Správa cloudových identit

Aktivace 2-faktorového ověření pro službu T-Cloud VDC

Datum poslední aktualizace návodu: 23. 11. 2025

Preambule

Účelem tohoto dokumentu je podrobný popis kroků, které jsou nutné pro aktivaci 2FA (dvou-faktorové autentifikace) pro přihlášení do administrace cloudu (VMware Cloud Director). Pro úspěšnou aktivaci 2FA je nutné mít na mobilním telefonu nainstalovanou aplikaci Microsoft Authenticator. (Další podporované jsou: Google Authenticator a FreeOTP.)

Autentifikátor poskytuje druhý ochranný faktor (prvním je uživatelské jméno a heslo). Zmíněným druhým faktorem je OTP (One Time Password), 6-místný číselný údaj, bez kterého není možné se do cloudové administrace přihlásit.

2FA je realizována pomocí portálu pro správu identit (dále též jako *PSI*), kde se řeší správa identit vůči administraci cloudu. Výchozí účet, kterému je umožněno spravovat identity, je ***IDMadmin***. Resp. přesný název účtu je **idmadmin@ACCxxx** . Pokud je v dalším textu použito pojmenování *IDMadmin* (velká písmena na začátku jsou použita pouze pro lepší přehlednost), je tím vždy míněn účet **idmadmin@ACCxxx**.

DOTČENÁ URL

Administrace cloudu
https://vcdx.dc.t-mobile.cz/tenant/ACCxxx
kde vcdx = vcd2 nebo vcd3
kde ACCxxx = unikátní identifikátor cloudového prostředí

Portál pro správu identit
https://kca-cust.vdi.cz.net/admin/ACCxxx/console | správa všech uživatelů (administrátorský kontext, lze se přihlásit jen účtem IDMadmin)
https://kca-cust.vdi.cz.net/realms/ACCxxx/account | správa dané identity (uživatelský kontext)
ACCxxx = viz výše

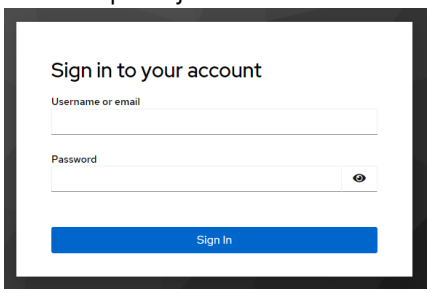
POZNÁMKY

1) *Nelze mít v PSI stejně pojmenovaný účet, jako je ten současný lokální.*
   Řešení je tedy lokální účet přejmenovat anebo v PSI použít jiný.
2) *Pokud máte, v rámci stejného internetového prohlížeče, v jedné záložce otevřen PSI portál a ve druhé administraci cloudu (https://vcdX.t-mobile.cz), může to být zdrojem chyb přihlašování. Snažte se této situaci vyvarovat.*
3) *Politika hesel*
   - *Délka min. 14 znaků*
   - *Nutné použít velká a malá písmena, číslici a speciální znak*
   - *Expirace po 365 dnech.*

4) *T-Cloud VDC podporuje i jiné druhy SAML ověření. Má-li tedy zákazník správu identit v MS Azure (EntraID), může využít tento typ ověření.*
   Návod na provázání T-Cloud VDC s EntraID zde: https://www.t-mobile.cz/ke-stazeni#/1274371 .

Krok č. 1 | První přihlášení do portálu pro správu identit

Přihlaste se do PSI (https://kca-cust.vdi.cz.net/admin/ACCxxx/console), který jste obdrželi e-mailem. Pro přihlášení použijte dočasné heslo k účtu *IDMadmin*. Tento účet slouží pouze pro administraci uživatelů, nelze se s ním přihlásit do cloudu. Toto rozhraní bude i v budoucnu sloužit ke správě uživatelských profilů (přístupů do cloudové administrace), url si tedy uschovejte pro případné pozdější využití.



Po nastavení 2FA pro hlavního uživatele *IDMadmin* lze vytvářet další uživatele a přidělovat jim patřičné role.

