Logowanie

Aplikację uruchamia się poprzez kliknięcie na plik DMS.exe.



– ikona pliku uruchamiającego aplikację Comarch DMS

Aplikacja Comarch DMS ma domyślnie wprowadzonego użytkownika Administrator, który ma dostęp do konfiguracji aplikacji.

Aby zalogować się po raz pierwszy do aplikacji Comarch DMS w polu *Login* należy wpisać "*Administrator*", natomiast pole *Hasło* należy zostawić puste.

Następnie należy kliknąć ikonę ^(→) [Zaloguj się], aby przejść do aplikacji desktop Comarch DMS.

Uwaga Po zalogowaniu się do aplikacji **należy ustawić hasło dla** Administratora.

Wskazówka Jeżeli podczas logowania do nowoutworzonej bazy pojawia się komunikat: "Nieprawidłowy login lub hasło" zobacz<u>tutaj</u>

Wskazówka Jeżeli podczas próby zalogowania się do ComarchDMS pojawia się komunikat: Wystąpił błąd przy pobieraniu klucza licencji: 3 – zobacz <u>tutaj</u> Od wersji 2023.0.0 aplikacja desktop Comarch DMS domyślnie otwiera się na stronie startowej (zob. <u>Strona startowa</u>).

Użytkownik może zmienić to ustawienie w zakładce **Panel** użytkownika] tak, aby po zalogowaniu wyświetlana była lista dokumentów (zob. <u>Panel użytkownika</u>).

Strona startowa jest dostępna w każdej chwili w zakładce [Strona startowa]

W wersji 2024.3.0 wprowadzono funkcjonalność uwierzytelnienia dwustopniowego. Uwierzytelnienie dwustopniowe może być:

- Obowiązkowe jeśli zostało włączone przez administratora dla wszystkich użytkowników (zob. <u>Narzędzia</u>)
- Dobrowolne jeśli zostało ustawione przez danego operatora z jego własnej woli (zob. Konfiguracja)

Jeżeli administrator włączył obowiązkowe logowanie dwustopniowe dla wszystkich użytkowników, a dany operator nie ustawił wcześniej logowania dwustopniowego, wówczas musi je skonfigurować podczas kolejnego logowania – po wprowadzeniu loginu i hasła i kliknięciu "Zaloguj" zostaje otwarte okno "Włącz logowanie dwuetapowe".

1. Pobierz 2. Zeskanu 3. Zapisz k mógł odz	aplikację Google Authenticator na urządzeniu mobilnym. uj kod QR lub przepisz kod do aplikacji Google Authenticator. klucz bezpieczeństwa na zewnętrznym nośniku. Dzięki temu będziesz yskać dostęp do konta np. podczas utraty telefonu.	
mógł odz 4. Wpisz k	yskać dostęp do konta np. podczas utraty telefonu. od weryfikacyjny z aplikacji Google Authenticator.	
	Klucz bezpieczeństwa W6SU XRIT 7G5S 5DO3	
	Wpisz kod weryfikacyjny z aplikacji Google Authenticator.	
	Zapisz Anuluj	

Okno "Włącz logowanie dwuetapowe" wyświetlone przy logowaniu do aplikacji desktop Comarch DMS w przypadku, jeśli administrator włączył wymuszenie logowania dwuetapowego, a dany operator nie miał go uruchomionego

Następnie operator musi kolejno wykonać następujące czynności:

Pobrać aplikację Google Authenticator na urządzeniu mobilnym

2. Otworzyć aplikację Google Authenticator

3. W aplikacji Google Authenticator kliknąć w przycisk "Dodaj kod"

4. Wybrać jedną z następujących możliwych ścieżek postępowania:

 kliknąć w opcję "Zeskanuj kod QR" w aplikacji Google Authenticator i zeskanować kod QR widoczny w oknie "Włącz logowanie dwuetapowe" w aplikacji Comarch DMS

lub

 kliknąć w opcję "Wpisz klucz konfiguracyjny" w aplikacji Google Authenticator, a następnie w polu "Nazwa konta" wprowadzić nazwę, pod jaką będzie widoczne konto w aplikacji Google Authenticator, a w polu "Twój klucz bezpieczeństwa" wpisać 16cyfrowy kod dostępny w ramach pola "Klucz bezpieczeństwa" w oknie "Włącz logowanie dwuetapowe" w Comarch DMS. Po wprowadzeniu wartości należy nacisnąć przycisk "Dodaj" w aplikacji Google Authenticator

