



# **Dokumentace**

**k projektu Czech POINT**

**JIP/KAAS: Editační webová služba**

**Technický popis**

**Výběr kapitol týkajících se nové politiky hesel**

Vytvořeno dne: 10. 12. 2025

Aktualizováno: -

Verze: 1.0

© 2025 DIA

# 1. Úvod

## 1.1. Účel dokumentu

Tento dokument obsahuje technický popis editační webové služby JIP/KAAS, která slouží pro editaci údajů v JIP.

## 1.2. Manažerské shrnutí

Tento dokument obsahuje pouze vybrané kapitoly z plnohodnotného dokumentu s popisem editační webové služby JIP/KAAS, která je používána pro editaci údajů subjektů, uživatelů, úřadoven, složek krizového řízení a zřizovaných organizací v JIP.

Tento dokument (který zrovna čtete) se zaměřuje na připravované nasazení nové politiky hesel v systému Czech POINT a obsahuje podrobné informace o této změně a popis pouze relevantních metod webové služby, které byly/budou změněny z důvodu nasazení nové politiky hesel.

Popis ostatních metod a další informace o webové službě (např. adresy přístupových bodů) naleznete v plnohodnotném dokumentu.

**Tento dokument je určen pro vývojáře aplikací třetích stran, které zajímají pouze ty části webové služby, které jsou ovlivněny plánovanou změnou politiky hesel v systému Czech POINT.**

Ode dne 16. 4. 2026 bude v systému Czech POINT platit nová bezpečnostní politika hesel, která bude klást přísnější požadavky na hesla uživatelů. Nová politika hesel je již nasazena v testovacím prostředí, kde si ji vývojáři aplikací třetích stran mohou otestovat.

## 2. Metody pro práci s uživateli

### 2.1. GetUser

Tato metoda vrátí detailní informace o uživateli ze specifikovaného subjektu.

#### Příklad požadavku GetUserRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<GetUserRequest object-id="jnovak" xmlns="http://userportal.novell.com/ws/WS-LA-1.0"/>
```

#### Popis datové struktury požadavku

Atribut	Popis
object-id	Přihlašovací jméno uživatele.

#### Příklad odpovědi GetUserResponse

Elementy zvýrazněné pomocí **azurového podbarvení** jsou momentálně dostupné pouze v testovacím prostředí a do produkčního prostředí budou nasazeny v rámci nasazení nové politiky hesel (viz kap. 4).

```
<up:GetUserResponse xmlns:up="http://userportal.novell.com/ws/WS-LA-1.0">
  <up:titulPred>MUDr.</up:titulPred>
  <up:firstname>Jan</up:firstname>
  <up:surname>Novák</up:surname>
  <up:titulZa>bc.</up:titulZa>
  <up:isLocalAdmin text="Ano">true</up:isLocalAdmin>
  <up:pwdChangedTime>20220915112956Z</up:pwdChangedTime>
  <up:passwordExpirationTime/>
  <up:photo>/9j/4A60...UUVJ1n/9k=</up:photo>
  <up:loginDisabled/>
  <up:address>
    <up:addressCode>5119413</up:addressCode>
    <up:street>Marš. Rybalka</up:street>
    <up:cityCode>567027</up:cityCode>
    <up:city>Most</up:city>
    <up:region>Ústecký</up:region>
    <up:postalCode>43401</up:postalCode>
    <up:metropolitanDistrict/>
    <up:cityPart>Most</up:cityPart>
    <up:houseNumber>784</up:houseNumber>
    <up:sequenceNumber/>
  </up:address>
  <up:email>
    <up:item>
      <up:type text="oficiální">1</up:type>
      <up:email>public@test.tt</up:email>
      <up:description>public</up:description>
    </up:item>
  </up:email>
  <up:telephoneNumber>
    <up:item>
      <up:type text="mobilní">2</up:type>
      <up:number>+420780425630</up:number>
    </up:item>
    <up:item>
      <up:type text="fax">3</up:type>
      <up:number>+420222656700</up:number>
    </up:item>
  </up:telephoneNumber>
  <up:crisisTelephoneNumber>
    <up:item>
      <up:type text="mobilní">2</up:type>
```

