

Integrace přihlášení do docházky z jiných systémů

Tento návod popisuje několik možností jak přihlášení zaměstnance do uživatelského menu docházky integrovat do jiných systémů, například pro vytvoření ikony na plochu nebo integrace do vašeho intranetového portálu.

Pokud potřebujete do jiných systémů načítat z docházky data nebo je do docházky přenášet, jedná se o jinou problematiku a tu najdete popsanou v příručce *webapi.pdf* na instalačním či aktualizacím disku docházky ve složce /Příručky/

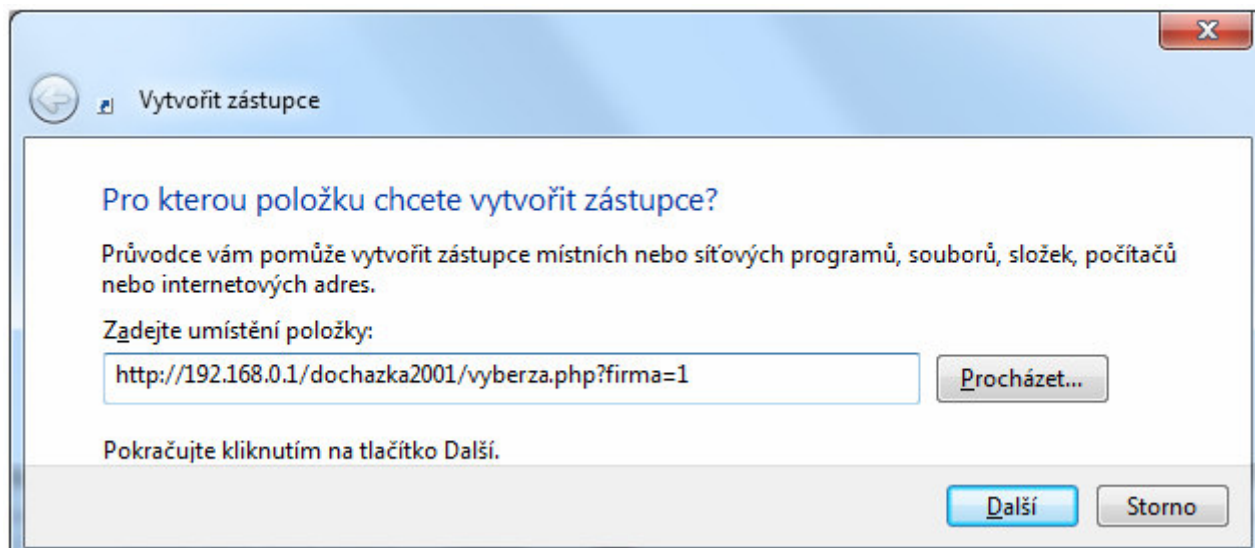
Případně pokud řešíte jen potřebu přihlášení do docházky stejným heslem jako je v doméně Windows a chcete třeba i ověřování přihlášení provádět vůči doméně, najdete postup v programu v menu „Zaměstnanci / Editace údajů / Import-Export z Active Directory (LDAP)“ – ikona modrého otazníku vpravo dole

Ikona na plochu windows počítače zaměstnance pro vstup na přihlášení do docházky:

Vytvoření ikony na plochu pro naštvení přihlašovacího formuláře docházky je velice snadné. Metodu lze použít i pro vytvoření odkazu například pro integraci do vašeho intranetu..

Při vytváření ikony (odkazu) na ploše Windows přes pravé tlačítko myši a volby "Nový / Zástupce" se do pole "Zadejte umístění položky" vloží webový http odkaz na docházku. Například takto:

http://192.168.0.1/dochazka2001/vyberza.php?firma=1



Místo IP adresy *192.168.0.1* zadejte IP adresu či DNS název vašeho PC s docházkou.