Pozn.: V situaci, kdy má do cloudové administrace přístup pouze jedna osoba, bude tato disponovat dvěma účty – IDMadmin účtem pro správu identit a vlastním účtem pro přihlášení do cloudové administrace.

Krok č. 2 | Přidání záznamu pro uživatele IDMadmin do aplikace Microsoft Authenticator (nebo jiné)

Po přihlášení se zobrazí dialog (*Mobile Authenticator Setup*) dle obrázku. Pokud nemáte na mobilním telefonu nainstalovánu (ideálně) aplikaci Microsoft Authenticator (MSA), doinstalujte ji.

Pozn_1.: Zde popsané sledy kroků je nutné opakovat pro každého uživatele, který má mít aktivní 2FA pro přihlašování do rozhraní cloudové administrace.

Pozn._2: Nejdříve je nutné 2FA aktivovat pro vlastní účet idmadnin (viz výše), následně i pro účty, skrze které se budete hlásit do cloudové administrace.

Další aktivity již v MSA:

a) V MSA *tapnout* na [**+**] pro přidání nového security tokenu

b) Vyberte položku [**Pracovní nebo školní účet**], následně [**Skenovat kód QR**]. Naskenujte QR kód (1), zobrazený okně *Mobile Authenticator Setup*. V MSA se vytvoří nový záznam **idmadmin** (umístěný na konci seznamu, pokud tam již máte jiné záznamy).

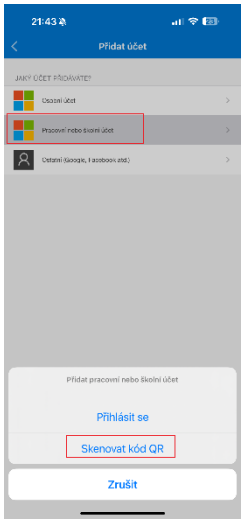
c) Klikněte na nově vytvořený záznam, zobrazené *Jednorázové heslo* (6-místné číslo) přepište do dialogu *Mobile Authenticator Setup* - textové pole *One-time code* (2). Do textového pole *Device Name* (3) vepište pojmenování zařízení s MSA dle vlastního uvážení.

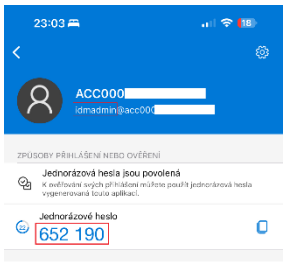
Pozn.: Doporučujeme nejdříve vyplnit Device name a teprve poté OTP. Předejdete tím situaci se selháním operace, protože vložený OTP kód již přestal platit.

d) Aplikaci MSA je možné opustit.

V okně *Mobile Authenticator Setup* klikněte na [**Submit**] (4). Postupujte dle dále uvedených kroků.

Tímto postupem došlo k aktivaci 2FA pro uživatele *IDMadmin*, který se použije pro přístup do portálu.



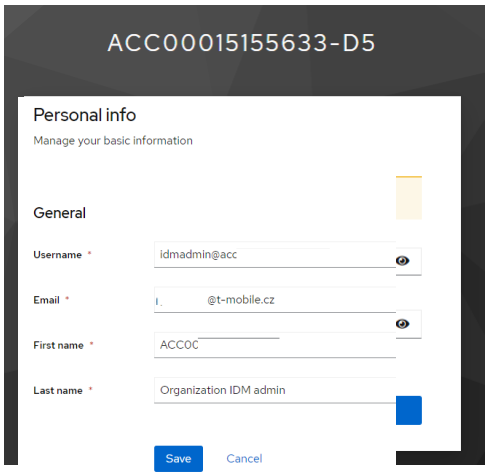


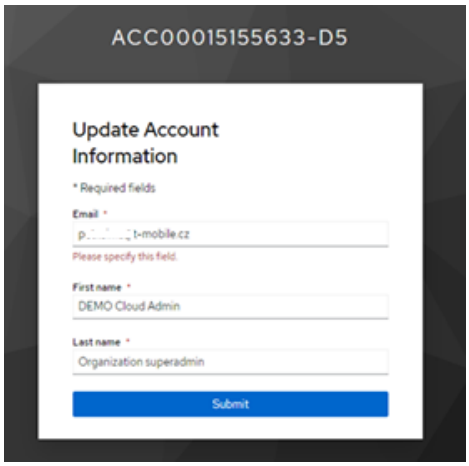
Krok č. 3 | Změna výchozího hesla uživatele IDMadmin

Pokud předchozí krok proběhl správně, zobrazí se dialog *Update password*. Zadejte nové heslo(1) do pole *New password*, znovu do pole *Confirm password*, poté zvolte [**Submit**].

