e201401 jsme přešli na implicitní hodnotu

dnešní datum + 40 dní.

Pokud si v organizaci chcete nastavit jiný limit, je k tomu určen parametr

Adm21 / Konfigurační parametry / Limit dní vyhodnocování práv do budoucnosti.

Záporné hodnoty nejsou akceptovány, maximum je 9999.

Toto platí pro přístup ke kmenovým datům, k navigačním seznamům (typicky navigační seznam Osob/PV) nabídkovým comboboxům resp. k datům v sestavách z jiné oblasti než jsou zúčtované mzdy (zde se práva vyhodnocují ze zaprotokolovaných údajů).

V praxi to obvykle umožňuje si připravovat údaje pro příští období s použitím těch zařazení, která v příštím období budou platná. Vše vychází z referenčního data, které si uživatel zvolí při přihlášení, resp. změní během práce v EGJE.

* + 1. **Nastavení přístupových práv v aplikaci**

**Přiřazení / Vytvoření uživatele**

Pokud Osoba uživatele/referenta ještě v db není a nemá v ní jako zaměstnanec, zakládáme ji pomocí průvodce **Adm01p**. Takto ji vytvoříme jako osobu s PV se statusem 21.

Uživatelé referenti, zaměstnanci, manažeři, kteří jsou v db již evidováni (obvykle jako zaměstnanci), mít speciální uživatelský PV nemusí. Specifikaci atributů uživatele pak zadáme pomocí formuláře **Adm01** resp**. Adm10**.

U uživatele zadáme profil a jazyk, případně omezení na Organizaci a pomocí zadání "Profil - autentizace" propojíme autentizaci s Osobou v db. Autentizační přihlašovací jméno (jména) zadáváme v tomto (těchto) tvarech:

Autentizace Windows NT

***WinDoména\uživatel*** př. MOTOR\jigecz

Autentizace kerberos, LDAP

***uživatel@doména*** př. jigecz@motor.cz

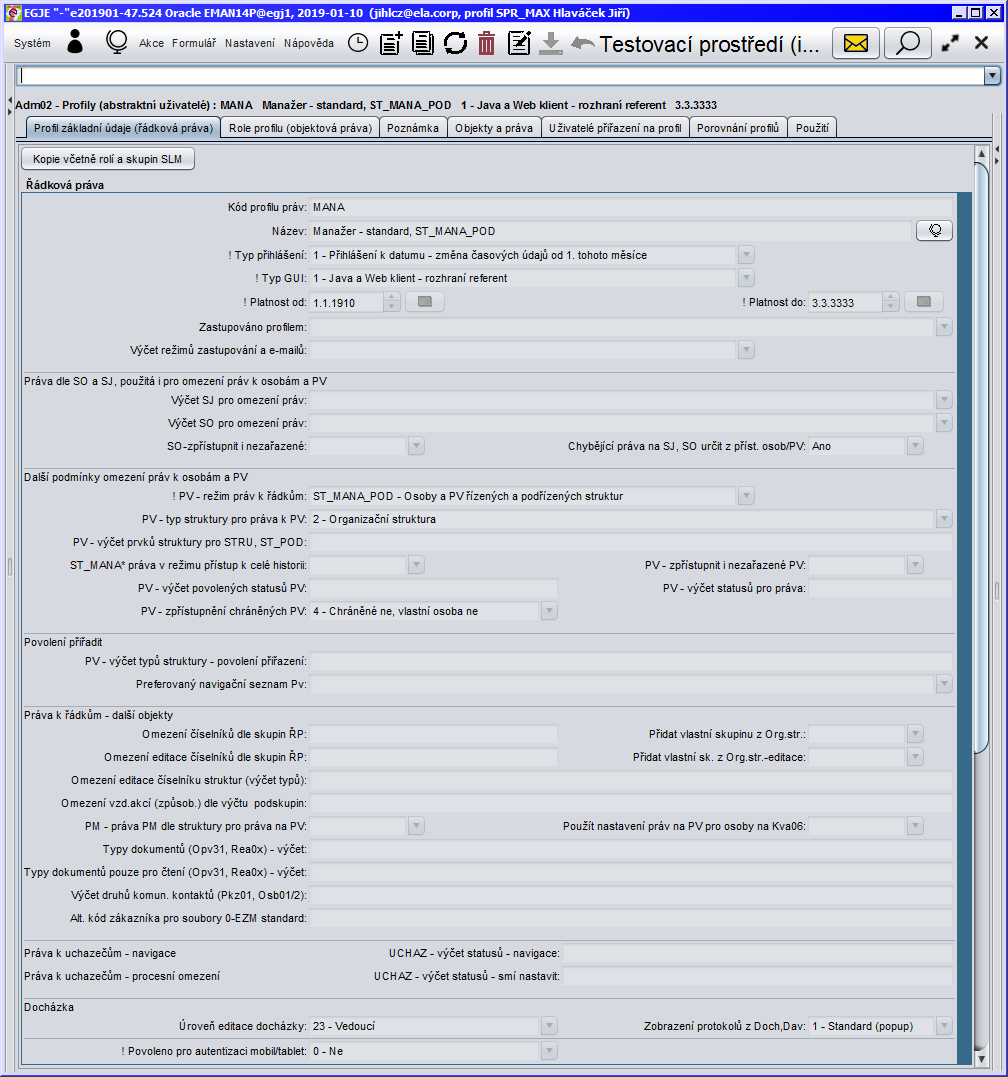
Autentizaci uživatele buď přebírá z operačního systému (SSO) nebo ji interaktivně zadá (jméno heslo). Režim jsou popsány v předcházející kapitole [Nastavení - configurator\_egje](EGJE_provdoc.docx#_Ověření).

U každého přiřazení profilu vyplňujeme jazyk uživatelského rozhraní.

Upozornění: ve státní správě všem vyplňujeme jazyk "cs\_ST" místo standardního "cs".

**Vytvoření a editace profilu**

Profil vytváříme a editujeme na formuláři Adm02.



#### U profilu na první záložce definujeme typ přihlášení a přístupová práva k řádkům:

* Typ přihlášení - rozlišení mezi personalistickým přihlášením ke dni a mzdářským přihlášením k období

Zároveň položka definuje nabízení data při editaci časově sledovaných položek.

K dispozici jsou typy:

1 Přihlášení k datumu - změna časových údajů od 1.tohoto měsíce

2 Přihlášení k období - změna časových údajů od 1.zvoleného období

3 Přihlášení k datumu - změna časových údajů od ref.data

4 Přihlášení k datumu - změna časových údajů od 1.násl.měsíce

5 Přihlášení k období - změna časových údajů od 1.násl. období

* Typ GUI - pro jaké UI je profil určen. Hodnoty jsou:

1 - Java a Web klient - rozhraní referent

2 - Starý Web klient

3 - Web klient - rozhraní referent

4 - Java klient - rozhraní referent

11 - HR portál - rozhraní zaměstnanec samostatně prodávaný produkt

12 - HR portál - rozhraní manažer samostatně prodávaný produkt

21 - Pouze WS - Bez přístupu do UI EGJE, přístup pouze webovou službou

Práva dle SO a SJ, použitá i pro omezení práv k osobám a PV

* SJ resp. SO pro omezení práv - organizace je (resp. může být) rozdělena na správní jednotky (SJ) a správní oddíly (SO). SJ je rozdělením navenek - je protějškem různých institucí typu Zdravotní pojišťovna, Finanční úřad atd.  
  Skládá se z minimálně jednoho (ale může jich být i více) SO.   
  SO je rozdělením pro zpracování mezd. Pro SO definujeme výplatní termín, na SO provádíme hromadné výpočty a uzávěrky.  
  **Upozornění: Pro zrychlení zpracování práv k řádkům doporučujeme SJ, SO na profilu, tam kde je to možné, uvádět**, zpracování práv je pak rychlejší a promítne se i do nabídkových ComboBoxů SJ a SO, ve kterých je nabídka SJ či SO a nikoliv osoby a PV.
* U zaměstnaneckého, manažerského ale i u některých referenčních profilů, které jdou přes celou organizaci by vyplňování SJ, SO vedlo k tomu, že by se profily musely vytvářet pro každý SO zvlášť.

Aby to nutné nebylo, je pro tyto případy vhodné použít nastavení atributu "**Chybějící práva na SJ, SO určit z příst. osob/PV:"** = Ano.

Pracuje to tak, že se projdou všechny PV, na které má uživatel práva a zjistí se jejich všechny SO, SJ a Legislativy. Tyto se pak vezmou a tvoří omezení uživatele v těchto třech parametrech a také pak omezují nabídkové ComboBoxy SJ a SO.

* SO zpřístupnit i nezařazené - definice má význam pro ty typy PV, které se na SO nepřiřazují (uživatel, lektor, uchazeč...). Nastavením na Ano se takové osoby (PV) stanou viditelnými  
  (Přiřazení PV k SO se provádí na Opv01 záložka Správní oddíl).  
  Pozn.: Pro sestavy, které čerpají z mezd a řádková práva se u nich vyhodnocují z mezd položka nemá význam, neboť ve mzdách jsou pouze osoby/PV zařazené na SO.

Další podmínky omezení práv k osobám a PV

* PV - režim práv k řádkům - možnost zadat další aditivní podmínku k omezení pomocí SJ, SO.   
  Může nabývat těchto hodnot:

|  |  |
| --- | --- |
| VSE | Všechno (v rámci dalších podmínek na SO, SJ, statusy, chráněné PV) |
| STRU | Osoby a PV zařazené na strukturu |
| STRU\_PRIMO\_HIST | Osoby a PV zařazené na strukturu,  přístup v celé historii, ale max do data, kdy má přístup k osobě |
| ST\_POD | Osoby a PV zařazené na struk.a podř. struk. |
| VL\_OSO | Vlastní osoba |
| ST\_MANA | Osoby a PV ze struktur, u kterých je uživatel označen jako manažer |
| ST\_MANA\_POD | Osoby a PV ze struktur, u kterých je uživatel označen jako manažer a podřízená střediska |
| ST\_MANA\_PRIMO | Od ST\_MANA se liší tím, že kromě zaměstnanců, kterým je uživatel manažerem (dle uvedené struktury) má přístup i k manažerům přímo podřízených jednotek.  Obvykle jde o podřízené vedoucí v organizační struktuře. |
| ST\_MANA\_POD\_OBD | Od ST\_MANA\_POD se liší tím, že vyhodnocuje, zdali zaměstnanec pod uživatele patřil alespoň jeden den v období (měsíci). |
| ST\_MANA\_OBD | dtto ale pro režim ST\_MANA |
| ST\_POD\_OBD | dtto ale pro režim ST\_POD |
| STRU\_OBD | dtto ale pro režim STRU |
| ST\_KUMUL, ST\_KUMUL\_POD | Instalace na VŠE umožňuje nastavit další 2 režimy.  V následující Adm02 položce "PV typ struktury" správce vyplní 8. PV výčet prvků zůstává prázdný.  Realizuje se tím režim zaměstnance pod dvěma manažery.  Předpokládá se zadání více prvků (středisek) struktury 8 na jedno PM v Pmi01 tzn. PM pracuje pro 2 střediska. Přístup k zaměstnanci na tomto PM tak získávají 2 manažeři 2 prvků (středisek) struktury 8. |

**Pozor: všechny \_OBD režimy platí pouze pro přímé přiřazení struktury použité pro definici práva! Přiřazení se provádí na PV v Opv01/Struktury.**

**Pozn.: Pro účely práv typu \*MANA\* manažera zaniklého střediska už nepovažujeme za manažera, jemuž náleží zařazení a podřízení. Jinými slovy k datumu zjišťování bereme u těchto režimů v potaz vznik a zánik prvku (Str01).**

* PV - typ struktury pro práva k PV  
  typ struktury (Str01)
* PV - výčet prvků struktury pro práva k PV:  
  Pro typ STRU, ST\_POD a ST\_POD\_OBD se zde uvádí kód(y) struktur pro omezení právy.  
  Používá se kód resp. kódy oddělené čárkou. Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále [[odstavec](#Negativni_prava)](bookmark://Negativni_prava).  
  Pokud ponecháme hodnotu nevyplněno, bere se struktura (typicky středisko), na které je zařazen přihlašující se uživatel resp. které je manažerem (ST\_MANA, ST\_MANA\_POD, ST\_MANA\_PRIMO, ST\_MANA\_OBD, ST\_MANA\_POD\_OBD).  
    
  Pro VSE,VL\_OSO, ST\_MANA, ST\_MANA\_POD, ST\_MANA\_PRIMO, ST\_MANA\_OBD, ST\_MANA\_POD\_OBD položka nemá význam.
* ST\_MANA\* práva v režimu přístup k celé historii:   
  Příznak se používá u referentů typu mzdová účetní, jejichž práce má roční charakter. Nastavení na Ano pak referentovi navíc zpřístupňuje zaměstnance, které měl ve aktuálním roce alespoň jeden den přístupné.   
  Tento režim je dostupný pouze pro ST\_MANA\*. V ostatních režimech toto není podporováno
* PV - zpřístupnit i nezařazené PV - definice má význam pro ty typy PV, které se na strukturu nepřiřazují (uživatel, lektor, uchazeč...). Nastavením na Ano se takové osoby (PV) stanou viditelnými  
  (Přiřazení PV na strukturu se provádí na Opv01 záložka Zařazení do struktur).
* PV - výčet povolených statusů PV - aditivní definice práv na základě výčtu položky Opv01/Popis/Status vztahu osoba org.  
  Častou hodnotou bývá např. pro mzdové účetní omezení 1,2 (tedy ta počítaná) resp. 1,2,3
* PV - výčet statusů pro práva- aditivní definice práv na základě výčtu položky Opv01/Popis/Status - práva. Na rozdíl od minulé položky, kde číselník je ve správě Elanoru, u této položky je číselník ve správě uživatele (Jpc01 / status\_prava). Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále [[[[odstavec](#Negativni_prava)](bookmark://Negativni_prava)](https://odstavec)](#Negativni_prava).
* PV - zpřístupnění chráněných PV - aditivní definice práv na základě příznaku, který správce může osobě - PV nastavit v Adm11 / PV / Chráněná osoba.

Všechny tyto podmínky jsou vyhodnocovány jako "a zároveň". Nastavení více podmínek tedy obvykle vede k větší restrikci.

**Vlastní vyhodnocení práv k řádkům:**

Ve většině míst aplikace se práva k řádkům vyhodnocují z průběžných kmenových dat.   
Tzn. z dat formulářů Opv01 (Trvání, Popis, Struktury), Str01 (Hierarchie od-do, Jiné struktury, Manažer – osoba v EGJE).

V datech, kde převažuje pohled na zúčtované mzdy, však EGJE vychází z toho jako to bylo v tom měsíci zúčtováno.

Tzn. Vyp02/Kopie struktur (dle Str01/Použití struktury=1-MZDY), Vyp01 (výpočet), Str05.

Jde o tyto sestavy: Aps03, Coe01, Coe05, Con24, Dan16, Evs15, Kon14, Poj02, Poj05, Poj07, Poj10, Poj32, Poj34, Poj41, Pos02, Pos32, Rek02p, Rek05p, Rek11, Rek12, Rek22, Rek23, Rek24, Rek25, Rek26, Sra03, Sra04, Sra06, Sra08, Vyk27, Vyk32, Vyk33, Vyp14, Vyp17, Vyp19, Vyp20, Vyp21, Vyp24.

Plus formuláře Vyp07, Vst01h, Slm05.

Povolení přiřadit

* PV - výčet typů struktury - povolení přiřazení:  
  je-li prázdné, tak bez omezení, je-li vyplněno výčtem typů struktury (navigace Str01) tak omezují, které struktury smí uživatel zaměstnanci přiřazovat (Opv01, Opv04, Opv05)
* Preferovaný navigační seznam Pv  
  Pro profil je možné vybrat implicitní navigační seznam pro formuláře s tímto navigačním seznamem (např. Osb02, Opv01, Vyp01, Kva01, Dav01...)

Práva k řádkům - další objekty

(systém skupin ŘP je komplexněji popsán v [[Adm\_uzdoc](Adm_uzdoc.htm)](Adm_uzdoc.htm) - kapitola Adm06)

* Omezení číselníků dle skupin ŘP - uživatel uvidí (obvykle v nabídkových ComboBoxech) jen ty hodnoty z příslušného číselníku, které jsou označeny touto skupinou (výčet oddělovaný čárkou, nebo intervaly oddělené čárkou. Např. 1,7-9,23-26,29, … atd). Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále odstavec.
* Přidat vlastní skupinu z Org.str. - přidá ke skupinám v předchozím řádku ještě tu skupinu, která je uvedena u organizačního střediska, na které je uživatel zařazen.
* Omezení editace číselníků dle skupin ŘP - pro uživatele, kteří editují číselníky - musí zde mít výčet všech skupin, jimiž označené řádky v číselníku mají vidět a editovat (jinak vidí jen řádky bez označení skupinou). Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále odstavec.
* Přidat vlastní sk. z Org.str. - editace - dtto úvodní dvojice, ale pro účel editace číselníků
* Omezení editace číselníku struktur (výčet typů) - výčet typů struktury (navigace Str01), které uživatel smí editovat. Např. 2,3 způsobí, že uživatel v Str01 uvidí a může editovat pouze Organizační strukturu (2) a Pracovní místa (3).  
  To může být zkombinováno s omezením editace jen některých řádků (pomocí předchozích dvou parametrů)
* PM - práva k PM dle organizační struktury  
  nastavení na Ano způsobí, že v navigačním seznamu pracovních míst (Pm), budou pouze ta PM, která jsou na organizačních střediscích, ke kterým má uživatel přístup (předpokládá se definování práv podle organizační struktury). Navigační seznam je použit např. u Pmi01, Pmi08, Pmi09.  
  Není-li položka vyplněna, omezení není uplatňováno.
* Typy dokumentů (Opv31, Rea0x) - výčet  
  Parametr poskytuje možnost zadat výčet typů dokumentu, které smí uživatel u zaměstnance, resp. uchazeče vidět a editovat. Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále odstavec.
* Typy dokumentů pouze pro čtení (Opv31, Rea0x) - výčet  
  Parametr poskytuje možnost zadat výčet typů dokumentu, které smí uživatel u zaměstnance, resp. uchazeče vidět, ale nikoliv zadávat a editovat.   
  Pro zadání negativní podmínky “vše kromě” se před výčet napíše znak ”!" - viz dále odstavec.

Výčet druhů komun. kontaktů (Pkz01, Osb01/2) - analogicky – zadává se výčet čísel druhů, včetně záporného výčtu iniciovaného znakem ”!".

Práva k uchazečům - navigace

* UCHAZ - výčet statusů - navigace  
  možnost omezit zobrazovaný seznam uchazečů pomocí výčtu statusů (čárkami oddělované číselné hodnoty statusu uchazeče).  
  Týká se i statusů.

Práva k uchazečům - procesní omezení

* UCHAZ - výčet statusů - smí nastavit  
  možnost zadat výčet statusů, které smí uživatel u uchazeče nastavit / přiřadit

Docházka – definice verifikační úrovně uživatele pro oblast docházky

* **Úroveň editace docházky -** verifikační a editační úroveň profilu pro ověření řádků resp. pro oprávnění přístupu k řádkům v evidenci docházky (DD, DZ, MV, MZ, doklady).  
  K dispozici jsou úrovně:  
  3 Zaměstnanec; 13 Vedoucí I.; 23 Vedoucí; 33 Správce resp. mzdová účetní

Zobrazení protokolů z DOCH, DAV

1 - Standard (popup) (tj. jako dosud)

2 - Potlačit zobrazování protokolu v dialogu tzn. nezobrazovat vůbec

3 - V EGJEWEB protokol do záložky EGJE (ve std. klientovi popup - 1)

Typické použití je celoobrazovkový režim terminálů s EGJEWEB.

Chybějící práva na SJ, SO určit z podřízených osob (ST\*, VL\_OSO)

Manažerský/zaměstnanecký profil obvykle bývá průřezový pro celou organizaci a nevytvářejí se jeho varianty pro různé SJ/SO. Zapnutím této volby je možné výčty SJ, SO online dopočítávat při přihlášení dle SO, SJ zařazených manažerovi přístupných PV.