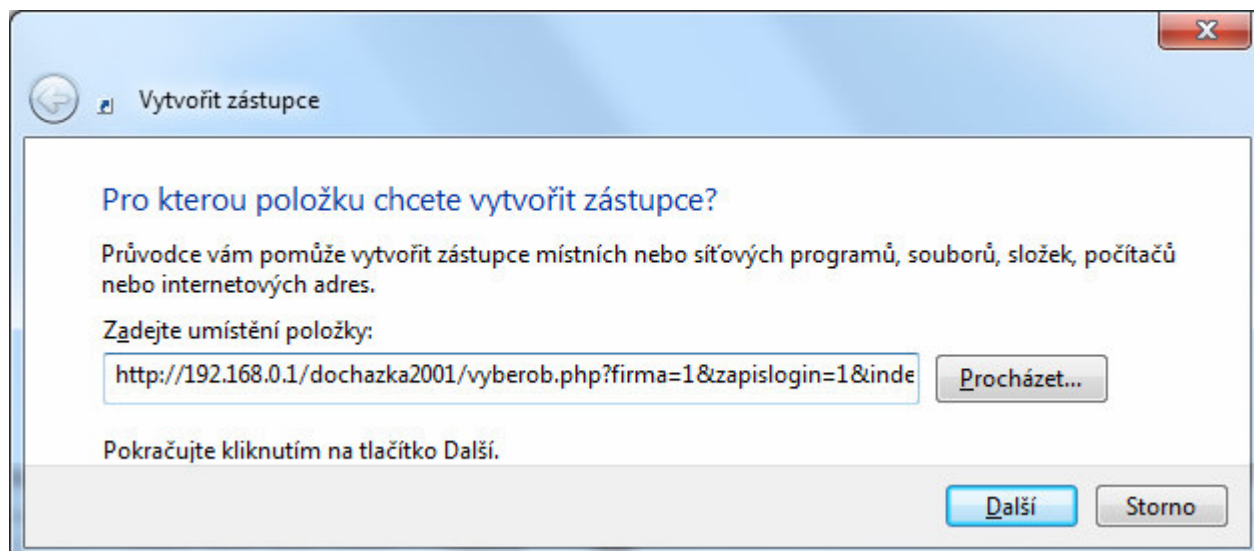
Jakmile pak uživatel na ikonu klikne, zobrazí se mu standardní přihlašovací dialog docházky, takže vybere své jméno, zadá heslo a klikne na tlačítko *Přihlásit*. Jelikož si docházky podle IP adresy pamatuje kdo se z tohoto počítače hlásil minule, tak pokud má každý uživatel své PC (se statickou IP adresou), bude již uživatel předvybrán, takže stačí zadat heslo a přihlásit se, což je ještě rychlejší.

Ikona na plochu windows zaměstnance pro vstup do docházky bez přihlášení heslem: (nedoporučuje se)

Pokud chcete zajistit zaměstnancům co nejrychlejší a nejpohodlnější přístup do SW docházky do uživatelského menu, je zde možnost vytvořit na ploše ikonu odkazující na docházku obsahující v parametrech údaje pro přihlášení včetně osobního čísla a hesla. Takže pak pracovník na ikonu jen klikne a naskočí mu již přihlášená docházka. Což lze využít například i v případě, když se uživatel do windows přihlašuje přes doménu odkud se mu plocha načítá a tak máte logování ošetřeno přes ActiveDirectory či podobný systém a nechcete uživatele nutit znovu zadávat heslo pro přístup do docházky. Vše ale konzultujte s vaším pracovníkem pověřeným ochranou osobních údajů (gdpr) – viz dále.

Při vytváření ikony (odkazu) na ploše Windows přes pravé tlačítko myši a volby "Nový / Zástupce" se do pole "Zadejte umístění položky" vloží webový http odkaz na docházku. Například takto:

http://192.168.0.1/dochazka2001/vyberob.php?firma=1&zapislogin=1&indexa=6&heslo=mojeheslo



Místo IP adresy *192.168.0.1* zadejte IP adresu či DNS název vašeho PC s docházkou.

Položku *indexa* nastavíte na osobní číslo (index) tohoto pracovníka pod kterým je zadaný v docházce. A položku *heslo* nastavíte na heslo které zaměstnanec při přihlášení do docházky používá.

Následně kliknete na *Další* a název zadáte například *Docházka* a nakonec kliknete na *Dokončit*.