V navazujícím dialogovém okně *Update Account Information* zadejte e-mail do pole *Email* (daný e-mail nelze použít u dalších účtů: platí tedy, každý účet má svůj unikátní e-mail), dále do textových polí *First name* a *Last name* patřičné údaje (anebo nechte předvyplněné výchozí hodnoty). Poté zvolte [**Submit**].

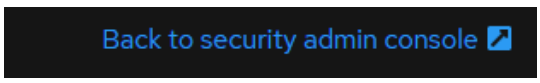
(1) Heslo je možné později změnit, viz dále.





Po provedení předchozího kroku se zobrazí kontext účtu idmadmin. (*Personal Info.*) Pro pokračování na krok č. 4 níže se z této stránky odhlaste. (Vpravo nahoře [**Sign out**].)

Pozn.: Jste-li na stránce, kde je v url slovo „realms“, jedná se o stránku (kontext) daného uživatele, zde nelze provádět administraci všech uživatelů.



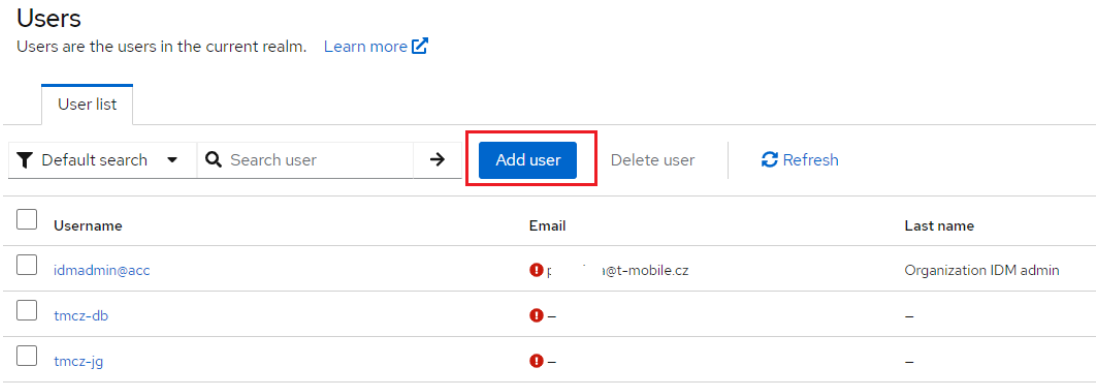
Pokud je vpravo nahoře dostupný odkaz [**Back to security admin console**], klikněte na něj – dostanete se na stránku pro správu uživatelů.

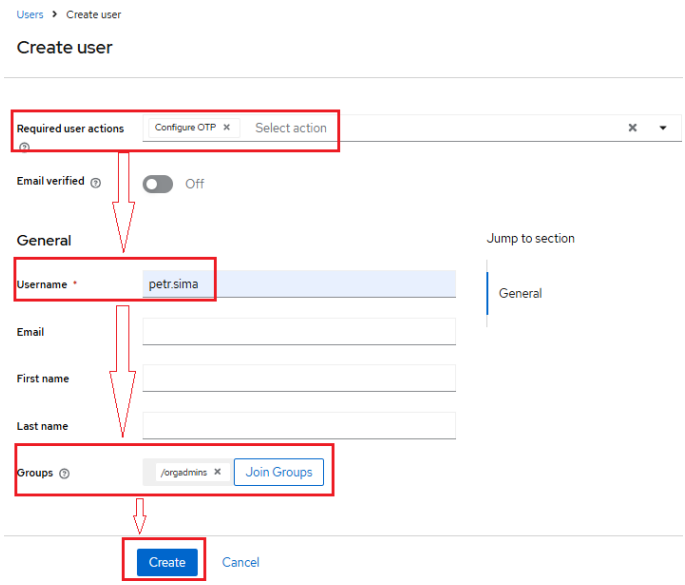
Krok č. 4 | Přidání nového účtu pro přístup ke cloudové administraci

(Dále uvedený postup platí obecně pro přidání libovolného nového účtu, který má přístup do administrace cloudu.)