5. Zapisać kod z pola "Klucz bezpieczeństwa" na nośniku zewnętrznym – umożliwi to dostęp do konta w przypadku utraty lub usterki urządzenia mobilnego

6. W polu "Wpisz kod weryfikacyjny z aplikacji Google Authenticator" dostępnym w oknie "Włącz logowanie dwuetapowe" w Comarch DMS wpisać 6-cyfrowy kod weryfikacyjny wyświetlany w aplikacji Google Authenticator, zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w Comarch DMS należy wpisać kolejny wygenerowany kod

7. Kliknąć przycisk



[Zapisz].

 Pobierz aplikację Google Authenticator na urządzeniu mobilnym. Zeskanuj kod QR lub przepisz kod do aplikacji Google Authenticator. Zapisz klucz bezpieczeństwa na zewnętrznym nośniku. Dzięki temu będziesz mógł odzyskać dostęp do konta np. podczas utraty telefonu. Wpisz kod weryfikacyjny z aplikacji Google Authenticator. 	
Klucz bezpieczeństwa W6SU XRIT 7G5S 5DO3	
872 364 Zapisz Anuluj	

~

Okno "Włącz logowanie dwuetapowe" – wprowadzanie kodu w polu "Wpisz kod weryfikacyjny z aplikacji Google Authenticator"

Po kliknięciu przycisku **Zapisz [Zapisz]** operator zostanie zalogowany do aplikacji desktop Comarch DMS.

Jeżeli operator ma już włączoną weryfikację dwuetapową, wówczas przy kolejnym otwarciu okna logowania do aplikacji desktop i wprowadzeniu loginu i hasła, a następnie kliknięciu

w przycisk **Zaloguj się**] zostaje wyświetlone okno "Podaj kod z aplikacji". W ramach tego okna należy wprowadzić 6cyfrowy kod weryfikacyjny wyświetlany w aplikacji Google Authenticator (zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w oknie "Podaj kod z aplikacji" należy wpisać kolejny wygenerowany kod. Następnie operator powinien

kliknąć w przycisk (Zaloguj się] dostępny w ramach okna "Podaj kod z aplikacji".

COMARCH DMS	×
Login	
 Administrator	
Wpisz kod weryfikacyjny z aplikacji Google Authenticator.	

Okno logowania do aplikacji stacjonarnej Comarch DMS z oknem "Podaj kod z aplikacji"

COMARCH DMS	×
Wpisz kod weryfikacyjny z aplikacji Google Authenticator. 881 643	
(\ni
Okno "Podaj kod z aplikac wprowadzanie kodu w polu "Wpi weryfikacyjny z aplikacji	cji" - isz koc Google

Authenticator"

Po wprowadzeniu prawidłowego kodu weryfikacyjnego i naciśnięciu przycisku i okno "Podaj kod z aplikacji" zostają zamknięte, a otwiera się aplikacja desktop Comarch DMS.

W wersji 2024.1.1 wprowadzono możliwość **zablokowania logowania** po określonej liczbie prób logowania na wybrany okres czasu.

W tym celu w pliku Web.config znajdującym się w katalogu z plikami aplikacji serwerowej (dawna web) wprowadzono dwa nowe klucze:

- <add key='MaxLoginAttempts' value="5"/> w ramach tego klucza należy podać, jaka ma być maksymalna liczba prób logowania dla operatora zanim nastąpi zablokowanie logowania – domyślna wartość to 5
- -<add key='LoginBlockTime' value="60"/> w ramach tego klucza należy podać, po jakim czasie (liczonym

w sekundach) operator będzie mógł podjąć kolejną próbę logowania, po tym, jak logowanie zostało zablokowane – domyślna wartość to 60.

