



NetIQ® Identity Manager

Podręcznik użytkownika aplikacji do zarządzania tożsamością

Maj 2024 r.

Informacje prawne

Copyright 2009–2024 Open Text.

Jedynie gwarancje na produkty i usługi firmy Open Text, jej podmiotów stowarzyszonych i licencjodawców („Open Text”) zostały wyraźnie sformułowane w oświadczeniach gwarancyjnych dotyczących takich produktów i usług. Niniejszy dokument nie może być interpretowany jako dodatkowa gwarancja. Open Text nie ponosi odpowiedzialności za błędy techniczne lub redakcyjne ani za pominięcia, które mogą wystąpić w niniejszym dokumencie. Informacje zawarte w tym dokumencie mogą ulec zmianie bez powiadomienia.

Dodatkowe informacje, takie jak uwagi dotyczące certyfikatów i znaków towarowych, można znaleźć na stronie <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).

Spis treści

Informacje o niniejszym podręczniku i bibliotece	7
I Witamy w aplikacji Identity Manager	9
1 Rozpoczynanie pracy	11
Informacje o rolach i zasobach	11
Informacje o aplikacjach do zarządzania tożsamością	11
Informacje o pulpicie nawigacyjnym aplikacji Identity Manager	11
Przegląd pulpitu nawigacyjnego	12
Informacje o stronie Aplikacje	13
Informacje o zadaniach	14
Typowe sposoby korzystania z aplikacji do zarządzania tożsamością	14
Działanie funkcji Samoobsługa tożsamości	14
Działanie funkcji Role i zasoby	15
Działanie funkcji Żądanie przetwarzania	16
Działanie stanowiska pomocy technicznej	16
2 Korzystanie z aplikacji do zarządzania tożsamością	19
Uwagi na temat uzyskiwania dostępu do aplikacji do zarządzania tożsamością	19
Logowanie po raz pierwszy	20
Odpowiadanie na sprawdzanie preferowanych ustawień regionalnych	21
Rozwiązywanie problemów z logowaniem	22
Jeśli zapomnisz hasła	22
W przypadku problemów z logowaniem	22
W przypadku monitu o dodatkowe informacje	22
Wylogowanie	23
II Dostosowywanie pulpitu nawigacyjnego	25
3 Zarządzanie formantami i układami	27
Zarządzanie globalnym pulpitem nawigacyjnym	28
Zmienianie układu pulpitu nawigacyjnego	28
Dodawanie formantu	29
Dodawanie formantów ogólnych	30
Dodawanie formantów Identity Managera	31
Dodawanie formantów aplikacji Identity Governance	32
Opcje formantów	32
Konfigurowanie formantu	33

III Zarządzanie uprawnieniami i profilem tożsamości	35
4 Zarządzanie zadaniami nadania uprawnienia	37
Wyświetlanie uprawnień	37
Zgłaszanie żądań uprawnień	39
Wyświetlanie żądań	40
Śledzenie żądania	40
Anulowanie żądania	40
Wystawianie zgłoszenia pomocy technicznej	41
Unieważnianie uprawnień	41
Tworzenie głębokich łączy z żądaniem	42
5 Zarządzanie aplikacjami	45
Tworzenie elementów wyróżnionych	45
Dodawanie aplikacji	45
Dodawanie uprawnień	46
Dodawanie, modyfikowanie lub usuwanie kategorii	46
Dodawanie kategorii	46
Zmienianie kategorii	46
Usuwanie kategorii	47
6 Zarządzanie zadaniami	49
Wyświetlanie zadań	49
Zarządzanie zadaniami do zatwierdzenia lub odrzucenia	50
Zarządzanie zadaniami stanowiska pomocy technicznej	52
7 Działanie w imieniu innej osoby	53
Wyświetlanie przypisania pełnomocnictwa	53
Występowanie w roli pełnomocnika	53
Zarządzanie przypisaniami pełnomocnictwa	53
8 Zarządzanie delegowaniami	55
9 Zarządzanie dostępnością	57
10 Zarządzanie profilem	59
Aktualizowanie profilu	59
11 Zarządzanie schematem organizacyjnym	61
Wyświetlanie schematu organizacyjnego	61
Informacje o schemacie organizacyjnym	62
Praca ze schematem organizacyjnym	63
Resetowanie encji głównej w widoku schematu organizacyjnego	64
Przełączanie widoku schematu organizacyjnego	64
Wybór relacji do wyświetlenia	65
Przechodzenie do następnego poziomu w hierarchii relacji	66

Wysyłanie wiadomości e-mail do użytkowników ze schematu organizacyjnego	67
Wyświetlanie szczegółowych informacji o użytkowniku.	67
12 Zarządzanie hasłami	69
Korzystanie z samoobsługowego zarządzania hasłem w programie Identity Manager.	69
Informacje o odzwie dla hasła	70
Zmiana hasła	70
Stan założeń haseł	71
Korzystanie ze starszej wersji zarządzania hasłami.	71
Odzew dla hasła	72
Zmiana wskazówki do hasła	73
Zmień hasło	73
Stan założeń haseł	74
Stan synchronizacji hasła.	74
IV Zarządzanie użytkownikami, grupami i zespołami	75
13 Zarządzanie użytkownikami	77
Tworzenie użytkownika	77
Edytowanie informacji o użytkowniku.	77
Wyświetlanie listy użytkowników	78
Wyszukiwanie użytkowników.	79
Sortowanie użytkowników	81
14 Zarządzanie zespołami	83
Wyświetlanie zespołów	83
Tworzenie zespołu.	84
Modyfikowanie zespołu	84
15 Zarządzanie grupami	85
Tworzenie grupy	85
V Załącznik	87
A Korzystanie z programu Identity Manager Approvals	89
Wymagania dotyczące produktu	89
Instalowanie aplikacji Approvals	90
Konfigurowanie aplikacji Approvals.	90
Zgłaszanie żądania dostępu mobilnego za pośrednictwem aplikacji użytkownika.	90
Korzystanie z łącza do konfiguracji lub kodu QR	91
Ręczne konfigurowanie aplikacji Approvals.	92
Przegląd aplikacji Approvals.	94
Widok Zadania	95
Widok szczegółowy	95
Tryb zbiorczy.	95
Widok Zakończone zadania.	96
Widok Ustawienia logowania	96

Widok Ustawienia zaawansowane	96
Zmiana języka wyświetlania aplikacji Approvals.	97

Informacje o niniejszym podręczniku i bibliotece

W niniejszym podręczniku opisano, w jaki sposób użytkownicy końcowi i niektórzy administratorzy mogą używać aplikacji do zarządzania tożsamością NetIQ Identity Manager, a zwłaszcza aplikacji Pulpit i Aplikacja Użytkownika.

Docelowi odbiorcy

Niniejszy podręcznik zawiera informacje przeznaczone dla osób znających zagadnienia związane z administrowaniem i odpowiedzialnych za wdrażanie bezpiecznego, rozproszonego modelu administrowania.

Inne informacje w bibliotece

Więcej informacji na temat biblioteki dla aplikacji Identity Manager zawiera witryna z [dokumentacją aplikacji Identity Manager \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

Witamy w aplikacji Identity Manager

NetIQ Identity Manager to oprogramowanie systemowe, które służy do bezpiecznego zarządzania dostępem wspólnoty użytkowników w organizacji. Również członkowie wspólnoty użytkowników mogą odnieść wiele korzyści z korzystania z aplikacji Identity Manager. Aplikacja Identity Manager umożliwia organizacji na przykład:

- ♦ Szybkie przyznawanie użytkownikom praw dostępu do potrzebnych im informacji (m.in. do grupowych schematów organizacyjnych, wydziałowej książki adresowo-informacyjnej lub do funkcji wyszukiwania pracowników), jak również ról i zasobów (np. sprzętu i kont w systemach wewnętrznych).
- ♦ Zsynchronizowanie wielu haseł do postaci wspólnego logowania dla wszystkich systemów.
- ♦ Natychmiastowe zmodyfikowanie lub wycofanie praw dostępu, kiedy jest to konieczne (np. gdy pracownik zmieni oddział lub wydział albo jeśli odejdzie z firmy).
- ♦ Zachowanie zgodności z obowiązującymi przepisami.

Przeczytaj najpierw tę część, aby uzyskać informacje na temat aplikacji do zarządzania tożsamością Identity Manager oraz rozpoczynaniu pracy z nimi. Podręcznik został zaprojektowany z myślą o ułatwianiu wykonywania następujących typów działań online w organizacji:

- ♦ Zarządzanie tożsamością online powiązaną z zasobami organizacyjnymi.
- ♦ Wyświetlanie oraz modyfikowanie dostępu do ról oraz zasobów organizacyjnych.
- ♦ Zatwierdzanie żądań dostępu do zasobów i ról.
- ♦ Zarządzanie uprawnieniami powiązanymi z oprogramowaniem i innymi zasobami, które organizacja udostępnia swoim członkom.

1 Rozpoczynanie pracy

W tym rozdziale omówiono rozpoczynanie pracy z aplikacjami do zarządzania tożsamością. Tematy obejmują następujące zagadnienia:

- ♦ „Informacje o rolach i zasobach” na stronie 11
- ♦ „Informacje o aplikacjach do zarządzania tożsamością” na stronie 11
- ♦ „Informacje o pulpicie nawigacyjnym aplikacji Identity Manager” na stronie 11
- ♦ „Przegląd pulpitu nawigacyjnego” na stronie 12
- ♦ „Informacje o zadaniach” na stronie 14
- ♦ „Typowe sposoby korzystania z aplikacji do zarządzania tożsamością” na stronie 14

Informacje o rolach i zasobach

W aplikacjach do zarządzania tożsamością **uprawnienie** to prawo dostępu użytkownika lub grupy użytkowników do roli bądź zasobu. **Rola** określa zestaw uprawnień związanych z jednym lub większą liczbą docelowych systemów lub aplikacji. Na przykład rola administratora użytkowników może mieć uprawnienie do resetowania hasła użytkownika, natomiast rola administratora systemu może mieć możliwość przypisania użytkownika do konkretnego serwera. **Zasób** to dowolna encja cyfrowa, taka jak konto użytkownika, komputer lub baza danych, do której użytkownik biznesowy potrzebuje mieć dostęp.

Informacje o aplikacjach do zarządzania tożsamością

Aplikacje do zarządzania tożsamością Identity Manager to zestaw połączonych ze sobą aplikacji internetowych działających w przeglądarce. Umożliwiają one organizacji zarządzanie kontami użytkowników i uprawnieniami przypisanymi do różnych ról i zasobów dostępnych dla użytkowników. Aplikacje do zarządzania tożsamością można skonfigurować w taki sposób, aby umożliwiały użytkownikom samodzielne wykonywanie takich operacji, jak zgłaszanie żądań przypisania roli czy zmiana hasła. Można również skonfigurować przepływy pracy usprawniające zarządzanie rolami i zasobami oraz ich przypisywanie.

Informacje o pulpicie nawigacyjnym aplikacji Identity Manager

Pulpit nawigacyjny aplikacji NetIQ Identity Manager (Pulpit nawigacyjny) to podstawowy portal wejściowy aplikacji do zarządzania tożsamością. Pulpit nawigacyjny może zawierać jeden lub większą liczbę formantów, które zapewniają szybki dostęp do informacji o konkretnym działaniu. Pulpit nawigacyjny umożliwia wykonywanie następujących działań:

- ♦ Zarządzanie ustawieniami profilu i hasłem.
- ♦ Wyświetlanie szczegółów schematu organizacyjnego.