Přihlaste se do PSI: https://kca-cust.vdi.cz.net/admin/ACCxxx/console. (Použijete účet idmadmin, heslo nastavené v kroku č. 3 a jednorázové heslo.)

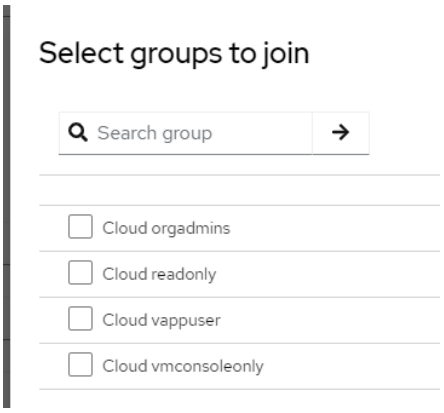
V menu vyberte [Users], zvolte [**Add user**].





V dialogovém okně *Create user* v roletovém menu *Required user actions* vyberte [**Configure OTP**]. Do pole *Username* zadejte patřičné uživatelské jméno (může být klidně e-mail), volitelně zadejte další údaje (*Email*, *First name*, *Last name*).

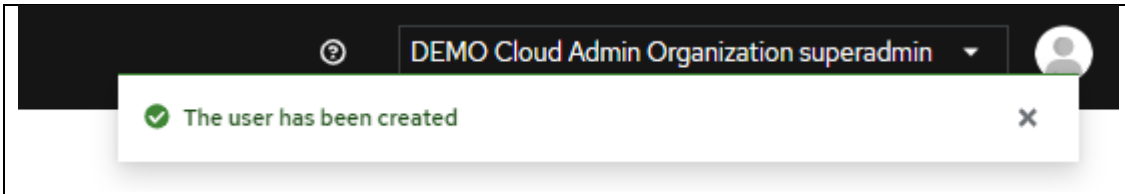
Pozn.: E-mail není ověřován, takže lze zadat cokoli, co má strukturu e-mailu. Nicméně pro případ, kdy bude nutné resetovat heslo nebo OTP se doporučuje zadat fungující e-mail.
Tato poznámka se týká pouze situace, že se nejedná o nové cloudové prostředí. Username nového uživatele se nesmí shodovat s již lokálně existujícím uživatelem. Pokud tedy máte již existujícího uživatele karel.novak, Username v PSI může být třeba karel.novak2.



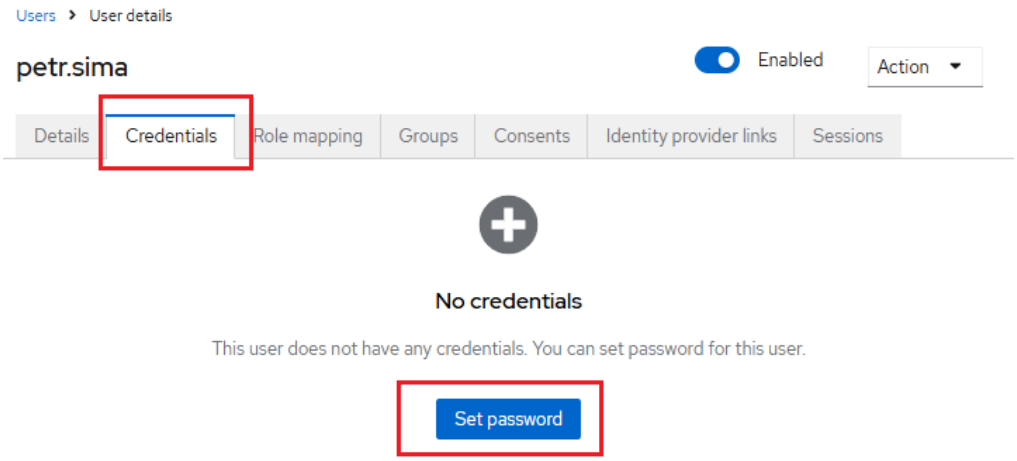
Dále je potřeba přiřadit patřičnou administrátorskou roli (nebo více rolí) skrze tlačítko [**Join Groups**]. V nově otevřeném dialogovém okně *Select groups to join* vyberte roli (role), které mají být danému účtu delegovány [1]. Po zaškrtnutí patřičné role (nebo rolí) zvolte [**Join**].