Tato práva na SJ/SO se pak typicky používají v různých nabídkových comboboxech a to v sestavách i formulářích.

Implicitně příznak není zapnutý a tato aditivní akce se po přihlášení neprovádí.

**Doporučené a obvyklé profily**

V tabulce zmiňujeme jen ty atributy, které se odchylují hodnot předvyplněných při Adm02/Nový profil.

|  |  |
| --- | --- |
| **Typ** | **Popis** |
| Zaměstnanec | SJ, SO nevyplněno,  Chybějící práva na SJ, SO určit z podřízených osob = Ano  PV režim práva = **VL\_OSO** |
| Manažer - osoby ze struktur, jichž je manažerem | SJ, SO nevyplněno,  Chybějící práva na SJ, SO určit z podřízených osob = Ano  PV režim práva = **ST\_MANA**  PV Typ struktury = 2 (obvykle org. struktura)  Pozn. U každého prvku struktury 2 musí být vyplněn manažer (Str01, Str02 / Manažer - Osoba v EGJE  Může i nemusí mít přístupnou vlastní osobu (PV - zpřístupnění chráněných PV) |
| Manažer - dtto + manažeři podřízených středisek | dtto  PV režim práva = **ST\_MANA\_PRIMO** |
| Manažer - všichni podřízení | dtto PV režim práva = **ST\_MANA\_POD** |
| Manažer, pověřená osoba - osoby ze struktury, na kterou je sám zařazen | SJ, SO nevyplněno,  Chybějící práva na SJ, SO určit z podřízených osob = Ano  PV režim práva = **STRU** (resp. ST\_POD pro všechny z podstředisek)  PV Typ struktury = 2 (obvykle org. struktura ale může jít i o jinou)  PV výčet prvků struktury pro STRU, ST\_POD = nevyplněno |
| Referent mzdová účetní - celý SO | SJ, SO vyplněn (mohou být výčty) PV režim práva = **VSE** |
| Referent mzdová účetní - přiřazené PV | SJ, SO pokud konstantní tak vyplněn (mohou být výčty) PV režim práva = **ST\_MANA**  PV Typ struktury = 14 - Mzdová účetní  Pozn. U každé mzdové účetní tj. prvku struktury 14 musí být vyplněna vazba na osobu/uživatele tj.Str01, Str02 / Manažer - Osoba v EGJE. Tím je dosaženo, že profil pro více mzdových účetních může být jeden a přesto má každá MÚ svoje zaměstnance.  Zaměstnanci mohou být zařazeni pod mzdovou účetní (struktura 14):  na PV v Opv01/Struktury  na PM v Pmi01, Str01, Str02  na Org. středisku v Str01, Str02  U referenta tohoto typu je vhodné nastavit příznak „ST\_MANA\* práva v režimu přístup k celé historii:“ na Ano a zpřístupnit tak referentovi i data svěřených zaměstnanců z doby před vznikem PV referenta. |
| Jiný referent - přiřazené PV | dtto mzdová účetní, pouze číslo struktury bývá jiné  typicky 15 - 18 resp. 13 |

Výhodou použití profilů ST\_MANA pro referenty je to, že se pro všechny (nebo alespoň skupinu) referentů daného typu může použít společný profil.

Na tento profil se pak dají přehledně vázat další konfigurace:

Adm06 - obecné skupiny, skupiny SLM, skupiny kalendářů

Epr02 - eProposal

Adm02 - role zařazené na profil

Mail - možnost odeslat zprávu všem na profile

Při vytvoření speciálního profilu pro každého referenta zvlášť je potřeba uvedené konfigurace udržovat pro každý profil samostatně a to může být u většího počtu referentů pracné a nepřehledné.

Typicky mívá takový referent profil s tímto nastavením:

SJ, SO vyplněn (mohou být výčty)  
PV režim práva = **STRU**

PV Typ struktury = některá ze struktur 13-18

PV výčet prvků struktury pro STRU, ST\_POD

= seznam uživatelských kódů prvků struktury oddělených čárkou

**Jak nakonfigurovat struktury, aby byly použitelné pro přístupová práva podle struktur (tj. režimy ST\*).**

Na Str01 je potřeba nastavit:

Vazby mezi strukturami:

Zadává-li se struktura na PM, pak   
"Podřízená struktura (vyplňuji kde)" bude 3 - Pracovní místo   
a "Nadřízená (vyplňuji co)" bude např. 14 - Mzdová účetní

Pokud údaje zadávám už na Organizačním středisku, pak   
"Podřízená" bude 2 - Organizační struktura.

Pokud zadáváme na PV (Opv01 / Struktury), pak v záložce Použití struktury zadáváme pro tu konkrétní strukturu (např. 14 - Mzdová účetní) hodnotu 2-KMEN-PV.

Pozn.: pokud v Opv01 / Struktury smí tuto strukturu přiřazovat jen někdo, je možné ostatním profilům se zápisovým právem na tuto záložku nastavit výčet Adm02 / PV - výčet typů struktury - povolení přiřazení: takový, aby tuto strukturu neobsahoval.

Na strukturách platí zásady nepřímého přiřazení. Na organizačním středisku tedy mohu vyplnit nečastější hodnotu (třeba tu Mzdovou účetní do Str01 / Stru / Manažer osoba v EGJE, odchylky pak vyplnit na PM a nebo až na PV.

Tak je možné výhodně minimalizovat počet míst, kde je údaj vyplňován.

Pro práva typu ST\_MANA\*, použitého pro referenty, je možné řešit situaci, kdy referentů je pro tu samou skupinu osob/PV více a jsou rovnocenní. V tom případě se zaškrtne checkbox (např. u té struktury 14) v Str01 / Jméno struktury a jejích hladin / Smí být paralelně více manažerů/osob.

Následně je pak možné v Str01 / Stru / / Manažer osoba v EGJE), zadat více paralelních referentů.

Tento režim by se ale neměl používat u struktur, použitých pro schvalování (workflow dle Adm14), proto jej nenabízíme pro strukturu 2, která je takto použita nejčastěji.

**Negativní vymezení přístupu k Osobám a PV**

Od e201809 je možné kromě standardního zadání "všichni, kteří mají cosi" zadat přístupová práva k řádkům (tj. osobám a PV) negativně, tedy "všichni, kromě těch, kteří mají cosi".

Dává to tak snadnou alternativu k "PV - zpřístupnění chráněných PV", které používá atribut Adm11/PV/"Chráněná osoba/PV".

Všichni kromě umožňujeme zadat pro:

* PV - výčet statusů pro práva
* PV - výčet prvků struktury pro STRU, ST\_POD (právě a pouze pro tyto 2 režimy)
* Omezení číselníků dle skupin ŘP
* Omezení editace číselníků dle skupin ŘP
* Typy dokumentů (Opv31, Rea0x) - výčet. Čtení i zápis
* Výčet druhů komun. kontaktů (Pkz01, Osb01/2)

Negativní výčet se zadá tak, **že se do prvního znaku položky pro hodnotu zadá znak"!".**

Tedy např. pokud do "PV - výčet statusů pro práva" zadáme např. hodnotu **"!5",** pak budou **přístupné ty PV, které nemají** v položce Opv01 / Popis / Status práva hodnotu **"5"**.

Znak "!" je funkční právě a pouze na místě prvního znaku a říká, že vše za tím bude vyhodnoceno negativně. Není tedy možné v rámci jedné položky kombinovat pozitivní a negativní zpracování.

**Alternativní vyhodnocování práv k osobám a PV (řádková práva offline)**

Na větších databázích je často u manažerských a referentských přístupů dlouhé úvodní otevírání oken, které je spojené s načítáním navigačních seznamů a seznamů v combo boxech.

Od e202109 umožňujeme řešení, které pracuje částečně offline, a které toto načítání a tím první otevření oken typu Wflow, Epr01, Kva01,... výrazně urychlí.

Zprovoznění je volitelné a má více kroků, které spolu souvisejí:

* na profilu se nastavuje, že profil je v oblasti řádkových práv vyhodnocován pomocí offline kopií dat: ***Adm02 / PV - práva k řádkům přes Elis51:* Ano**
* offline práva jsou generována procesní sestavou **Elis51**. Její spouštění zaevidujte na **Adm53** a spouštějte ji jedenkrát denně, typicky ráno nebo v noci.  
  Sestava má parametry:  
   ! Společný číselník struktur - hierarchický

! Zařazení PV do struktur

! Manažery struktur

! Kompetence na strukturách

Pro účely offline práv je zapotřebí potřeba nastavit první dva parametry. Přímo u Elis51 se to dělá checkboxy, v Adm53 se u parametrů   
 *r\_FillDataCstr, r\_FillDataTpvStr* nastaví/ponechá „1“, další 2 je možné pro účely práv dát na „0“.

Je k zvážení, u kterých profilů offline vyhodnocení nastavit – primárně je to určeno pro profily manažerů, resp. referentů s právy přes struktury (ST\*). Je vhodné vše odzkoušet. Daní je, že práva jsou vyhodnocována k času spuštění, resp. dokončení sestavy Elis51. Její častější spouštění než 1x či dvakrát denně by mohlo působit výkonové potíže, nicméně principiálně možné je.

Na **Adm10** jezáložka **Struktury offline**, která dává nahlédnout do prvních dvou offline úložišť, na záložce je také online pohled do záznamů přiřazení manažerů struktury. Zde jsou používány online hodnoty, tj. ty, které jsou také z jiného pohledu na Str01, Str02 / „Manažer/Osoba v EGJE“.

**Adm01 / Přístupná PV** pak zobrazuje výsledek, tj. jaké osoby / PV bude mít uživatel na profilu přístupné.

**Vytvoření a editace role**

Roli vytvářením a editujeme na formuláři **Adm03**.

Role s čísly 1- 499 jsou ve správě Elanor a jsou pro uživatele needitovatelné.

Uživatelské role mají vyhrazený interval 500-999.

Často se používá, že uživatel má v profilu nějakou (nějaké) standardní roli elanor (1-499) a správce mu navíc přiřadí nějakou(é) roli nad 500, ve které práva přidává resp. ubírá práva ke standardním rolím. Ubírání práv se děje nastavením záporné hodnoty práva v uživatelské roli. Tedy např. přiřazení práva -2 Odnětí zápisu i čtení způsobí, že přiřazení práva zápisu a čtení definované ve standardní roli pro uživatele přestane být platné.

Práva přiřazujeme na záložce Práva k objektům. A zde na záložce Objekt nastavujeme Souhrnnou hodnotu přístupového práva. Pro formuláře dvojstupňově ( 0 nic / 1 čtení / 2 zápis i čtení), pro sestavy a procesy pak jednostupňově (0 nesmí spustit / 1 smí spustit). S tím obvykle vystačíme. Upozorňujeme, že souhrnná hodnota by měla obsahovat maximum z práv přiřazených případně na Podřízené objekty.

V případě nutnosti je možné u některých formulářů v záložce Podřízené objekty - editace nastavit práva i detailnějším částem formuláře (záložka, datový formulář, položka). Práva se zde nastavují jako kaskáda. Tedy od hrubého k jemnějšímu. Vyhodnocení pak pokračuje v této hierarchii, dokud je alespoň nějaké právo ( > 0) až k úrovni položka. Pro zjištění kódových označení si správce může příslušný formulář, k němuž nastavuje práva, spustit z příkazové řádky s parametrem „-edit“ (př. Opv01 -edit ). Následně ve formuláři vidí pojmenování jednotlivých komponent.

Tento aparát se používá i pro selektivní přiřazení hromadné změny.

Standardním režimem je, že uživatel má přístupné všechny části formuláře s výjimkou těch, které mu správce zakáže buď pomocí práv (Adm03), nebo pomocí konfigurace (Adm04)

Systém však od e201303 umožňuje také režimy 1 a 2. Jejich volba se provede v Adm03 položkou "Práva uvnitř formuláře - režim" s hodnotami

0 - Standard - dle typu práv

1 - Implicitně žádná práva na záložky a datové formuláře

2 - Implicitně žádná práva na nic včetně položek

Kde 0 je implicitní hodnota a indikuje standardní režim.

Režim 1 znamená, že správce vyjmenuje přístupné záložky a datové formuláře, zatímco položky datového formuláře budou přístupné všechny resp. ty, které nezakáže.

V režimu 2 je i položky třeba vyjmenovávat. Upozorňujeme, že pokud má mít uživatel přístup i pro zápis, je třeba mu přidělit všechny povinné položky (indikovány vykřičníkem před nadpisem) a položky, které jsou pro interní logiku a případné kontroly nezbytné.

Upozorňujeme, že některé části formulářů mohou mít povinné ovládací prvky, bez kterých nebude formulář funkční, popř. nebude zobrazovat data.

Nastavení je tedy citlivou věcí. Správci může pomoci si formulář zobrazit ve standardním klientovi z příkazové řádky s parametrem -edit kdy uvidí interní názvy částí formuláře a snadněji se poté v záložce Podřízené objekty - editace zorientuje.

Pro usnadnění jsme v nových režimech udělali automatické zpřístupnění panelů, které jsou také ve vnitřní struktuře formuláře uloženy.

Nastavený režim je tedy vždy třeba vyzkoušet. Nemůžeme garantovat, že všechny nastavené režimy práv budou funkční dle představ.

Uživatel může mít práva k formuláři zprostředkované více rolemi včetně podřízených objektů:

Od e201601 jsme upravili logiku zpracování této situace.

Před e201601 měla explicitně zadaná práva na Podřízený objekt přednost před právy zděděnými z nadřízeného prvku.

Od e201601 jsou oboje práva brána rovnocenně a i zděděná práva, pokud jsou vyšší než ta explicitně zadaná, se mohou uplatnit.

V praxi šlo obvykle o vyhodnocení práv na položky, kdy v jedné roli byla například zadána práva ke čtení přímo na konkrétní položky

(ať už to bylo v kterémkoliv z režimů "Práva uvnitř formuláře - režim" viz výše)

a v druhé roli bylo právo na zápis na celou záložku.

Před e201601 tedy vyhodnocení bralo přednostně ta čtecí práva zadaná na jednotlivé položky,

Od e201601 zohledňuje i zděděné právo, vyhodnocení bere to vyšší právo z obou, a tím jsou v tomto příkladu zápisová práva definovaná na celou záložku.

Od e201605 pak řešíme situaci Master tabulka + více detailových záložek, kdy jedna z nich je hlavní, přes kterou se obsluhují data master tabulky.

U Master-Detail se zohlední práva i na tuto hlavní detailovou komponentu. Pokud má uživatel k hlavnímu detailu práva pouze na čtení, celá Master-Detail bude také pouze pro čtení. Práva z detailu se ale nedědí na ostatní případné záložky v detailu, dědí se pouze ta práva, která jsou nastavená na celý Master-Detail.

Pokud tedy chcete například nastavit uživateli zápisová práva na Str01/Struktura hierarchicky/Manažer, nastavíte zápisová práva k MasterDetail (ZalStrHier), čtecí práva k Detail (ZalStrHierDetail) a zápisová práva k Manažerovi (cecstrmanaPan).

Pozn. MasterDetail (ZalStrHier) může také zdědit zápisová práva ze záložky Struktura hierarchicky (ZalStrHierPanel).

* + 1. **Objekty práv konfigurace**

V minulé kapitole je popsáno, jak nastavujeme práva jednotlivým uživatelům. Pokud však správce ví, že některé okno, sestavu, proces nepoužívá organizace vůbec, je vhodné objekt zakázat konfigurací. Objekt takto jedním škrtem ze systému vymizí a "nepřekáží" ani v komplikovaných formulářích přiřazování práv (Adm03).

Vyřazení nastavujeme ve formuláři **Adm04** na záložce Konfigurace použití položkou **Hodnota vyřazení.** Zde -1 a nezadáno je to samé; 0 je úplné vyřazení z použití. Hodnoty 1 a 2 pak jsou určitou restrikcí použití. 1 objekt bude vždy pouze pro čtení. 2 vyřazení částí dle rozpisu ve spodní části záložky. Zde je opět kaskádovitý princip popsaný v přiřazování práv do rolí.

Položky, které jsou v databázi nebo v položkové repository EGJE označeny jako povinné jsou nyní indikovány znakem „!“ zobrazeným před nadpisem položky.

V Adm04 potom správce může v případě potřeby na záložce Struktura práv objektu dodefinovat další položky jako povinné („Povinnost vyplnění“ = Ano). U jiných typů než položka je hodnota bezpředmětná. Doporučujeme obezřetné zapínání povinnosti!

Tímto způsobem může správce přidat povinnost některým položkám, nicméně nemůže jí zrušit u těch položek, kde je povinnost nastavena „výrobcem“ už na úrovni databáze.

* + 1. **Zastupování uživatele na profilu**

Na formuláři Adm01 nastavujeme také zastupování uživatele jiným uživatelem. Zastupování se odehrává v rámci profilu práv. Toto přiřazuje správce : zadá tedy zastupujícímu uživateli profil uživatele, kterého má zastupovat a vybere tohoto uživatele (položka Zastupovaná osoba). Doplní ještě datumy od a do, ve kterých bude zastupování probíhat.

Zastupujícímu uživateli pak při přihlášení do systému přibude ještě jeden řádek ve výběru profilů, přičemž ve sloupci Profil je přiřazen uživateli uvidí zastupovaného uživatele a indikaci zastupování "(Z)". Pokud si tento profil zvolí, systém nastaví přístupová práva tak, jako by se hlásil zastupovaný uživatel. Přesto však je u všech změněných uživatelů během tohoto sezení ukládáno auditní razítko přihlášeného (tj. zastupujícího) uživatele.

Pozn.: V řadě organizací je e-mail přesměrován na zastupující osobu prostředky mail serveru.

Pokud zastupování své osoby má zadávat uživatel sám, může tak činit analogickým postupem pomocí formuláře Adm15 - Zastupování vlastní osoby. Zde je navíc možnost specifikovat režim "Režim zastupování a WFL e-mailů ", který umožní, aby i zástupci dostávali určité e-mailové zprávy (viz [Adm\_uzdoc / Adm15](Adm_uzdoc.htm#Adm15_popis)). Parametr také nastavuje schvalovací kompetence zastupujícího uživatele ve Wflow.

* + - 1. **Určení profilu pro zastupování**

Profil pro zastupování je často jiný než vlastní manažerský profil manažera, bývá vybaven jen některými kompetencemi.

V Adm02 k manažerskému profilu (př. "MANA") vyplní správce položku "Zastupováno profilem" (je uprostřed v odstavci Povolení přiřadit). Když ji nevyplní, profil se manažerovi v Adm15 nenabízí. V Adm15 se tedy manažerovi nabízejí pouze ty profily, které mají v Adm02 položku Zastupováno profilem vyplněnou a také takto se profil manažerovi nabízí.

Pro správce z toho plyne, že musí v Adm02 u všech profilů, nad kterými se zastupování v organizaci používá položku "Zastupováno profilem" vyplnit.

Pokud se v organizaci nepoužívají různé profily pro zastupování a pro manažera, vyplňuje správce v Adm02 k profilu přímo ten samý profil (př. k profilu "MANA" vyplní Zastupováno profilem: "MANA").

* + 1. **Dílčí (limitovaný) správce**

Uživatele Adm12, Adm01p dělíme na plnohodnotného správce a na dílčího správce.

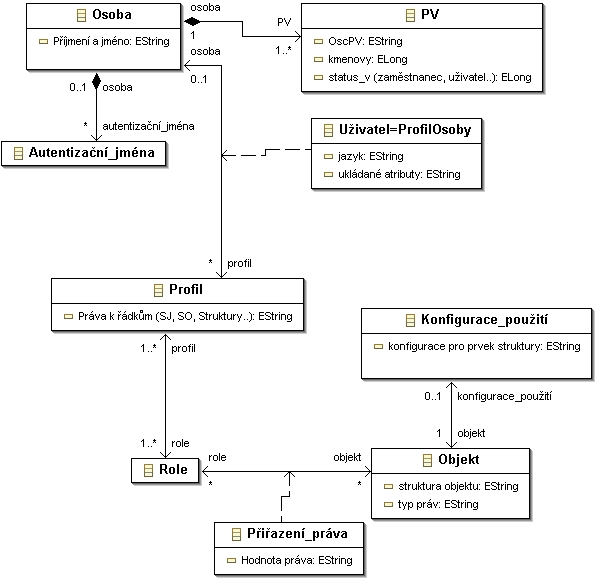
Plnohodnotný správce má práva pro zápis alespoň na jeden z formulářů Adm02 nebo Adm03 nebo Adm10. Dílčí nikoliv.