```

    <up:number>+42011111111</up:number>
  </up:item>
</up:crisisTelephoneNumber>
<up:clientCertificate>
  <up:item>
    <up:type text="komerční">V</up:type>
    <up:number>77EEEE</up:number>
    <up:issuer>postsignum</up:issuer>
  </up:item>
</up:clientCertificate>
<up:role>
  <up:item text="Czech POINT">czp</up:item>
</up:role>
<up:roleCzechPoint>
  <up:item text="Správce skupiny">Spravce skupiny</up:item>
</up:roleCzechPoint>
<up:roleCzpAtOffice>
  <up:item text="Konverze z moci úřední">kzmu</up:item>
  <up:item text="Agenda obchodního rejstříku">oro</up:item>
  <up:item text="Agenda rejstříku trestů">iczp</up:item>
</up:roleCzpAtOffice>
<up:roleVirtuos>
  <up:item text="Virtuos">virtuOS</up:item>
</up:roleVirtuos>
<up:roleCentralniNakup>
  <up:item text="Přístup do centrálního nákupu">KPLZENSKY_ISCNPK</up:item>
</up:roleCentralniNakup>
<up:aisRole>
  <up:item text="Editor číselníku">ATS18948ad165ec.editorcis</up:item>
</up:aisRole>
<up:ovmPersonType text="vedoucí útvaru">17</up:ovmPersonType>
<up:function>vedoucí</up:function>
<up:url>
  <up:item>
    <up:type text="získání informací">2</up:type>
    <up:url>http://www.info.cz/</up:url>
  </up:item>
</up:url>
<up:predchoziZamestnavatel>Microsoft</up:predchoziZamestnavatel>
<up:uvolnenZeZamestnani text="Ne">FALSE</up:uvolnenZeZamestnani>
<up:verejnaOsoba text="Ano">TRUE</up:verejnaOsoba>
<up:osobaKrizovehoRizeni/>
<up:poznamka>k testovani</up:poznamka>
<up:cisloJednaci/>
<up:agendy>
  <up:item text="Obecní policie">a420</up:item>
</up:agendy>
<up:cinnostniRole>
  <up:item text="Zřizování a řízení obecní policie" agenda="a420">cr786</up:item>
</up:cinnostniRole>
<up:casPosledniZmeny>1329404714</up:casPosledniZmeny>
</up:GetUserResponse>

```

### Popis datové struktury odpovědi

Atribut	Popis
titulPred	Titul před jménem
firstname	Křestní jméno
surname	Příjmení
titulZa	Titul za jménem
isLocalAdmin	Příznak, zda je daný uživatel lokálním administrátorem subjektu.
pwdChangedTime	Časová značka poslední změny hesla uživatelem. Nyní je dostupná pouze v testovacím prostředí. Do produkčního prostředí bude přidána po nasazení nové politiky hesel.

Atribut	Popis
passwordExpirationTime	Časová značka konce platnosti hesla. Před vypršením hesla je uživatel během přihlašování vyzván k jeho změně (více viz kap. 4.3.2). Nyní je dostupná pouze v testovacím prostředí. Do produkčního prostředí bude přidána po nasazení nové politiky hesel.
photo	Fotografie uživatele
loginDisabled	Příznak, je-li uživatelský účet zablokován.
address	Adresa uživatele. Pokud je zadán kód adresy, adresa je ověřena a doplněna z RUIAN. Není-li kód zadán, adresa se neověřuje a je považována za dočasnou.
email	Seznam e-mailů.
telephoneNumber	Seznam kontaktních telefonních čísel.
crisisTelephoneNumber	Telefonní čísla pro krizové řízení.
clientCertificate	Seznam certifikátů uživatele obsahující sériové číslo certifikátu, identifikaci vydavatele a typ certifikátu (Q pro kvalifikovaný, V pro komerční).
role	Přístup do agend Czech POINT.
roleCzechPoint	Seznam rolí pro přístup do Czech POINT.
roleCzpAtOffice	Seznam rolí pro přístup do CzechPOINT@office.
roleVirtuos	Seznam rolí pro přístup do aplikace Virtuos.
roleCentralniNakup	Seznam rolí pro přístup do aplikace Centrální nákup.
aisRole	Seznam přístupových rolí do AIS.
ovmPersonType	Typ osoby v OVM.
function	Funkce osoby.
url	Url adresa.
predchoziZamestnavatel	Předchozí zaměstnavatel.
uvolnenZeZamestnani	Příznak, je-li osoba uvolněna z předchozího zaměstnání pro výkon funkce.
verejnaOsoba	Příznak, zda se jedná o veřejnou osobu. Tj. je zobrazena na stránkách Seznamu datových schránek.
osobaKrizovehoRizeni	Příznak, zda se jedná o osobu krizového řízení.
poznamka	Poznámka
cisloJednaci	Dodatkový text k číslu jednacím. Používá se v Czech POINT.
agendy	Seznam agend z RPP, které se vztahují k činnostním rolím uživatele.
cinnostniRole	Seznam činnostních rolí z RPP, které jsou přiřazeny uživateli.
casPosledniZmeny	Datum a čas, kdy došlo k poslední změně v údajích uživatelského účtu.

## 3. Metody pro práci s uživateli zřizovaných organizací

### 3.1. GetOrganizationUser

Tato metoda vrátí detailní informace o uživateli zadané zřizované organizace.

#### Příklad požadavku GetOrganizationUserRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<GetOrganizationUserRequest
  object-path="skola" object-id="novak" xmlns="http://userportal.novell.com/ws/WS-LA-1.0"/>
```