[1] Nejčastěji se bude jedna to roli [**Cloud orgadmins**], která má veškerá oprávnění pro ovládání cloudové administrace.

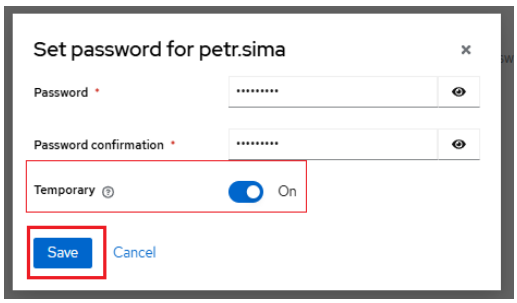
Opět v okně *Create user* zvolte [**Create**] pro vytvoření uživatele. Úspěšné vytvoření uživatele notifikuje zpráva v pravém horním rohu.



Ještě je potřeba danému účtu nastavit heslo. Na záložce *Credentials* zvolte [**Set password**].



V následujícím dialogu zadejte heslo do pole *Password*, opakujte do pole *Password confirmation*. Výchozí nastavení je, že dané heslo je *Temporary*. (Tedy, při prvním přihlášení nového uživatele do PSI bude nutné zadat heslo nové.) T-Mobile <u>důrazně</u> doporučuje ponechat volbu *Temporary* na **On**.



Po kliknutí na [**Save**] je zobrazen dialog, zda chcete opravdu nové heslo uložit. Zvolte [**Yes**].

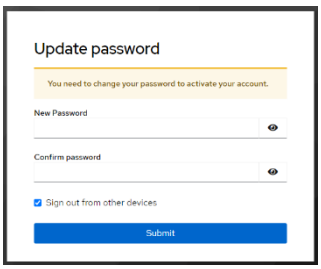
Jeli „aktivován“ nový účet v tom samém webovém prohlížeči, odhlaste (jako IDMadmin) z PSI. Přihlaste se jako nový uživatel, který byl v předchozím kroku vytvořen. Postupujte stejně, jako v případě aktivace IDMadmin účtu.

Pozn.: Pokud uživatele vytváříte pouze pro sebe sama, tak můžete nastavit finální heslo a volbu *Temporary* můžete ponechat vypnutou.

Krok č. 5 | Aktivace nového uživatele

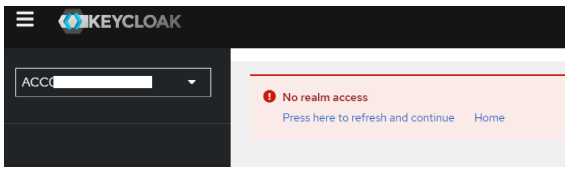
Nový uživatel provede následující sled kroků:

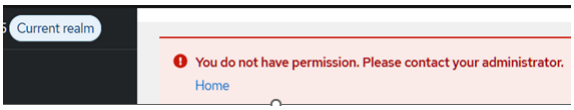
a) Přihlásí se ke speciálnímu url (PSI: https://kca-cust.vdi.cz.net/admin/ACCxxx/console) pomocí uživatelského jména (vytvořeno v kroku č. 4) a dočasného hesla.
b) Aktivace 2FA v MSA (viz krok č. 2).
c) Změna dočasného hesla – zadat nové:



d) Aktivace uživatele, který bude mít možnost přihlásit se do cloudové administrace, je dokončena.

e) Obvykle se poté zobrazí „chybový“ stav No realm access nebo You do not have pesmisson. Je to očekávaná situace, hlášku ignorujte.