- Przeglądanie i wykonywanie zadań, takich jak zatwierdzanie wniosków użytkowników o dostęp.
- Składanie wniosków o uprawnienia do ról, zasobów lub procesów.
- Przegląd stanu i historii wniosków o uprawnienia.
- Wyszukiwanie innych użytkowników w organizacji.
- Personalizowanie pulpitu nawigacyjnego przez dodawanie formantów i zmienianie ich położenia zgodnie z własnymi preferencjami.
- Ustawianie dowolnego użytkownika jako pełnomocnika z systemu.
- Delegowanie zadań do innych użytkowników z systemu.

Dysponując odpowiednimi **uprawnieniami**, można wykonywać następujące zadania:

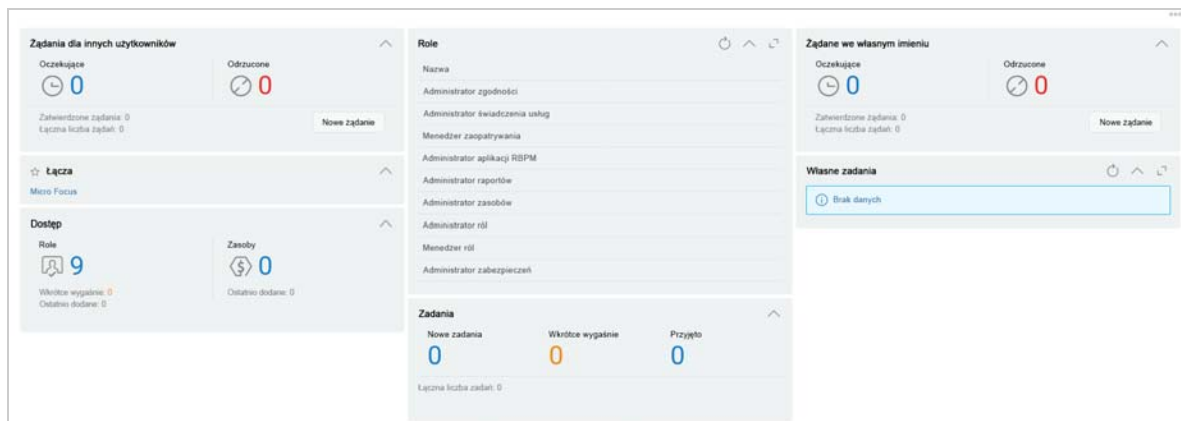
- Tworzenie i modyfikowanie profili użytkowników.
- Wyświetlanie szczegółów schematu organizacyjnego innych użytkowników.
- Tworzenie i modyfikowanie zespołów, które reprezentują zbiór użytkowników i grup mogących realizować wnioski o przydzielenie i zadania zatwierdzenia przypisane do zespołu.
- Składanie wniosków o uprawnienia lub unieważnianie uprawnień w imieniu innych użytkowników w organizacji.

Przegląd pulpitu nawigacyjnego

Pulpit nawigacyjny zapewnia szybki dostęp do informacji o zadaniach, uprawnieniach i wnioskach przy użyciu formantów. Możesz przechodzić do określonych stron lub aplikacji jednym kliknięciem. Możesz też dodawać, usuwać i konfigurować formanty oraz zmieniać ich ustawienie. Więcej informacji na temat personalizowania pulpitu nawigacyjnego zawiera [Rozdział 3, „Zarządzanie formantami i układami”](#), na stronie 27.

Poniższy przykład przedstawia domyślne opcje formantów pulpitu nawigacyjnego.

Rysunek 1-1 Przykładowy osobisty pulpit nawigacyjny



Pulpit nawigacyjny aplikacji Identity Manager umożliwia zarządzanie różnymi działaniami w aplikacji Identity Manager. Poniżej przedstawiono strony ułatwiające zarządzanie zadaniami i działaniami:

Aplikacja

Zawiera listę wszystkich aplikacji dostępnych dla użytkownika. Udostępnia domyślne łącza do kilku obszarów, aby uprościć wykonywanie podstawowych zadań w aplikacji Identity Manager. Aby uzyskać więcej informacji, zobacz „[Informacje o stronie Aplikacje](#)” na stronie 13.

Zadania

Przedstawia wszystkie zadania oczekujące na wykonanie działania. Mając przypisaną odpowiednią rolę, można wyświetlać zadania innych użytkowników. Na przykład rolę menedżera zespołu.

Dostęp

Umożliwia wyświetlanie uprawnień i żądań uprawnień. Aby wyświetlić stan żądania uprawnień, należy przejść do strony **Historia żądań**. Na tej stronie wyświetlane są wszystkie żądania i ich stan.

Osoby

Umożliwia wyświetlanie innych użytkowników lub grup w systemie, a także **schematu organizacyjnego** innego użytkownika. Ułatwia to wizualizowanie relacji między użytkownikami i grupami.

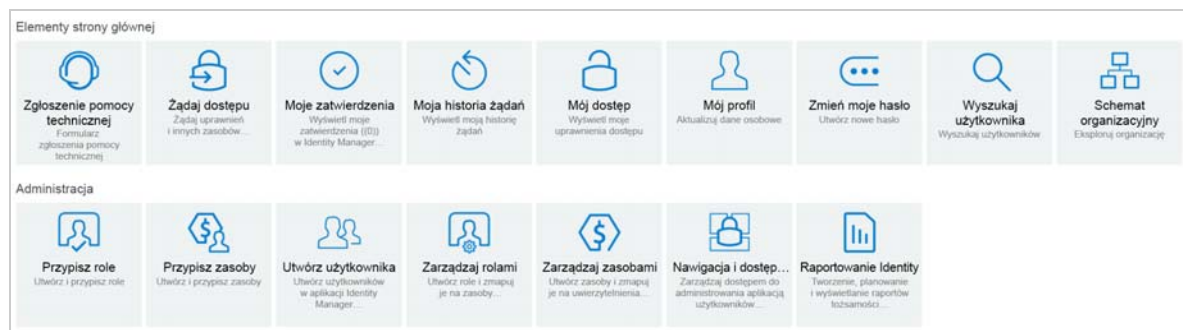
Administracja

Umożliwia wyświetlanie ról, zasobów, uzgodnień uprawnień oraz konfiguracji, a także zarządzanie nimi. Ta opcja jest widoczna tylko dla administratorów. Więcej informacji na temat zadań administracyjnych zawiera sekcja [Administrowanie aplikacjami do zarządzania tożsamością](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Informacje o stronie Aplikacje

Drugim istotnym widokiem na pulpicie nawigacyjnym jest strona **Aplikacje** ([Rysunek 1-2](#)), która udostępnia domyślne łącza do kilku obszarów w celu uproszczenia podstawowych zadań wykonywanych przez użytkowników końcowych i administratorów w aplikacji Identity Manager.

Rysunek 1-2 Przykładowa strona Aplikacje na pulpicie nawigacyjnym



Domyślnie na stronie **Aplikacje** wyświetlany jest element **Zgłoszenie pomocy technicznej**. Ta opcja umożliwia wysłanie zgłoszenia do stanowiska pomocy technicznej.

Administrator zarządzania tożsamością dostosowuje stronę **Aplikacje**, umieszczając na niej kafelki kierujące użytkownika do zasobów lub aplikacji, z których regularnie korzysta. Jeśli dysponuje odpowiednią rolą administracyjną, może skonfigurować dostęp użytkownika do tych kafelków. Należy przejść do opcji **Identyfikator użytkownika > Ustawienia > Dostęp**, aby dodać dysponentów dla wymaganych elementów nawigacyjnych. Więcej informacji znajduje się w dokumencie [Zarządzanie dostępem użytkownika](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Niektóre kafelki na tej stronie mogą być widoczne wyłącznie dla użytkowników z przypisaną rolą administracyjną w aplikacjach do zarządzania tożsamością. Na przykład osoba, która może tworzyć lub modyfikować role, powinna widzieć kafelki podobne do **Utwórz użytkownika** i **Zarządzaj rolami**.

Aby uzyskać więcej informacji na temat korzystania z pulpitu nawigacyjnego, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Informacje o zadaniach

Na stronie **Zadania** można zatwierdzać lub odrzucać działania związane z zadaniami znajdującymi się na liście.

Pulpit nawigacyjny aplikacji Identity Manager umożliwia zarządzanie zadaniami aplikacji Identity Manager i Identity Governance ze strony Zadania. Obecnie można wyświetlać i zatwierdzać zadania aplikacji zarówno Identity Manager, jak i Identity Governance w tym samym interfejsie użytkownika.

Typowe sposoby korzystania z aplikacji do zarządzania tożsamością

Poniżej przedstawiono kilka przykładowych sposobów, w jakie użytkownicy zazwyczaj korzystają z aplikacji do zarządzania tożsamością w organizacji.

- ♦ „Działanie funkcji Samoobsługa tożsamości” na stronie 14
- ♦ „Działanie funkcji Role i zasoby” na stronie 15
- ♦ „Działanie funkcji Żądanie przetwarzania” na stronie 16
- ♦ „Działanie stanowiska pomocy technicznej” na stronie 16

Działanie funkcji Samoobsługa tożsamości

- ♦ Ella (użytkownik końcowy) odzyskuje zapomniane hasło za pomocą funkcji samoobsługi tożsamości podczas logowania.

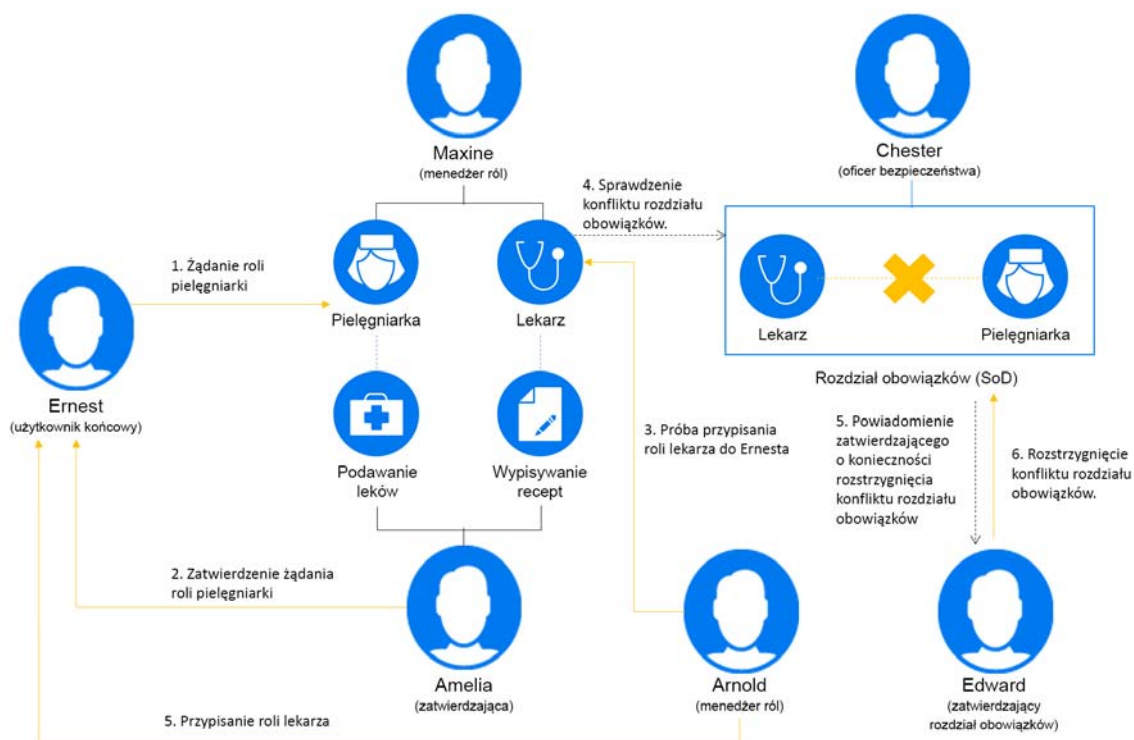
Domyślnie w aplikacji Identity Manager używana jest funkcja Self Service Password Reset (SSPR), która umożliwia użytkownikom modyfikowanie swoich haseł. Jednak w aplikacjach do zarządzania tożsamością można wykorzystywać inne metody zarządzania zapomnianymi hasłami.