Omezení dílčího správce:

* Nabídka profilů Adm12, Adm01p nenabízí profily se zápisovým právem na Adm02 nebo Adm03 nebo Adm10.
* Dílčímu správci se nenabízejí osoby, které nějaký z takových správcovských profilů mají přidělený resp. se mu nenabízí jeho vlastní osoba
* Nemůže nikomu přiřadit login, pod kterým je zrovna přihlášen (Adm01p, v Adm12 se dílčí správce ani nevidí)

Shrnutí: Dílčí správce nechť má zápisová práva na Adm12, Adm01p, zatímco na další správcovské formuláře práv nechť má pouze čtecí nebo žádná práva (Adm01, Adm02, Adm03, Adm10).

* + 1. **Příloha – model přístupových práv EGJE**



* + 1. **Speciální objekty přístupových práv**

Většina objektů přístupových práv je pojmenována kódem formuláře, sestavy, dávky sestav, procesu nebo menu objektu. Kromě nich však existuje také skupina speciálních objektů, viz tabulka.

Pro oblast DOCH a Schvalovaní odchylek, je část speciálních objektů popsaná v [Doch\_dopl\_uzdoc](Doch_dopl_uzdoc.htm).

| **Objekt** | **Popis** | **Význam** |
| --- | --- | --- |
| Adm11mazaniSpoc | Právo mazat osoby spočtené předloni a dříve | Obecně uživatel s právem zápisu v Adm11 smí mazat osoby+PV, které ještě nevstoupili do mezd. Když má uživatel také toto právo, smí mazat osoby, jejichž nejnovější výpočet v uzavřeném měsíci je z předloňska nebo ještě starší. |
| Cep01emp | Funkčnost zaměstnanec | Skupinové objekty pro jednotlivé typové role ve funkčnosti formuláře Cep01 - workflow cestovní příkazy (viz též WflowAdmin) |
| Cep01mana | Funkčnost manažer |
| Cep01pokl | Funkčnost pokladna |
| Cep01ref | Funkčnost referent |
| Cep01jenObd | Uživatel smí zadat CP jen do období s otevřenou DOCH | Objekt zamezí možnost, aby uživatel zadal cestovní příkaz do období se statusem VT > 2 (uzavřen). |
| Cep01zal0 | Právo vynucuje zálohu = 0 pro možnost "Storno" | Uživatel s tímto právem nemůže provést storno cestovního příkazu, dokud není vyrovnaná záloha. |
| CepTypVT | Přístup k VT cestovních příkazů | Přístup k sadě typů výplatního termínu příslušejících k cestovním příkazům (10-39) Např. u tiskových sestav s výběrem typu VT.  viz též VypTypVT |
| Dan12email | Umožní zaslat sestavu Dan12 na mail zaměstnance | Přístup k dalším param sestavy Dan12, díky kterým lze sestavu zaslat na mail zaměstnance |
|  |  |  |
| Dav01Admin | Přístup na záznamy všech zadavatelů | Objekt umožní zpracovaní vstupů DAV bez omezení podle časového přiřazení PV k uživateli |
| Dav01Kopie | Formulář Dav01 | Právo pro zobrazení tlačítka Dav01, Vstupy, Kopíruj vstupy, standardně se tlačítko nezobrazuje (až po přidání práva) |
| Dav01Protokol | Přístup k protokolům výpočtů DAV | Objekt umožní uživateli přístup na záložku Dav01, Protokoly |
| Dav01SadaZkrNazev | Dav01, Zkrácený název sady struktur z názvu | Plnění sloupce Dav01, Sada struktur, Zkrácený název (10) z položky Název.  Automaticky není zařazeno do žádné ze standardních rolí. |
| Dav01SmazatVse | Přístup k mazání všech záznamů | Objekt umožní uživateli použít tlačítko [Smazat vše] na záložce Dav01, Vstupy |
| Dav01Vratit | Přístup na funkci Dav01 - Vrátit zadavateli | Objekt umožní uživateli použít uvedené tlačítko na záložce Dav01, Vstupy |
| Dca02rezimAllSK |  | Zpřísnění kontrol formuláře Dca02 pro Allsk |
| Dca02ViceOdp | Dca02, více typů odpr. doby | V rámci formuláře Dca02, povoluje alternativní název základních tlačítek pro začátek a konec odpr. doby a zobrazení další sady tlačítek pro začátek a konec odpr. doby.  Nezařazuje se do žádné ze standardních rolí. |
| Dcd01GenDDSLM | Povinnost zadání SLM při generovaní záznamu DD | Zpřísnění chování záložky Dcd01/Generování DD |
| Dcd01Korekce | Povolení pro záložky Dcd01 | Zpřístupnění záložky Dcd01, záložka Korekce FPD. |
| Dcd01specfunc | Speciální funkce Dcd01 | Povolení smazat denní docházku a denní záhlaví |
| Dcd01HromZmenaSlm | Přístup k hromadné změně SLM na Dcd01 | Zobrazení tlačítka [Změna SLM] na záložce Dcd01, Převod a uzavření, pro spuštění funkce hromadné změny SLM na Dcd01, Vstupy. |
| Dcd01RekDniUkol | Konfigurace Dcd01 | Zobrazení sloupce Úkol na záložce Dcd01, Rekapitulace dní (vazba na Úkolové mzdy). |
| Dcd01VzorDenOblib | Konfigurace Dcd01 | Povolení použití oblíbených vzor. dní na záložce Dcd01, Vstupy, Záhlaví |
| Dcd01TypPrescas | Konfigurace Dcd01 | Povolení aktivace dialogu na Dcd01 pro volbu zvýhodnění za práci  přesčas a práci ve svátek |
| Dcd01UzavriDen | Konfigurace Dcd01 | Zobrazení tlačítka Dcd01, Převod a uzavření, tlačítko Nastavení DZ … |
| Dcd21fppfSmazatVse | Přístup k mazání všech záznamů Pracovního výkazu | Slouží pro zpřístupnění tlačítka [Smazat vše] a [Smazat vše pro všechna PV v navigačním seznamu] na formuláři Dcd21fppf.  Při založení obj. práva, nebylo vložené do žádné ze standardních rolí. |
| Dcd27fppfSmazatDen | Konfigurace Dcd27fppf | Povolení tlačítka Dcd27fppf, Výkaz Den, Smazat den |
| Dcd27fppfSmazatVse | Konfigurace Dcd27fppf | Povolení tlačítka Dcd27fppf, Výkaz Den, dialog Zadání výkazu, Smazat |
| Dcd27fppfEditZkrNazev | Konfigurace Dcd27fppf | Povolení editace sloupce Zkrác. název |
| Dcd51RekDniUkol | Konfigurace Dcd51 | Zobrazení sloupce Úkol na formuláři Dcd51 (vazba na Úkolové mzdy). |
| DcgAdmin | Správce úkolových mezd | Povolení tzv. administrátorských funkcí pro oblast úkolových mezd správce aplikace u zákazníka. Také umožňuje uzavření formulářů úkolových mezd na úroveň 2. |
| DcgAdminEla | Speciální funkce úkolových mezd | Povolení tzv. administrátorských funkcí konzultanta ELANOR pro oblast úkolových mezd. Nejedná se o funkce vázané na právo DcgAdmin. |
| Dcg01Parametry | Řízení přístupu k záložce Dcg01, Parametry výpočtu | Současně s právem Dcg01 umožňuje editaci na záložce Dcg01, Parametry výpočtu.  Právo automaticky zařazeno do standardních rolí 1 a 3. |
| Dcg02SmazatVse | Hromadně smazat výkaz | Povolení funkce hromadného vymazání výkazu úkolových mezd pro všechny PV v nav. seznamu formuláře Dcg02. |
| Dcm01expert | Dcm01 expert | Původní nastavení pro výčet slm, které v tomto formuláři smí uživatel zadat. Bylo nahrazeno právy, ke skupinám SLM (Adm06) Na Dca02,Dcm01 zál. Vstupy - detail pak objekt zpřístupňuje zobrazení záznamů z dokladů (pd\_zdroj = 21) |
| Dcm01specfunc | Speciální funkce Dcm01 | Povolení smazat měsíční vstupy a měsíční záhlaví |
| Dcm01VstupySouhrnPrvni | Dcm01, Zobrazení záložky Vstupy - souhrn na prvním místě | Zobrazení jako první záložky Vstupy - souhrn na formuláři Dcm01 |
| Dcp01EditRezervaNeprit | Editace plánované rezervy nepřítomnosti | Povolení editace pro záznamy rezervy celozávodního volna v Dcp01/Dcp02/Dov16 |
| Dcs02objuzav | Objednávka stravenek po uzavření DCS | Uživatel s tímto oprávněním může používat aktualizační funkce i po uzavření stravy podle datumu uzavření stravy na Dcu02.  Při vytvoření nebylo zařazeno do žádné ze standardních rolí. |
| Dcs02ProtokolVse | Dcs02, zobraz protokoly všech uživatelů | Formulář Dcs02, záložka Protokoly, při nastavení „Smí spustit“, se aktuálnímu uživateli zobrazí protokoly stravy od všech uživatelů za aktuální období.  Automaticky není zařazeno do žádné ze standardních rolí. |
| Dcs02VyhodnoceniPrvni | Formulář Dcs02 | Právo umožňuje pro profil/uživatele, při otevření formuláře Dcs02, zobrazit záložku Vyhodnocení jako první - aktuální |
| Dcs02ZalTypNaroku | Formulář Dcs02 | Povolení zobrazení záložky Typ nároku na formuláři Dcs02 |
| Dcs03specfunc | Speciální funkce Dcs03 | Povolení smazat vyhodnocení stravy |
| Dcu06ctiDOCH | Dcu06 - záznamy z DD a MV pouze pro čtení | Uživatel s tímto oprávněním je omezen v Dcu06 tak, že může zpracovávat pouze vstupy ze schvalování, nikoliv však vstupy z docházky.  Také nemůže použit funkce z nabídky tlačítka [Funkce] a tlačítka [Otevřít]/[Uzavřít]  Při vytvoření nebylo zařazeno do žádné ze standardních rolí. |
| Dcu06\_inspektor | Dcu06 - rozšíření položek v dialogu (Skup. SLM, Zdroj, Stav) | Umožňuje na editačních obrazovkách formuláře Dcu06:  - v názvu tlačítka pro volbu SLM zobrazit číselnou identifikaci skupiny SLM podle Adm06  -zobrazit položky Skupina SLM, Zdroj, Stav editace.  Při vytvoření nebylo zařazeno do žádné ze standardních rolí. |
| Dcu06Korekce | Povolení pro funkce Dcu06 | Zpřístupnění funkce formuláře Dcu06, Funkce a Výběry: Korekce FPD. |
| Dcu06pocitaj | Povolení kalkulace záznamu denní/měsíční evidence docházky při uložení na formuláři Dcu06 | Standardně se při uložení záznamu na Dcu06 neprovádí jeho kalkulace (očekává se aut. noční kalkulace nebo uzavření), nastavením tohoto práva, se kalkulace provede již při uložení (snížení odezvy).  Při vytvoření nebylo zařazeno do žádné ze standardních rolí. |
| Dcu06editPlSmen | Dcu06 - smí editovat plánovanou směnu | Uživatel s tímto oprávněním je v Dcu06 na formuláři Plán směn oprávněn provádět změnu směn.  Právo není zařazené do žádné ze standardních rolí. |
| Dcu06nesmiUzavrit | Dcu06 - Uživatel nemá právo uzavřít záznam | Pro neschvalované vstupy (SLM ze skupiny 22/23 a 24/25/26) nelze používat tlačítka [Uzavřít]/[Otevřít]  Právo není zařazené do žádné ze standardních rolí. |
| Dcu06nezobrazitZdroje | Dcu06 - Na formuláři Dcu06 se nezobrazí tlačítko [Omezení zdrojů] | Právo není zařazené do žádné ze standardních rolí. |
| Dcu06nezobrazitFunkce | Dcu06 - Na formuláři Dcu06 se nezobrazí tlačítko [Funkce a výběry] | Právo není zařazené do žádné ze standardních rolí. |
| Dcu06SmazatVse | Přístup k mazání všech záznamů | Slouží pro zpřístupnění tlačítka [Smazat Měsíc] na formuláři Dcu06.  Při založení obj.práva, nebylo vložené do žádné ze standardních rolí. |
| Dcu06schvalit | Přístupnost tlačítek [Schválit], [Zamítnout] | Slouží pro zpřístupnění tlačítka [Schválit] a [Zamítnout] na formuláři Dcu06.  Při založení obj.práva, nebylo vložené do žádné ze standardních rolí. |
| Dcu06ZobrazProtokol | Dcu06, Zobraz volbu protokol | Při nastavení Smí spustit je povolené použití ikony Protokol na formuláři Dcu06.  Právo se automaticky nezařazuje do žádné ze standardních rolí. |
| Dcu06HromZmenaSlm | Přístup k hromadné změně SLM na Dcu06 | Zobrazení tlačítka [Změna SLM] v nabídce Funkce a Výběry, pro spuštění funkce hromadné změny SLM přesčasů na Dcu06.  Právo se automaticky nezařazuje do žádné ze standardních rolí. |
| Dcu06ZakazUzavrit | Uživatel nemá právo Uzavřít/Otevřít docházku | Při nastavení „Smí spustit“, uživatel nemá povolené použití tlačítek Uzavřít/Otevřít na formuláři Dcu06.  Právo se automaticky nezařazuje do žádné ze standardních rolí. |
| Dov056emp | Schval. dov. - funkčnost zaměstnanec | Skupinové objekty pro typové role pro workflow schvalovaní dovolené |
| Dov056koor | Schval. dov. - funkčnost koordinátor |
| Dov056ved | Schval. dov. - funkčnost manažer |
| Dov056ved1 | Schval. dov. - funkčnost manažer 1 |
| Dov056KalJenPlusDov | Žádost o dovolenou jen s kladným zůstatkem (IA 21) | Nedovolí uživateli odeslat žádost při překročení v tu chvíli vyhodnoceného nároku viz též [Dov\_uzdoc](Dov_uzdoc.htm) / Dov05 |
| Dov056KalJenPlusPVol | Žádost o pracovní volno jen s kladným zůstatkem (IA 26, 5151) | dtto |
| Dov056KalJenPlusPlan | Plán SLM jen s kladným zůstatkem (IA 21 Dov01, IA 26, 5151 Dov02) | dtto |
| Dov056KalNV | Žádost o čerpání náhr.volna, kontrola na saldo | Aktivace kontroly čerpání NV na aktuální saldo NV, při uložení/odeslaní schválované SLM z formuláře Dov05/Dov06/Dcu06. Odchylka se i při nesplnění podmínky, po zobrazení hlášení, uloží /odešle.  Automaticky nedoplněno do žádné ze standardních rolí. |
| Dov056KalNVJenPlus | Žádost o čerpání náhr.volna, jen pro kladné saldo | Aktivace kontroly čerpání NV na aktuální saldo NV, při uložení/odeslaní schválované SLM z formuláře Dov05/Dov06/Dcu06. Odchylka se i při nesplnění podmínky, po zobrazení hlášení, neuloží /neodešle.  Automaticky nedoplněno do žádné ze standardních rolí. |
| Epr01Admin | Editace záznamů všech uživatelů | Objekt zpřístupní pro zápis všechny eProposaly |
| Epr01Insp | Čtení záznamů všech uživatelů | Objekt zpřístupní pro čtení všechny eProposaly (vlastní budou přístupné pro zápis) |
| Epr01EprPosledniho | Přístup na Epr, kde se schvaluje na status 30 | Právo přidává oprávnění "Promítnout data do kmenových dat" u viditelného eProposalu uživateli, který schvaluje poslední krok i když nemá právo Epr01Admin |
| Epr01Protected | Přístup na chráněné eProposaly | U nového eProposalu je možnost vyplnit údaj "Chráněné workflow". |
| Epr01Kopie | Přístup na Zkopírovat tento eProposal | Uživatelům s tímto právem se zpřístupní záložka "Kopie" a v ní tlačítko "Zkopírovat tento eProposal" |
| fDokPrivat | Přístup na všechny dokumenty PV | Objekt zpřístupní i dokumenty které nejsou označeny jako Veřejné |
| fEditDochUzavDoch | Editace docházky v období uzavřeném pro docházku (status 3) | Povolení viz popis |
| fEditDochUzavMzdy | Editace docházky v období uzavřeném pro mzdy (status 9) | Povolení viz popis |
| fexportXLS | Export do Excelu | Povolení interaktivní funkce exportu tabulkového zobrazení do Excelu (lokální menu). |
| fGenKal | Generování kalendářů | Povolení generovat všechny kalendáře na Vyp02 |
| fHodOdemkni | Odemknout hodnocení | Povolení odemknout hodnocení na Hod01 |
| fHodZamkni | Zamknout hodnocení | Povolení zamknout hodnocení na Hod01 |
| fKopCis | Měsíční kopie číselníků SLM a struktur | Povolení spustit kopírování číselníků SLM a struktur na Vyp02 |
| fKopCisSlm | Měsíční kopie číselníku SLM | Povolení spustit kopírování číselníku SLM na Vyp02 |
| fKopCisStr | Měsíční kopie struktur | Povolení spustit kopírování číselníku struktur na Vyp02 |
| fKopCisMulti | Měsíční kopie čís. - právo spustit i v multiorg. | Povolení:  Spustit kompletní kopírování číselníků u multiorganizační db uživateli omezenému organizací.  resp.  spustit jej u jednoorganizační multiSJ db uživateli omezenému SJ. |
| fKopPV | Měsíční kopie PV v rámci VT | Povolení spustit Měsíční kopii PV v rámci VT na Vyp02 |
| fLang\_cs, fLang\_sk, fLang\_en | Jazyk uživatelského rozhraní - čeština, slovenština, angličtina | Ikona pro přepínání jazyka:  Uživateli se nabízí jednak jazyky, které má přiřazené pomocí přiřazení profilu a pak případně základní jazyky ("cs", "sk", "en") povolené příslušným fLang\* objektem. Pokud jich je více než jeden, má k dispozici ikonu pro přepínání. |
| fonlyHTML | Povoleny pouze sestavy HTML (web v záložce) | Uživatel s tímto oprávněním může zvolit u sestavy pouze formát HTML. Platí pouze tehdy, když sestava formát HTML podporuje.  Sestava se zobrazí v záložce bez ohledu na nastavení v Adm21 |
| fonlyPDFplug | Povoleny pouze sestavy PDF (web v záložce - plugin) | Uživatel s tímto oprávněním může zvolit u sestavy pouze formát PDF. Platí pouze tehdy, když sestava formát PDF podporuje.  Sestava se zobrazí v záložce bez ohledu na nastavení v Adm21 |
| fPlanSměnZobrazNeprit | Plan směn, zobrazit nepřítomnosti | Režim zobrazení nepřítomnosti z evidence docházky v Dcp03.  nezařazen do žádné ze standardních rolí |
| fPvDochHist | Zobrazit v nav. seznamu DOCH v historii všechny nyní přístupné PV) | Při přidělení práva se v navigačním seznamu pro historické uzavřené období zobrazí i PV, které jsou přístupné uživateli v aktuálním období, ale dříve přístupní nebyli.  Standardně neobsaženo v žádné ze standardních rolí. |
| fReaPrijHrom | Přijetí uchazeče - hromadné | Tlačítko na Rea01 / Přijetí uchazeče / Přijetí všech uchazečů v seznamu |
| fReaPrijInd | Přijetí uchazeče - individuální | Tlačítko na Rea01 / Přijetí uchazeče / Přijetí uchazeče |
| fSchvalSLMPoznamka | Povinnost vyplnit poznámku u schvalované SLM | Povinnost vyplnit poznámku WFL při odeslání SLM ze započitatelnosti Slm02.DOCH03.H-Offic z formuláře Dov05, Dov06 nebo Dcu06. |
| FtpAdmin | Výměna souborů - správce | Uživatel, který má toto právo nemusí být zařazován k jednotlivým činnostem nad složkami výměny dokumentů (čtení, nahrání, smazání) |
| fUrepImpDelAll | Právo na mazání uživ.importů jiných uživatelů | Objekt je používán u uživatelský importních sestav a umožní rušit importní dávky vytvořené touto sestavou, ale jiným uživatelem. |
| fUzavMes | Měsíční uzávěrka - výpočet/zrušení | Povolení spustit měsíční uzávěrku na Vyp02 |
| fUzavRoc | Roční uzávěrka - výpočet/zrušení | Povolení spustit roční uzávěrku na Vyp02 |
| fUziAdmin | Správa uživatelských sestav | Povolení interaktivního vytváření uživ. sestav (lokální menu na vybraných menu objektech navigačního menu v levé horní části std. klienta) a mazání vlastních i cizích sestav |
| fUziCrea | Vytváření uživatelských sestav | Povolení interaktivního vytváření uživ. sestav (lokální menu na vybraných menu objektech navigačního menu v levé horní části std. klienta) a mazání vlastních sestav |
| fVsechnaRazitka | V mzd. sestavách nabízet všechna razítka z Opv31 typ 11 | Umožňuje uvedené a je použitelný pro razítka zahrnující celou mzdovou účtárnu, a ne konkrétní osobu.  Objekt není v žádné standardní roli. |
| fVypBlok | Právo provádět výpočet mezd / rušení i při jeho blokování. | Hlavní mzdová účetní (tj. uživatel s tímto právem) smí na Vyp02/Blokování výpočet mezd blokovat ostatním, ale sama jej provádět může. |
| fVypListHrom | Právo na hromadný tisk výplatních lístků | Právo pro standardní Vyp11 (CZ), Vyp31(SK) a pro outsourcingové výplatní lístky Vyp11fq (CZ) a Vyp31fq(SK) které zpřístupňuje parametry pro jejich hromadné zpracování a rozesílání. |
| fVypStatusAdmin | Právo nastavit libovolný status VT | Právo je uplatněno na Vyp02 |
| fVypZrus6 | Právo vrátit zpět zpřístupněný VT (status 6) Právo smazat VT  (VT musí být se statusem < 4) | Právo je uplatněno na Vyp02 |
| fVypZrusHrom | Hromadný výpočet a jeho zrušení | Povolení spustit hromadný výpočet a jeho rušení na Vyp01, Vyp02, Vyp03  V kombinaci **pouze** s právem **fVypStazeni** zpřístupňuje tisk ve statusu výplatního termínu ve stavech 4 – 9. |
| fVypZrusInd | Individuální výpočet a jeho zrušení | Povolení spustit individuální výpočet a jeho rušení na Vyp01, Vyp03  Právo také zpřístupňuje tisk výplatních tiskovin ve statusu výplatního termínu 5, kdy ještě není tento zpřístupněn koncovým uživatelům.  V kombinaci **pouze** s právem **fVypStazeni** zpřístupňuje tisk ve statusu výplatního termínu ve stavech 4 – 9.  V kombinaci s právem **fVypZrusHrom** zpřístupňuje tisk ve stavech 1-20.  (je uplatněno u standardních VL, form Vyp25, Vyp26, u sestav Dan03, Das03, Vyp11, Vyp11fq, Vyp31, Vyp31fq a některých zákaznických VL) |
| fVypStazeni | Možnost stažení Výplatní pásky ve stavech 4-9 | Právo umožní stažení výplatní pásky zaměstnanců ve stavu výpočtu 4-9 |
| Gen01expimp | Export/Import z generátoru dotazů | Povolení Importu a Exportu dotazu z a do souboru v Gen01. |
| Jpc01locEditOnly | Editace Jpč pouze z lokálních menu |  |
| Kal01GenTypDne11x12 | Kal01 Aktualizovat i pro typ dne 11..17 | Funkce generování rozpisu směn kalendáře (Kal01, Adm53/33, Kal09, …).  Povolení přegenerování záznamů s posunem směny (typ dne = 11 až 17)  Režim smí spustit. Právo nezařazené do žádné ze standardních rolí. |
| Kva06\_noinsert | Zákaz vkládání/mazání na Kva06/Základní údaje | Jediné právo, které funkčnost odnímá. Nastavuje Kva06 do režimu, kdy nejde zadat vzdělávací akce. Ty je pak třeba zadávat pouze přes Kat01. |
| MENU\_Fav, MENU\_All | Oblíbené Události, dotazy, navigace | Prvky menu, které uživatel dostává, i když je nemá v profilu (roli). Je ale možné je zakázat pomocí uživatelské role a práva -1 - Odnětí |
| nav\_Pv\_seznam\_datnar | Navigační seznam Dat. narození, SO, kat., od, do, druh PV | Právo k navigačnímu seznamu Pv (Osb02, Opv01...) |
| nav\_Pv\_seznam\_druh\_od\_do\_pm | Navigační seznam Druh PV, od, do, PM, ORG |
| nav\_Pv\_seznam\_druh\_prof | Druh PV, Profese, Org. |
| nav\_Pv\_seznam\_druh\_rp | Druh PV, od, do, Str. dle ř.práv |
| nav\_Pv\_seznam\_odruh\_od\_do\_pred | Druh PV, od, do, předp.ukon. |
| nav\_Pv\_seznam\_pm\_so | PM, SO |
| nav\_Pv\_seznam\_datnar | Navigační seznam Dat. narození, SO, kat., od, do, druh PV |
| nav\_Pv\_seznam\_druh\_od\_do\_pm | Navigační seznam Druh PV, od, do, PM, ORG |
| nav\_Pv\_seznam\_druh\_prof | Druh PV, Profese, Org. |
| nav\_Pv\_seznam\_druh\_rp | Druh PV, od, do, Str. dle ř.práv |
| nav\_Pv\_seznam\_odruh\_od\_do\_pred | Druh PV, od, do, předp.ukon. |
| nav\_Pv\_seznam\_pm\_so | PM, SO |
| nav\_PvD\_seznam\_5\_str\_rp | Standard + struktura dle řád.práv | Právo k navigačnímu seznamu PvDOCH (Dcd01, Dcm01...) |
| nav\_PvD\_seznam\_6\_druh\_so\_prof | Druh PV, SO, Profese |
| Nav01bezMana | Nav01 - potlačení zobrazení manažerů u názvu str. z Adm21/2 a 8 | Restriktivní objekt - potlačí zobrazení manažera u organizační struktury a projektu. |
| Nav01vsechnyOsoby | Nav01 - všechny Osoby/PV z org. bez ohledu na práva k řádkům | Držitel oprávnění uvidí v Nav01 všechny osoby/PV v rámci omezení organizací a nejen ty, na které má práva |
| Nav01spojeni | Nav01 - strom -1 se služebními e-maily a telefony | Restriktivní objekt - odejme volbu   -1 Spojení |
| Opv05vlaICO | Opv05 zobrazí v tabulce na první stránce jen osoby a PV ze stejné IČO | restriktivní objekt přístupových práv sloužící k ochraně údajů v rámci IČO.  Pokud jej uživatel Opv05 má, pak "Kontrola existence zadané osoby v databázi" zobrazuje výsledky kontroly pouze v rámci uživatelova IČO. |
| Opv06fvseAdmin | Dohody VŠE - editace záznamů všech uživatelů | Uživatel s tímto právem může editovat formulář Opv06fvse – Dohody VŠE – kmen všech uživatelů. |
| Opv07fvseAdmin | Dohody VŠE - editace potvrzení všech uživatelů | Uživatel s tímto právem může editovat formulář Opv07fvse – Dohody VŠE – potvrzení všech uživatelů. |
| Opv08fvseAdmin | Dohody VŠE - editace rozpisů všech uživatelů | Uživatel s tímto právem může editovat formulář Opv08fvse – Dohody VŠE – rozpis všech uživatelů. |
| Opv08fvseInsp | Dohody VŠE - čtení rozpisů všech uživatelů | Uživatel s tímto právem může číst formulář Opv08fvse – Dohody VŠE – rozpis všech uživatelů. |
| Opv09fvseAdmin | Dohody VŠE - editace sumářů všech uživatelů | Uživatel s tímto právem může editovat formulář Opv09fvse – Dohody VŠE – sumář všech uživatelů. |
| Opv09fvseInsp | Dohody VŠE - čtení sumářů všech uživatelů | Uživatel s tímto právem může číst formulář Opv09fvse – Dohody VŠE – sumář všech uživatelů. |
| Opv02zpet | Přístup na všechny historické tarify | Opv02 zobrazuje údaje s datumovou restrikcí, kdy (datumově) uživateli patří.  Typicky přechod zaměstnance mezi SO tj. mezi referenty.  Pokud chcete, aby uživatel z nové SO viděl i staré tarify, vybavte jej právem "Opv02zpet", které je zpřístupní. |
| Poj15email | Umožní zaslat sestavu Poj15 na mail zaměstnance | Přístup k dalším param sestavy Poj15, díky kterým lze sestavu zaslat na mail zaměstnance |
| Rtf10all | Administrace RTF šablon | Zpřístupní všechny RTF šablony, které byly v db zaevidována. Standardně uživatel vidí jen ty, které sám zaevidoval. |
| Str01CopyTree | Právo kopírovat část organizační struktury | viz popis - Str01 / Struktura hierarchicky / Detail / Kopie části stromu |
| Vst10Admin | Přístup na záznamy všech uživatelů | Přístup ve Vst10 i na záznamy, kde nejsem uveden v položce Uživatel |
| Vst13Admin | Přístup na záznamy všech uživatelů | Přístup ve Vst13 i na záznamy, kde nejsem uveden v položce Uživatel |
| Vyk62Admin | Přístup na všechny žádosti | Držitel práva má přístup na všechny žádosti ve Vyk62 (v rámci práv na organizaci a SJ, SO). Viz [Zam\_dok\_uzdoc](Zam_dok_uzdoc.htm) |
| VypTypVT | Přístup k standardním VT | Přístup k sadě typů výplatního termínu příslušejících ke mzdám (<=10) Např. u tiskových sestav s výběrem typu VT.  viz též CepTypVT |
| WflowAdmin | Workflow administrátor | Uživatel s tímto práva může ručně nastavovat status, který je jinak spravován Workflow (např. Cep01 záložka Administrace) Uživatel také ve formuláři Wflow jednak může vidět všechna workflow a může je i rušit (tlačítko Zrušit workflow) |
| WflowHrom | Hromadné schvalování urč. workflow | Uživatel s tímto právem může ve schvalovacím formuláři Wflow použít hromadné schvalování na workflow 2, 3, 4, 11-20 (u 11, 14 ale pouze vlastní schválení cesty - vč. zálohy) |