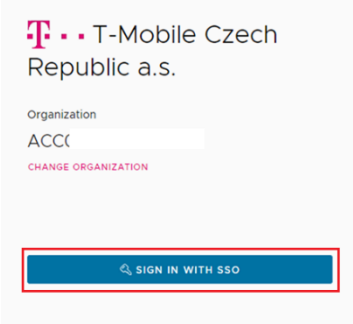




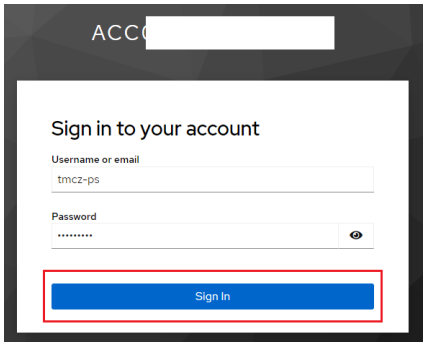
Krok č. 6 | Přihlášení do cloudové administrace

Postupujte takto:

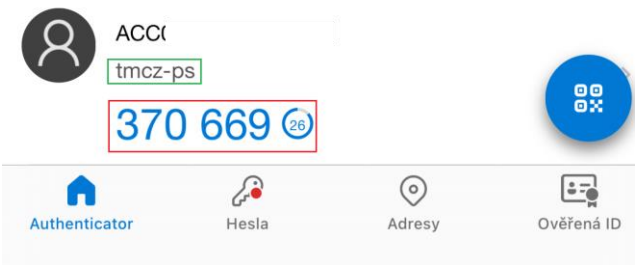
a) Přihlaste se do rozhraní cloudové administrace (https://vcdx.dc.t-mobile.cz/tenant/ACCxxx), klikněte na [**SIGN IN WITH SSO**].

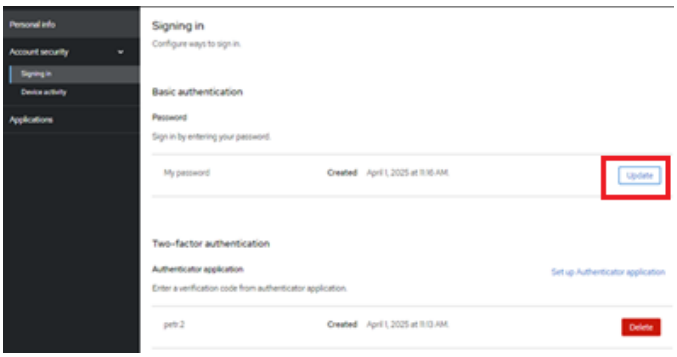
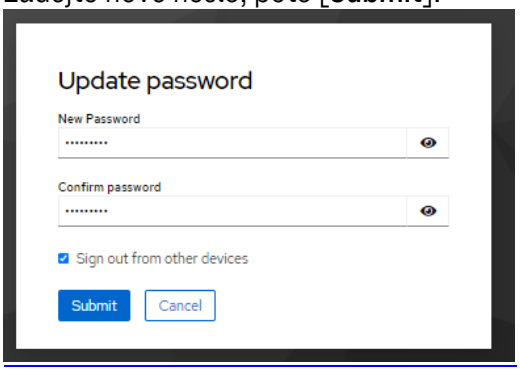


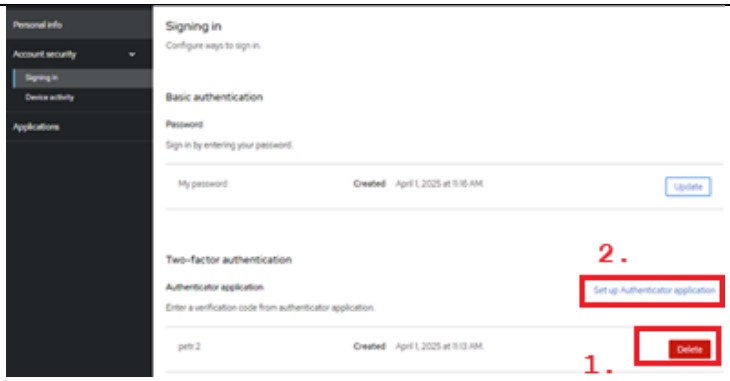
b) V další kroku (*Sign in to your account*) zadejte uživatelské jméno a heslo, poté zvolte [**Sign in**].