#### Popis datové struktury požadavku

Atribut	Popis
object-id	Přihlašovací jméno uživatele.
object-path	Zkratka zřizované organizace.

#### Příklad odpovědi GetOrganizationUserResponse

Elementy zvýrazněné pomocí **azurového podbarvení** jsou momentálně dostupné pouze v testovacím prostředí a do produkčního prostředí budou nasazeny v rámci nasazení nové politiky hesel (viz kap. 4).

```
<up:GetOrganizationUserResponse xmlns:up="http://userportal.novell.com/ws/WS-LA-1.0">
  <up:titulPred>MUDr.</up:titulPred>
  <up:firstname>Jan</up:firstname>
  <up:surname>Novák</up:surname>
  <up:titulZa/>
  <up:pwdChangedTime>20220915112956Z</up:pwdChangedTime>
  <up:passwordExpirationTime/>
  <up:photo/>
  <up:loginDisabled/>
  <up:address>
    <up:addressCode>21745242</up:addressCode>
    <up:street>Jugoslávská</up:street>
    <up:cityCode>554782</up:cityCode>
    <up:city>Praha</up:city>
    <up:region>Hlavní město Praha</up:region>
    <up:postalCode>12000</up:postalCode>
    <up:metropolitanDistrict>Praha 2</up:metropolitanDistrict>
    <up:cityPart>Vinohrady</up:cityPart>
    <up:houseNumber>567</up:houseNumber>
    <up:sequenceNumber>16</up:sequenceNumber>
  </up:address>
  <up:email>
    <up:item>
      <up:type text="podatelna">2</up:type>
      <up:email>novak@skola.cz</up:email>
      <up:description>hlavni</up:description>
    </up:item>
  </up:email>
  <up:telephoneNumber>
    <up:item>
      <up:type text="stolní">1</up:type>
      <up:number>+420785998</up:number>
    </up:item>
  </up:telephoneNumber>
</up:GetOrganizationUserResponse>
```

```

</up:telephoneNumber>
<up:uvolnenZeZamestnani/>
<up:roleCentralniNakup/>
</up:GetOrganizationUserResponse>