- ♦ Erik (użytkownik końcowy) wyszukuje w swojej lokalizacji wszystkich pracowników mówiących po niemiecku.
- ♦ Eduardo (użytkownik końcowy) przegląda schemat organizacyjny, odnajduje Ellę i klika ikonę wiadomości e-mail, aby wysłać do niej wiadomość.

Działanie funkcji Role i zasoby

Poniżej przedstawiono przykład objaśniający przepływ żądania dotyczącego ról i zasobów w systemie:

Rysunek 1-3 Przykładowy scenariusz przypisania roli



- ♦ Maxine (menedżer ról) tworzy role biznesowe Pielęgniarka i Lekarz oraz role informatyczne Administrowanie lekami i Wypisywanie recept. Maxine tworzy kilka zasobów, które są wymagane dla tych ról, oraz powiązanie tych zasobów z rolami.
- ♦ Maxine (menedżer ról) definiuje relację między rolami Pielęgniarka i Administrowanie lekami, wskazując, że rola Pielęgniarka zawiera rolę Administrowanie lekami. Max definiuje również relację między rolami Wypisywanie recept i Lekarz, wskazując, że rola Lekarz zawiera rolę Wypisywanie recept.
- ♦ Chester (oficer bezpieczeństwa) definiuje ograniczenie rozdziału obowiązków, które wskazuje na istnienie potencjalnego konfliktu między rolami Lekarz i Pielęgniarka. To oznacza, że w normalnych warunkach ten sam użytkownik nie powinien być przypisany jednocześnie do obu ról. W pewnych okolicznościach osoba żądająca przypisania roli może chcieć wymuszenia zniesienia tego ograniczenia. Aby zdefiniować wyjątek rozdziału obowiązków, osoba zgłaszająca żądanie przypisania musi przedstawić uzasadnienie.
- ♦ Ernest (użytkownik końcowy) przegląda listę dostępnych dla niego ról i żąda przypisania do roli Pielęgniarka.
- ♦ Amelia (użytkownik zatwierdzający) odbiera powiadomienie o żądaniu zatwierdzenia w wiadomości e-mail, która zawiera adres URL. Klika łącze, zapoznaje się z formularzem zatwierdzenia oraz akceptuje go.

- Arnold (menedżer ról) żąda przypisania Ernesta do roli Lekarz. Otrzymuje powiadomienie o występowaniu potencjalnego konfliktu między rolą Lekarz i rolą Pielęgniarka, do której Ernest został już przypisany. Przedstawia uzasadnienie dotyczące utworzenia wyjątku od ograniczenia rozdziału obowiązków.
- Edward (użytkownik zatwierdzający rozdział obowiązków) otrzymuje wiadomość e-mail z powiadomieniem o konflikcie rozdziału obowiązków. Zatwierdza zgłoszone przez Arnolda żądanie wymuszenia zniesienia ograniczenia rozdziału obowiązków.
- Amelia (użytkownik zatwierdzający) otrzymuje wiadomość e-mail z powiadomieniem o żądaniu zatwierdzenia dotyczącym roli Lekarz. Zatwierdza zgłoszone przez Arnolda żądanie przypisania Ernesta do roli Lekarz.
- Bill (audytor ról) przegląda raport dotyczący naruszeń i wyjątków rozdziału obowiązków (SoD) i widzi, że Ernest został przypisany zarówno do roli Lekarz, jak i Pielęgniarka. Ponadto zauważa on, że Ernest został przypisany do zasobów powiązanych z tymi rolami.

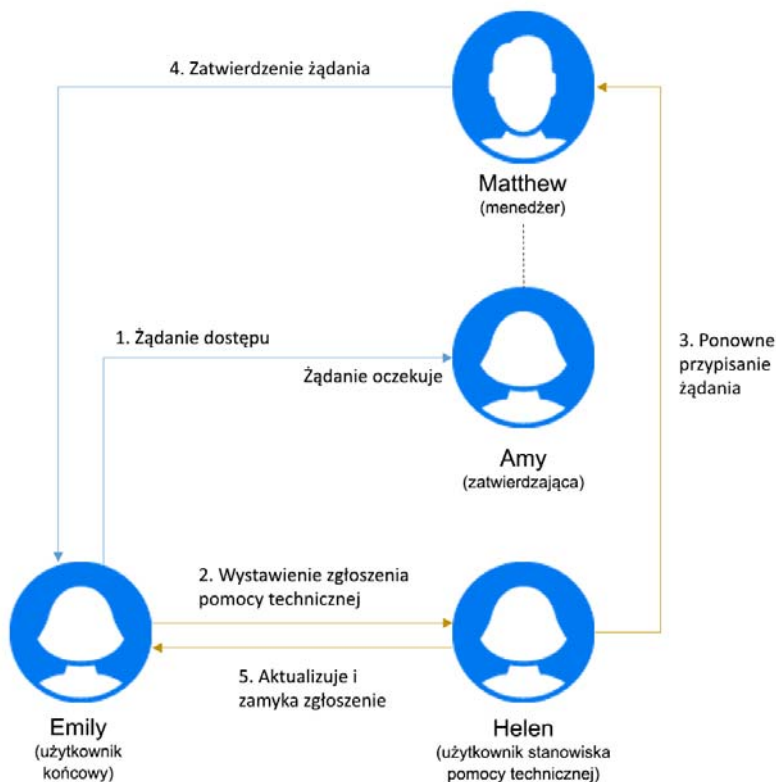
Działanie funkcji Żądanie przetwarzania

- Ernie (użytkownik końcowy) przegląda listę dostępnych dla niego zasobów i żąda dostępu do systemu Siebel*.
- Amy (użytkownik zatwierdzający) odbiera powiadomienie o żądaniu zatwierdzenia w wiadomości e-mail, która zawiera adres URL. Klika łączy, zapoznaje się z formularzem zatwierdzenia oraz akceptuje go.
- Ernest sprawdza stan poprzedniego żądania dotyczącego dostępu do systemu Siebel (zostało ono przesłane drugiej osobie do zatwierdzenia). Widzi, że jest ono dalej rozpatrywane.
- Amy udaje się na urlop, więc wprowadza informację o swojej tymczasowej niedostępności. Podczas jej nieobecności nie są jej przypisywane nowe zadania zatwierdzania.
- Amy otwiera listę zadań zatwierdzania i widzi, że jest ich zbyt wiele, aby mogła na czas sama wszystkie przetworzyć. Dlatego też przypisuje niektóre zadania swoim współpracownikom.
- Pat (asystent ds. administracyjnych, pełnomocnik Amy) otwiera listę zadań Amy i wykonuje w jej imieniu zadanie zatwierdzenia.
- Max (menedżer) przegląda listę zadań pracowników w swoim dziale. Wie, że Amy jest na urlopie, więc przypisuje zadania do innych pracowników działu.
- Max wysyła żądanie utworzenia konta bazy danych dla pracownika działu, który bezpośrednio mu podlega.
- Max przypisuje Dana jako autoryzowanego delegata Amy.
- Dan (który jest teraz delegowanym użytkownikiem zatwierdzającym) odbiera zadania Amy podczas jej nieobecności.
- Max przyjmuje pracownika na bezpłatny staż. Informacje na temat stażysty nie powinny być wprowadzane do systemu kadrowego. Administrator systemu tworzy rekord użytkownika dla stażysty i żąda nadania mu dostępu do programu Notes, usługi Active Directory* i systemu Oracle*.

Działanie stanowiska pomocy technicznej

Poniżej przedstawiono przykład objaśniający przepływ zgłoszenia do pomocy technicznej w systemie:

Rysunek 1-4 Przykład dotyczący stanowiska pomocy technicznej



- Emily (użytkownik końcowy) złożyła wniosek o dostęp do drukarki biurowej. Wniosek ten jest w stanie oczekiwania przez dłuższy czas. Dlatego wysłała ona zgłoszenie do pomocy technicznej.
- Helen (użytkownik stanowiska pomocy technicznej) otrzymuje powiadomienie o zgłoszeniu pomocy technicznej na swojej liście zadań.
- Helen analizuje problem i stwierdza, że ten wniosek jest przypisany do Amy (osoba zatwierdzająca).
- Wniosek jest w stanie oczekiwania w systemie, ponieważ Amy jest nieobecna.
- Helen ma uprawnienie do zmiany przypisania żądań wykonania zadania. Zmienia przypisanie tego żądania do Mathew (menedżera Amy).
- Mathew otrzymuje wniosek i zatwierdza go. Emily może uzyskać dostęp do drukarki biurowej.
- Helen aktualizuje i zamyka zgłoszenie do pomocy technicznej.

2 Korzystanie z aplikacji do zarządzania tożsamością

Dostęp do aplikacji do zarządzania tożsamością, na przykład do pulpitu nawigacyjnego, można uzyskać za pomocą przeglądarki internetowej. Aplikacja Identity Manager obsługuje najpopularniejsze wersje przeglądarek. Aby uzyskać informacje o obsługiwanych przeglądarkach lub pomoc przy instalacji, należy skontaktować się z administratorem systemu. Adres URL i poświadczenia wymagane w celu uzyskania dostępu do tych aplikacji powinny zostać udostępnione przez organizację.