1. **Hromadná korespondence**

Aparát hromadné korespondence je postaven na číselníku předloh Rtf10 a standardních sestavách Rtf11, Rtf12, Rtf13. K těmto standardním/vzorovým sestavám je možné v případě potřeby dalších položek vytvářet zákaznické klony. V případě java klienta a jeho správné konfiguraci je také možné načíst předlohu z Rtf10 a spolu s daty ji postoupit MS WORD a iniciovat jejich zpracování hromadnou poštou viz kap. 8.3.

Přístupný je také původní formulář Rtf01, který umožňuje export personálních a tarifních údajů osob. Není však měnitelný a také neumí načíst předlohu z Rtf10 a postoupit ji MS WORD.

Tlačítko Export do XLS osoba uloží do zvoleného souboru údaje o vybrané osobě, tlačítko Export do XLS vše uloží údaje o všech osobách. Údaje se ukládají na záložku Data. Veškeré předchozí údaje jsou při exportu ze záložky vymazány.

Záložka "Personální údaje" poskytuje údaje, bez citlivých dat mzdového charakteru, o ty je naopak rozšířena druhá záložka "Personální a mzdové údaje". Záložky jsou předmětem přístupových práv. Je tedy rozdíl, ze které záložky uživatel Export volá.

Vytvořený soubor se pak použije jako zdroj dat pro hromadnou korespondenci v s kancelářském balíku, který podporuje její zpracování (typicky MS Office, OpenOffice). Součástí implementace EGJE může být i úprava předloh pro hromadnou korespondenci.

* 1. **Použití MS Office**

Pokud chcete vytvořit formulářové dopisy, adresní štítky, obálky, adresáře a hromadně distribuovat e-maily a faxy, použijte podokno úloh Hromadná korespondence. Postupujte podle následujících základních kroků:

* Otevřete nebo vytvořte hlavní dokument.
* Jako zdroj dat použijte XLS soubor, do kterého jste si vyexportovali údaje o osobách.
* Přidejte nebo upravte slučovací pole v hlavním dokumentu:  
  Zobrazte si panel nástrojů hromadná korespondence. V něm je pak tlačítko "Vložit sloučená pole"
* Proveďte sloučení dat ze zdroje dat do nového dokumentu a vytvořte nový sloučený dokument.

Když již je dokument vytvořený a upravený je tedy celkový postup následující:

* Otevření formuláře Rtf01 a příslušné záložky
* Případné provedení nebo načtení výběru nad osou Pv
* Provedení exportu do datového xls souboru (je uveden v záhlaví dokumentu s tím, že si formulář pamatuje jeho minulé umístění) tlačítkem Export do XLS osoba resp. vše.  
  Pozor: v tuto chvíli nesmí být otevřen žádný Word dokument, který jej používá jako zdroj dat (neuděláte chybu když Word zavřete)
* Otevření MS Word a v něm již dříve vytvořený dokument pro hromadnou korespondenci s kladnou odpovědí na dotaz o spuštění SQL selectu z Data$. Následuje výběr zdroje dat přičemž v položce název souboru (rozkliknutím šipky) si Word pamatuje minulé použité zdroje - bude si tedy pamatovat i ten Váš, vytvářený v bodu 3.
* Nyní word provede načtení dat a zobrazí dokument o jedné osobě (Pv). Pokud chcete vytvořit dokument se všemi osoby ze zdroje dat zavolejte funkci (tlačítko) "Sloučit do nového dokumentu". Vytvořený dokument pak můžete vytisknout, resp. uložit.

Poznámka : pokud se ve vytvořeném word dokumentu objeví hláška **Chyba! V záznamu záhlaví nebylo nalezeno pole SlučPole.** nejpravděpodobnějším důvodem je to, že jste datový soubor vyexportovali z první záložky, zatímco dokument používá i položky ze záložky druhé.

Formát zobrazení datumu v MS Word. Místo implicitního amerického formátu bývá obvykle vhodné zadat u datumového pole formát kontinentální.   
Př. { MERGEFIELD DAT\_NAST \@ "d.M.yyyy"} {MERGEFIELD "DAT\_UKON" \@ "dd. MM.yyyy"}

U desetinných čísel je pak obvyklé použít formátovací řetězec podle následujícího příkladu:.

{ MERGEFIELD "CASTKA\_ENC" \# "### ###,##" }

Do režimu editace kódů se v MS Word vstupuje klávesami Alt+F9.

Viz též: <http://www.gmayor.com/formatting_word_fields.htm>

Microsoft Word, Excel a Windows jsou ochranné nebo registrované ochranné známky společnosti Microsoft Corporation Inc.

* 1. **Použití OpenOffice**

Hromadné dopisy se v aplikaci OpenOffice.org Writer vytváří pomocí Průvodce hromadnou korespondencí. Jako zdroj dat pro databázi kontaktů si nastavte XLS soubor, do kterého se exportovaly údaje o osobách. Princip práce je shodný jako u MS Office.

* 1. **Rtf sestavy a uživatelské sestavy - přímé volání MS Office**
     1. **Technologický předpoklad**

Celý aparát vyžaduje:

* OS MS Windows
* Instalovaný MS Office (2016, 2019, 2021), Microsoft 365
* Upravenou předlohu egje\*.egje pro spouštění EGJE

Pro 32-bitový JVM je zapotřebí přidat tag

<resources arch="x86" os="Windows">  
 <nativelib href="egjelib/egjelib-win-x86.jar"/>  
</resources>

a také mít uvedenou knihovnu v adresáři egjelib (ews předlohy).

* Pro použití 64-bitového JVM je zapotřebí, aby ve spouštěcím \*.egje souboru nebylo omezení na architekturu.

Tzn. <resources os="Windows" >

<nativelib href="egjelib/egjelib-win-x86.jar"/>

</resources>

Alternativou je zadání arch="x86 amd64".  
Upozornění - spolupráce s 64-bitovým office není testována

* Při spouštění z bat se do příkazového řádku doplňuje parametr

-Djava.library.path=./egjelib

a v egjelib adresáři musí být soubor jacob-1.16.1-x86.dll  
resp. jacob-1.16.1-x64.dll (pro 64-bitové JVM prostředí)  
př.  
*start javaw -splash:elanor.jpg -Xmx700m -Djava.library.path=./egjelib -cp egjelib/eman.jar;egjelib/egjelib.jar cz.elanor.eman.sgui.navig.RunGui -Cconfig\_jar=egjelib/config\_egje.jar*

Pozn. Parametry před cz.elanor.eman.sgui.navig.RunGui jsou považovány za parametry pro JVM, parametry za cz.elanor.eman.sgui.navig.RunGui jsou parametry aplikace. Pro správnou funkčnost musí být java.library.path nastaven jako parametr JVM.   
Parametr -ea má smysl nastavovat pouze v testovacím prostředí, v produkčním by neměl být nastaven.

* + 1. **Použití**

Aparát sestav RTF umožňuje:

* uložení předlohy do databáze
* zapouzdření konkrétní předlohy a datového zdroje do formy sestavy EGJE
* EGJE si Microsoft Word samo zavolá a spustí akci pro spojení předlohy a dat

Předlohy v db jsou evidovány pomocí formuláře Rtf10.

Standardně uživatel může k vlastním předlohám, má-li ještě právo Rtf10all může ke všem předlohám.

Výběr předlohy je parametrem sestavy.

Sestava Rtf11 je potom vzorovou sestavou, která poskytuje stejná data jako první záložka Rtf01. Sestava nabízí předlohy označené jako 1 - Personální.

Sestava Rtf12 pak analogicky poskytuje stejná data, jaká jsou zobrazena na druhé záložce Rtf01. Sestava nabízí předlohy označené jako 2 - Personální a mzdové.

Pro uživatelské sestavy je pak vyhrazen typ 6 - Ostatní.

**Tvorba šablony**.

Šablona se nejlépe vytváří buď editací jiné šablony nebo pomocí průvodce (MS Word 2021, Microsoft 365)

Pro tvorbu šablony je zapotřebí datový soubor xls.

Ten získáte, když sestavu (typicky Rtf12) necháte vytvořit jako "Výstup do XLS (pouze data)". Standardní "Výstup do RTF" tento soubor sice také vytváří, ale pouze jako dočasný v TEMP, který je po sloučení v MS Word ihned automaticky vymazáván.

* 1. **Hromadná korespondence – Dokumenty DOCX ELA**

Nevýhodou tradičních sestav typu „RTF“ tedy např. Rtf11, Rtf12 je:

- méně komfortní volání z EGJEWEB2,

- probíhá plně v MS Word, není tedy možné výsledek vzít a někam uložit,

- java klient - technologická závislost na správnou konfiguraci spouštěče EGJE a na nainstalování správné verze MS Word (32/64) na stanici,

- MS Word hromadná korespondence neumí pracovat s hromadnými záznamy typu Struktury, ale pouze s nenásobnými údaji typu Struktura1, Struktura2.

Sestavy Rtf21, Rtf22 fungují jinak:

Používají také DOCX předlohy, nicméně jejich zpracování je čistě v aparátu EGJE.

Ten provede zpracování i při volání z EGJEWEB2, a také umožňuje (po PV „naporcované“) vytvořené dokumenty ukládat do Opv31.

