Povolení / vynucení dvoufaktorové autentizace v Kerio Connect

Povolení dvoufaktorové autentizace v Kerio Connect

Přehled

Chcete na svých serverech Kerio Connect povolit dvoufaktorovou autentizaci pro zvýšení bezpečnosti, nebo se jen chcete připravit na povinnou 2FA autentifikaci?. Potřebujete pokyny, jak získat přístup k této funkci a jak ji povolit.

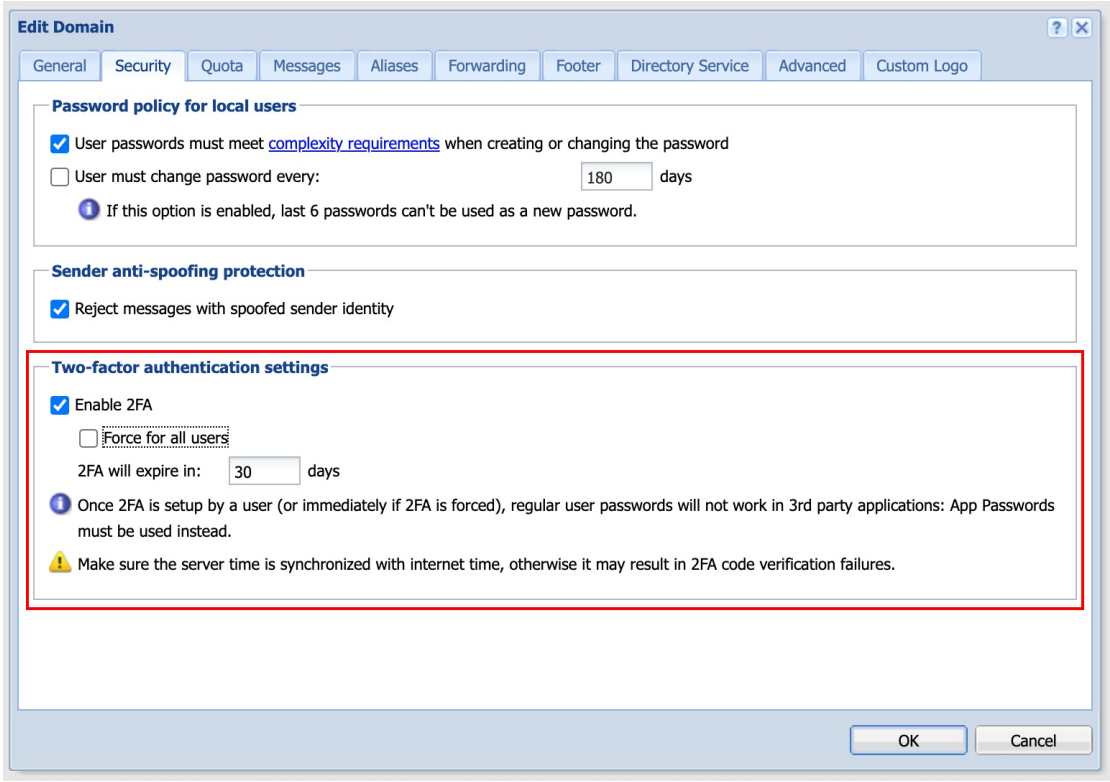
Řešení

Počínaje verzí Kerio Connect 9.4 můžete nyní využít dvoufaktorové ověřování (2FA) pro další zabezpečení přístupu. Využívá autentizátory mobilních zařízení Google a Microsoft k poskytnutí tokenu v reálném čase, aby administrátoři řídili potřebnou úroveň ochrany.

Proces aktivace funkce se provádí ve dvou částech – Povolení funkce pro konkrétní doménu a následná konfigurace funkce na úrovni uživatele.

Poznámka: Vzhledem k tomu, že ověřovací kód ve dvou krocích je založen na čase, je nutné zkontrolovat OS čas na serveru, kde je poštovní server Kerio Connect nasazen. Čas operačního systému by měl být synchronizován s časem internetu; jinak může dojít k selhání ověření.

Povolení dvoufaktoru pro doménu

1. Přejděte na **WebAdmin > Konfigurace > Domény** .
2. Upravte požadovanou doménu a vyberte kartu **Zabezpečení** .
3. V části „Nastavení dvoufaktorové autentizace“ zaškrtněte „ **Povolit 2FA** “.
1. 