- ♦ „Uwagi na temat uzyskiwania dostępu do aplikacji do zarządzania tożsamością” na stronie 19
- ♦ „Logowanie po raz pierwszy” na stronie 20
- ♦ „Odpowiadanie na sprawdzanie preferowanych ustawień regionalnych” na stronie 21
- ♦ „Rozwiązywanie problemów z logowaniem” na stronie 22
- ♦ „Wylogowanie” na stronie 23

Uwagi na temat uzyskiwania dostępu do aplikacji do zarządzania tożsamością

Przed uzyskaniem dostępu do pulpitu nawigacyjnego lub innych aplikacji do zarządzania tożsamością należy zapoznać się z następującymi uwagami:

- ♦ W przeglądarce internetowej należy włączyć pliki cookie oraz język JavaScript*.
- ♦ W przeglądarce Internet Explorer należy ustawić co najmniej **Średni** poziom prywatności. Należy również zaznaczyć opcję **Za każdym razem, gdy odwiedzam witrynę internetową** w obszarze **Narzędzia > Opcje internetowe > Ogólne, Historia przeglądania > Ustawienia > Sprawdzaj nowsze wersje zapisanych stron**. Jeśli ta opcja nie zostanie zaznaczona, niektóre przyciski mogą nie być poprawnie wyświetlane.
- ♦ Jeśli wcześniej uzyskiwano dostęp do aplikacji użytkownika Identity Manager, może być możliwe użycie tej samej nazwy użytkownika i hasła w celu uzyskania dostępu do pulpitu nawigacyjnego.
- ♦ Nie można uzyskać dostępu do aplikacji do zarządzania tożsamością przy użyciu konta, które zawiera w nazwie dowolny z następujących znaków:

 \ / , * ? . \$ # +
- ♦ Jeśli nie można się zalogować, można kliknąć opcję **Nie pamiętam hasła**. Aby uzyskać więcej informacji, zobacz „Jeśli zapomnisz hasła” na stronie 22.

- ♦ Jeśli po uzyskaniu dostępu do interfejsu użytkownika aplikacji Identity Manager pierwsza strona wygląda inaczej, oznacza to, że aplikacja została dostosowana do potrzeb organizacji. Podczas pracy można zauważyć, że zostały dostosowane również inne funkcje aplikacji do zarządzania tożsamością.

W takim przypadku należy się skontaktować z administratorem systemu, aby dowiedzieć się, czym różnią się dostosowane aplikacje do zarządzania tożsamością od konfiguracji domyślnej opisanej w tym podręczniku.

Logowanie po raz pierwszy

Aby zalogować się do aplikacji do zarządzania tożsamością, takiej jak pulpit nawigacyjny, trzeba być autoryzowanym użytkownikiem. Aby uzyskać pomoc dotyczącą nazwy użytkownika i hasła umożliwiających zalogowanie, należy skontaktować się z administratorem systemu.

Przy pierwszym logowaniu do aplikacji do zarządzania tożsamością aplikacja Identity Manager wymaga ustanowienia parametrów zabezpieczeń dla konta, aby ułatwić zresetowanie hasła w przyszłości. W przypadku zapomnienia hasła i próby jego zresetowania przy następnym logowaniu aplikacja Identity Manager zadaje te skonfigurowane pytania i prosi o podanie poprawnej odpowiedzi. Hasło można zresetować, gdy odpowiedź jest zgodna z zapisaną na tej stronie.

Aby skonfigurować pytania zabezpieczające podczas pierwszego logowania:

- 1 Wprowadź nazwę użytkownika i hasło, a następnie kliknij przycisk **Logowanie**.
- 2 Strona logowania automatycznie przekierowuje użytkownika do strony **Odzew**.
- 3 Podaj pytania i odpowiedzi na pytania zabezpieczające.

[Menedżer konfiguracji](#) [Edytor konfiguracji](#) [Obejrzyj dziennik](#)

Konfigurowanie pytań zabezpieczających

[Wyloguj](#)

Jeśli nie pamiętasz swojego hasła, możesz uzyskać dostęp do konta, odpowiadając na pytania zabezpieczające.

Wybierz pytania i odpowiedzi, których można użyć do weryfikacji Twojej tożsamości, gdy nie będziesz pamiętał swojego hasła. Ponieważ odpowiedzi na te pytania umożliwią dostęp do Twojego konta, upewnij się, że podane odpowiedzi nie będą łatwe do zgadnięcia lub wykrycia przez inne osoby.

Wpisz odpowiedzi zabezpieczające

— Wybierz pytanie z listy —

— Wybierz pytanie z listy —

— Wybierz pytanie z listy —

— Wybierz pytanie z listy —

— Wybierz pytanie z listy —

» Zapisz odpowiedzi

« Anuluj

- 4 Kliknij przycisk **Zapisz odpowiedzi**. Nastąpi przekierowanie do pulpitu nawigacyjnego.

Odpowiadanie na sprawdzanie preferowanych ustawień regionalnych

Jeśli podczas logowania zostanie wyświetlony monit o wybór preferowanych ustawień regionalnych, oznacza to, że administrator skonfigurował w aplikacjach do zarządzania tożsamością sprawdzanie języka w przeglądarkach użytkowników. Może to być konieczne, aby zapewnić, że treść widoczna dla użytkowników jest wyświetlana w obsługiwanym języku.

Po wyświetleniu monitu o dodanie ustawień regionalnych należy otworzyć listę **Dostępne ustawienia regionalne**, wybrać odpowiednią pozycję i kliknąć przycisk **Dodaj**. Więcej informacji na ten temat zawiera sekcja [Dodawanie nowego języka do aplikacji do zarządzania tożsamością](#).

Rozwiązywanie problemów z logowaniem

Ta sekcja zawiera rozwiązania następujących typowych rodzajów problemów z logowaniem:

- ♦ „Jeśli zapomnisz hasła” na stronie 22
- ♦ „W przypadku problemów z logowaniem” na stronie 22
- ♦ „W przypadku monitu o dodatkowe informacje” na stronie 22

Jeśli zapomnisz hasła

Jeśli nie pamiętasz hasła, możesz skorzystać z pomocniczego łącza **Zapomniane hasło**. Po wyświetleniu monitu to łącze jest domyślnie wyświetlane na stronie logowania. Z tego łącza można skorzystać, jeśli administrator systemu skonfigurował odpowiednie założenia dotyczące haseł.

- 1 Po wyświetleniu monitu o zalogowanie kliknij łącze **Zapomniane hasło**.
- 2 Wprowadź nazwę użytkownika i kliknij przycisk **Prześlij**.

Jeśli aplikacja Identity Manager nie może znaleźć odpowiednich założeń dotyczących hasła, należy skontaktować się z administratorem systemu.

- 3 Odpowiedz na wyświetlone pytania zabezpieczające. Aplikacja Identity Manager wyświetla monit o odpowiedź na skonfigurowane pytania. Hasło można zresetować, gdy odpowiedź jest zgodna z zapisaną wcześniej. Kliknij przycisk **Prześlij**. Na przykład:

Odpowiedz na pytania dotyczące odzewu, aby uzyskać pomoc dotyczącą hasła. W zależności od skonfigurowanych przez administratora systemu założeń hasła można wykonać następujące działania:

- ♦ odebrać wiadomość e-mail zawierającą hasło,
- ♦ zresetować hasło.

W przypadku problemów z logowaniem

Jeśli nie można się zalogować, należy się upewnić, że została wprowadzona poprawna nazwa użytkownika i hasło (pisownia, wielkie i małe litery itd.). W przypadku dalszych problemów należy skontaktować się z administratorem systemu. Pomocne jest dostarczenie szczegółowych informacji o problemie (takich jak komunikaty o błędach).

W przypadku monitu o dodatkowe informacje

Bezpośrednio po zalogowaniu może zostać wyświetlony monit o podanie informacji innego rodzaju. Zależy to od skonfigurowanych przez administratora systemu ewentualnych założeń hasła. Na przykład:

- ♦ Podczas pierwszego logowania może zostać wyświetlony monit o zdefiniowanie zabezpieczających pytań i odpowiedzi.
- ♦ Jeśli hasło wygasło, wyświetlany jest monit o jego zresetowanie.

Wylogowanie

Po zakończeniu pracy z pulpitem nawigacyjnym i innymi aplikacjami do zarządzania tożsamością można się wylogować. Kliknij na pulpicie nawigacyjnym nazwę użytkownika wyświetloną w prawym górnym rogu i wybierz opcję **Wyloguj się**.



Dostosowywanie pulpitu nawigacyjnego

Aplikacje do zarządzania tożsamością udostępniają wiele opcji zmiany ekranu *pulpitu nawigacyjnego* i zapisania go jako widoku spersonalizowanego. Możesz na przykład dodawać formanty i zmieniać ich położenie zgodnie z własnymi preferencjami. Możesz też skonfigurować i spersonalizować pola formantów. Ten dokument przedstawia różne opcje personalizowania *pulpitu nawigacyjnego*.

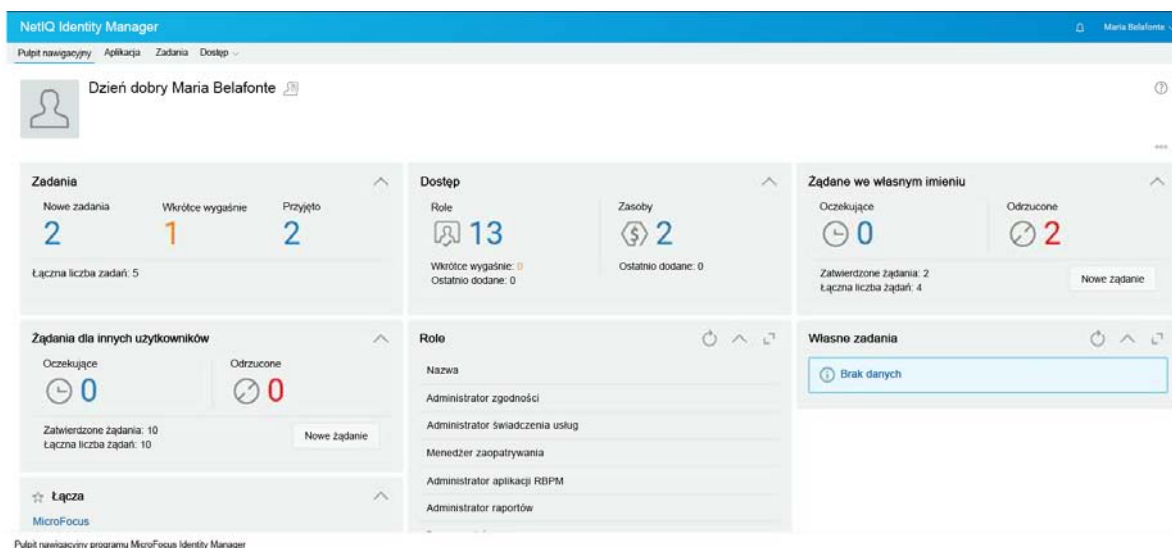
3 Zarządzanie formantami i układami

Formanty to obiekty na pulpicie nawigacyjnym, które zawierają określone szczegółowe informacje o użytkowniku w kontekście określonej aktywności. Formant **Zadania** zawiera szczegółowe informacje o nowych zadaniach, przyjętych zadaniach lub zadaniach, których termin niedługo upływa. Na swoim pulpicie nawigacyjnym możesz skonfigurować wiele innych formantów.

Administratorzy z dostępem do strony **Ustawienia** mogą przypisywać formanty do użytkownika, grupy, kontenera lub roli z poziomu strony **Identyfikator użytkownika > Ustawienia > Formanty pulpitu nawigacyjnego**.

Aby dostosować pulpit nawigacyjny, przejdź do swojego **Pulpitu nawigacyjnego** i kliknij **...**.

Rysunek 3-1 Personalizowanie pulpitu nawigacyjnego



Użyj następujących opcji, by spersonalizować swój pulpit nawigacyjny:

Rysunek 3-2 Opcje personalizacji



Formanty

Umożliwia dodawanie formantów do pulpitu nawigacyjnego. Zobacz „Dodawanie formantu” na stronie 29.

Układ

Umożliwia zmianę układu pulpitu nawigacyjnego. Zobacz „Zmienianie układu pulpitu nawigacyjnego” na stronie 28.