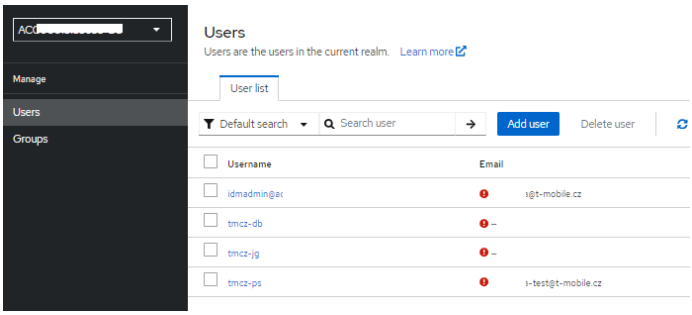
c) Zadejte OTP do textového pole *One-time code*, poté zvolte [**Sign in**]. Jste přihlášeni v cloudové administraci.



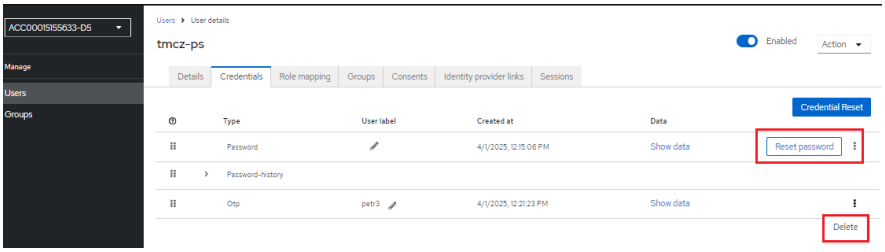
JAK ŘEŠIT RŮZNÉ ŽIVOTNÍ SITUACE	
Situace	**Řešení**
V cloudové administraci nelze vytvářet ani měnit uživatele.	V rámci přechodu na 2FA (dvou-faktorové ověřování) je zakázána možnost manipulace s lokálními účty. Jediná správná cesta je použít portál pro správu identit. Uživatel, vytvořený via portál pro správu identit má jako *Provider Type* uveden **SAML**.  Pozn.: Pokud je uživatel z PSI vymazán, v CD zůstane jako SAML zděděný záznam. Jedná se o přirozené chování platformy. Pouze na straně PSI se definuje, které účty mají přístup do cloudové administrace.
Jak si uživatel změní heslo?	Přihlaste se do PSI (https://kca-cust.vdi.cz.net/realms/ACCxxx/account) V PSI zvolte [Account Security] -> [Signing in] -> [**Update**].  Zadejte nové heslo, poté [**Submit**]. 
Jak lze přenést OTP pro již existujícího uživatele do nového Authenticatoru?	Přihlaste se do uživatelského kontextu PSI (https://kca-cust.vdi.cz.net/realms/ACCxxx/account). V PSI zvolte [Account Security] -> [Signing in] -> [**Delete**], potvrďte [**Confirm deletion**]. Pokračujte kliknutím na [**Set up Authenticator application**].

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Uživatel zapomněl heslo nebo potřebuje resetovat 2FA.</td><td>Přihlaste se do administrátorského kontextu PSI (https://kca-cust.vdi.cz.net/admin/ACCxxx/console) pomocí účtu IDMadmin.

V menu vyberte [Users], klikněte na vybraného uživatele.