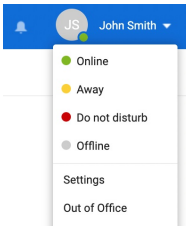
4. Po aktivaci můžete provádět úpravy na úrovni domény
    1. vynutit používání funkce 2FA výběrem možnosti **Force for all users** , tj. uživatelé musí nastavit 2FA, aby se mohli přihlásit, a
    2. upravit období, ve kterém 2FA vyprší.
    Poznámka : Při nastavování 2FA tato `2FA will expire in` hodnota definuje životnost tokenu 2FA v prohlížeči. Hodnota 30 dní například znamená, že jakmile se uživatel přihlásí pomocí kódu 2FA, nebude po dobu 30 dní **ve stejném prohlížeči znovu požádán o zadání kódu 2FA** (na jiném prohlížeči nebo počítači bude požádán o nový token). Pokud jej nastavíte na 0, bude uživatel **při každém zavření prohlížeče požádán o zadání kódu 2FA.**

Poznámka: Jakmile uživatel nastaví 2FA (nebo okamžitě, pokud je vynuceno), běžná uživatelská hesla již nebudou fungovat v aplikacích třetích stran (např. e-mailové klienty). Místo toho musí používat hesla aplikací (**Webmail/KCC > Nastavení > Hesla aplikací)** definovaná pro konkrétní aplikaci, ke které chtějí přistupovat.

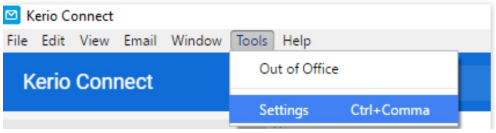
Konfigurace dvoufaktoru pro běžného uživatele

Jakmile bude funkce povolena pro doménu, uživatelé budou muset tuto funkci nakonfigurovat v aplikaci Webmail nebo Kerio Connect Desktop Client. Pokud jste se rozhodli vynutit používání nové funkce, uživatelé budou vyzváni ke konfiguraci dvoufaktoru při příštím přihlášení (nebo dokud nebude nakonfigurován). Jinak se mohou přihlásit k používání funkce a spustit stejnou konfigurační obrazovku.

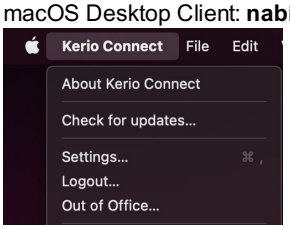
1. Otevřete Webmail nebo Kerio Connect Desktop Client
2. V uživatelském rozhraní přejděte do nabídky Nastavení
    1. Webmail: **Avatar > Nastavení:**



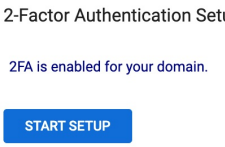
    2. Desktopový klient Windows: **nabídka Nástroje > Nastavení:**



    3. macOS Desktop Client: **nabídka Kerio Connect > Nastavení...:**



3. V dolní části levé navigační nabídky vyberte **Nastavení 2FA.**
4. Klikněte na tlačítko „Start 2FA Setup“:



5. V dialogovém okně potvrďte, že chcete zahájit nastavení dvoufázového ověření.
6. Tím se otevře panel Nastavení dvoufaktorové autentizace:

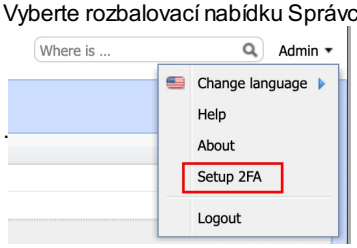
1. **Poznámka:** Toto je panel, který uživatelé uvidí při prvním přihlášení, pokud je pro doménu vynuceno 2FA.

7. Zadejte sekundární e-mailovou adresu, kterou chcete použít k obdržení resetovacího kódu pro dvoufázové ověření.
    1. **Poznámka:** Sekundární e-mailová adresa se musí lišit od aktuální e-mailové adresy. Doporučujeme, aby sekundárním e-mailem byla e-mailová adresa mimo domény, ke které máte přístup.
8. Naskenujte QR kód pomocí preferované ověřovací aplikace.
9. Aplikace Authentication vygeneruje šestimístný kód. Zadejte kód do sloupce Authentication token.
10. Po správném zadání všech informací systém požádá o konečné ověření.
11. Po ověření vás systém bude informovat, zda bylo dvoufázové ověření úspěšně nakonfigurováno. V závislosti na nastavení domény můžete být požádáni o odeslání ověřovacího kódu ve dvou krocích.