—	c [2]					
VVeb.co	ontig 🖬					• •
178						^
179	</th <th>"ERPSQLServer1" - 1</th> <th>t is necassary to define SQL Serv</th> <th>ver for ERP XL</th> <th>database. THE</th> <th>KEY</th>	"ERPSQLServer1" - 1	t is necassary to define SQL Serv	ver for ERP XL	database. THE	KEY
180	</th <th><add key="ERPSQLSer</th><th>verl" value="."></add>></th> <th></th> <th></th> <th></th>	<add key="ERPSQLSer</th><th>verl" value="."></add> >				
181					1 . 1	
182	</th <th>"ERPSQLServer2" - 1</th> <th>t is necassary to define SQL Serv</th> <th>Ver for ERP XL</th> <th>datapase. THE</th> <th>KEY</th>	"ERPSQLServer2" - 1	t is necassary to define SQL Serv	Ver for ERP XL	datapase. THE	KEY
100	<:	<add key="ERPSQLSer</th><th>verz value= <SQL server name> /</th><th>>></th><th></th><th></th></tr><tr><th>104</th><th>codd</th><th></th><th>admaReamderDirectionics" th="" wolver"<=""><th></th><th></th><th></th></add>				
105		key="DMUSersidallow	edioReorderDirectiories Value=	. />		
197	<pre>codd</pre>	kow-"we : Enable Brows	enlink" woluo-"false" />			
188	\auu	Key- VS.EnableBlows	ernink value- laise //			
189	bbc>	key="CompanyNameSea	rchModeEnabled" value="false" />			
190	lauu	кеу сотранунатереа	remodelinabled value laise //			
191	</th <th>UseRepository - def</th> <th>inition of cooperation workflow m</th> <th>nodule with th</th> <th>e repository m</th> <th>odul</th>	UseRepository - def	inition of cooperation workflow m	nodule with th	e repository m	odul
192	<add< th=""><th>kev="UseRepository"</th><th>value="false" /></th><th></th><th>e repositorij n</th><th></th></add<>	kev="UseRepository"	value="false" />		e repositorij n	
193			,.			
194	<add< th=""><th>kev="RepositoryUrl"</th><th>value="" /></th><th></th><th></th><th></th></add<>	kev="RepositoryUrl"	value="" />			
195	<add< th=""><th>key="WebClientUrl"</th><th>value="" /></th><th></th><th></th><th></th></add<>	key="WebClientUrl"	value="" />			
196		-				
197	</th <th>"PerformanceAnalysi</th> <th>sTimeRange" - time ranges for cha</th> <th>arts in perform</th> <th>mance analysis</th> <th>, sh</th>	"PerformanceAnalysi	sTimeRange" - time ranges for cha	arts in perform	mance analysis	, sh
198	<add< th=""><th>key="PerformanceAna</th><th>lysisTimeRange" value="1000,5000"</th><th>'/></th><th></th><th></th></add<>	key="PerformanceAna	lysisTimeRange" value="1000,5000"	'/>		
199						
200	</th <th>Number of possible</th> <th>login attempts before temporary]</th> <th>login blocking</th> <th>></th> <th></th>	Number of possible	login attempts before temporary]	login blocking	>	
201	<add< th=""><th>key="MaxLoginAttemp</th><th>ts" value="5" /></th><th></th><th></th><th></th></add<>	key="MaxLoginAttemp	ts " value="5" />			
202	</th <th>Determines for what</th> <th>time (in seconds) login will be</th> <th>blocked after</th> <th>unsuccessful</th> <th>attei</th>	Determines for what	time (in seconds) login will be	blocked after	unsuccessful	attei
203	<add< th=""><th>key="LoginBlockTime</th><th>" value="60" /></th><th></th><th></th><th></th></add<>	key="LoginBlockTime	" value="60" />			
204						
205	<th>ettings></th> <th></th> <th></th> <th></th> <th>\checkmark</th>	ettings>				\checkmark
206 -	</th <th></th> <th></th> <th></th> <th></th> <th>`</th>					`
						-
eXtensible	N length : 29	882 lines : 462	Ln:121 Col:65 Pos:9362	Windows (CR LF)	UTF-8-BOM	IN

Plik Web.config z nowymi kluczami MaxLoginAttempts i LoginBlockTime

Jeśli operator próbował zalogować się do aplikacji desktop Comarch DMS za pomocą błędnego loginu i/lub hasła, a liczba prób przekroczyła wartość wprowadzoną w ramach klucza <add key='MaxLoginAttempts' value="5"/>, wówczas poniżej pola "Hasło" zostanie wyświetlona informacja Wykryto zbyt wiele nieudanych prób logowania. Poczekaj i spróbuj ponownie.