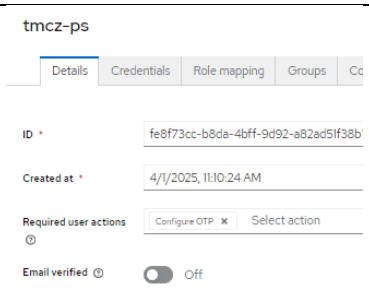
 

Dle situace zvolte [Reset password] anebo Otp -> [Delete]. Pokud je pro daného uživatele použit reálný e-mail, lze též použít [Credential Reset].

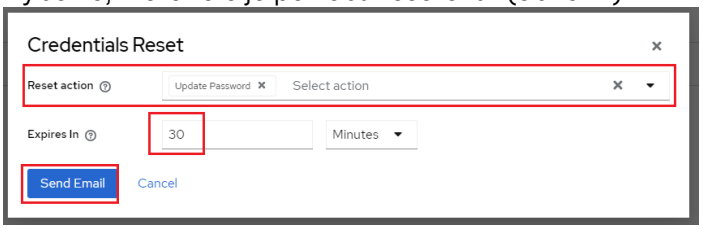
[Reset password]
a) Zadejte nové dočasné heslo, [Save], [Reset].
b) Uživatel se do uživatelského kontextu PSI (https://kca-cust.vdi.cz.net/realms/ACCxxx/account) přihlásí stávajícím uživatelským jménem a dočasným heslem, po zadání OTP z existující tokenu v MSA je zobrazen dialog pro zadání nového hesla. Po zadání zvolte [Submit].
c) Heslo je změněno, lze se přihlásit do administrace cloudu.

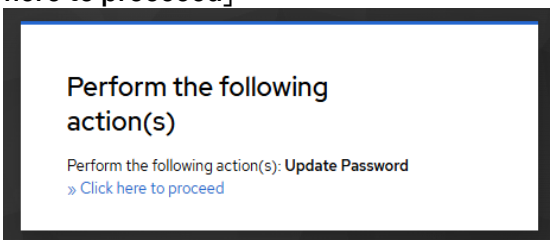
Otp -> [Delete]
a) Zvolte [Delete] pro Otp záznam, potvrďte [Delete].
b) Na záložce Details v menu Required user action zvolte akci [Configure OTP], poté [Save].</td></tr>
</table>

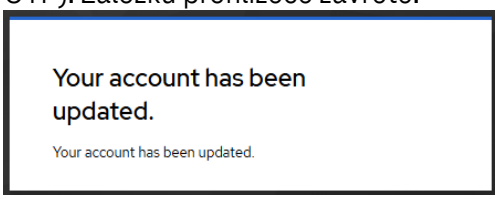
<table>
<tr>
<td></td>
<td>


Pozn.: Pokud již máte v MSA záznam pro účet, kterému se obnovuje OTP, je potřeba tento smazat. Anebo nový záznam jinak pojmenovat.

c) Uživatel se do uživatelského kontextu PSI (https://kca-cust.vdi.cz.net/realms/ACCxxx/account) přihlásí stávajícím uživatelským jménem a heslem. Poté je zobrazen dialog Mobile Authenticator Setup. Postup je shodný s tím, který je uveden v kroku č. 2 (str. 3).

[Credential Reset]
a) Vyberte, které role je potřeba resetovat (obnovit)


b) Do cca 1 minuty přijde e-mail (odesílatel: sso@dc.t-mobile.cz = T-Mobile SSO)
Další kroky provádí dotčený uživatel:
c) Kliknutí na odkaz v e-mailu
d) V dialogu Perform the following action(s) klikněte na [Click here to proceeed]


e) Proveďte požadované (zadání nového hesla či aktivace nového OTP). Záložku prohlížeče zavřete.


</td>
</tr>
<tr>
<td>Může být OTP pro idmadmin účet ve více autentifikátorech?</td>
<td>Ano, tento scénář je podporovaný. Pro více informací kontaktujte petr.sima@t-mobile.cz.</td>
</tr>
<tr>
<td>Jak lze resetovat OTP pro účet IDMadmin?</td>
<td>Tento požadavek řešte s TMCZ podporou: dohled@t-mobile.cz nebo non-stop linka 800 73 73 11.

Identifikujte tuto službu jejím ID, které jste obdrželi po zřízení služby.</td>
</tr>
</table>