Dokumenty nepoužívají „Pole“ ve smyslu MS Word, ale čistě textovou náhradu, přičemž místo

př. místo «PRIJMENI» resp. {MERGEFIELD „PRIJMENI“}

se píše běžný text {{PRIJMENI}} tedy v dvojitých složených závorkách.

Tisk z násobných vět je umožněn pomocí řídícího makra {{REPEAT}}.

Více je popsáno v [Rtf\_uzdoc](Rtf_uzdoc.htm) v kapitole Rtf21, Rtf22.

1. **Uživatelské sestavy**
   1. **Schema**

Uživatelské sestavy jsou ukládány do databáze. Uživatel je připravuje v uživatelském adresáři nástroji JasperSoft Studio editora textový editor.

Firma Elanor navíc disponuje aparátem, který umožní sestavu vytvořenou zákaznickou podporou Elanor odeslat zákazníkovi (správci) i mimo termín výdeje resp. patche.

Celý aparát je přístupný na základě objektového práva „fUziCrea“ - „Vytváření uživatelských sestav“.

Dále je vhodné, aby uživatel měl ve svém profilu zařazenu také nějakou uživatelskou roli (>=500, Adm03, Adm02). Tu je pak možné použít pro přidělení práva k nově vzniklé sestavě.

* 1. **Popis aparátu**

Uživatel buď používá volání editorů přímo z tlačítek na oknu pro spouštění sestavy (když je v režimu úprav sestavy) nebo pracuje přímo nad pracovním adresářem, ve kterém soubory sestavy jsou.

Uživatel potřebuje tyto pomůcky :

JasperSoft Studio - ve verzi shodné s verzí jasperreports používané v systému. Nyní:

6.6.0

XML editor - pro editaci souborů \*.xml. Např.:

C\:\\Program Files\\PSPad editor\\PSPad.exe

.properties editor - pro editaci jazykově závislých textů. Typicky

PropertiesEditor.jar

Nutné pouze pro tvorbu vícejazyčných sestav resp. úpravu textů v kopiích sestav Elanor.

Při editaci pomocí tlačítek z EGJE není potřeba.

Pro editaci pomocí tlačítek na oknu spouštěné sestav je zapotřebí nastavit cesty k editorům, které se používají pro upravování uživatelských sestav.

Menu Nastavení / Uživatelská nastavení / parametry

JasperSoft Studio editor

XML editor

Při upravování sestavy EGJE se soubory, z kterých se sestava skládá vytvoří v adresáři %USER\_HOME%/Dokumenty/Eman/userreports/. (pokud není nastaveno v „Nastavení / Uživatelská nastavení / Adresář pro export“ jinak).

* 1. **Vlastní vytvoření a editace sestavy**

Uživatelské sestavy se vytváří pomocí průvodce, který se zobrazí po zvolení položky **Nová sestava** v kontextovém menu v levém navigačním panelu (uzly menu formulářů a sestav). V prvním kroku můžeme zvolit, jestli chceme vytvářet zcela novou sestavu nebo zda chceme vytvořit kopii existující sestavy. V druhém kroku nastavíme název sestavy, kód sestavy, menu, pod kterým bude nová sestava zařazena a přístupová práva pro novou sestavu. Novou sestavu vytvoříme stiskem tlačítka Dokončit. Pokud je tlačítko dokončit neaktivní, znamená to, kód sestavy nemá správný formát nebo sestava či formulář se zvoleným kódem už existuje.

Aparát hlídá, aby kód sestavy byl tvořen třemi znaky poté dvěma číslicemi a na 6.pozici vyžaduje znak "u" (uživatel)

Nedoporučujeme přímo upravovat sestavy vytvořené elanorem (na 6.pozici "f") vždy je lepší udělat její uživatelský klon "u".Pokud se však přesto rozhodnete z nějakých důvodů editovat sestavu "f", zašlete ji zpět do Elanoru pomocí helpdesku se stručným popisem úpravy.

Uživatelské sestavy upravujeme pomocí nabídky, která se zobrazí po stisku tlačítka „**Uprav sestavu**“ ve spouštěcím okně sestavy. Tuto volbu obsahuje také kontextové menu sestavy v levém navigačním panelu.

**Tabulka 1 - editace uživatelských sestav**

|  |  |
| --- | --- |
| **Akce** | **Popis** |
| Uprav datový zdroj | Otevře datový zdroj sestavy v textovém editoru |
| Vytvoř Jasper soubory | Vytvoří základní verzi sestavy se standardní hlavičkou, zápatím atd. Přepíše jen ty soubory, které neexistují. |
| Spusť JasperSoft Studio editor | Spustí editor sestav, program JasperSoft Studio a otevře v něm aktuální sestavu |
| Kompiluj | Přeloží sestavu do zkompilované formy (xml => jasper) |
| Zobraz složku | Zobrazí složku se sestavou |
| Uprav název sestavy | Umožňuje změnit název sestavy |
| Edituj texty | Otevře v textovém editoru soubor s příponou .properties, který obsahuje lokalizované texty použité v sestavě. |

**Na závěr editace sestavy nezapomeňte sestavu uložit zpět do db tlačítkem „Ulož sestavu“ !**

* + 1. **Přenesení uživatelské sestavy na jinou db**

Uživatelskou sestavu můžete vyexportovat pomocí volby Export sestavy z kontextového menu volaného přímo z této sestavy v navigačním menu.

Do nové db ji nahrajete standardním způsobem pomocí Adm51 (viz následující kapitola)

## Distribuce uživatelské sestavy Elanor

Uživatelská sestava vytvořená firmou Elanor je distribuována jako jar soubor se sestavou a změnovým skriptem.

Pozn.: dříve byl přikládán i xml soubor změnového skriptu, nyní je uvnitř jar souboru.

Soubor nahrajte do společného adresáře a v Adm51 / Změna Db / Instalace uživatelské sestavy spusťte jej jako změnový skript.

Ten provede načtení sestavy do systému.

Sestava je k dispozici při příštím přihlášení do EGJE.

* 1. **Předchozí verze sestavy**

Pokud jsou v db uloženy předchozí verze sestavy, jsou k dispozici v kontextovém menu ve spodní části. U sestavy je zobrazeno datum vložení resp. poslední změny.

Upozornění - ne všechny sestavy označené jako uživatelské (tj. písmeno f na 6.pozici jsou vytvářeny technologií uživatelských sestav. Některé jsou standardní součástí systému a popsané funkčnosti uživatelských sestav pro ně k dispozici nejsou.

1. **Instalace patch a výdejů pomocí utility SuperConfigurator**

Tato víceúčelová utilita umožňuje:

* Instalovat (do již nainstalovaného systému EGJE) patche a výdeje
* Monitorovat běžící aplikační servery a web servery
* Spouštět změnové skripty resp. instalovat uživatelské sestavy na více instalacích najednou
* Generovat změnové skripty z vybraných konfiguračních číselníků.

Utilita neslouží k první instalaci EGJE v novém prostředí.

Jazyk programu je možné nastavit pomocí parametru EGJELANG uvnitř spouštěcí dávky

př. -DEGJELANG=en způsobí spuštění v angličtině.

* 1. **Instalace patche - výdeje:**
* informovat uživatele o nutnosti opuštění systému
* zastavení servlet kontejneru Tomcat s aplikací (aplikacemi) EGJEWEB2 a Aplikačních serverů EGJE, které budou upgradovány
* spuštění SuperConfigurator z výdejového/patchového adresáře. (při prvním spuštění uživatelem výběr/sestavení seznamu instalací - viz dále 10.2.1)
  + **na záložce Instalace / Instalace, výdej patche tlačítkem "…"   
    vybrat adresář s patchem / výdejem (indikovaný pomocí souboru patch.properties)**
  + v seznamu instalací vybrat příslušnou/příslušné instalace a tlačítkem "Instaluj vybrané" provést vlastní instalaci
    - Superconfigurator provede instalaci programu a změnového skriptu
    - Z instalace změnového skriptu je k dispozici protokol "patch\_*DB\_datum*.html" (ten v případě chyby při realizaci změnového skriptu předejte na support elanor)
    - Celá instalace se v bodech zapisuje do souboru egje\_patch\_protocol.txt
* Manuální instalace dokumentace - pokud je použita položka Configurator / Obecné / "Http resp. disková složka pro help soubory" pro přesměrování helpu na jiné místo. Rozzipujte tam doc.zip.
* Manuální instalace egjews-embed.jar - zákazníci používající server webových služeb EGJE
* spuštění Tomcat a AS EGJE

V rámci instalace se generuje WAR balíček webové aplikace. V závislosti na instalované verzi Tomcatu (9.0.x nebo 10.1.x) je nutné pomocí utilitky Configurátor správně nastavit, na kterou verzi se má webová aplikace nainstalovat. Současně je potřeba stáhnout odpovídající distribuční sadu pro vybranou verzi Tomcatu, protože v opačném případě se WAR balíček nevytvoří.

Poznámka: upozorňujeme, že Tomcat Manager neumí běžící aplikaci EGJEWEB2 korektně odinstalovat (neboť ji neumí úplně zastavit). Tomcat manager je tedy možné použít jen pro první instalaci aplikace, resp. je nutné po instalaci pomocí manageru tomcat restartovat.

* 1. **Vlastní instalace utility**

Instalaci SuperConfiguratoru provádí pracovník Elanor. Skládá se z částí:

* Výběr serveru a adresáře se souborovými přístupy k aplikacím
* Úprava dávky SuperConfigurator v tomto novém adresáři, nahrání aktuálních eman.jar, egjelib.jar
* Vytvoření souboru egje\_instalace.txt.   
  Obsahuje seznam souborových cest k config\_egje.jar souborům.  
  Uvedeme-li odkaz na config klienta AS, je tato instalace v SuperConfiguratoru zobrazována na záložce Monitor Serverů.   
  A naopak, uvedeme-li odkaz na config std.klienta bez AS, nebo vlastní AS (tj. config s DB připojením) je poté zobrazován na záložce Instalace a umožňuje přes toto připojení instalovat patche/výdeje (část změnový skript).

Pro monitorování web aplikace je potřeba uvést její http adresu.

Přepokladem je cesta na program java. U OS Windows jde o java.exe, který standardní instalace java JRE nahrává do Windows\System32/ SysWOW64 adresáře.

Od verze 8 pak do \ProgramData\Oracle\Java\javapath.

Resp. je potřeba mít v Proměnné prostředí / Path nastavenou cestu do adresáře *javaJRE*\bin resp. *javaJDK*\bin.Spouštěnou verzi java zjistíte z příkazového řádku OS, příkazem java -version.

* + 1. **SuperConfigurator - restrikce spuštění pomocí Adm51**

Na úrovni databáze umožňujeme správci pomocí 3 položek v Adm51/Znovuověření přihlášení omezit funkce SuperConfiguratoru na konkrétní db :

Možnost provést zm. skript pomocí SuperConfiguratoru

Povolit export číselníků pomocí SuperConfiguratoru

Výčet IP adres pro přístup do SuperConfiguratoru

Je to proto, že tato správcovská utilita nepodléhá EGJE autentizaci a správce může chtít např. omezit její použití jen na určité IP adresy.

První 2 parametry jsou typu Ano/Ne a umožňují nastavit omezení na konkrétní činnost, zatímco poslední parametr umožňuje omezit, odkud se smí utilita volat.

U omezení činnosti je tlačítko pro spuštění skriptu resp. exportu nepřístupné, u omezení na IP adresu má celý řádek (tj. databáze) ve sloupci Verze aplikace text "Neplatná IP adresa".

Implicitně je funkčnost SuperConfiguratoru povolena.

* + 1. **Spuštění SuperConfiguratoru bez parametru**

SuperConfigurator je primárně určen pro spouštění s parametrem, kterým je textový soubor s výčtem konfigurací.

Při spuštění bez parametru, má následující funkčnost.

Typickým spuštěním bez parametru je dávka SuperConfigurator.bat spuštěná přímo z instalačního adresáře výdejové verze (z patche nikoliv, ten obvykle neobsahuje egjelib.jar).

Utilita jednak vede uživatele k vytvoření tohoto konfiguračního souboru (egje\_instalace.txt), a také umožňuje interaktivní povýšení war souboru egjeweb

Funkčnost utility:

* Sestavit soubor s instalacemi (egje\_instalace.txt)
* Vybrat již vytvořený soubor s instalacemi - ten si pak pamatuje při příštím spuštění (ukládání v OS home uživatele)
* Povýšení war souboru egjeweb - záložka "Příprava EGJEWEB.war"  
  také zde je uplatněno "chytré" vyplňování a předvyplňování parametrů
  1. **Další funkčnost**
* Monitorování
  + monitorování běhu AS
    - v egje\_instalace.txt musí být odkaz na klientský config\_egje.jar soubor, protože v něm je konfigurace rmi připojení k serveru.
  + monitorování běhu EGJEWEB
    - v egje\_instalace.txt musí být odkaz na web aplikaci *http(s)\_adresa\_web\_aplikace*
* Export číselníků (3 záložky)

Princip je ten, že export vytvoří změnový skript.

Ten je podepsán, aby jej nebylo možné měnit.

Skript pak uživatel může pustit na jiné db (jiných db), typicky pomocí této utility - záložka Spuštění změn.skriptu.

Jednotlivé datové oblasti

Složky mezd (Slm01)

Vytvoří skript z celého číselníku nebo z výčtu SLM (oddělených čárkou)

Volitelně export obsahuje i atributy SLM týkající se docházky

Při volbě celého číselníku před nahráním dosavadní, k dnešnímu datu platné SLM, ukončí (k období 2000-01) a nastaví u nich Možno pořizovat ve vstupech = Ne

Započitatelnosti SLM

Také buď pro všechny, nebo jen pro některé započitatelnosti. Ty pak před nahráváním do jiné db napřed promazává.

Na závěr spouští plošnou aktualizaci Zařazení SLM na základě zařazení IA (Slm02 - tlačítko Proveď aktualizaci)

Transformace do účetnictví (Uct01)

Obsahuje též export započitatelnosti UCTO

Před nahráním smaže dosavadní účetní tabulku a smaže dosavadní obsah započitatelnosti UCTO.

Číselník mzdových tarifů (Cmt01)

Před nahrání smaže minulý obsah Tarifů v tabulkách, Seznamu tabulek, Dalšího rozčlenění a Tarifních stupnic.

Tarifní stupně jsou ponechány, nové stupně přidávány / přepisovány na základě shody položky Tarifní stupeň.

Archiv je ponechán.

Číselník struktur (Str01)

Všechny nebo vybrané typy.

K dnešnímu dni platné prvky struktur jsou před nahráním ukončeny k datu 1.1.2000. Vazby mezi v jednom exportu vybranými typy jsou smazány a poté jsou nahrány nové.   
Export import se tedy hodí spíš pro počáteční naplnění resp. pro ty zákazníky, kterým postačuje automatické udržování historie ve mzdových archivech (Str05)

Dále jsou přenášena data ze záložek Použití struktury a Jméno struktury a jejích hladin.

Data záložky Vazby mezi strukturami jsou přenášena s omezením na ty, které jsou mezi typy přenášenými v jednom exportu.

Export rozlišuje záznamy i pomocí označení organizace. Pokud je unikátní kód číselníku v rámci databáze (Adm31/Další konf.), je možné, že export/import z jednoho prostředí ohlásí chybu při změně organizace u záznamu v jednom z prostředí. V tom případě je třeba před importem z cílového prostředí takový záznam smazat a import opakovat.

Jednopoložkové číselníky (Jpc01)

Všechny nebo vybrané typy. Ty pak před nahráváním do jiné db napřed promazává.

Role (zákaznické, nad 500)

Před nahrání smaže minulý obsah přenášených rolí, dosavadní role, které přenášeny nejsou, nejsou nijak měněny ani mazány.

Chybové hlášky - nastavení jejich důležitosti

Při volbě "všechny" potom v cílové db dosavadní nastavení nejprve smaže, jinak přepisuje vybrané.

Dávky sestav

Vždy, i při volbě "všechny" pouze přepisuje dávky se shodným kódem.

Kalendáře

Exportuje vzorové dny, vzorové úseky, limity kontrol, typy zaokrouhlení a vlastní kalendáře.

Vždy, i při volbě "všechny", pouze přidává do cílových číselníků resp. přepisuje záznamy se shodným kódem.

Více o exportu struktur

Tento export je primárně určen pro prvotní naplnění databáze

Lze jej ale použít i během užívání systému. Struktury si lze přenést na testovací prostředí, upravit a přenést zpět.

Export z důvodů uplatnitelnosti a dohledatelnosti vazeb přenáší vazby pouze mezi těmi strukturami, které se exportu účastní.

Také zařazení Osob/PV ani jiných kmenových přiřazení přenášeno není.

Vše je dobré si důkladně vyzkoušet ve směru Ostrá => Testovací databáze.

Startovní exporty (záložka Exporty číselníků III.)

Startovní export ORG, SJ, SO, Skupin práv, Profilů – obsahuje checkboxy:

- rozšířit o všechny struktury s jejich rozšiř.tab.

- rozšířit o slm a konfiguraci DOCH (vč. SLM, Kal.)

- rozšířit o bank. cesty

Řada číselníků je vázána na struktur organizací, SJ a SO (Adm21-Adm23).

Proto i dosavadní export struktur z první záložky Export číselníků je řešen tak, aby co možná nejvíce umožnil přenos struktur mezi úplně jinými databázemi, přenáší tedy jen jejich základní kostru.

Tento export je určen pro přenos mezi Testovacím (vývojovým) a Produkčním prostředím, hlavně v začátcích implementace. Naší snahou je přenést z uvedených konfiguračních číselníků, co možná nejvíce.

# Výčet povolených formátů pro nahrání do systému

Tyto formáty jsou z bezpečnostních důvodů povoleným výčtem formátů, které lze nahrát do systému:

* docx, doc, rtf, pdf, txt, odt, xlsx, xls, xlsm, ods, xml, jpg, jpeg, png, gif, tif, tiff, pfx, cfd

**Příloha A1. Instalace verze Oracle**

Instalaci EGJE do db provádí pracovník Elanor podle interní metodiky.

Při instalaci je se prochází zhruba tímto postupem:

* verze databáze, patche
* unicode kódová stránka databázové instance (standardní znaky a NCHAR znaky)
* komponenta XML\_DB
* velikost bloku (db\_block\_size) minimálně 8192.
* inicializační parametr open\_cursors nastavit na minimálně 1000
* role EMANOWNER
* ostrá a testovací db formou vlastníka nebo formou samostatné instance
* vlastník objektů versus uživatel pro připojení aplikací
* vlastník objektů vytváří context
* uživatel pro připojení aplikací vlastní trigger after logon
* import
  + řešení položek LOB při importu do jiného tablespace
* objekty znovuvytvářené po importu
  + role EMANUSER\_xxx   
    (pomocí procedury ce\_crea\_role spuštěné vlastníkem objektů)
* nastavení úlohy pro aktualizaci statistik (Adm51/Oracle statistiky/Vytvořit-Obnovit job na aktualizaci statistik)  
  preferujeme tuto úlohu před jiným nastavením sběru statistik na úrovni db

**Příloha A2. Instalace verze MS SQL**

Při instalaci se prochází zhruba tímto postupem:

* verze databáze
* kódová stránka, třídění
* autentizace SQL server
* nested triggers
* vytvoření databází (ostrá a testovací)
* vytvoření loginů a uživatelů
* struktura a data

Doporučujeme databázi přepnout do režimu read\_committed\_snapshot on

Databáze pak používá verzování řádků v TEMPDB a nepoužívá tolik zamykání, což je častý problém MS SQL instalací, kdy ve standardním režimu, pokud někdo do dat zapisuje, brání tím ostatním uživatelům ve čtení. Tedy nejčastěji pokud někdo ještě počítá, uzavírá a jiný už chce z této datové oblasti tvořit výstupy, bývá často blokován hláškami o zamčených datech.

Od 8.10.2015 jsme tak nastavili i naši vzorovou db.

