

Výpočetní služba – zapnutí HTTPS

Výpočetní služba přepočítává docházku. Pokud běží na **jiném stroji než aplikační server**, posílá si s ním data po síti – a tehdy je vhodné spojení zašifrovat pomocí HTTPS. Tento návod popisuje ruční nastavení pro verzi **Aktion.NEXT 5.3**.

Tip: Instalátor HTTPS sám nenastavuje, ale ručně provedené nastavení při aktualizaci zachová.

KDY HTTPS POTŘEBUJETE

Instalace	Jak služba poslouchá	HTTPS
Služba na stejném stroji jako aplikační server (výchozí)	http://localhost: – ze sítě nedostupná	není potřeba
Služba na jiném stroji (samostatná komponenta instalátoru)	http://*: + výjimka ve firewallu	doporučeno

Aplikační server posílá službě s každým požadavkem sdílený klíč v hlavičce X-Calculatation-Key. **Bez HTTPS putuje klíč i obsah požadavků po síti nešifrovaně.**

Ve verzi 5.3 volá výpočetní službu pouze aplikační server (serverové API eNextu chodí přes něj). Nastavení se proto mění jen na dvou místech: ve službě a v konfiguraci aplikačního serveru.

NEŽ ZAČNETE

Co	Podrobnosti
Instalace	Hotová instalace na dvou strojích: nejdřív aplikační server s adresou služby, potom služba na druhém stroji. Přepočty přes HTTP už fungují.
Certifikát	Vystavený na plné jméno stroje se službou (FQDN), se soukromým klíčem, uložený v úložišti LocalMachine\My na stroji se službou. Certifikační autorita, která ho vydala, musí být důvěryhodná na stroji s aplikačním serverem.
Port	Volný TCP port pro HTTPS, například 2224. Instalátor ho nezná – u více instancí na jednom stroji ohlídejte, aby se porty nepřekrývaly.
Oprávnění	Správce na obou strojích.
Odstávka	Restart obou služeb, řádově minuty. Automatické přepočty počkají ve frontě v databázi, ruční přepočet spuštěný během restartu skončí chybou.

POSTUP V KOSTCE

1. **Stroj se službou:** najděte jméno certifikátu.
2. **Stroj se službou:** vytvořte soubor `appsettings.Production.json` s nastavením HTTPS.
3. **Stroj se službou:** firewall – nic není potřeba, volitelně pravidlo zúžíte.
4. **Stroj s aplikačním serverem:** změňte adresu služby na `https://...`
5. **Oba stroje:** restartujte služby a ověřte spojení.

KROK 1 – CERTIFIKÁT (STROJ SE SLUŽBOU)

V PowerShellu vypište certifikáty v úložišti počítače. Budete potřebovat jméno z pole **Subject**:

```
Get-ChildItem Cert:\LocalMachine\My | Format-List Subject, NotAfter, Thumbprint, HasPrivateKey
```

Zkontrolujte, že certifikát není prošlý (NotAfter) a má soukromý klíč (HasPrivateKey = True). Služba běží pod účtem LocalSystem, takže ke klíči v úložišti počítače má přístup bez dalšího nastavování.

KROK 2 – NASTAVENÍ SLUŽBY (STROJ SE SLUŽBOU)

Ve složce služby `{instalace}\CalculationService` vytvořte soubor `appsettings.Production.json` s tímto obsahem (jméno certifikátu a porty upravte podle sebe):

```
{
  "Kestrel": {
    "Endpoints": {
      "Http": { "Url": "http://localhost:2223" },
      "Https": {
        "Url": "https://*:2224",
        "Certificate": {
          "Subject": "vypocet.firma.local",
          "Store": "My",
          "Location": "LocalMachine"
        }
      }
    }
  }
}
```

Co jednotlivé části znamenají:

- **Http** – přesune nešifrovaný přístup jen na tento stroj (localhost). Řádek nevynechávejte: bez něj by původní adresa `http://*`: z instalace zůstala otevřená do sítě vedle HTTPS. Port ponechte stejný jako při instalaci.
- **Https.Url** – hvězdička znamená všechna síťová rozhraní. Má-li stroj více síťových karet, je lepší uvést konkrétní IP adresu.
- **Certificate.Subject** – jméno z certifikátu z kroku 1. Certifikát jde načíst i ze souboru (Path + Password), heslo by ale bylo čitelně v souboru – proto doporučujeme úložiště.
- Ověřování volajícího se nemění – párování klíčem, které nastavil instalátor, zůstává.

Proč právě tento soubor? Soubor `appsettings.json` instalátor při každé instalaci skládá znovu. Soubor `appsettings.Production.json` nechává být a jeho hodnoty mají přednost – nastavení HTTPS tak přežije aktualizaci.

KROK 3 – FIREWALL (STROJ SE SLUŽBOU)

Nic nového nastavovat nemusíte. Instalátor samostatné službě přidal pravidlo `AktionNEXT.CalculationService` pro program služby, platí tedy pro všechny její porty. U vícenásobné instalace má pravidlo za názvem jméno instance v závorce.

Volitelně můžete pravidlo zúžit jen na adresu aplikačního serveru:

```
Set-NetFirewallRule -DisplayName 'AktionNEXT.CalculationService' -RemoteAddress 10.0.0.15
```

KROK 4 – ADRESA SLUŽBY (STROJ S APLIKAČNÍM SERVEREM)

V souboru `{instalace}\AppServer\AppServer.exe.config` změňte adresu služby na HTTPS:

- Jméno v adrese musí odpovídat certifikátu. IP adresa projde jen tehdy, když ji certifikát obsahuje.
- Klíče `DochazkaVypocetSluzbaKlic` a `DochazkaVypocetVlastnik` neměňte.
- Adresu jde zadat i v průvodci instalátoru – pole s adresou služby na jiném počítači přijme i `https://`.
- Verzi protokolu TLS určuje nastavení Windows. Na straně aplikačního serveru se nic dalšího nenastavuje.