Poslední parametr odkazu (heslo) je ale zároveň velice slabým místem tohoto postupu, protože heslo do docházky se zde uvádí v čitelné textové podobě a může je tak snadno zjistit kdokoli, kdo se dostane k PC tohoto zaměstnance. Což je hlavní důvod, proč se tento postup nedoporučuje a není ani v souladu s ochranou dat a GDPR i když je s ním pro zaměstnance přihlášení do programu pohodlné.

Pokud tedy chcete tuto metodu použít, doporučuje se aby uživatelé používali do docházky jiná hesla než mají do jiných systémů, aby případné zjištění hesla do docházky neoprávněnou osobou neohrozilo přístup jinam, například do windows, e-mailu atd.

Navíc lze v docházce nastavit povolenou IP adresu ze které se může zaměstnanec přihlašovat, takže pokud používáte statické přidělování IP adres počítačům nebo v DHCP serveru vázané na MAC adresu, nelze se přihlásit z jiného PC než z toho, které zaměstnanci patří, takže samotné zjištění hesla neoprávněnou osobou již ještě nestačí k tomu, aby se do docházky na někoho cizího přihlásila, musela by mít přístup ještě i k jeho PC a znát tedy přihlášení do windows, kde se ale pro zvýšení zabezpečení doporučuje mít jiná hesla než do docházky, takže zjištění hesla do docházky pak pro přihlášení nestačí. A v docházce lze v menu *Historie logování* dohledat případné neplatné pokusy o přihlášení, takže lze pokus o přihlášení neoprávněnou osobou snadno odhalit. Přehled logování vidí i samotný pracovník ve svém uživatelském menu, takže i on sám může snadno zjistit že se pod jeho účtem snažil přihlásit někdo jiný, kdy se tak dělo a z jakého PC (podle IP adresy uvedené v historii logování).

Postup zároveň funguje jen tehdy, když je v administraci v nastavení firmy prázdná položka pro *Standardní heslo*. Pokud tam nějaké standardní heslo zadané je, musíte jej předat parametrem *heslo*

Postup s tímto odkazem je možné použít nejen jako ikonu na plochu, ale odkaz můžete vložit například do intranetu do části pro přihlášené uživatele, takže když se uživatel přihlásí do vaší intranetové aplikace, nabídne se mu odkaz sestavený dle příkladu pro ikonu výše a tak lze docházku volat přímo z uživatelské sekce vaší intranetové aplikace a uživateli se pak rovnou zobrazí přihlášená docházka například v novém rámu webového prohlížeče.

Přístup do přihlášeného uživatelského menu přes šifrovaný odkaz s parametry předávanými hešem:

Od verze 9.36 Docházky 3000 lze použít další metodu přímého přihlášení do docházky ikonou na ploše windows nebo odkazem z intranetu bez nutnosti vybírat zaměstnance a zadávat heslo, a to pomocí heše. Tento heš je „zašifrovaný“ parametr pomocí kterého si Docházka zaměstnance dohledá aniž by v odkaze či ikoně muselo být uvedeno přihlašovací heslo a číslo zaměstnance v otevřené textové podobě. Heslo se v tomto případě vůbec nepoužívá a tak lze provést snadnější integraci například do vašeho intranetového portálu. Metodu lze ale použít i pro vytvoření ikony na plochu Windows.

V parametru URL či ikoně stačí šifrovat osobní číslo doplněné o nějaký *tajný* pevný prefix. Například

http://192.168.0.1/dochazka2001/hashloginza.php?firma=1 &login=5213fda5634ce87b2d40888692df42d6

kde v příkladu je obsah parametru *login* výstupem hešovací funkce MD5 z textu *ZamestnanecCislo1234* ve kterém je část *ZamestnanecCislo* tímto „tajným“ prefixem a 1234 je osobním číslem přihlašovaného pracovníka. Tu "tajnou" část zadáte do konfigurace docházky takže jí můžete v případě potřeby snadno měnit a stejně tak si vyberete vhodný hešovací algoritmus ze zhruba 40 dostupných.

Docházka pak z hešovaného parametru *login* pozná zaměstnance tak, že zkouší všechna osobní čísla všech zaměstnanců doplněná „tajným“ prefixem tak dlouho, dokud výstupní heš použitého šifrovacího algoritmu neodpovídá haši předanému v parametru *login*.