Anuluj

Cofa wszystkie zmiany wprowadzone na pulpicie nawigacyjnym.

Zapisz

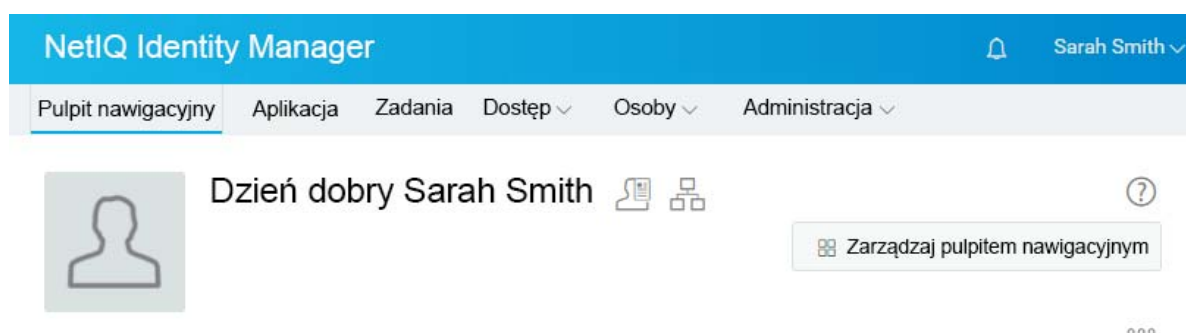
Zapisuje wszystkie zmiany i wprowadza je na pulpicie nawigacyjnym.

Zarządzanie globalnym pulpitem nawigacyjnym

Globalny pulpit nawigacyjny zawiera zbiór formantów, które będą się wyświetlać na pulpicie nawigacyjnym każdego użytkownika w systemie. Formanty te wyświetlają się odpowiednio do przypisanych przez administratora uprawnień poszczególnych użytkowników. Opcja **Zarządzaj pulpitem nawigacyjnym** umożliwia dodawanie, zmianę lub usuwanie formantów z globalnego pulpitu nawigacyjnego.

UWAGA: Z opcji **Zarządzaj pulpitem nawigacyjnym** mogą korzystać wyłącznie użytkownicy o statusie dysponenta.

Rysunek 3-3 Przykładowy globalny pulpit nawigacyjny



Administrator może dodać dowolnego użytkownika, grupę, kontener lub rolę jako dysponenta uprawnionego do zarządzania globalnym pulpitem nawigacyjnym. Aby zmienić dysponentów uprawnionych do zarządzania pulpitem nawigacyjnym, przejdź do **Twoje ID > Ustawienia > Dostęp** i kliknij **Globalny pulpit nawigacyjny** z listy. Więcej informacji na temat modyfikowania dostępu do konfiguracji znajduje się w sekcji **Zarządzanie formantami pulpitu nawigacyjnego** w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Zmienianie układu pulpitu nawigacyjnego

Globalny pulpit nawigacyjny zawiera zbiór formantów, które będą się wyświetlać na pulpicie nawigacyjnym każdego użytkownika w systemie.

- 1 Kliknij na **pulpicie nawigacyjnym** przycisk **...**.
- 2 Wybierz **Układ**.
- 3 Wybierz układ, który chcesz wyświetlić na pulpicie nawigacyjnym.

Rysunek 3-4 Zmiana układów

EDYTUJ PULPIT NAWIGACYJNY

×

Tytuł

Pulpit nawigacyjny

Struktura

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

3-9 (12/6-6)

WAŻNE: Kliknij **Zapisz**, aby zachować wprowadzone zmiany.

Dodawanie formantu

Aby dodać nowy formant do pulpitu nawigacyjnego, przejdź do swojego **Pulpitu nawigacyjnego**, kliknij **...** i wybierz **Formanty**.

Rysunek 3-5 Dodawanie formantów

DODAJ NOWY FORMANT

×

Ogólne

IDM

IG

Dodawanie formantów ogólnych

Kategoria **Ogólne** umożliwia dodawanie formantów do pulpitu nawigacyjnego poza standardowymi formantami aplikacji Identity Manager. Można wpisać adres URL interfejsu API REST docelowego formantu i wyświetlić wymagane informacje w postaci wykresu liniowego, wykresu kołowego lub tabeli.

1 Wybierz z listy dowolny z następujących typów formantów:

- ♦ **Wykres liniowy:** Wyświetla żądane informacje o wybranym elemencie w postaci wykresu liniowego.
- ♦ **Łączy:** Umożliwia tworzenie zakładki, które umożliwiają szybki dostęp do często używanych łączy.
- ♦ **Wykres kołowy:** Wyświetla żądane informacje o wybranym elemencie w postaci wykresu kołowego.
- ♦ **Tabela:** Wyświetla listę żądanych informacji o wybranym elemencie w postaci tabeli.

2 Kliknij , aby skonfigurować formant dodany do Twojego pulpitu nawigacyjnego.

3 (Warunkowo) W przypadku formantów w postaci **Wykresu liniowego**, **Wykresu kołowego** i **Tabeli** należy podać następujące szczegółowe informacje:

- ♦ **Tytuł:** Określa nazwę formantu, która będzie się wyświetlać na pulpicie nawigacyjnym.
- ♦ **Adres URL:** Określa adres URL interfejsu API REST docelowego formantu, który ma być wyświetlany na pulpicie nawigacyjnym.
- ♦ **Element główny:** Określa element z kodu interfejsu API REST, którego wykres chcesz wyświetlić. W tym polu rozróżniana jest wielkość liter. Wpisz dokładnie taką samą nazwę, jaka widnieje w kodzie interfejsu API REST.
- ♦ **Kolumny:** Określa kolumny, które chcesz wyświetlić w swoim formancie. Możesz dodać wiele kolumn. **Tytuł** określa nazwę wyświetlaną kolumny. **Ścieżka** określa nazwę kolumny wyszczególnioną w interfejsie API REST. W polu **Ścieżka** rozróżniana jest wielkość liter. Wpisz dokładnie taki sam ciąg znaków, jaki widnieje w kodzie interfejsu API REST.

Poniżej przedstawiono przykładowy kod interfejsu API REST na stronie **Role**:

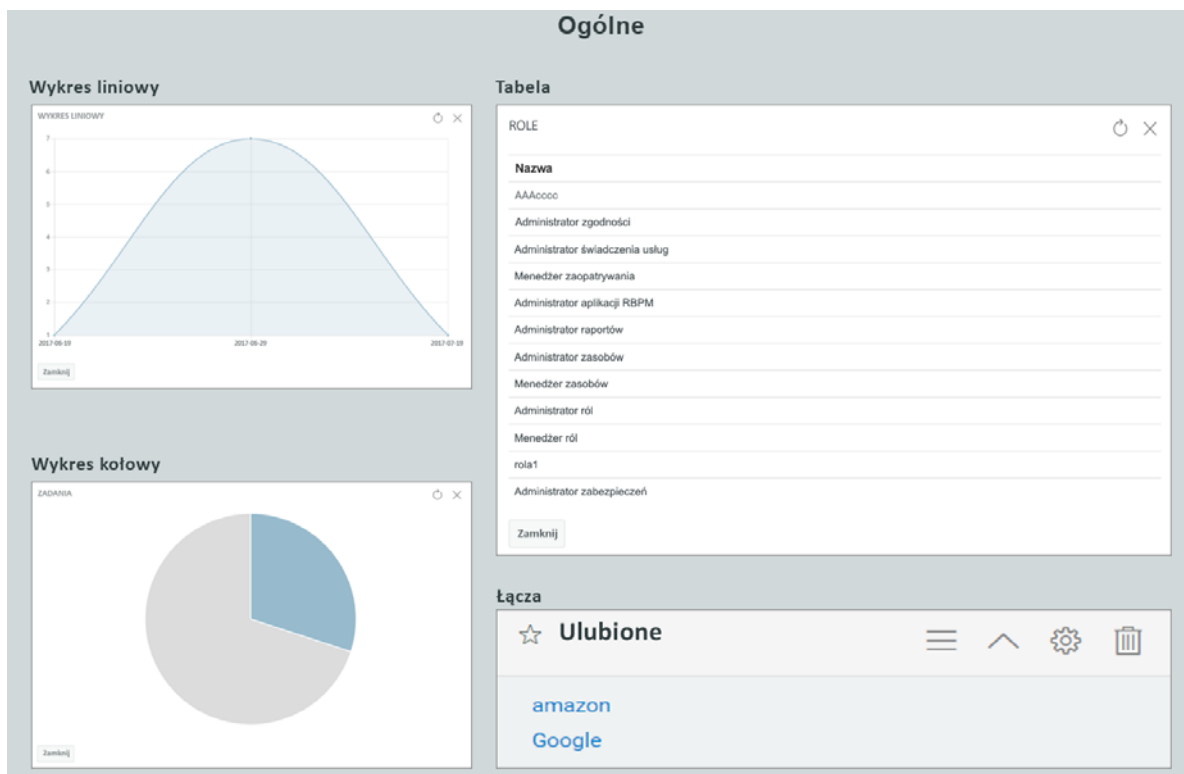
```
{
  "total": 12,
  "nextIndex": 0,
  "token": "60045d6be10f4419a2da9fa728683b06",
  "assignments": [
    {
      "id":
"cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
application driver,cn=driverset1,o=system",
      "name": "AAAcxxx",
      "description": "afasfdsf",
      "entityType": "role",
      "link": "/IDMProv/rest/access/assignments/item",
      "bulkRemovable": "true",
      "categories": [
        {
          "categoryId": "default",
          "categoryName": "Default"
        }
      ]
    }
  ]
}
```

W tym przykładzie elementem głównym jest przypisanie, a nazwa jest wybraną kolumną, która będzie wyświetlana na formancie. Możesz też tworzyć zakładki dowolnego adresu URL, do którego chcesz przechodzić ze swojego pulpitu nawigacyjnego.

- 4 (Warunkowo) W przypadku formantów **Łącza** należy określić **Tytuł** łączy i dodać łącza, które mają być dostępne z poziomu pulpitu nawigacyjnego.
- 5 Kliknij **Zapisz**, aby wprowadzić zmiany.

Poniżej przedstawiono przykładowe formanty w postaci wykresów i łączy, które można dodać do pulpitu nawigacyjnego.

Rysunek 3-6 Przykładowe formanty ogólne



Dodawanie formantów Identity Manager

Kategoria **IDM** umożliwia dodawanie standardowych formantów aplikacji Identity Manager do pulpitu nawigacyjnego.

Na przykład:

- ♦ **Dostęp**: Wyświetla licznik ról i zasobów oraz inne informacje na ich temat.
- ♦ **Żądania dla innych użytkowników**: Wyświetla liczbę oczekujących i odrzuconych żądań innych użytkowników oraz umożliwia tworzenie żądań dla tych użytkowników.
- ♦ **Żądania we własnym imieniu**: Wyświetla liczbę żądań oczekujących i odrzuconych oraz umożliwia tworzenie nowych żądań.
- ♦ **Zadania**: Wyświetla liczbę zadań nowych, oczekujących oraz zadań, które wkrótce wygasną.

Informacje na temat konfigurowania tych formantów znajdują się w sekcji „[Konfigurowanie formantu](#)” na stronie 33.