Starší instalace, které nastavení nemají, jej mohou nastavit skriptem:

use [master]

go

alter database <DB EGJE> set single\_user with rollback immediate;

go

alter database <DB EGJE> set multi\_user;

go

alter database <DB EGJE> set read\_committed\_snapshot on with no\_wait

go

Skript je nutno pustit v SQL Server Management Studiu pod SQL administrátorem. Před spuštěním se musí ve skriptu nahradit text <DB EGJE> skutečným názvem databáze EGJE na Vašem SQL serveru. Skript provede odpojení všech spojení na danou DB, takže není vhodné jej spouštět, pokud bude DB EGJE aktivně využívána.

**Příloha B. Instalace programového vybavení (std. klient)**

Instalaci programového vybavení EGJE provádí pracovník Elanor podle interní metodiky.

Základní body jsou následující:

* volba serveru
  + intranetový web server (doporučeno)
  + souborový server
* volba rozvržení vztahu aplikace - databáze

standardní rozvržení je toto:



**Instalace předlohy pro spouštění std. klienta pomocí EWS**

Systém EWS - EGJE Web Start je vydáván jako samostatná distribuce a jeho funkčnost je popsána v dokumentu „EWS – dokumentace.pdf“ v distribuční sadě EWS.

1. Vytvoření adresářové struktury z interního instalačního média Elanor (verze\_spec/1inst)

(obvykle do dvou adresářů pro ostrou a pro testovací verzi)

2. Konfigurace web serveru - zpřístupnit v každé verzi adresář egje (pod názvem evokujícím ostrou a testovací verzi)

3. Editace všech EGJE souborů pro EGJEweb start

Vytvoření spouštěcího .egje souboru pro ostré a testovací prostředí.

Zkopírujte a upravte vzorový soubor EWS\egjevzor.egje

Obvykle stačí nastavit správnou <jnlp codebase=

a zvážit hodnotu max-heap-size= (cca 550m - 1000m)

a rozhodnout se, zdali uživatelů generovat ikony (plocha, resp. menu Start).

4. Spuštění konfiguračního programu pro vyplnění připojení k db

a) configurator\_egje.bat

Http / file adresa pro distribuční složku - kontrola parametru již nastaveného do codebase=,

editace parametrů (připojení k AS resp. k db, autentizace)

5. Editace linků na egje soubor v default.htm, resp. jejich umístění na intranet - zdůraznit ostrou a testovací verzi.

(nebo zástupce u souborového serveru)

Tím je předloha hotova.

Na uživatelských PC správce spustí EWS\EgjeWS-1.0.4.msi (akt. verzi) a tím instaluje spouštěcí runtime egje (registrace přípony egje a instalace vlastního ews programu, který aplikaci stahuje, aktualizuje a spouští).

**Instalace - přímé a dávkové spouštění std. klienta EGJE**

EGJE lze spouštět buď přímo pomocí java/javaw nebo pomocí dávkového souboru.

Toto je zvlášť výhodné pro terminálové instalace (typicky Citrix)

Přímé spouštění :

* př. zástupce resp. citrix exportované aplikace  
  "C:\WINDOWS\system32\javaw.exe" -splash:elanor.jpg –Xmx512m -Djava.library.path=./egjelib -cp egjelib/eman.jar;egjelib/egjelib.jar cz.elanor.eman.sgui.navig.RunGui   
   -Cconfig\_jar=egjelib/config\_egje.jar  
  přičemž „Kde začít“ je v adresáři EGJE na sdíleném disku  
  Pozn.: místo C:\WINDOWS\system32\javaw.exe může být volána javaw.exe z rozbaleného java.zip (viz dále java11)
* pokud chcete přidat ještě spouštěcí parametry, přijdou na konec (za config\_egje.jar)   
  Př.:  
  -CLaF="jGoodies Plastic3D font +2" -f Dca02

Podporujeme též spouštění klienta EGJE pomocí dávkového souboru. Vzorovým dávkovým spouštěcím souborem je configuratorsample\_egjew.bat:

*start javaw -splash:elanor.jpg -Xmx800m -Djava.library.path=./egjelib -cp egjelib/eman.jar;egjelib/egjelib.jar cz.elanor.eman.sgui.navig.RunGui -Cconfig\_jar=egjelib/config\_egje.jar*

*exit*

V obou případech je u instalací, kde je konfiguračních souborů více (klient, AS, EGJEWEB), zapotřebí upravit dávku/příkaz tak, aby ukazovala na ten správný config\_egje\*.jar (parametr -Cconfig).

Pozn. Parametry před cz.elanor.eman.sgui.navig.RunGui jsou považovány za parametry pro JVM, parametry za cz.elanor.eman.sgui.navig.RunGui jsou parametry aplikace. Pro správnou funkčnost musí být java.library.path nastaven jako parametr JVM.

Parametr -ea má smysl nastavovat pouze v testovacím prostředí, v produkčním by neměl být nastaven.

Od e201611 je součástí instalačního adresáře verze také podadresář "launcher". Jde o třetí způsob jak EGJE java klienta na OS Windows spouštět. Jde o dávkové spouštění skládající se ze 2 fází - první je kontrola a nahrání na lokální disk (domovský adresář uživatele ".javacache" ), druhá je vlastní spuštění z lokální cache, tedy podobný princip jako java web start, ale pouze z namapovaného disku. Více je v launcher\launcher\_popis.txt.

Může být důležité v dávce nastavit proxy (např. pro Adm24 Kurzy), viz kap. 3.3

Pro **vzhled JGoodies** a při spuštění přes **JAVA 17** se projevil problém s těmito vzhledy. Pokud tedy klient chce tyto vzhledy využívat je nutné přidat parametr do spouštěcího souboru:

**--add-exports=java.desktop/com.sun.java.swing.plaf.windows=ALL-UNNAMED**

**To samé se musí přidat do dávkového soboru, při spouštění přes dávkový soubor.**

**java 9, 11:** Při spouštění dávkou / příkazem / launcherem je třeba některé parametry také doplnit (jako parametry spouštěného programu java (javaw), před dosavadní -D):

**-XX:+IgnoreUnrecognizedVMOptions --add-modules=java.xml.bind --illegal-access=permit**

kde první parametr je použit pro případ, kdy část uživatelů spouští přes javu 8 a část přes javu 9, 11.

**java 11 a používání html editorů v EGJE:**

Html editor používají ti, kteří mají nastaveno Ano v   
 Adm21/Par.komun/ *HTML editory pro Wflow, Mail:*, resp. *HTML editory pro Popisy:*  
Html editor však není součástí java 11 ale java FX.

Místo OpenJDK 11 pak, správce rozbalí na serveru java.zip, který je o html editor z java FX doplněn a ve spouštěcím příkazu spustí javaw z tohoto adresáře.

**Java 11.0.20 a 17.0.8 a vyšší:**

Pro tyto Javy je potřeba zvětšit velikost očekávaného MANIFEST.MF který je součástí eman.jar. Velikost se zvedne přidáním JVM parametru do dávkového souboru:

-Djdk.jar.maxSignatureFileSize=16000000

**Instalace - možnost společného programového vybavení pro více databází**

EGJE je také možné používat v režimu jedné instalace programového vybavení použité vůči více databázím.

Struktura vzoru je v interním instalačním vzoru Elanor v souboru vzorMultiDB.zip. Jde o instalaci, kdy jedno programové vybavení standardního klienta egje je používáno pro více databází.

Instalaci tohoto typu je vhodné realizovat v koordinaci s pracovníky Elanor provádějícími instalaci systému.

**Instalace - možnost spouštění standardního klienta**

* **look&feel (skin) při spuštění standardního klienta.**

Správce aplikace může nastavit vzhled aplikace platný pro všechny uživatele. Této možnosti může využít např. k odlišení testovacího prostředí od ostrého.

Nastavená hodnota má přednost před uživatelským nastavením v okně Změna vzhledu.

Realizuje se to nastavením systémové proměnné LaF

Př. -CLaF="jGoodies Windows font +1" pro bat resp. pro JNLP (do elementu application-desc):

<argument><![CDATA[-CLaF=Tiny Look&Feel - Golden]]></argument>

Možnosti:

|  |
| --- |
| **Hodnota parametru LaF** |
| Windows |
| Windows +1 |
| Windows +2 |
| Windows +3 |
| Metal |
| Motif |
| jGoodies Windows |
| jGoodies Windows font +1 |
| jGoodies Windows font +2 |
| jGoodies Windows font +3 |
| jGoodies Plastic3D |
| jGoodies Plastic3D font +1 |
| jGoodies Plastic3D font +2 |
| jGoodies Plastic3D font +3 |
| jGoodies Plastic |
| jGoodies PlasticXP |
| Nimbus |
| Nimbus font +1 |
| Nimbus font +2 |
| Nimbus font +3 |
| Nimbus font +4 |
| Tiny Look&Feel - Golden |
| Tiny Look&Feel - Silver |
| Tiny Look&Feel - Plastic |
| Tiny Look&Feel - Forest |
| Tiny Look&Feel - Nightly |
| Tiny Look&Feel - Unicode |
| Tiny Look&Feel - Unicode font +1 |
| Tiny Look&Feel - Unicode font +2 |
| Tiny Look&Feel - Unicode font +3 |
| Tiny Look&Feel - Golden - old ico |
| Tiny Look&Feel - Plastic - old ico |
| jGoodies Plastic3D - new ico |
| jGoodies Plastic3D font +1 - new ico |
| jGoodies Plastic3D font +2 - new ico |
| jGoodies Plastic3D font +3 - new ico |

Další parametry

Všechny parametry Nastavení / Lokální nastavení je možné nastavit pomocí parametrů spouštění. I v tomto případě má takto správcem nastavený parametr přednost a uživatel jej nemůže měnit. Výjimkou jsou parametry s adresářovou cestou, v případě, že tato není na PC uživatele platná, uživatel ji může změnit.

Parametry:

s hodnotou cesty, adresáře:

-Cacrobat - PDF prohlížeč

-CviewerRtf - RTF, DOCX, ODT prohlížeč

-CviewerXls - XLS prohlížeč

-CviewerTxt - TXT prohlížeč

-CviewerHtml - HTML prohlížeč

-Cireport - JasperSoft Studio editor

-Cxmleditor - XML editor

-CadresarProExport - Adresář pro export

s výčtem hodnot:

-CExpForm - formát exportů - povoleny jsou csv, xlsx, xls, (ignoruje velikost písmen, pokud je vyplněn špatně vrátí xls)

s hodnotami true/false:

-CCloEgje - zavřít egje bez dotazu

-CSmDirCle - chytré promazání adresáře

-CCretSubDir - vytváření podadresáře dle organizace

-CRelGrFr - přenačtení dat při návratu na formulář

Poznámka:

Parametry lokálního nastavení zadávané v aplikaci jsou ukládány do souboru

%USERPROFILE%\.eman\config\_local\_user.properties

Správce by měl mít v patrnosti, že při přesunu účtu uživatele v tomto souboru nemusí být platný parametr adresarProExport a některé další.

**Příloha C1. Instalace EGJEWeb2**

**Postup:**

Instalace java (OpenJDK, Oracle SE Subscription JDK).

Instalace Tomcat 9.0.x a 10.1.x na server (Windows resp. Linux).

Pro verzi Tomcat 9.0.x doporučujeme použít minimální verzi 9.0.102, pro verzi Tomcat 10.1.x pak minimální verzi 10.1.40.

Je-li Tomcat na OS linux, je vhodné do jeho spouštění přidat parametr

-Dfile.encoding=Cp1250

Nejvhodnější místo je soubor setenv.sh

(jinak je obvykle problém s diakritikou serverových protokolů)

Na OS windows bývá tato kódová stránka nastavena přímo v OS, pokud není a je Tomcat instalován jako služba, je třeba Cp1250 nastavit jako její parametr (tomcat properties / Java / Java Options)

V případě chybného kódování textů (např. měsíce v datumových editorech) je třeba (obvykle na OS Windows) nastavit v základním web.xml v defalt servletu, tj. v

<servlet>

<servlet-name>default</servlet-name>

parametr

<init-param>

<param-name>fileEncoding</param-name>

<param-value>UTF-8</param-value>

</init-param>

Konfigurace paměti pro Tomcat:

(parametry pro Maximální memory pool - Xmx

windows v panelu Java např.:

java options pouze kódová stránka

Initial memory pool 768 MB

Maximum memory pool 2560 MB)

Konfigurace https komunikace.

Konfigurace max. velikosti souboru pro upload aplikace přes Tomcat-manager

soubor /webapps/manager/WEB-INF/web.xml   
 parametr <max-file-size> na minimálně 300 MB tj. 307200

<max-request-size> dtto

Aplikace EGJEWeb2:

1. Vytvoření aplikace pro Tomcat:

Pomocí utility configurator\_egje(\_en), která je na instalačním médiu v adresáři configurator si připravíte config\_egje.jar pro EGJEWeb2 aplikaci.

Můžete také využít již vytvořený soubor pro java klienta (AS) a pouze v něm udělat úpravy.

Pro Tomcat 10.1.x je zapotřebí v configuratoru na záložce „Instalace verze, patche“ zapotřebí nastavit „Instalovat na Tomcat 10: Ano“.

Vzniklý soubor config\_egje.jar umístíte na server s Tomcat tak, aby na něj běžící Tomcat měl přístup.

1. Spustíte z instalačního adresáře SuperConfigurator

Zvolíte poslední záložku "Příprava EGJEWEB2(HR Portál).war"

a na ní přepnete na "První instalace" a vyplníte cestu ke config\_egje.jar (cestu vyplníte z pohledu serveru Tomcat)

Do pole "War souboru uložit do (bez cesty - akt.složka)" vyplníte cílové jméno aplikace (obvykle se v názvu zohledňuje prostředí - produkční versus testovací)

Stisknete "Proveď update EGJEWEB2\*.war souboru" , což vytvoří požadovanou Tomcat aplikaci s vestavěným odkazem na konfigurační soubor (WEB-INF/web.xml)

Pozn. alternativou ke grafickému prostředí SuperConfigurator  
je dávkový soubor, který vytvoříte z předlohy buildEgjeweb2Example.bat(sh) popřípadě pro Tomcat 10.0.x buildEgjeweb2Example\_tc10.bat(sh), ve kterém upravíte

* + - jméno cílového war souboru
    - cestu k config\_egje.jar z pohledu Tomcat

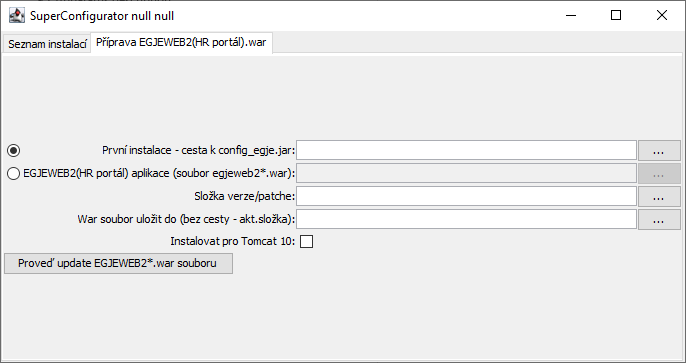
2a. Při aktualizaci již nainstalované aplikace je nutné, v závislosti na používané verzi Tomcatu, případně zaškrtnout volbu „Instalovat pro Tomcat 10:“

3a. Pokud máte k instalačnímu prostředí (ve kterém Vám nyní běží SuperConfigurator) připojený i svazek s Tomcat, je možné do " War souboru uložit do" dávat přímo cestu do Tomcat/webapps. Pokud to takto uděláte, musí být bezpodmínečně v okamžiku, kdy provádíte akci "Proveď update EGJEWEB2\*.war souboru", Tomcat vypnutý!

3b. Pokud svazek přístupný nemáte, vytvoříte war soubor a provedete jeho instalaci na Tomcat (Tomcat manager deploy).

Pokud instalujete kopírováním, musí být tomcat vypnutý a před nakopírováním war souboru je nutné smazat podadresář se jménem Tomcat aplikace (ve webapps . V opačném případě budete spouštět mix současné a minulé aplikace!

Poznámka: upozorňujeme, že Tomcat Manager neumí běžící aplikaci EGJEWEB2 korektně odinstalovat (neboť ji neumí úplně zastavit). Tomcat manager je tedy možné použít jen pro první instalaci aplikace, resp. je nutné po instalaci pomocí manageru tomcat restartovat.



Technické poznámky pro ruční konfiguraci a instalaci:

* + celá aplikace pro Tomcat 9 je v balíku egjeweb2.war
  + celá aplikace pro Tomcat 10 e v balíku egjeweb2\_tc10.war
  + každý balík se z ESP stahuje zvlášť
  + WAR balíčky nejsou kompatibilní s jinými verzemi Tomcatu, než pro které byly vytvořeny
  + extrakce web.xml z egjeweb2.war\WEB-INF\web.xml
  + editace web.xml
    - přidání/konfigurace parametrů „config\_jar“,který je odkazem na serverový konfigurační soubor EGJE (spravovaný pomocí Configurator)
    - konfigurace parametru „<display-name>“ - umožňuje pojmenování aplikace viditelné v Tomcat
  + návrat souboru web.xml do egjeweb2.war\WEB-INF\web.xml
  + případné přejmenování egjeweb2.war (zvláště, je-li více egje web aplikací na jednom serveru)
  + deploy aplikace na servlet kontejner Tomcat (viz bod 3b)

Důležité upozornění: nikdy nekopírujte celý web.xml ze staré aplikace do nově instalované! Soubor web.xml může být jiný a na rozdíl se přijde poměrně obtížně, neboť typicky nefunguje pouze část aplikace.

Linux servery "headless"

* V této konfiguraci je problém s exporty dat z formuláře, resp. exportních sestav typu java do excelu. V případě problémů s touto funkcionalitou zkuste nastavit systémovou java proměnnou

java.awt.headless=true

Typicky se to provádí ve skriptu setenv.sh

### Rozdíly v instalaci Tomcat 9 a Tomcat 10

V rámci distribuce EGJE jsou pro řady Tomcat 9 a 10 vydávány specifické WAR balíčky. Důvodem je přechod z Java EE na Jakarta EE. Pro každý Tomcat je nutné stáhnout samostatný ZIP soubor, který se rozbalí do stejné složky s distribuční sadou EGJE. V distribuční sadě se nachází soubor egjeweb2.war pro Tomcat 9 a egjeweb2\_tc10.war pro Tomcat 10. Ke každému balíčku existuje také skript pro manuální instalaci: buildEgjeweb2Example.bat (.sh) a buildEgjeweb2Example\_tc10.bat (.sh).

**Konfigurace v utilitě Configurátor:**

Pokud má aplikace běžet na Tomcatu 10, je třeba v utilitě Configurátor na záložce „Instalace verze, patche“ zaškrtnout možnost „Instalovat na Tomcat 10: Ano“.

**Instalace pomocí utility SuperConfigurator:**

Chování utility SuperConfigurator se liší v závislosti na způsobu použití:

* **Spuštění bez souboru se seznamem instalací:**
  + V tomto případě je k dispozici záložka „Příprava EGJEWEB2 (HR portál).war“.
  + Pro „První instalaci“ je nutné zadat cestu ke konfiguračnímu souboru, který určuje, zda se má použít balíček pro Tomcat 9, nebo 10.
  + Při volbě možnosti „EGJEWEB2 (HR portál) aplikace…“ se konfigurační soubor nezadává a v případě potřeby je nutné zaškrtnout políčko „Instalovat pro Tomcat 10“.
* **Spuštění se souborem se seznamem instalací a přímou instalací pro vybraná prostředí:**
  + Výběr balíčku pro Tomcat se řídí nastavením v konfiguračním souboru.
  + V tomto okně je také možné otevřít configurator pro dané prostředí a provést další nastavení.

### Tomcat a SSL/TLS

Někdo sice provozuje v interní síti tomcat přímo pod http protokolem, nicméně bývá obvyklé opatřit Tomcat certifikátem a používat provoz přes https.

Popis je například na stránkách tomcat: <https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html>

Protokol http na konkrétním portu je pak možné v server.xml zakázat, nebo jej lze přesměrovat na https. To se může dělat buď pomocí tomcat nebo pomocí reverzního proxy.

Pomocí tomcat se to udělá tak, že se v server xml definuje Connector s redirect (např. 8080 na 8443) a poté se do globálního web.xml přidá za všechna servletová mapování odstavec, který vlastní přesměrování dělá.