Takže pokud máte v programu 5 zaměstnanců s osobními čísly 1231 až 1235 a „tajný“ prefix nastavený dle příkladu výše na text *ZamestnanecCislo*, zkouší docházka hešovat vstupy *ZamestnanecCislo1231*, *ZamestnanecCislo1232*, *ZamestnanecCislo1233*, *ZamestnanecCislo1234* kdy u čísla 1234 bude heš odpovídat parametru *login* (*5213fda5634ce87b2d40888692df42d6*) a tak docházka ví koho má přihlásit.

Podporované hešovací algoritmy a jejich výstupy pro uvedený příklad jsou na obrázku na další straně, takže pokud by se vám MD5 nezdálo jako dostatečně bezpečné, lze použít i jiný z uvedených algoritmů.

Konfiguraci pro toto přihlašování přes parametry předávanými hešem naleznete od verze 9.36 v admin. menu „Zaměstnanci / Editace údajů“ dole v části „Přihlašování hešem“, kde podporu pro tuto metodu zapnete, vyberete hešovací algoritmus a zadáte „tajný“ prefix pro tvorbu heše z tohoto prefixu a osobního čísla.

Přístup do přihlášeného uživ. menu hešem

Umožňuje zpřístupnit přihlášené uživatelské menu jedním kliknutím přes ikonu na ploše windows nebo odkaz pro integraci například do intranetu bez nutnosti výběru zaměstnance a zadání jeho hesla. Podrobný popis naleznete v [této PDF příručce](#) v části nazvané *Přístup do přihlášeného uživatelského menu přes šifrovaný odkaz s parametry předávanými hešem*.

Povolit přístup zaměstnanců do přihlášeného uživatelského menu hešem

Výběr hešovacího algoritmu:	sha512	<input type="button" value="Test rychlosti CPU"/>
Zadejte tajný prefix pro tvorbu heše:	MujTajnyPrefix	
Ochrana proti útoku <i>hrubou silou</i> :	<input checked="" type="checkbox"/>	
<input type="button" value="Ulož"/>		

Prefix doporučujeme psát bez diakritiky kvůli vyloučení problémů s použitím různého kódování mezi různými systémy (ISO-Latin-2 vs Win1250 vs UTF8).

Volbu pro ochranu před útokem hrubou silou zapněte, čímž znemožníte útočníkovi zkoušet rychle různé heše. Což funguje tak, že pokud se někdo bude snažit přihlásit špatným hešem, další pokusy se na vteřinu zablokují aniž by byly vyhodnocovány, takže i pro slabý algoritmus MD5 by útočník potřeboval miliardy miliard let.

Dole pod nastavením je pak i tabulka s odkazy včetně hešů pro jednotlivé zaměstnance i s možností tisku, což se může hodit pro diagnostiku v případě, že by přihlášení z jiného systému nefungovalo. Prostě zde uvidíte jaké má být heš pro kterého pracovníka, takže můžete zkontrolovat zda vám váš externí systém, do kterého se snažíte přihlásit do docházky implementovat, generuje správné heše. Pokud ne, může být problém buď v odlišném algoritmu, osobním čísle zaměstnance nebo tajném prefixu (případně kódování jeho znaků – viz předchozí strana).

Přehled odkazů s heši loginu algoritmem sha512 u jednotlivých pracovníků:


Pracovník	Odkaz
Abrahám Adam (1134)	/hashloginza.php?firma=7&login=20b6fa3c5847a43fd70ccdc1c1553d22f9bec0ac134b8d3e0e3cc
Abrahám Josef (840)	/hashloginza.php?firma=7&login=f2af688d11a6b10a46b4068a2d2b7f443284f44e0a2158dc17a47
Adamcová Jaroslava (6)	/hashloginza.php?firma=7&login=3c9ad55147a7144f6067327c3b82ea70e7c5426add9ceea4d07d
Antoš Jiří (829)	/hashloginza.php?firma=7&login=53c8f80d12935e4f864111f554188011fe46348aab1433c578444
Blatný Josef (853)	/hashloginza.php?firma=7&login=702ae30824d43702a05820f53e32551f6f012fac3087a049445d5f
Svobodová Bohuslava (823)	/hashloginza.php?firma=7&login=318145b23c716032c101166b8836852b9d39f56e6c4c642a40ce
Zich Karel (809)	/hashloginza.php?firma=7&login=b4ff647683bab9ffc22801a2fe12122b3d8d18e024d4e127a4e6



