WAŻNE: Kliknij **Zapisz**, aby zachować wprowadzone zmiany.

Dodawanie formantów aplikacji Identity Governance

Aby wyświetlić formanty aplikacji Identity Governance, należy zainstalować i skonfigurować aplikację Identity Governance za pomocą pulpitu nawigacyjnego aplikacji Identity Manager.

Kategoria **IG** umożliwia dodawanie standardowych lub zdefiniowanych formantów aplikacji Identity Governance do pulpitu nawigacyjnego. Na przykład:

Zadania realizacji

Wyświetla liczbę żądań dostępu, ról biznesowych i błędów przypisania uprawnień w systemie.

Zadania przeglądania

Wyświetla liczbę oczekujących i zakończonych przeglądów w systemie.

Naruszenia SoD

Wyświetla liczbę naruszeń rozdziału obowiązków (SoD) w systemie, które nie zostały ocenione, zostały zatwierdzone lub są w trakcie rozstrzygania.

Opcje formantów

Możesz wykonać następujące czynności dotyczące formantów:



Odśwież

Aktualizuje zawartość formantu o najnowsze informacje.

Przesuń

Umożliwia zmianę położenia formantu na pulpicie nawigacyjnym.

Konfigurowanie

Umożliwia konfigurację właściwości formantu. Aby uzyskać więcej informacji, zobacz „[Konfigurowanie formantu](#)” na stronie 33.

Usuń

Usuwa formant z pulpitu nawigacyjnego.

Zwiń

Ukrywa informacje o formancie i wyświetla wyłącznie tytuł formantu.

Otwórz formant w trybie pełnoekranowym

Wyświetla informacje o formancie w trybie pełnoekranowym.

UWAGA

- Opcje **Odśwież** i **Otwórz formant w trybie pełnoekranowym** są wyświetlane wyłącznie w przypadku formantów należących do kategorii **Ogólne**.
 - Kliknij **Zapisz**, aby zachować wprowadzone zmiany.
-

Konfigurowanie formantu

Każdy formant dodany do pulpitu nawigacyjnego można skonfigurować. Można na przykład aktywować lub wyłączać pola formantu lub zmieniać kolory pól.

1 Kliknij  na formancie, który chcesz skonfigurować.

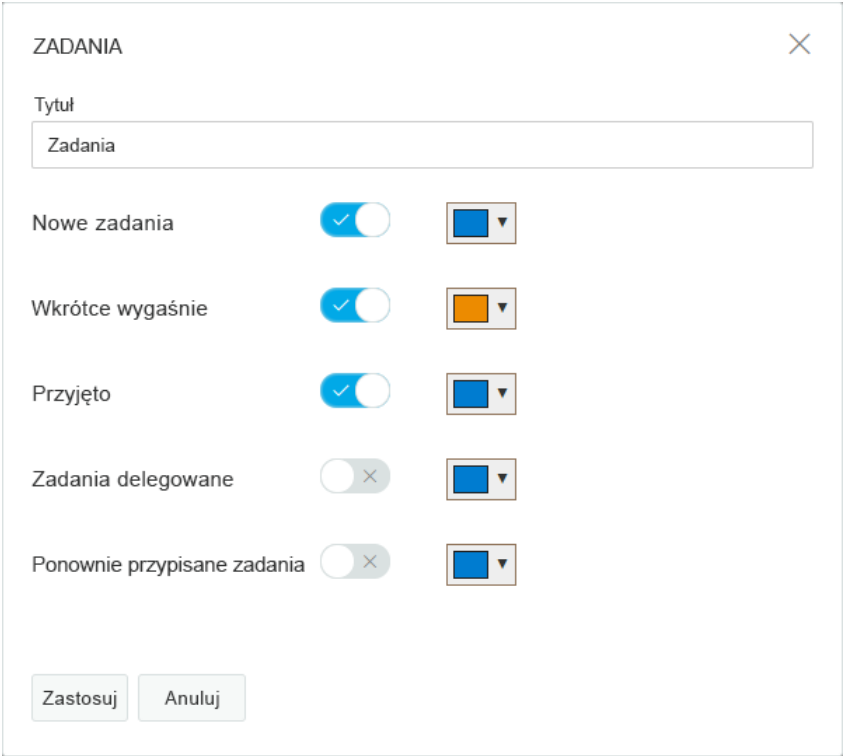
2 Zmień właściwości formantu.

Możesz na przykład zmienić tytuł formantu lub kolor etykiety pola formantu. Możesz też aktywować lub wyłączyć pole formantu na stronie właściwości.

3 Kliknij **Zastosuj**, aby wyświetlić zmiany na pulpicie nawigacyjnym.

Na przykład można zmodyfikować formant zadań w sposób przedstawiony poniżej:

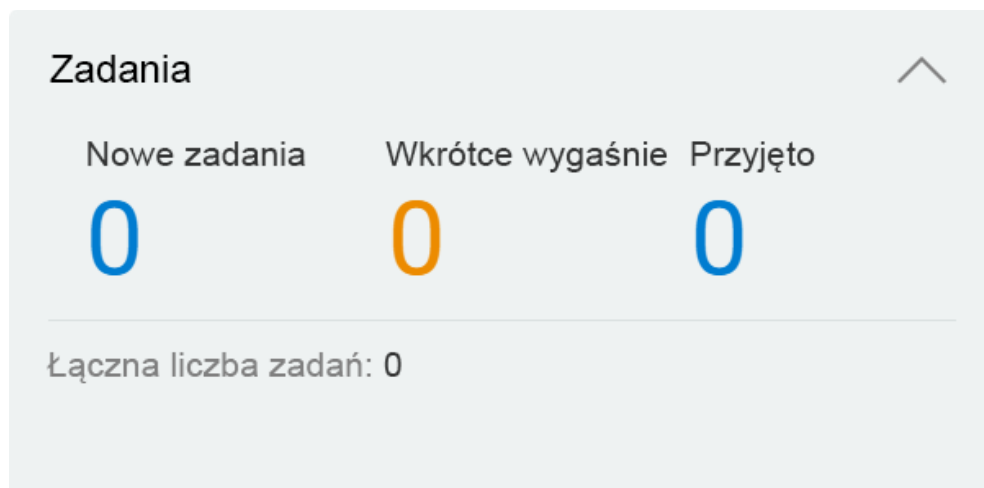
Rysunek 3-7 Przykład konfiguracji formantu



Okno konfiguracji formantu o tytule "ZADANIA" zawiera następujące elementy:

- Tytuł: Pole tekstowe z wartością "Zadania".
- Nowe zadania: Przełącznik włączony (niebieski) i wybór koloru (niebieski kwadrat).
- Wkrótce wygaśnie: Przełącznik włączony (niebieski) i wybór koloru (pomarańczowy kwadrat).
- Przyjęto: Przełącznik włączony (niebieski) i wybór koloru (niebieski kwadrat).
- Zadania delegowane: Przełącznik wyłączony (szary) i wybór koloru (niebieski kwadrat).
- Ponownie przypisane zadania: Przełącznik wyłączony (szary) i wybór koloru (niebieski kwadrat).
- Na dole znajdują się przyciski "Zastosuj" i "Anuluj".

Kliknij opcję **Zastosuj**, aby wyświetlić zmiany na pulpicie nawigacyjnym.



Aby skonfigurować formanty ogólne, zmodyfikuj opcje, które są wyświetlane podczas dodawania formantów. Patrz „[Dodawanie formantów ogólnych](#)” na stronie 30.

WAŻNE: Kliknij **Zapisz**, aby zachować wprowadzone zmiany.



Zarządzanie uprawnieniami i profilem tożsamości

Pulpit nawigacyjny aplikacji Identity Manager pozwala zgłaszać żądania dostępu do zasobów i ról, które są niezbędne przy wykonywaniu codziennych zadań. W środowisku aplikacji Identity Manager można także wykonywać działania na dowolnych przypisanych do siebie zadaniach, takich jak zatwierdzanie żądań dostępu. Procesem tym mogą zarządzać właściciele zasobów i ról.

Po zgłoszeniu żądania uprawnienia aplikacja Identity Manager inicjuje proces efektywnego przeglądu żądania, aby udostępnić użytkownikowi potrzebną rolę lub zasób. Menedżer otrzymuje w wiadomości e-mail albo na pulpicie nawigacyjnym powiadomienie dotyczące sprawdzenia żądania. W niektórych przypadkach żądanie może zostać również zatwierdzone przez inne osoby w organizacji.

Niektórzy użytkownicy mogą także zgłaszać żądania w imieniu innych osób lub występować w roli pełnomocnika innego użytkownika.

- ♦ [Rozdział 4, „Zarządzanie żadaniami nadania uprawnienia”, na stronie 37](#)
- ♦ [Rozdział 5, „Zarządzanie aplikacjami”, na stronie 45](#)
- ♦ [Rozdział 6, „Zarządzanie zadaniami”, na stronie 49](#)
- ♦ [Rozdział 7, „Działanie w imieniu innej osoby”, na stronie 53](#)
- ♦ [Rozdział 8, „Zarządzanie delegowaniami”, na stronie 55](#)
- ♦ [Rozdział 9, „Zarządzanie dostępnością”, na stronie 57](#)
- ♦ [Rozdział 10, „Zarządzanie profilem”, na stronie 59](#)
- ♦ [Rozdział 11, „Zarządzanie schematem organizacyjnym”, na stronie 61](#)
- ♦ [Rozdział 12, „Zarządzanie hasłami”, na stronie 69](#)

4 Zarządzanie żadaniami nadania uprawnienia

Ta sekcja zawiera wskazówki dotyczące następujących działań:

- ♦ „Wyświetlanie uprawnień” na stronie 37
- ♦ „Zgłaszanie żądań uprawnień” na stronie 39
- ♦ „Wyświetlanie żądań” na stronie 40
- ♦ „Unieważnianie uprawnień” na stronie 41
- ♦ „Tworzenie głębokich łączy z żądaniem” na stronie 42

Informacje na temat tych działań można również znaleźć w informacjach o pulpicie nawigacyjnym, korzystając z ikony .

Wyświetlanie uprawnień

Uprawnienia to konta, role lub zasoby, do których masz dostęp. Uprawnienia mogą zostać przypisane do użytkownika automatycznie przez organizację lub można zgłosić żądanie konkretnych uprawnień. Możesz też dziedziczyć niektóre uprawnienia pośrednio przez relacje ról lub jeśli jesteś członkiem grupy lub kontenera.

Aby wyświetlić role i zasoby, do których masz dostęp, wybierz na pulpicie nawigacyjnym opcję:

Dostęp > Uprawnienia

Następnie możesz wybrać określone uprawnienie, aby wyświetlić dodatkowe szczegóły dotyczące danej roli lub zasobu. Mogą to być również informacje o przyczynach przypisania uprawnienia. Aby znaleźć określone uprawnienie na dłuższej liście, wpisz w polu wyszukiwania jego nazwę, CN lub opis. Listę można również filtrować.