```

### Popis datové struktury odpovědi

Atribut	Popis
titulPred	Titul před jménem.
firstname	Křestní jméno.
surname	Příjmení.
titulZa	Titul za jménem.
pwdChangedTime	Časová značka poslední změny hesla uživatelem. Nyní je dostupná pouze v testovacím prostředí. Do produkčního prostředí bude přidána po nasazení nové politiky hesel.
passwordExpirationTime	Časová značka konce platnosti hesla. Před vypršením hesla je uživatel během přihlašování vyzván k jeho změně (více viz kap. 4.3.2). Nyní je dostupná pouze v testovacím prostředí. Do produkčního prostředí bude přidána po nasazení nové politiky hesel.
photo	Fotografie uživatele.
loginDisabled	Příznak, že účet uživatele je zablokován.
address	Adresa uživatele zřizované organizace. Pokud je zadán kód adresy, adresa je ověřena a doplněna z RUIAN. Není-li kód zadán, adresa se neověřuje a je považována za dočasnou.
email	Seznam kontaktních e-mailů.
telephoneNumber	Seznam kontaktních telefonních čísel.
uvolnenZeZamestnani	Příznak, je-li osoba uvolněna z předchozího zaměstnání pro výkon funkce.
roleCentralniNakup	Seznam rolí pro přístup do aplikace Centrální nákup.

## 4. Bezpečnostní politika hesel v Czech POINTu

Pokud budete vytvářet nového uživatele (metody CreateUser nebo CreateOrganizationUser), nebo měnit heslo uživateli (metody UpdateUser nebo UpdateOrganizationUser), musí heslo uživatele předávané v requestu splňovat požadavky politiky hesel, která je implementována v systému Czech POINT.

Dne 16. 4. 2026 bude nová politika hesel s přísnějšími požadavky nasazena do produkčního prostředí Czech POINT.

Nová politika hesel je již nyní nasazena v testovacím prostředí Czech POINT, kde mohou vývojáři aplikací třetích stran testovat kompatibilitu svých aplikací s touto novou politikou hesel.

### 4.1. Bezpečnostní požadavky na hesla

Následující tabulka obsahuje bezpečnostní požadavky na „složitost“ hesel, a to jak pro stávající, tak i pro novou politiku hesel, která bude v produkčním prostředí nasazena od 16. 4. 2026 (v testovacím prostředí je již nasazena).

Parametr	Stávající politika	Nová politika
Minimální délka hesla	7 znaků	12 znaků
Maximální délka hesla	20 znaků	64 znaků
„Složitost“ hesla	Heslo musí obsahovat alespoň jednu číslici. Lze použít malá i velká písmena a speciální znaky.	V hesle musí být zastoupeny alespoň 3 z těchto 4 skupin znaků: 1. velká písmena 2. malá písmena 3. číslice 4. speciální znaky
Povolené speciální znaky	. ; _ : @   ! * % = + - ? ,	. ; _ : @   ! * % = + - ? , & [ ] # \$ ( ) " /
Opakování stejných znaků v hesle	Heslo musí obsahovat alespoň 4 jedinečné znaky. Příklady: abcabc1 – v pořádku aaabbb1 – nesplňuje	Heslo musí obsahovat alespoň 4 jedinečné znaky. Příklady: Aaaabbbbccc1 – v pořádku AAAAAabbbb1 – nesplňuje
Historie hesel	Není zavedena	Heslo nesmí být totožné s 12 posledními hesly.
Další požadavky	Heslo nesmí obsahovat uživatelské jméno, křestní jméno ani příjmení.	Heslo nesmí obsahovat uživatelské jméno, křestní jméno ani příjmení.

Po nasazení nové politiky hesel bude možné v heslech používat českou diakritiku. V současnosti není česká diakritika v heslech oficiálně podporována.

### 4.2. Doba platnosti hesel

V současnosti mají hesla neomezenou platnost.

Po nasazení nové politiky hesel (v produkčním prostředí od 16. 4. 2026, v testovacím prostředí je již nasazena) budou mít hesla nastavenou dobu platnosti cca **18 měsíců**.