Tisk tabulky hešů pro zaměstnance

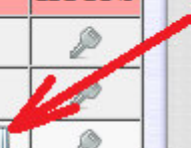
Pokud chcete pro zajímavost zjistit nevhodnější algoritmus dle CPU vašeho serveru pro optimální poměr bezpečnosti a rychlosti zpracování, použijte tlačítko "Test rychlosti CPU", kde vám program změří kolik váš procesor stihne spočítat hešů za vteřinu pro jednotlivé algoritmy.

Funkce	Počet hešů za vteřinu dle CPU a algoritmu pro PHP funkci hash() v Docházce 300							
	AMD Opteron X3216 na 2.8GHz, rok 2017	Pentium Dual Core E2220 na 2.4GHz, rok 2008	Pentium 4 2.6GHz, rok 2003	Intel Xeon X5560 na 2.8 GHz, rok 2010	AMD Athlon A8 5600K na 3.6GHz, rok 2012	Pentium Core2Duo E8400 na 3GHz, rok 2008	IBM PowerPC G5 na 2 GHz, rok 2003	
md2	207 331	55 196	19 320	225 490	60 052	68 792	131 934	
md4	909 786	569 723	387 203	1 352 749	824 604	716 554	319 818	
md5	906 512	549 681	358 477	1 330 154	792 345	693 246	324 123	
sha1	745 245	506 914	334 573	1 062 951	716 042	625 518	303 864	
sha224	642 195			786 349			244 933	
sha256	634 933	391 026	283 907	783 820	556 761	478 973	241 036	
sha384	553 722	162 265	90 754	663 020	207 109	203 508	127 541	
sha512	545 545	160 733	89 805	645 759	203 065	200 768	128 469	
ripemd128	719 509	367 166	265 220	1 004 839	557 001	455 736	264 939	
ripemd160	647 883	357 191	257 484	847 937	508 591	443 512	253 890	
ripemd256	755 549	392 048	268 377	963 691	554 864	481 500	266 853	
ripemd320	591 101	347 511	247 086	791 143	486 803	431 265	246 784	
whirlpool	460 810	213 561	125 295	573 030	252 565	268 225	92 762	
tiger128,3	752 330	428 354	253 313	1 136 003	599 761	518 708	261 619	
tiger160,3	668 965	403 910	254 818	1 131 554	605 541	514 692	259 821	

Ale dnešní procesory zvládnou u většiny algoritmů spočítat miliony hešů za vteřinu, i přes 20 let starý procesor Pentium 4 zvládne statisíce hešů za vteřinu, takže není potřeba mít obavy ze zatížení procesoru i kdybyste měli tisíce zaměstnanců a každý z nich se přihlašoval do docházky mnohokrát denně.

Od verze 9.43 jsou přihlášení přes heš rozpoznatelná od ostatních v menu *Firma / Historie logování* ikonou 

Datum	Pracovník	IP adresa	OS info	Stav	HTTPS
05.01.2024 09:13:22	Administrátor 	200.1.1.26	 / 	 OK	
06.01.2024 13:39:00	Bez Fondů (824)	200.1.1.4	 / 	 OK	
06.01.2024 13:46:50	Bez Fondů (824)	200.1.1.4	 / 	 OK	
06.01.2024 17:02:13	Administrátor 	200.1.1.75	 / 	 OK	