UWAGA:

- ♦ Domyślnie wyświetlana jest lista uprawnień, które są przypisane bezpośrednio do Ciebie lub zatwierdzone. Jest to jednak zależne od sposobu, w jaki administrator skonfigurował ustawienia tej strony. Więcej informacji znajduje się w sekcji [Ustawienia użytkownika](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.
 - ♦ Aby wyświetlić uprawnienia podrzędne zmapowane z przypisanymi lub zatwierdzonymi uprawnieniami, kliknij ikonę .
-

Wyświetlanie szczegółów uprawnień

Wybierz uprawnienie, o którym chcesz wyświetlić więcej szczegółów. W poniższej tabeli wymieniono pola wyświetlane dla poszczególnych uprawnień:

Tabela 4-1 Pola uprawnień i ich opisy

Pola	Opis
Opis	Opis roli lub zasobu.
Data efektywna	Data i godzina przypisania uprawnień.
Data wygaśnięcia	Data, po której uprawnienie nie będzie już przypisane do użytkownika. Jest ona wyświetlana tylko dla uprawnień, które mają włączoną opcję wygasania.
Przyczyna	Określa przyczynę przypisania uprawnienia do użytkownika.
Uprawnienie przypisane przez	Określa, kto przypisał dane uprawnienie użytkownikowi. Jeśli rola jest przypisana do użytkownika bezpośrednio w procesie zatwierdzania, w opcji Wyświetl informacje o zatwierdzeniu roli możesz zobaczyć listę osób zatwierdzających, które zatwierdziły żądanie przypisania. Jeśli rola jest dziedziczona przez użytkownika przez przynależność do grupy lub kontenera, w opcji Wyświetl informacje o przypisaniu roli do grupy wyświetlane są następujące szczegóły: ♦ Żądane przez:: Określa, kto zażądał uprawnień. ♦ Opis żądania: Opis podany podczas wysyłania żądania uprawnień. ♦ Szczegóły zatwierdzającego: Kliknij łącze, aby wyświetlić listę osób zatwierdzających, które zatwierdziły żądanie przypisania roli.

Jeśli jesteś administratorem aplikacji do zarządzania tożsamością, możesz wyświetlać uprawnienia innych członków zespołu na karcie **Inni**. Przejdź na kartę **Inni** i wyszukaj według nazwy użytkownika lub szczegółów uprawnienia.

- ♦ Wyszukiwanie według użytkownika powoduje wyświetlenie listy wszystkich przypisanych uprawnień danego użytkownika. Następnie można wybrać konkretne uprawnienie, aby sprawdzić jego szczegóły, takie jak data przypisania, osoba, która przypisała uprawnienie, a także przyczyna przypisania uprawnienia, jeśli została podana. Więcej informacji można znaleźć w podręczniku [Tabela 4-1 na stronie 38](#).
- ♦ Wyszukiwanie według uprawnienia powoduje wyświetlenie listy wszystkich użytkowników, zarówno indywidualnych, jak i należących do grupy bądź kontenera, do których przypisano dane uprawnienie.

UWAGA: Wyszukiwanie według szczegółów uprawnień nie jest obsługiwane w przypadku użytkowników będących menedżerami lub nadzorcami zespołu. Mogą oni jednak wyświetlać uprawnienia członków swojego zespołu, wyszukując nazwę lub opis zespołu. Ponadto na stronie dostępne jest również wyszukiwanie według nazwy użytkownika, co umożliwia wyszukiwanie i przeglądanie uprawnień konkretnego członka zespołu.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Zgłaszanie żądań uprawnień

Aby zgłosić żądanie roli lub zasobu, kliknij opcję **Dostęp > Żądania**.

Przed zgłoszeniem żądania uprawnień należy zapoznać się z następującymi uwagami:

- ♦ Istnieje możliwość zgłoszenia żądania dostępu w imieniu innego użytkownika. Na przykład menedżer zespołu zwykle może działać w imieniu członków zespołu. Proces jest taki sam z wyjątkiem tego, że należy wskazać, że żądanie dotyczy innej osoby (**Inni**), a nie siebie (**Własne**).
- ♦ Podczas zgłaszania żądania uprawnień nie należy używać znaków interpunkcyjnych. Jeśli nazwa uprawnienia, którego dotyczy żądanie, zawiera znaki interpunkcyjne, należy je pominąć podczas wyszukiwania.
- ♦ Różne uprawnienia wymagają różnych informacji w zależności od tego, w jaki sposób administrator skonfigurował formularz uprawnień. Jeśli uprawnienie wymaga szczegółowych informacji, pulpit nawigacyjny przekierowuje użytkownika do osobnego okna podczas wyboru uprawnienia.
- ♦ Można zgłosić żądanie wielu uprawnień jednocześnie.
Jeśli jednak formularz uprawnienia dla jednego z żądań wymaga specjalnego rodzaju informacji, uwzględnienie tego uprawnienia w żądaniu wielu uprawnień może nie być możliwe. Aby możliwe było zgłoszenie żądania wielu uprawnień jednocześnie, formularze poszczególnych żądań nie mogą wymagać szczegółowych informacji.
- ♦ Podczas zgłaszania żądania zasobu lub roli można określić datę wygaśnięcia.

Aby zażądać uprawnień programu Identity Governance:

*Ma zastosowanie tylko w dwóch przypadkach: jeśli włączono opcję **Wyświetl katalog IG na stronie żądania** na stronie **Konfiguracja > Identity Governance** oraz jeśli użytkownik żąda uprawnień dla siebie (**Własne**).*

- ♦ **Katalogi IDM:** Zawiera listę wszystkich ról, zasobów i przepływów pracy dostępnych w programie Identity Manager.
- ♦ **Aplikacje IG:** Zawiera listę wszystkich aplikacji zgromadzonych w programie Identity Governance. Umożliwia też wybranie uprawnień powiązanych z wybraną aplikacją.
- ♦ **Role techniczne IG:** Zawiera listę wszystkich ról technicznych dostępnych w programie Identity Governance. Wybierz role IG, których przyznania chcesz zażądać, i określ powód żądania.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Wyświetlanie żądań

Aby wyświetlić stan żądania w trakcie realizacji i żądania ukończone, wybierz na pulpicie nawigacyjnym opcję:

Dostęp > Historia żądań

Menedżer lub nadzorca zespołu może wyświetlić historię żądań innych członków zespołu na karcie **Inni**.

Zgłoszenie pomocy technicznej można wysłać również w przypadku żądań oczekujących.

- ♦ „Śledzenie żądania” na stronie 40
- ♦ „Anulowanie żądania” na stronie 40
- ♦ „Wystawianie zgłoszenia pomocy technicznej” na stronie 41

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

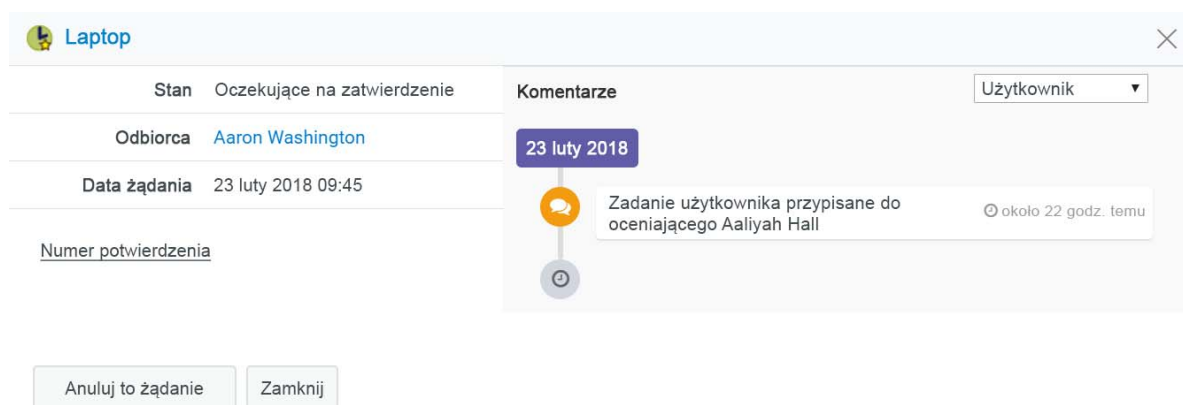
Śledzenie żądania

W każdym żądaniu możesz wyświetlać nie tylko własne czynności, ale też przepływ pracy w procesie zatwierdzania lub odrzucania żądania. Każdy etap w tym procesie ma znacznik czasu.

UWAGA: Jeśli zgłaszasz żądanie aplikacji lub ról technicznych na karcie **Aplikacje IG** bądź **Role techniczne IG**, nie możesz go śledzić na stronie **Historia żądań**. Aby śledzić żądania aplikacji IG, można dodać adres URL historii IG ze strony **Aplikacje** na pulpicie nawigacyjnym.

Aby śledzić żądanie oczekujące, wybierz to żądanie, a następnie zmień menu w prawym górnym rogu na **Użytkownik i system**. Na pulpicie nawigacyjnym zostanie wyświetlony bieżący stan żądania w trakcie procesu zatwierdzania.

Rysunek 4-1 Śledzenie żądania



Anulowanie żądania

Żądanie *oczekujące* można anulować na stronie **Historia żądań**. Wybierz żądanie z listy, a następnie opcję **Anuluj to żądanie** w kolejnym oknie.

Wystawianie zgłoszenia pomocy technicznej

W przypadku żądań, z którymi przez dłuższy czas nic się nie dzieje, można poprosić o pomoc stanowisko pomocy technicznej.

Zgłoszenie pomocy technicznej można wystawić w następujących miejscach:

- ♦ **Dostęp > Żądanie**, kliknij opcję **Zgłoszenie pomocy technicznej**.
- ♦ **Aplikacje**, kliknij opcję **Zgłoszenie pomocy technicznej**.
- ♦ **Dostęp > Historia żądań**, kliknij ikonę  na żądaniu, w sprawie którego chcesz wystawić zgłoszenie pomocy technicznej.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Pracownicy stanowiska pomocy technicznej otrzymają powiadomienie o zgłoszeniu pomocy technicznej. Otrzymasz powiadomienie dotyczące Twojego zgłoszenia po jego rozstrzygnięciu lub zamknięciu.

Unieważnianie uprawnień

Jeśli nie potrzebujesz już dostępu do roli lub zasobu, możesz unieważnić odpowiednie uprawnienie. Aby unieważnić uprawnienie, przejdź do opcji **Dostęp > Uprawnienia**, wybierz wymagane uprawnienie i podaj przyczynę jego unieważnienia.

Możesz też unieważnić uprawnienie w imieniu innych użytkowników. Jeśli na przykład członek Twojego zespołu został przeniesiony z działu 1 do działu 2 i nie potrzebuje już dostępu do określonego zasobu, aplikacja Identity Manager umożliwia unieważnienie uprawnienia tego użytkownika. Aby unieważnić uprawnienie, wybierz opcję **Inni** i usuń uprawnienie. Istnieje możliwość unieważnienia wielu uprawnień jednocześnie. Uprawnienia te można dodać do kolejki w celu sprawdzenia przed podjęciem decyzji o unieważnieniu.

Uprawnienia innych użytkowników może unieważniać tylko administrator i menedżer zespołu. Administrator może unieważniać uprawnienia wszystkich użytkowników w organizacji, natomiast menedżer zespołu może unieważniać uprawnienia tylko członków swojego zespołu.