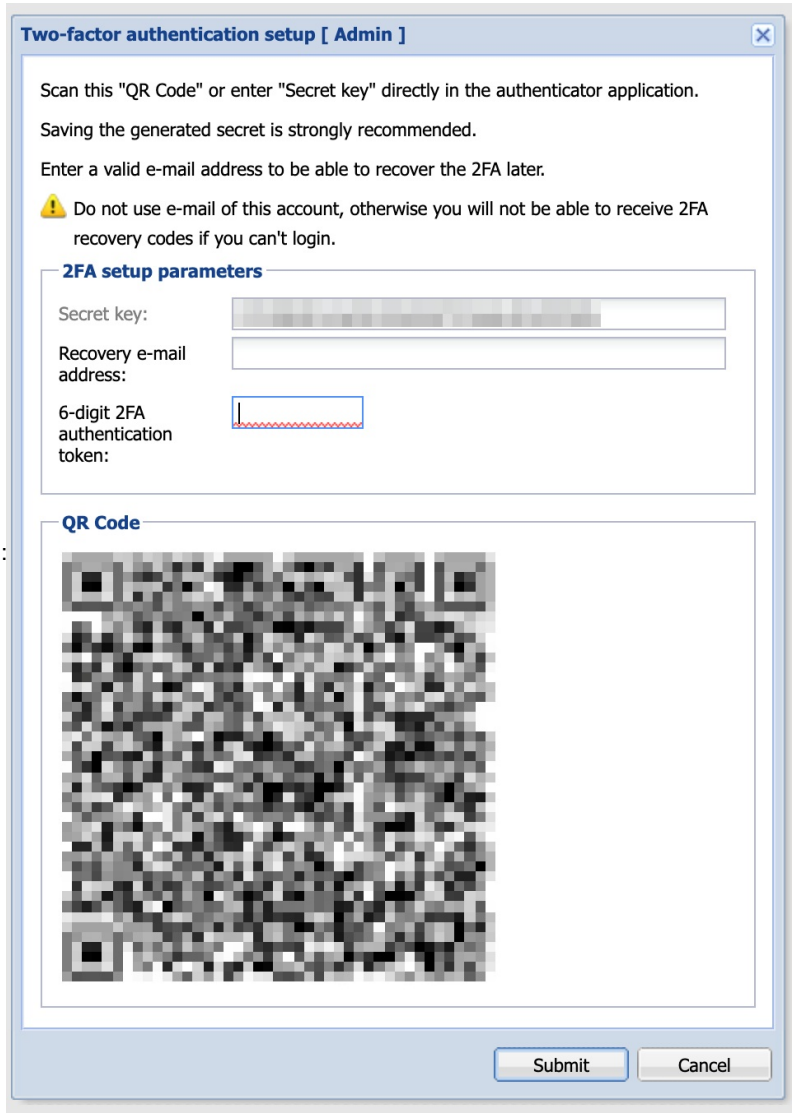
Konfigurace dvoufaktoru pro uživatele s oprávněním správce

Proces nastavení 2FA pro administrátory (vestavěné a vyhrazené administrátory) je stejný jako u běžných uživatelů výše, ale způsob, jakým přistupují k úvodnímu konfiguračnímu panelu 2FA, se liší.

1. Přihlaste se do WebAdmin pomocí svého administrátora.
2. Vyberte rozbalovací nabídku Správce v pravém horním rohu



3. Vyberte **Nastavení 2FA**
4. Zobrazí se podobné dialogové okno, abyste dokončili výše uvedené kroky 2FA


Two-factor authentication setup [Admin]
Scan this "QR Code" or enter "Secret key" directly in the authenticator application.
Saving the generated secret is strongly recommended.
Enter a valid e-mail address to be able to recover the 2FA later.
Do not use e-mail of this account, otherwise you will not be able to receive 2FA recovery codes if you can't login.
2FA setup parameters
Secret key:
Recovery e-mail address:
6-digit 2FA authentication token:
QR Code
Submit
Cancel