 Přihlášení Hešem

```
hash(algorithmus, "ZamestnanecCislo1234")
Algorithmus: md2 = b50a0baf3402d75a1af37466854749c8
Algorithmus: md4 = d17e7d52aa211a28671281be16ba4141
Algorithmus: md5 = 5213fda5634ce87b2d4d0888692df42d6
Algorithmus: sha1 = 13c663dc0ddff268be10c7d3b8752b2147ba7e9
Algorithmus: sha256 = b7b87ae50467725a0db44a19be07e67017b557cae34cd3aec80f90050cf4098b
Algorithmus: sha384 = b86dd27c2b055187445439ff216ce6eae9b16e556382e9a2d3d0dfbad6cb536dde9808de8bdff965f920d0f272dc2b6b44
Algorithmus: sha512 = f83f232aa6d7a793281097d30d96a7e9b4a873a30ddd6df72f0d5b7bae682f6b3171e0aa014d383890faa235f42b7f7e680a55529afe5f0cfa4fd216e91adc
Algorithmus: ripemd128 = ff87a7e6e866214a811ed87c29d8e37
Algorithmus: ripemd160 = bd02d1172a70e255d19e07680ce992445988a2de
Algorithmus: ripemd256 = 5cdceace6c5b1355b4c41aff36f9e76bcd27042286686db4032194dbc7134681
Algorithmus: ripemd320 = 5a9606a3dbdd66dd466dd4648f54187b8ad249baad3db38ca526e54745a114ecc85ea66139591c
Algorithmus: whirlpool = da9b0fc18eaca22c4bf7dbbc116c0b97c77fe8ad9aaddd8b6ef908e1f89d7eff2cb9a4c4f29b9f212bdff574fc518242a62379143059be1c4ffba91a6615e67b7
Algorithmus: tiger128,3 = 5fc315dea5abd67d53eab0230ec2a6a2f232156b2
Algorithmus: tiger160,3 = 5fc315dea5abd67d53eab0230ec2a6a2f232156b2
Algorithmus: tiger192,3 = 5fc315dea5abd67d53eab0230ec2a6a2f232156bb578e0ec
Algorithmus: tiger128,4 = 73272814414346f55d05aad55dee7c49
Algorithmus: tiger160,4 = 73272814414346f55d05aad55dee7c495eb2d49e
Algorithmus: tiger192,4 = 73272814414346f55d05aad55dee7c495eb2d49e8111257c
Algorithmus: snefru = 303b3f50904cdec8e83110d23db1b620c6ca8bda0fca82e9e1281702e8f582
Algorithmus: gost = 18b66bdateb05cded71a8894b08544b86f26f5a114e0e016db3d238c037874f
Algorithmus: adler32 = 3e076752
Algorithmus: crc32 = a946527b
Algorithmus: crc32b = 7293eebd
Algorithmus: havall128,3 = 2213e335899363a692491d2bc788546c
Algorithmus: havall160,3 = 1a34fce94ba824f63adc0442e40d5ff729cacad
Algorithmus: havall192,3 = ba5e451d46f0bc5d9e973839473e55cab3a2fc5447c85b77
Algorithmus: havall224,3 = e791822ef4f346e83d28db0205b6c581cdafb1482d1e62fdb260b9b2
Algorithmus: havall256,3 = 7eb2b50a3e6c805817b5d9189445c0bb070d15ba6e89c1832c4031511a87c3
Algorithmus: havall128,4 = 3f0505e44140a4b7f5462579e02193c7
Algorithmus: havall160,4 = 709316eef664e7b8563a16748b9d54f2a86a2f
Algorithmus: havall192,4 = 716f1b8995ad2f63874de0b3bd66de884765e9e99ec97b87
Algorithmus: havall224,4 = 1407df1009e59031a283ab7bf58e1d1df44a59869c75267d9b2af42d
Algorithmus: havall256,4 = 3a0952ce45ce9c7110f2eb0161fa00d819b6ab9d901be119bf6b379aec9d40e
Algorithmus: havall128,5 = 98fa2cb3771116c163590b982569fe74
Algorithmus: havall160,5 = 5bc3b02c434e66d29650d9b10f870596189ee3ef
Algorithmus: havall192,5 = bdf881a84206b91a96c4b81a8fb3ad435e6a195e2572a4f5
Algorithmus: havall224,5 = efc3d97e0d33a239ff7163e48929acd947b93d52b286de1e1abaf9889
Algorithmus: havall256,5 = 9ab5157a11d719eb4d6b9ea512dd4f7af5f0ca5d978add52cead8b80005fade0
```