Typicky:

<security-constraint>

<web-resource-collection>

<web-resource-name>Restricted URLs</web-resource-name>

<url-pattern>/\*</url-pattern>

</web-resource-collection>

<user-data-constraint>

<transport-guarantee>CONFIDENTIAL</transport-guarantee>

</user-data-constraint>

</security-constraint>

Pozn.: Nepodporujeme variantu přidávání tohoto přesměrování do web.xml aplikace.

### Tomcat a cookie - atribut SameSite

Pro Tomcat lze nastavit, aby všem cookies nastavoval atribut SameSite. Více o hodnotách atributu naleznete na <https://tomcat.apache.org/tomcat-9.0-doc/config/cookie-processor.html>

Samotné nastavení se provede ve složce Tomcatu /conf a souboru context.xml přidáním následujícího řádku mezi elementy <Context> a </Context>:

*<CookieProcessor className=“org.apache.tomcat.util.http.Rfc6265CookieProcessor“ sameSiteCookies=“lax“ />*

Doporučujeme nastavit hodnotu na **lax.**

Nastavení atributu SameSite je možné až od verzí Tomcatu 9.0.21.

**Provoz EGJEWeb2 přes loadbalancer**

Loadbalancer není součástí dodávky EGJE. V zásadě se mu ale nebráníme a u některých zákazníků jej mají nastavený.

V konfiguraci loadbalanceru nutné zohlednit několik požadavků

1. nastavení správné cesty u cookie JSESSIONID,

viz direktiva ProxyPassReverseCookiePath

2. nastavení správné cesty u hlavičky X-GWT-Module-Base:

nejjednodušší způsob řešení je nastavení stejného relativního URL na loadbalanceru jako na jednotlivých web serverech.

viz. diskuse na https://groups.google.com/forum/#!topic/google-web-toolkit/y0W90PgoVns a https://groups.google.com/forum/?fromgroups#!searchin/google-web-toolkit/proxypass$20serialization/google-web-toolkit/3wE9yWLMJo4/Mebd0XgW1EIJ

3. svázání klienta s webserverem, na kterém je jeho session

to je možné realizovat několika způsoby, vyzkoušeli jsme variantu řídící se hodnotou cookie ROUTEID

Interně jsme otestovali loadbalancer Apache httpd 2.4

V konfiguraci byly povoleny následující moduly

LoadModule headers\_module modules/mod\_headers.so

LoadModule lbmethod\_bybusyness\_module modules/mod\_lbmethod\_bybusyness.so

LoadModule lbmethod\_byrequests\_module modules/mod\_lbmethod\_byrequests.so

LoadModule lbmethod\_bytraffic\_module modules/mod\_lbmethod\_bytraffic.so

LoadModule lbmethod\_heartbeat\_module modules/mod\_lbmethod\_heartbeat.so

LoadModule proxy\_module modules/mod\_proxy.so

LoadModule proxy\_balancer\_module modules/mod\_proxy\_balancer.so

LoadModule proxy\_http\_module modules/mod\_proxy\_http.so

LoadModule slotmem\_shm\_module modules/mod\_slotmem\_shm.so

Celá konfigurace loadbalancingu

<Proxy "balancer://mycluster">

BalancerMember "http://xxxsrv:8090/egjeweb2" route=xxxsrv

BalancerMember "http://xxxsrv2:8080/egjeweb2" route=xxxsrv2

ProxySet stickysession=ROUTEID

</Proxy>

<Location /egjeweb2 >

Header always add Set-Cookie "ROUTEID=.%{BALANCER\_WORKER\_ROUTE}e; path=/" env=BALANCER\_ROUTE\_CHANGED

ProxyPass balancer://mycluster

ProxyPassReverse balancer://mycluster

ProxyPassReverseCookiePath / /egjeweb2/

</Location>

**Bezpečnostní filtr**

Do aplikace je integrován bezpečnostní filtr Tomcat HTTP Header Security Filter.

Aplikační web.xml obsahuje mj. tyto zabezpečovací prvky:

- zákaz HTTP metod OPTIONS a TRACE

- nastavování HSTS hlaviček v případě přístupu přes SSL (filtr httpHeaderSecurity)

**HSTS filtr má tyto konfigurační parametry** (config\_local.properties)

z dokumentace filtru vypisujeme**:**

egjeweb.httpHeaderSecurity.blockContentTypeSniffingEnabled

Should the header that blocks content type sniffing (X-Content-Type-Options) be set on every response. If already present, the header will be replaced. If not specified, the default value of false will be used.

egjeweb.httpHeaderSecurity.xssProtectionEnabled

Should the header that enables the browser's cross-site scripting filter protection (X-XSS-Protection: 1; mode=block) be set on every response. If already present, the header will be replaced. If not specified, the default value of true will be used.

egjeweb.httpHeaderSecurity.hstsEnabled

Will an HTTP Strict Transport Security (HSTS) header (Strict-Transport-Security) be set on the response for secure requests. Any HSTS header already present will be replaced. See RFC 6797 for further details of HSTS. If not specified, the default value of true will be used.

egjeweb.httpHeaderSecurity.hstsMaxAgeSeconds

The max age value that should be used in the HSTS header. Negative values will be treated as zero. If not specified, the default value of 0 will be used.

egjeweb.httpHeaderSecurity.hstsIncludeSubDomains

Should the includeSubDomains parameter be included in the HSTS header. If not specified, the default value of false will be used.

egjeweb.httpHeaderSecurity.hstsPreload

Should the preload parameter be included in the HSTS header. If not specified, the default value of false will be used. See https://hstspreload.org for important information about this parameter.

egjeweb.httpHeaderSecurity.antiClickJackingEnabled

Should the anti click-jacking header (X-Frame-Options) be set on the response. Any anti click-jacking header already present will be replaced. If not specified, the default value of true will be used.

**Nastavení hlaviček Apache httpd (Apache Hypertext Transfer Protocol Server)**

Aplikace EGJE nefunguje korektně v prohlížečích Chrome a MS EDGE pro následující nastavení hlaviček v Apache server:

* Header set Feature-Policy s parametrem sync-xhr ‘none‘ – doporučujeme tento parametr do hlavičky nevyplňovat.
* Header always set X-Frame-Options ’DENY‘ - doporučujeme hodnotu parametru místo DENY nastavit na SAMEORIGIN.

**Příloha D. Instalace Aplikačního serveru EGJE**

**Postup:**

**AS se instaluje jako služba realizovaná wrapperem na server s OS Windows nebo Linux/Unix. Na serveru je musí být nainstalována shodná verze prostředí java jako na klientské stanici**

**(Pro monitorování pomocí jvisualvm je potřeba jej instalovat - https://visualvm.github.io/).**

**Pozn.: Od e201905 může být AS spuštěn také pod tomcat / EGJEWeb2 (nastavení v Configurator viz 6.1.2 Režim Web server)**

**Spouštění, zastavení, restart AS je pak společné s web aplikací, tzn. Tomcat manager Reload tedy provede reload EGJEWeb2 i AS.**

**Server je popsán v souboru wrapper.conf:**

# Java Application

wrapper.java.command=java

#resp. je možná i konkrétní cesta k java do příslušného JRE

wrapper.java.classpath.1=../lib/wrapper.jar

wrapper.java.classpath.2=../lib/eman.jar

wrapper.java.classpath.3=../lib/egjelib.jar

wrapper.app.parameter.1=cz.elanor.eman.sgui.navig.RunServer

wrapper.app.parameter.2=-Cconfig\_jar=../lib/config\_egjeas.jar

wrapper.console.title=EGJEAS EMANEVMA

# Maximum Java Heap Size (in MB)

# pamatujte, že kromě této paměti je potřeba počítat s pamětí PermgenSpace

# a s pamětí pro operační systém. Jinak se Vám bude zdát, že AS zatuhává

wrapper.java.maxmemory=1024

#doporučené omezení log souboru

wrapper.logfile.maxsize=10m

wrapper.logfile.maxfiles=30

pro windows

# Name of the service

wrapper.ntservice.name=EGJEAS\_EMANEVMA

# Name of the service

wrapper.ntservice.name=EGJEAS\_EMANEVMA

# Display name of the service

wrapper.ntservice.displayname=EgjeAS EMANEVMA

pro linux je potřeba přidat

wrapper.java.additional.1=-Dfile.encoding=Cp1250

add wrapper.app.parameter.2=-Cconfig\_jar=../lib/config\_egjeas.jar

na tento souboru je zapotřebí mít nastavený configurator.bat a je zapotřebí v něm vyplnit potřebné údaje, hlavně db připojení a autentizaci.

Pokud chce správce vytvořit/použít wrapper.conf bez odkazu na config\*jar

je možné klíčové hodnoty z něj umístit přímo do wrapper.conf

př.

wrapper.app.parameter.1=cz.elanor.egjews.server.RunServerWithWS

wrapper.app.parameter.2=-CrmiPort=10089

wrapper.app.parameter.3=-CDBurl=jdbc:oracle:thin:@prgxxx:1521:egje8

wrapper.app.parameter.4=-CDBuser=eman

wrapper.app.parameter.5=-CDBpassword=lkajdfkjaoqezroqw

wrapper.app.parameter.6=-CDBOwnerPassword=eurzoqiuezroquw

wrapper.app.parameter.7=-CSQLAdapter=cz.elanor.eman.datasource.SQLOracle

wrapper.app.parameter.8=-CDBdriver=oracle.jdbc.driver.OracleDriver

wrapper.app.parameter.9=-Cauthentification=NTLogin2

wrapper.app.parameter.10=-Cdomain=XXXX

wrapper.app.parameter.11=-CdomainControllerIP=10.29.29.29

Další údaje o wrapperu jsou na http://wrapper.tanukisoftware.org/

V některých případech, zvláště u 64-bitového linuxu je třeba nastavit omezení restartu AS vynuceného wrapperem, tj. wrapper.ping.timeout=0

Windows service se instaluje pomocí dávky bin/InstallApp-NT.bat

(správa se pak provádí pomocí services.msc, net start, net stop)

Doporučujeme, aby service byl spouštěn pod speciálně vytvořeným uživatelem nikoliv pod uživatelem Local System Account.

Dále by měl mít nastavenou proměnnou TEMP na nechráněný existující adresář, do kterého má zápisová práva. Lze jej také nastavit pouze pro javu. Př.:

wrapper.conf:

wrapper.java.additional.1=-Djava.io.tmpdir=c:\tmp

Při použití autentizací **mswin\_\*** je vhodné do ***wrapper\lib*** nakopírovat z egjelib.jar knihovnu

***\com\sun\jna\win32-amd64\jnidispatch.dll***  resp. ***\com\sun\jna\win32-x86\jnidispatch.dll***

Když systém knihovnu na cestě nemá, vždy ji rozbaluje do temp adresáře pod unikátním jménem a inicializuje.

Service lze zrušit pomocí příkazu sc delete *service\_name*

Př. sc delete EGJEAS\_EMANEVMA

Linux service se instaluje např. takto:

vytvořit uživatele egjeas

upravit bin/egjeas

# Application

APP\_NAME="EGJEAS\_EMANEVMA"

APP\_LONG\_NAME="EGJEAS EMANEVMA "

RUN\_AS\_USER=egjeas

v /etc/init.d vytvoříme link ***as\_emanevma*** na soubor v bin/egjeas   
(ln -s ....resp. lze použít service ***as\_emanevma*** install)

nastavit runlevel pomocí chkconfig

chkconfig ***as\_emanevma*** on

service ***as\_emanevma*** start (stop, restart,status, install, remove)

Volitelný parametr

pomocí parametru retrydb=true

je možné iniciovat režim, ve kterém pokud při startu AS není přístupná databáze, aplikace přesto naběhne a každých 10 minut pak znovu zkouší, jestli db přístupná není. Když je, dokončí inicializaci aplikace.

Př. wrapper.app.parameter.*nn*=-Cretrydb=true

Linux servery "headless"

* V této konfiguraci je problém s exporty data z formuláře resp. exportní sestavy typu java do excelu. V případě problémů s touto funkcionalitou zkuste nastavit systémovou java proměnnou

java.awt.headless=true

Nastavení proveďte ve wrapper.conf

Př.: wrapper.java.additional.2=-Djava.awt.headless=true

Java 11.0.20 a 17.0.8 a vyšší:

* Pro tyto Javy je potřeba zvětšit velikost očekávaného MANIFEST.MF který je součástí eman.jar. Velikost se zvedne přidáním Java parametru:  
  wrapper.java.additional.x=-Djava.awt.headless=true

**Příloha E. Logování - AS, EGJEWEB2**

Logování EGJE můžeme rozdělit na provozní a datové.

Aplikační datové logování je rozmístěno na mnoha místech napříč aplikací podle konkrétní příslušnosti.

Viz [Adm\_uzdoc](Adm_uzdoc.htm) formuláře Adm52, Adm54 a logovací záložky na jiných formulářích Adm10, Adm11, Adm12, Adm53, Vyp01, Vyp12, Dcm01, Dcd01.

Nastavení délky uchovávání dat v těchto auditních tabulkách se provádí v Adm21.

Zde se ale budeme věnovat provoznímu logování.

AS i EGJEWEB2 vytvářejí textové souborové logy.

Mají provozní charakter, zachycují provozní a chybové stavy EGJE serveru.

Jejich tvar i názvové konvence jsou poplatné prostředí –buď se jedná o soubor vytvářený Tanuki wrapperem, který používá AS anebo se jedná, o standardní logování kontejneru Tomcat.

Umístění logů se pro AS definuje ve wrapper.conf, Standardně podadresář logs.

U EGJEWEB2 pak dle definice Tomcat Logging. Standardně podadresář logs.

Pokud chce správce přesměrovat logy mimo jejich standardní umístění:

AS přestaví ve wrapper.conf wrapper.logfile=../logs/egje.log

EGJEWEB2 – nastavení tomcat:



* Úrovně logování

Pomocí parametru log4jConfigFile lze interní logování řídit externím konfiguračním XML souborem **log4j.**

Lze tak např. i tímto způsobem směrovat do jiného souboru,

nebo pro některé části nastavit jinou úroveň logování

(config\_egje.jar / config\_local\_properties / parametr "log4jConfigFile")

př. log4jConfigFile=/opt/egje/log4j.local.xml

<?xml version="1.0" encoding="UTF-8"?>  
<Configuration xmlns:xi="http://www.w3.org/2001/XInclude" status="warn" >  
 <Appenders>  
 <Console name="Console" target="SYSTEM\_OUT">  
 <PatternLayout pattern="%-5p - %d{yyyy-MM-dd HH:mm:ss,SSS} - session:%X{sessionID} - wID:%X{wID} - lognameWithUid:%X{lognameWithUid} - prof: %X{kod\_profilu} - db: %X{db\_inst\_name} - %-26.26c{1} - %m\n" />  
 </Console>  
 <File name="File" fileName="/opt/logs/all.log" immediateFlush="true" append="true">  
 <PatternLayout pattern="%d{yyy-MM-dd HH:mm:ss.SSS} [%t] %-5level %logger{36} - %msg%n"/>  
 </File>  
 </Appenders>  
 <Loggers>  
 <logger name="cz.elanor.eman">  
 <level>info</level>  
 </logger>  
 <logger name="cz.elanor.eman.datasource">  
 <level>debug</level>  
 </logger>  
 …. další loggery

<Root level="error">  
 <AppenderRef ref="Console" />  
 <AppenderRef ref="File"/>  
 </Root>  
 </Loggers>  
</Configuration>

**Upozornění: nastavení logování příliš velkého množství informací výrazně snižuje výkon aplikace!**

* Logování AS

Log AS obsahuje také identifikaci uživatele (logname:).

Standardní předloha řádku je:

<PatternLayout pattern="%-5p - logname:%X{logname} - %-26.26c{1} - %m\n" />

* Logování EGJEWEB2

V logu EGJEWEB2 je 10 znaků z HTTP Session ID (session:), identifikace okna v prohlížeči (wID:) a identifikaci přihlášení uživatele (logname:).

Standardní předloha řádku je:

<PatternLayout pattern="%-5p - %d{yyyy-MM-dd HH:mm:ss,SSS} - session:%X{sessionID} - wID:%X{wID} - lognameWithUid:%X{lognameWithUid} - prof: %X{kod\_profilu} - db: %X{db\_inst\_name} - %-26.26c{1} - %m\n" />

* Logování klienta na AS

Pomocí parametru senLog2AS lze nastavit, aby se logované události v klientské části aplikace zasílali na server a byli následně zalogované i na serveru. Hlášky musí mít jak na klientu, tak na serveru nastavenou stejnou úroveň logování pro daný logger.Má význam nastavovat pouze v Java klientu s připojením k AS.

(config\_egje.jar / config\_local\_properties / parametr "sendLog2AS")př. sendLog2AS=true

**Příloha F1. Nastavení JRE pro servery - AS, EGJEWEB2**

Doporučujeme u AS a EGJEWEB2 Tomcat nastavit parametr virtuálního stroje

-XX:-OmitStackTraceInFastThrow

Důvodem je to, že chybový výpis stacktrace nebývá bez tohoto parametru občas úplný.

U AS se to provádí do wrapper.conf do parametrů additional

př. wrapper.java.additional.*7*=-XX:-OmitStackTraceInFastThrow

(7 je dle současného počtu parametrů, patří tam max + 1)

U tomcat se parametr zadá takto:

linux - do setenv.sh do řádku export CATALINA\_OPTS=

př. export CATALINA\_OPTS="-Dfile.encoding=Cp1250 -Xmx3000m -XX:MaxPermSize=512m -XX:-OmitStackTraceInFastThrow"

windows - ovládací program tomcat7w s parametry //ES//*jmenoServeru*

záložka java / Java Options - přidejte -XX:-OmitStackTraceInFastThrow

**Příloha G. Monitorování AS pomocí JMX**

Při provozování aplikačního serveru je vhodné sledovat jeho chování.

Základním nástrojem, který řekne, zdali je AS resp. Tomcat server pro WEB EGJE je Superconfigurator.

Je však vhodné v případě potíží mít k dispozici nějaký diagnostický nástroj. Je možné použít některý z obecně používaných monitorů, které se umějí připojit i k java aplikaci (např. nagios), ale je také možné použít základní monitorování, které poskytuje JDK a to Jvisualvm resp Jconsole.

Nevýhodou je, že sledují pouze současný stav, zatímco při diagnostice bývá často vhodné znát.

* průběh jednolivých java pamětí (heap, permgen space)  
  thread dump z problémové doby
* záznam z logu AS wrapperu
* export položek z Adm52 pro příslušný den

Užitečnou informací k paměťovému nastavení také bývá znalost HW parametrů (procesory, os, velikost paměti).

V následujícím odstavci popíšeme jednoduché permanentní monitorování pomocí **jvisualvm + plugin**

Monitor nastavíme přímo na AS serveru (windows) resp. linux s grafická nadstavbou

(resp. na jiném jiný počítač s graf. nadstavbou, který se připojí k linux bez grafiky.

Instalovat JDK pokud je tam jen JRE.

Do wrapper.conf přidat (jsou-li 2 AS dát každému jiný port)

wrapper.java.additional.1=-Dcom.sun.management.jmxremote.port=10984

wrapper.java.additional.2=-Dcom.sun.management.jmxremote.ssl=false

wrapper.java.additional.3=-Dcom.sun.management.jmxremote.authenticate=false

a restartovat AS

z JDK/bin spusti jvisualvm

Přidat JMX connection localhost:10984 (resp. jiný server a port)

a spustit monitorování (dvojklik).

Jednoduchý trace soubor lze generovat přidáním Trace Monitor pluginu:

menu Tools / Plugins / Available plugin (internet => obvykle je třeba nastavit proxy server a port)

Install / Tracer-Monitor Probes => restart

jvisualvm + Trace

spustit monitorování

záložka Tracer zvolit Cpu, Heap, PermGen (případně i Classes+Threads)

=>Start

Kdykoliv během monitorování nebo po jeho skončení je možné provést Export all data => uložit jako html soubor

(obvykle je v něm zapotřebí odstranit oddělovače tisíců resp. změnit . na , poté lze zpracovat v excelu)

Vhodné je také v problémové době (tedy např. kdy se nelze přihlásit k as) udělat thread dump.