Jakmile uplyne 530 dnů od poslední změny hesla, bude uživatel při prvním přihlášení do systému Czech POINT (nebo do jiného systému využívajícího přihlašování uživatelů



přes JIP/KAAS) vyzván systémem JIP/KAAS ke změně hesla z důvodu blížího se konce platnosti hesla. Výzvu ke změně hesla nebude možné přeskočit.

Uživatel bude mít 3 pokusy na změnu hesla, pokud technické problémy (zejména problémy se síťovým připojením) znemožní úspěšné dokončení změny hesla. Po vyčerpání všech pokusů nebude uživateli dovoleno se přihlásit a změnu hesla bude muset provést lokální administrátor ve Správě dat.

## 4.3. Informace poskytované editační webovou službou JIP/KAAS v souvislosti s bezpečnostní politikou hesel

### 4.3.1. Vytvoření nebo změna hesla

Pokud editační webová služba JIP/KAAS přijme požadavek na vytvoření nového uživatelského účtu (metody CreateUser a CreateOrganizationUser), nebo request na změnu hesla pro stávající účet (metody UpdateUser a UpdateOrganizationUser), provede kontrolu, zda v requestu obsažené heslo splňuje politiku hesel systému Czech POINT. Pokud je heslo „slabé“ nebo bylo již použito, vrátí webová služba v odpovědi chybový kód.

Systém komunikující s editační webovou službou by měl umět na tento chybový stav zareagovat v závislosti na dostupných možnostech. Např. pokud je webová služba JIP/KAAS volána ihned po změně hesla uživatelem v daném systému, měl by systém uživateli zobrazit chybovou hlášku, že heslo není dostatečně „bezpečné“, a požádat uživatele o zadání nového hesla.

Pokud je webová služba JIP/KAAS volána až v rámci backendových synchronizačních procesů bez interakce s uživatelem, musí být chybový stav např. zaznamenán do aplikačního logu, notifikován administrátorem systému či použit jiný mechanismus, který zajistí, že se problémem selhání synchronizace „slabého“ hesla do JIP/KAAS bude zabývat příslušná zodpovědná osoba, která např. požádá uživatele o zopakování změny hesla.

Problému synchronizace „slabých“ hesel se dá také předejít tak, že v systému napojeném na JIP/KAAS se nasadí stejná (nebo přísnější) bezpečnostní politika hesel jako v systému Czech POINT.

### 4.3.2. Vypršení platnosti hesla

Před vypršením platnosti hesla vyzve JIP/KAAS uživatele ke změně hesla uloženého v JIP. Vznikne tak nesoulad, kdy JIP obsahuje nové heslo uživatele, zatímco napojený systém obsahuje stále původní heslo.

Optimálním řešením je, aby uživatel vždy měnil své heslo v napojeném systému, který pak zajistí synchronizaci nového hesla do JIP/KAAS. Uživatel tak má v obou systémech nastaveno stejné heslo.

Editační webová služba bude poskytovat v informacích o uživateli (metody GetUser a GetOrganizationUser) datum poslední změny hesla (pwdChangedTime) a datum konce platnosti hesla (passwordExpirationTime). Napojený systém bude moci využít tyto údaje k určení časového okamžiku, kdy napojený systém sám vyzve uživatele ke změně hesla, a následně zajistí synchronizaci nového hesla do JIP/KAAS Czech POINT. Oba tyto údaje „pwdChangedTime“ a „passwordExpirationTime“ jsou nyní nasazeny v testovacím prostředí Czech POINT a do produkčního prostředí budou přidány v rámci nasazení nové politiky hesel v dubnu 2026.

## 4.4. Informace o testování nové politiky hesel

Nová politika hesel je již nyní nasazena v testovacím prostředí Czech POINT, kde si ji vývojáři aplikací třetích stran mohou testovat (prostřednictvím webových služeb JIP/KAAS nebo v aplikaci Správa dat).