KROK 5 – RESTART OBOU SLUŽEB

```
Restart-Service 'AktionNEXT.CalculationService' # stroj se službou
Restart-Service 'AktionNext.AppServer' # stroj s aplikačním serverem
```

U vícenásobné instalace mají obě služby v názvu příponu \$INSTANCE.

OVĚŘENÍ

Kontroly spouštějte **ze stroje s aplikačním serverem** – ověříte tím i cestu přes síť a důvěru v certifikát.

```
[Net.ServicePointManager]::SecurityProtocol = 'Tls12' # jen ve Windows PowerShell 5.1
```

```
# 1) dostupnost a platný certifikát: 200 + hlavička X-Calculatation-Owner: Service
Invoke-WebRequest https://vypocet.firma.local:2224/health -UseBasicParsing |
    Select-Object StatusCode, Headers
```

```
# 2) nešifrovaný port už ze sítě dostupný není: TcpTestSucceeded = False
Test-NetConnection vypocet.firma.local -Port 2223
```

Spojení je v pořádku, když:

1. První dotaz vrátí 200 a hlavičku X-Calculatation-Owner. Případná chyba certifikátu se projeví právě tady.
2. Druhý test skončí **neúspěchem** – port 2223 už poslouchá jen lokálně.
3. V logu aplikačního serveru ({instalace}\AppServer\AppServer.log) je po startu řádek „Vypocetni sluzba <https://vypocet.firma.local:2224/> je pripravena.“ Tím je ověřené šifrované spojení i klíč.
4. V logu služby (CalculationService\logs\calculation-.log) je řádek „Autentizace: schéma ApiKey, povolení volající: ...“ s volajícím AppServer (calc-admin).
5. Ruční přepoččet jedné osoby z klienta proběhne bez chyby – projde celou cestou včetně ověření.

CO SE STANE PŘI AKTUALIZACI

Kde	Co udělá instalátor	Důsledek
appsettings.json služby	Složí ho znovu (http://*: a klíč).	Nevadí – appsettings.Production.json má přednost.
appsettings.Production.json	Nesahá na něj.	HTTPS zůstává.

Adresa služby v konfiguraci aplikačního serveru	Předvyplní ji do průvodce a zapíše zpět; tichá instalace ji převezme.	Adresa https://... zůstává.
Klíč	Na obou stranách ho zapíše znovu z databáze.	Beze změny.
Pravidlo firewallu	Smaže ho a založí znovu.	Zúžení na adresu (krok 3) je potřeba zopakovat .

Tip: Po každé aktualizaci zopakujte kontroly z kapitoly Ověření.

ČASTÉ POTÍŽE

Příznak	Příčina	Řešení
Služba po restartu neběží; v logu služby nebo v protokolu událostí Windows je chyba certifikátu.	Certifikát podle Subject nebyl nalezen, je prošlý nebo nemá soukromý klíč.	Zopakujte krok 1 a opravte Subject.
Chyba důvěry nebo neshoda jména certifikátu.	Adresa neodpovídá certifikátu, nebo stroj s aplikačním serverem nezná vydávající autoritu.	Použijte jméno z certifikátu; autoritu naimportujte do LocalMachine\Root.
„Vypocetni sluzba ... neodpovida“	Špatný port v adrese, firewall, nebo služba neběží.	Test - NetConnection na port HTTPS, log služby.
401 / 403 a v logu aplikačního serveru rada o Calculation:Auth:Clients	Klíče na obou stranách se rozešly (ruční zásah do jedné z nich).	Srovnejte DochazkaVypocetSluzbaKlic s klíčem v nastavení služby, nebo znovu spusťte instalátor.
503 u ručního přepočtu	S HTTPS nesouvisí – služba výpočet nevlastní.	Srovnejte Calculation:Owner ve službě s DochazkaVypocetVlastnik v aplikačním serveru.
Po obnově certifikátu spojení přestane fungovat.	Certifikát se načítá při startu služby.	Restartujte službu; restart zařadte do postupu obnovy certifikátů.

OMEZENÍ

- **Varování o nešifrovaném přístupu se u instalace z instalátoru nevypíše.** Kontrola při startu služby adresu s hvězdičkou (http://*:) nepozná. Na log se proto nespolehejte – rozhoduje test portu z kapitoly Ověření.
- **Aplikační server nemusí certifikát ověřovat.** Synchronizace kalendářů s Exchange nebo Kerio a DataPro vypínají kontrolu certifikátů pro celý aplikační server. Spojení je pak šifrované, protistrana ale ověřená není a chybný certifikát se neohlásí.
- **Ověřování účtem Windows (Negotiate) aktualizaci nepřežije.** Instalátor aplikačního serveru se službou

na jiném stroji zapíše klíč při každé instalaci a s vyplněným klíčem se server účtem nehlásí. Pro službu na jiném stroji proto používejte klíč + HTTPS.

- **Klíč je uložený čitelně** – v konfiguraci obou stran i v databázi. Ruční zašifrování (dpapi :) instalátor při další instalaci přepíše. Počet pokusů o přihlášení klíčem služba neomezuje.
- **Od verze 5.4** bude službu volat přímo i serverové API eNextu. Pokud poběží na jiném stroji než služba, platí pro něj stejný požadavek na HTTPS a přibude mezi povolené volající v `appsettings.Production.json`.