Bohužel nejde automatizovat připojení k AS po restartu počítače nebo AS. Monitorování je ale vhodné v případě řešení problémů.

**Příloha H. Monitorování serverových procesů na AS z java klienta resp. EGJEWEB2**

EGJE standardní klient má k dispozici jednoduchý monitor:

Příkazový řádek egje:

-logger

Otevře se monitorovací okno. Poté se spustí v EGJE konkrétní akce (výpočet, měs.úpravy).

A nakonec v monitorovacím okně menu File / Save File např. jako trace.trc

Z tohoto souboru jsme schopni zjistit detail akce.

V případě práce přes aplikační server je to pro procesy, které běží na aplikačním serveru (výpočet, měs.úpravy, sestava...) složitější:

Příkazový řádek egje:

-startserverlog

-logger

Otevře se monitorovací okno. Poté se spustí v EGJE konkrétní akce (výpočet, měs.úpravy).

Server ale odesílá vše, co na něm v tu chvíli probíhá.

Příkazový řádek egje:

-stopserverlog

A nakonec v monitorovacím okně menu File / Save File např. jako trace.trc

Pozn. vypnutí serverového logu -stopserverlog je důležité, jinak jsou monitorovány všechny jeho akce a to výrazně zvyšuje jeho zátěž.

Threaddump z AS

Příkazový řádek egje:

-threaddump

vytvoří a zobrazí threaddump z aktuálního AS, ke kterému je uživatel připojen

příkaz je k dispozici i pro EGJEWEB2

-threaddump *server*:*port*

vytvoří a zobrazí threaddump z konkrétního AS

-threaddump client

vytvoří a zobrazí threaddump z klientské aplikace nikoliv ze serveru

Zazipovaný heapdump lze na AS/EGJEWEB2 pořídit analogicky. V EGJEWEB2 se neposílá na klienta, ale zůstává na web serveru jako soubor heapdump\*.gz

**Příloha I. Monitorování databáze**

Na monitorování je k dispozici celá řada nástrojů výrobce i třetích stran.

Zde uvádíme základní podporu a odkazy.

**DB Oracle**

* trace soubory - podpora EGJE:
  + zjištění nastavení adresáře udump (db server)
  + před problémovou akcí, sestavou zadáme v příkazovém řádku egje

-trace *jmeno*

* + spustíme akci (typicky sestavu)

*-*stoptrace

* + v udump adresáři je k dipozici trace soubor  
    ten interpretujeme utilitou tkprof  
    např. takto tkprof %1 %1.txt sys=no record=%1.rec sort=fchela

Doporučujeme databázový trace provádět na std. klientovi bez AS. Souborů je méně a je snadnější se v nich vyznat. Také -stoptrace funguje přímočařeji. U AS trace některých částí končí až odhlášením klienta resp. restartem AS.

* Oracle AWR

Umožňuje vygenerovat AWR Report a případně dává možnost nastavit snímkování např. na 15 minut. Je vhodné tuto funkcionalitu dopředu vyzkoušet.

Někdy se například udržují AWR podklady po dobu 5-10 dnů, aby bylo možno zpětně se podívat na akce, které generovaly (a jakým způsobem generovaly) zátěž serveru.

**DB Microsoft SQL Server**

SQL Server Profiler

**Příloha J. Monitorování EGJEWeb2(HR portál), AS pomocí Java Melody**

Webové aplikace i AS mají vestavěný systém provozního monitorování Java Melody.

JavaMelody je nástroj pro monitorování web aplikací v testovacích a produkčních prostředích. Provádí sběr a analýzu statistik operací probíhajících v aplikaci v závislosti na tom, jak je aplikace používána uživateli.

JavaMelody má malé nároky na systémové prostředky, proto může být nasazena jak v testovacím tak i v produkčním prostředí. Nicméně toto zatížení je úměrné činnosti uživatelů. Vhodnost pro Vaše produkční prostředí tedy posuďte podle zkušeností z testovacího.

Nicméně nasazujte jej jen v případě, že jej budete sledovat a využívat.

JavaMelody nezaznamenává údaje o jednotlivých událostech, do databáze se zaznamenávají pouze statistiky s počtem a trváním jednotlivých událostí.

Domovská stránka systému: https://code.google.com/p/javamelody/

Ukázky obrazovek jsou zde: <https://code.google.com/p/javamelody/wiki/Screenshots>

**Zprovoznění - webové aplikace:**

Základní konfigurace zapište do config\_egje\*.jar / config\_local.properties

javamelody.disabled – zapne/vypne monitorování, (výchozí hodnota true,tzn. vypnuto)

javamelody.storage-directory - určuje název adresáře, do kterého se ukládají nasbíraná data. (výchozí hodnota javamelody)

javamelody.resolution-seconds - konfiguruje rozlišení grafů. Aby se změna parametru projevila, je nutné smazat uložené soubory \*.rrd.

javamelody.no-database - vypne monitorování JDBC připojení a databázových dotazů.

Podrobnější popis parametrů naleznete v dokumentaci JM na https://code.google.com/p/javamelody/wiki/UserGuide#6.\_Optional\_parameters

Přístup k monitorovací stránce je možné zabezpečit jménem/heslem nebo omezením přístupu z určitých IP adres

javamelody.authorized-users= user1:pwd1, user2:pwd2

javamelody.allowed-addr-pattern=192\.168\..\*|123\.123\.123\.123

Upozornění: zabezpečení jménem a heslem způsobí narušení autentizace vlastní EGJEWEB2 aplikace, pokud běží v tu chvíli ve stejném prohlížeči.

<https://code.google.com/p/javamelody/wiki/UserGuide#16._Security>

Pro periodické zasílání reportů si v <tomcat\_home>/conf/server.xml vytvořte mail session určující SMTP server, přes který se reporty budou zasílat.

        <Resource name="mail/MySession" auth="Container" type="javax.mail.Session"

                mail.smtp.host="<smtp server>"

                mail.smtp.user="<login>"

                mail.from="no-reply@example.com"

        />

Do konfigurace JM přidejte následující parametry určující název mail session, adresy příjemců a periodu zasílání reportů

javamelody.mail-session=mail/MySession  
javamelody.admin-emails=admin@mail.cz,admin2@mail.cz  
javamelody.mail-periods=week,month

<https://code.google.com/p/javamelody/wiki/UserGuide#14._Weekly,_daily_or_monthly_reports_by_mail>

Odstavec typicky vypadá takto:

javamelody.disabled=false

javamelody.authorized-users=*admin*\:*heslo*

javamelody.admin-emails=*mail1@mail.cz,mail2@mail.cz*

javamelody.mail-session=mail/MySession

javamelody.mail-periods=*day,week,month*

Parametry se projeví po restartu webové aplikace.

Systém implicitně ukládá svá pracovní data do *tomcat*/temp/javamelody

Pracovní data jsou v řádu stovek MB. U zatíženějších systémů mohou být větší.

**Zprovoznění - aplikační server:**

Monitorování pomocí javaMelody se nastavuje ve wrapper.conf.

Je třeba nastavit parametry:

Pro vlastní spuštění javamelody:

javamelody.disabled=false

Přístup je pak buď přes http - př.

monitoring.http.port=8901

nebo přes https př.

monitoring.https.port=8902

monitoring.https.keystore=t:/keystore

monitoring.https.password=egjeas

ostatní parametry jsou společné s EGJEWEB - viz minulý odstavec

Ve wrapper.conf se pak předávají aplikaci v podobě parametrů wrapper.app.parameter.*nn*=-C...

Př. wrapper.app.parameter.12=-Cjavamelody.disabled=false

wrapper.app.parameter.13=-Cmonitoring.http.port=8901

wrapper.app.parameter.14=-Cjavamelody.storage-directory=/opt/egje/prub/as\_eman14p/javamelody

Monitorovací stránka je pak

http://server:8901/monitoring

**Přístup k datům:**

**1. Online stránka http(s)://*aplikace/*monitoring**

Při načtení stránky je požadován uživatel a heslo

- oboje je z parametru javamelody.authorized-users

V hlavičce je možné implicitní denní pohled změnit na větší časové období.

EGJEWeb je databázová aplikace a tak většina "zajímavých" údajů je v linku   
**Statistics sql Details**

resp. **Statistics app Details**

nicméně problematická místa mohou indikovat i další tabulky, i u nich je ze souhrnné tabulky odskok do podrobné přes link Details.

**2. Periodické reporty**

Systém umožňuje správcům uvedeným v javamelody.admin-emails

Zasílat denní, týdenní resp. měsíční reporty, dle toho, které jsou uvedeny v

javamelody.mail-periods=*day,week,month*

Struktura PDF reportu je obdobná jako u online stránky, velikost je v jednotkách MB.

**Vymazání statistik**

Pro vymazání statistik zastavte, vymažte adresář se statistikami (standardně javamelody v adresáři s dočasnými soubory webserveru) a restartujte server.

**Integrované monitorování více serverů společně**

Pokud byste měli zájem o centrální monitorování aplikací EGJE, obraťte se na helpdesk a dodáme Vám tomcat aplikaci javamelody.war.

Nasazení aplikace je popsáno v https://code.google.com/p/javamelody/wiki/UserGuideAdvanced#Optional\_centralization\_server\_setup

Vlastní instalace

1. Instalovat na Tomcat javamelody.war

2. Spustit aplikaci .../javamelody

3. Přidat monitorované aplikace:

jméno(bez diakritiky!) a URL adresa

jméno(bez diakritiky!) a URL adresa

...

4. Spuštění aplikace .../javamelody poté nabízí výběr monitorované aplikace

**Příloha J1. Monitorování pomocí JavaFlightRecorder**

**Java Flight Recorder** (JFR) je diagnostický nástroj pro profilování a diagnostiku výkonu Java aplikací. Je integrován do Java Virtual Machine (JVM). Umožňuje shromažďovat podrobné informace o výkonu a chování spuštěné Java aplikace s minimálním dopadem na její výkon.

JFR zaznamenává události, které se dějí v JVM a v aplikaci, jako jsou využití procesoru, paměti, vlákna, garbage collection a další.

JFR pomáhá při diagnostice složitých problémů, jako jsou paměťové úniky, zablokování vláken a pády aplikací.

JFR je navržen tak, aby měl minimální dopad na výkon spuštěné aplikace, takže jej lze používat i v produkčním prostředí.

Nastavení se doporučuje provádět pro řešení problémů aplikace.

**Nastavení pro klient:**

JFR nefunguje pro spuštění přes EgjeWebStart. EWS používá distribuci Java, která neobsahuje potřebné oduli pro spuštění JFR. Pro klienta je potřeba spouštět dávkovým souborem s plnohodnotným JDK.

Do \*.bat souboru pro spuštění EGJE přidat „-XX:StartFlightRecording=name=egje-jfr-recording,dumponexit=true,filename=egje\_jfr\_client.jfr“ do části k VM argumentům (před -cp, v části kde je např. -Xmx).

Soubor se vytvoří do složky odkud byla aplikace spuštěná.

**Nastavení pro aplikační server:**

V konfiguračním souboru pro aplikační server nastavit: „wrapper.java.additional.X=-XX:StartFlightRecording=name=egje-jfr-recording,dumponexit=true,filename=egje\_jfr\_as.jfr“

Kde wrapper.java.additional.X za 'X' dosadit číslo volného parametru. Číslo volného parametru zjistíte tak, že se podíváte do konfiguračního souboru a zjistíte které číselné označení již bylo použito.

Soubor se vytvoří do složky wrapperu/bin.

AS bude potřeba restartovat.

**Nastavení pro Tomcat:**

**Linux:** do **tomcat/bin/setenv.sh** do **CATALINA\_OPTS** zadat „-XX:StartFlightRecording=name=egje-jfr-recording,dumponexit=true,filename=/path/egje\_jfr\_web.jfr“

**Windows:** do nastavení Tomcat properties na záložce **Java** nastavit do **Java Options:**„-XX:StartFlightRecording=name=egje-jfr-recording,dumponexit=true,filename=egje\_jfr\_web.jfr“.

Soubor se vytvoří do složky Tomcatu.

**Příloha K. EGJE a webové služby**

**EGJE AS – standardní či uživatelská sestava volaná jako webová služba SOAP**

V EGJE existuje poměrně komplikované zákaznické rozšíření AS EGJE o volání libovolné sestavy jako webové služby (SOAP), při kterém volající program sestavu nejprve zavolá a pak opakovaně zjišťuje, jestli je již hotova a když ano, převezme si běžný výstup sestavy.

Je mu věnována samostatná dokumentace [EGJE\_WS\_provdoc](EGJE_WS_provdoc.htm).

**EGJEWEB2 jako server webových služeb typu REST – jádro vestavěno do EGJEWEB2**

Standardní EGJEWEB2 má od verze e201709 možnost exportovat jednodušší volání webové služby REST.

Daní za jednodušší volání je ale nutnost vytvářet speciální sestavy, jejichž design je takový, že "stručně odpovídají na stručný" dotaz. Ptají se tedy na konkrétní údaje např. pro konkrétní osobu (ale už ne třeba pro všechny osoby v db).

Pro export takové sestavy byl zřízen v Adm53 nový Typ AS úlohy:

3 - Webová služba REST (realizovaná uživ. sestavou)

Configurator na záložce AS / Web obsahuje novou hodnotu radio přepínače "Web server" , kde umožňuje pomocí checkboxů určit, které komponenty se mají pustit:

Spustit EGJEWEB2 / HR portál – běžné web aplikace

Spustit server Web services

Spustit server Web services zaškrtněte pouze v případě, že je opravdu chcete používat. Jelikož standardní EGJEWEB2 / HR portál jde odškrtnout, je možné udělat i dedikovaný server Web services, který standardní Web aplikace spuštěné nemá.

Také tyto WS jsou popsány v dokumentaci [EGJE\_WS\_provdoc](EGJE_WS_provdoc.htm).

V případě zájmu o konkrétní Web službu se obraťte na dodavatele SW EGJE prostřednictvím ESP.

**Příloha L. Více hlášek v některých protokolech**

Některé procesy, které generují protokol ze svého běhu, umožňují dočasně zapnout ladící režim, kdy je protokol obohacen o některé ladící hlášky. Tyto hlášky nejsou lokalizovány (tzn. jsou v češtině) a neslouží k trvalým výpisům, pouze pro hledání chyby ve spolupráci s helpedeskem Elanor.

Kterých akcí se týká:

* Měsíční uzávěrka (Vyp02)
* Výstup do účetnictví (Uct02)
* Roční uzávěrka (Vyp02)
* Import SLM (Vst06) – plánováno, ale zatím nerealizováno
* Přihlášky NP CZ (Poj18, Poj19), plánováno, ale zatím nerealizováno

Jak se zprovozní:

* Vyžádejte si s odkazem na tuto přílohu Provozní dokumentace přes HelpDesk script   
  /eman/z\_cust/a\_debug\_ela/**debug\_ela.xml**
* Spusťte tento změnový script pomocí Adm51 (či SuperConfiguratoru)
* Po novém přihlášení se na Vyp02 objeví nová záložka **Debug ELA**
* Pro konkrétní období, výplatní termín zaškrtněte ty akce, u kterých chcete detailní výpis
* Spusťte konkrétní akci – její protokol je rozšířen o hlášky začínající DEBUG\_

Ty mohou ozřejmit průběh některých akcí ať už Vám, nebo Helpdesku Elanor

Pozn.: Hlášení a možnost jej zapnout zůstane přístupná pouze v den spuštění, důvodem je, že trvalé ukládání nadbytečných hlášek by zatěžovalo databázi i diskový systém a také protokoly znepřehledňovalo.

**Příloha M. Základní popis databázových zámků**

**Zdroj popisu db zámků:** [**https://www.sqlshack.com/locking-sql-server/**](https://www.sqlshack.com/locking-sql-server/)

**Exclusive lock (X)** - tento typ zámku zajistí, že stránka nebo řádek budou vyhrazeny výhradně pro transakci, která exkluzivní zámek zavedla, dokud bude transakce držet zámek. Exkluzivní zámek bude transakcí vynucen, když bude chtít změnit data stránky nebo řádku, což je v případě příkazů DML DELETE, INSERT a UPDATE. Exkluzivní zámek lze na stránku nebo řádek uložit pouze v případě, že na cíli již není uložen jiný sdílený nebo exkluzivní zámek. To prakticky znamená, že na stránku nebo řádek lze uložit pouze jeden exkluzivní zámek a po jeho uložení nelze na uzamčené prostředky uložit žádný další zámek.

**Shared lock (S)** - tento typ zámku po jeho zavedení vyhradí stránku nebo řádek tak, aby byly dostupné pouze pro čtení, což znamená, že jakákoli jiná transakce nebude moci modifikovat zamčený záznam, dokud bude zámek aktivní. Sdílený zámek však může být nad stejnou stránkou nebo řádkem zaveden několika transakcemi současně a tímto způsobem může několik transakcí sdílet možnost čtení dat, protože samotný proces čtení nijak neovlivní aktuální data stránky nebo řádku. Kromě toho sdílený zámek umožní operace zápisu, ale nebudou povoleny žádné změny DDL.

**Update lock (U)** - tento zámek je podobný exkluzivnímu zámku, ale je navržen tak, aby byl svým způsobem flexibilnější. Aktualizační zámek lze zavést na záznam, který již má sdílený zámek. V takovém případě aktualizační zámek zavede další sdílený zámek na cílový řádek. Jakmile je transakce, která drží aktualizační zámek, připravena změnit data, změní se aktualizační zámek (U) na exkluzivní zámek (X). Je důležité si uvědomit, že aktualizační zámek je asymetrický, pokud jde o sdílené zámky. Zatímco aktualizační zámek lze zavést na záznam, který má sdílený zámek, sdílený zámek nelze zavést na záznam, který již má aktualizační zámek.

**Intent locks (I)** - tento zámek je prostředek, který transakce používá k informování jiné transakce o svém záměru získat zámek. Účelem tohoto zámku je zajistit správné provedení modifikace dat tím, že zabrání jiné transakci získat zámek na dalším objektu v hierarchii. V praxi, když chce transakce získat zámek na řádek, získá zámek záměru na tabulku, která je objektem vyšší hierarchie. Získáním zámku záměru transakce nedovolí jiným transakcím získat exkluzivní zámek na této tabulce (jinak by exkluzivní zámek zavedený některou jinou transakcí zrušil zámek řádku).

**Příloha N. Další Security opatření**

Konfigurační parametr **noshowserverinfo** – Možné hodnotytrue/false. Default false.

Nastavením konfiguračního parametru noshowserverinfo na hodnotu true zamezíte zobrazením některých potenciálně citlivých údajů koncovému uživateli EGJE. Typicky jde o údaje popisující síťovou infrastrukturu, jako např. na jakém serveru běží databáze atp. V okně O Aplikaci jsou hodnoty těchto konfiguračních položek zahvězdičkovány. Na jiných místech v aplikaci je pak jejich zobrazení zcela potlačeno. Jde např. o okno pro výběr profilu, o titulek okna webové aplikace Egje a další.

Mezi citlivé konfigurační položky řadíme následující: *dburl, domain, domaincontrollerip, domaincontrollername, ldapsslurl, proxyhost, proxyport, rmiservers*

**Zamezení zobrazení podrobných chybových informací pro neautentizovaného uživatele ve webové aplikaci.**

Egje webová aplikace nezobrazí podrobné chybové informace uživatele při neúspěšném pokusu o přihlášení. Chybová informace je v omezené formě zalogována na webovém serveru. Uživatel sám dostane pouze informaci o tom, že došlo k chybě.

**Cookies webové aplikace EGJE**

Egje webová aplikace nastavuje do prohlížeče cookies s nastavenými atributy **Secure** a **HttpOnly**. Správcům webového serveru doporučujeme provést i nastavení atributu **SameSite**. Nastavení tohoto atributu ovšem neprovádí aplikace, ale je potřeba provést příslušnou konfiguraci na úrovni webového serveru. Viz. Příloha C1, odst. 10.3.2

# Upozornění

Seznam přístupných částí dokumentace je [zde](index.htm)**.**