W takim przypadku operator musi poczekać, aż upłynie czas określony w ramach klucza <add key='LoginBlockTime' value="60"/>, aby znów spróbować się zalogować.

DM	S
Login	
Adminisartor	
Hasło	
Wykryto zbyt wiele nieudanych pró	b logowania. Poczekaj
i sprobuj ponownie.	
zmień język	Zmień hasło
I sprobuj ponownie. Zmień język zapamiętaj logowanie	Zmień hasło

Okno logowania do aplikacji desktop Comarch DMS w trybie jednofirmowym – jeśli operator próbował logować się za pomocą błędnych danych zbyt wiele razy

	OMS
Spółka	
Domyślna spółka	~
Login	
Administrrator	
Hasło	
•••••	
Wykryto zbyt wiele nieudany i spróbuj ponownie.	/ch prób logowania. Poczekaj
Zmień język	Zmień hasło
	(\rightarrow)

Okno logowania do aplikacji desktop Comarch DMS w trybie wielofirmowym – jeśli operator próbował logować się za pomocą błędnych danych zbyt wiele razy

Funkcjonalność logowania oferuje również opcję zapamiętywania logowania.

	COMARCH DMS	×
Login		
Hasło		
Zmień język	Zmień hasło	
zapamiętaj logowanie	(\rightarrow)	

Okno logowania do systemu

	COMARCH DMS	×
Spółka		
Domyślna spółka	~	
Login		
Hasło		
Zmień język	Zmień hasło	
zapamiętaj logowanie	(\rightarrow)	

Okno logowania do systemu w trybie wielospółkowym

Paramet r	[zapamiętaj logowanie] –
zaznaczenie parametru oznacza	a, że operator jest zalogowany w
Comarch DMS do momentu użyci	a funkcji 💻 [Wyloguj się].
Gdy zalogowany operator zamk	nie okno Comarch DMS za pomocą
przycisku ^{– ⊡} ⊠ , ponowne u wymagało wpisywania loginu automatycznie.	ruchomienie aplikacji nie będzie i hasła, logowanie przebiegnie

Link ^{Zmień język} [Zmień hasło] jest dostępny, jeśli:

podczas instalacji aplikacji serwerowej (dawna web)
 Comarch DMS za pomocą instalatora zaznaczono opcję
 "Prezentuj zmianę języka na ekranie logowania,

lub

 w pliku Web.config w ramach klucza "ShowChangeLanguage" wpisano wartość "true" (zob. przykładowo Instalacja aplikacji serwerowej (dawnej web) w trybie ręcznym)

Po kliknięciu w link ^{Zmień język} [Zmień hasło] otwierana jest lista, z której można wybrać jeden z 4 języków: polski, angielski, niemiecki albo francuski – po zalogowaniu do Comarch DMS aplikacja będzie wyświetlana w wybranym języku.

Spółka	
Dom	~
Login	
Hasło	
Polski 🗸	Zmień hasło
Polski	(\rightarrow)
English	\bigcirc
Deutsch	
Français	

Wybór języka wyświetlania Comarch DMS

W danym momencie operator może pracować tylko z jedną wersją (stacjonarną, WWW lub mobilną) aplikacji Comarch DMS.

Podczas logowania, aplikacja weryfikuje czy operator jest już zalogowany do innej wersji aplikacji.

Jeżeli weryfikacja wykaże, że obecnie operator zalogowany jest do innej wersji, wyświetlony zostanie **komunikat** z pytaniem dotyczącym automatycznego wylogowania. Zatwierdzenie komunikatu spowoduje wylogowanie operatora z dotychczasowej wersji aplikacji i umożliwi zalogowanie do nowej.



Komunikat wyświetlany podczas logowania do aplikacji serwerowej (dawna web)

Rozpoczynasz pracę z Comarch DMS i chcesz dowiedzieć się, jak korzystać z programu? A może masz już podstawową wiedzę o Comarch DMS i chcesz dowiedzieć się więcej?

Sprawdź Szkolenia Comarch DMS!

Powrót do początku artykułu