Uprawnienia innych użytkowników można unieważniać w następujący sposób:

Unieważnij uprawnienia 

Własne ☒ Inni

 Według użytkownika  Według uprawnień

- ♦ **Wyszukiwanie według użytkownika:** Umożliwia wyszukanie użytkownika i unieważnienie jego uprawnień. Można bezpośrednio unieważnić uprawnienie użytkownika lub dodać je do kolejki. Kolejka jest trwałym obszarem roboczym, w którym można tymczasowo przechowywać uprawnienia w celu ich przejrzenia i unieważnienia, jeśli to konieczne. Następnie można wyszukać inne uprawnienia danego użytkownika, które mają zostać unieważnione, i dodać je do kolejki. Dzięki temu można unieważnić wszystkie uprawnienia jednocześnie.

- ♦ **Wyszukiwanie według uprawnień:** Umożliwia wyszukanie konkretnego uprawnienia. Po wybraniu uprawnienia wyświetlana jest lista wszystkich użytkowników, którzy nim dysponują. Można bezpośrednio unieważnić uprawnienie wybranego użytkownika lub dodać je do kolejki, aby je unieważnić dla wielu użytkowników jednocześnie.

Menedżer zespołu: Menedżer zespołu może unieważniać uprawnienia członków zespołu na karcie **Inni**. Jednak musi mieć uprawnienie do unieważniania uprawnień innych użytkowników.

Administrator: Administrator może dać menedżerowi zespołu możliwość unieważniania uprawnień. Jeśli na przykład chcesz przyznać menedżerowi zespołu uprawnienie do unieważniania roli użytkownika: Przejdź do opcji **Osoby > Zespoły** i zmodyfikuj uprawnienia zespołu, aby umożliwić menedżerowi zespołu unieważnianie uprawnień.

Rysunek 4-2 Przykład przyznawania menedżerowi zespołu uprawnienia do unieważniania

Ta opcja umożliwia menedżerowi zespołu unieważnianie wybranej roli członków zespołu.

UWAGA: Po unieważnieniu uprawnienia lista uprawnień może nie od razu odzwierciedlać wprowadzoną zmianę. Może to wynikać z faktu, że uprawnienie jest powiązane z procesem unieważniania, który może zająć trochę czasu. Aby wyświetlić zmiany, należy odświeżyć listę.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Tworzenie głębokich łączy z żądaniem

Aplikacje do zarządzania tożsamością umożliwiają tworzenie głębokich łączy do określonego żądania przetwarzania (nazywanego również żądaniem zaopatrywania). Ta funkcja daje menedżerowi możliwość wysłania adresu URL określonego żądania przetwarzania do pracownika, dzięki czemu pracownik ten może szybko zażądać przetwarzania bez konieczności korzystania z pulpitu nawigacyjnego aplikacji Identity Manager. W przypadku głębokiego łącza do żądania przetwarzania formularz żądania jest wyświetlany w treści strony wraz z nagłówkiem dla aplikacji do zarządzania tożsamością.

Gdy żądanie uprawnienia zostanie zgłoszone, pojawi się na stronie **Dostęp > Historia żądań** osoby zgłaszającej, a także na stronie **Zadania** osoby oceniającej.

Adres URL używany w głębokich łączy do żądania przetwarzania ma następujący format:

- ♦ W przypadku starszych formularzy:

```
https://<server:port>/IDMProv/
requestForm.do?uid=<PRD_ID>&aqua=true&idmdash=true&recipient=<recipient>&jsa=<operation_type>
```

Poniżej znajduje się przykład pokazujący, jakiego adresu URL można użyć do utworzenia głębokiego łącza do definicji żądania zaopatrywania:

```
https://testserver:8543/IDMProv/requestForm.do?uid=cn=request mobile approval app,cn=requestdefs,cn=appconfig,cn=user application driver,cn=driverset1,o=system&aqua=true&idmdash=true&recipient=&jsa=%7B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22window.close%28%29%22%7D
```

- ♦ W przypadku nowych formularzy JSON:

```
https://<server:form_renderer_port>/forms/#/form/details?id=<formID>&recipient=<recipient>&pid=<workflowID>&sid=IDM&uri=<forms_uri>&formContainer=RequestForms&locale=<language>
```

Poniżej znajduje się przykład pokazujący, jakiego adresu URL można użyć do utworzenia głębokiego łącza do definicji żądania zaopatrywania:

```
https://testserver:18600/forms/#/form/details?id=cn%3DHelp-desk%20Request%20Form,cn%3DWorkflowForms,cn%3Dappconfig,cn%3DUser%20Application%20Driver,cn%3Ddriverset1,o%3Dsystem&recipient=&pid=cn%3Dhelpdeskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20driver,cn%3Ddriverset1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&formContainer=RequestForms&locale=en
```


5 Zarządzanie aplikacjami

Jako administrator Identity Applications możesz modyfikować stronę **Aplikacje**, aby wyświetlać wszystkie aplikacje, działania i uprawnienia, które mają być dostępne dla użytkowników. Identity Applications domyślnie zawierają kategorię **Elementy strony głównej**, której nie można usunąć.

Po wprowadzeniu zmian kliknij opcję **Edycja zakończona**, aby wrócić do strony **Aplikacje**.

Tworzenie elementów wyróżnionych

Możesz utworzyć dowolną liczbę aplikacji i uprawnień, które chcesz dodać do strony **Aplikacje**. Nie musisz dodawać tych elementów do kategorii **Elementów strony głównej** lub innych kategorii **Aplikacji**.

- 1 (Warunkowo) Aby utworzyć nowy element, kliknij ikonę + na karcie **Aplikacje** lub **Uprawnienia**.
- 2 Wypełnij formularz aplikacji lub uprawnień. Zobacz „Dodawanie aplikacji” na stronie 45 lub „Dodawanie uprawnienia” na stronie 46.

UWAGA: Musisz określić wartość wszystkich pól oznaczonych gwiazdką (*), takich jak nazwa i opis aplikacji.

- 3 (Opcjonalnie) Przeciągnij i upuść nową aplikację lub uprawnienie do kategorii.
- 4 (Warunkowo) Aby zmienić istniejący element, wybierz ikonę edycji w kafelku, a następnie zaktualizuj wartości.

Dodawanie aplikacji

Aby dodać aplikację, podaj następujące szczegóły:

(Warunkowo) Dodaj do kategorii

Określa kategorię danej aplikacji.

Nazwa

Określa nazwę aplikacji.

Opis

Określa charakter aplikacji.

(Opcjonalnie) Obraz

Określa logo lub obraz dla aplikacji.

Łącze

Określa łącze dla danej aplikacji. Patrz „Tworzenie głębokich łączy z żądaniem” na stronie 42.

(Opcjonalnie) Adres URL interfejsu API

Określa adres URL punktu końcowego REST z danymi JSON, które zawierają dodatkowe szczegóły, takie jak wartości parametrów i znaczek. Więcej szczegółów można znaleźć w dokumentacji.

Dodawanie uprawnień

Aby dodać uprawnienie, podaj następujące szczegóły:

Uprawnienia

Określa uprawnienie. Może to być rola, zasób lub PRD.

(Warunkowo) Dodaj do kategorii

Określa kategorię danej aplikacji.

(Opcjonalnie) Obraz

Określa logo lub obraz dla aplikacji.

Dodawanie, modyfikowanie lub usuwanie kategorii

Możesz uporządkować elementy na stronie **Aplikacje** w logiczne kategorie. Możesz utworzyć dowolną liczbę kategorii, których może potrzebować twoja organizacja. Możesz zmienić układ kafelków w kategorii lub przesuwać kafelki do innej kategorii.

Dodawanie kategorii

1 Wybierz **Nowa kategoria**.

Identity Manager dodaje kategorię na końcu grupy kategorii. Być może trzeba będzie przewinąć w dół, aby wyświetlić dodaną kategorię.

2 Podaj nazwę nowej kategorii.

3 Kliknij + i wybierz **Aplikacja** lub **Uprawnienie**.

4 Wypełnij formularz aplikacji lub uprawnień.

UWAGA: Musisz określić wartość wszystkich pól oznaczonych gwiazdką (*), takich jak nazwa i opis aplikacji.

5 Wybierz **+Dodaj**.

Zmienianie kategorii

Kategorię możesz zmienić w następujący sposób:

- ♦ Dodaj kafelki dla aplikacji i uprawnień: przeciągnij i upuść je z sekcji **Nowe elementy** i **Uprawnienia** po prawej stronie.
- ♦ Usuń aplikację lub uprawnienie, wybierając ikonę kosza na kafelku elementu.
- ♦ Zmień ustawienia elementu

- ♦ Zmień nazwę kategorii
- ♦ Zmień kolejność elementów w kategorii

Usuwanie kategorii

Aby usunąć kategorię, wybierz ikonę kosza po prawej stronie nazwy kategorii.

6 Zarządzanie zadaniami

Użytkownik odpowiedzialny za zatwierdzenie lub odrzucenie żądanych uprawnień w aplikacji Identity Manager może korzystać z pulpitu nawigacyjnego do zarządzania zadaniami. Wcześniej robił to w aplikacji użytkownika. Żądania można zatwierdzać lub odrzucać pojedynczo albo — jeśli żądania są proste i nie wymagają szczegółowych informacji — można to robić zbiorczo.

Aby przejrzeć żądania oczekujące, kliknij opcję **Zadania**.

Możesz również otrzymać powiadomienie e-mail z łączem, które umożliwia zatwierdzenie lub odrzucenie żądania w odpowiedzi.

Przed wykonaniem działań na żądaniach użytkowników należy zapoznać się z następującymi uwagami:

- Można wybrać wiele zadań do zbiorczego zatwierdzenia bądź odrzucenia.
- Pulpit nawigacyjny nie wyświetla pola wyboru przy żądaniach, które wymagają szczegółowych informacji. Żądania te należy zaakceptować lub odrzucić, wybierając po kolei każde z nich i wypełniając formularze.
- Jeżeli wybierzesz bardziej złożone żądanie do zatwierdzenia lub odrzucenia, pulpit nawigacyjny może otworzyć żądanie w oddzielnej karcie przeglądarki.
- Ogólnie rzecz biorąc, należy dodać komentarz z wyjaśnieniem przyczyny zatwierdzenia lub odrzucenia wybranych zadań.

Wyświetlanie zadań

Aby zarządzać swoimi zadaniami, wybierz opcję **Zadania**. Aby wyświetlić zadania przypisane do innych użytkowników, kliknij opcję **Inni**.

Jeżeli realizujesz zadania innych użytkowników w ramach pełnomocnictwa lub delegowania, możesz zajmować się zadaniami, które są przypisane do innych osób. Więcej informacji na temat przypisań pełnomocnictwa i przypisań delegowań znajduje się w sekcji [Występowanie w roli pełnomocnika](#).

Zatwierdzenia IDM: *Ma zastosowanie w przypadku włączenia opcji Wyświetl zatwierdzenia IG na stronie zadań na stronie Konfiguracja > Identity Governance.*

Ta karta zawiera listę wszystkich zadań programu Identity Manager. Domyślnie na liście znajdują się wszystkie **własne** zadania. Aby wyświetlić zadania innych użytkowników o odpowiedniej roli, kliknij opcję **Inni**.

- Podczas wyszukiwania swoich zadań możesz korzystać z filtrów **Ponownie przypisane zadania**, **Zwrócone zadania** lub **Zadania delegowane**. Użycie filtra **Zadania delegowane** dla opcji **Własne** powoduje wyświetlenie wyłącznie tych zadań, które oddelegowano do Ciebie.
- Jeżeli jesteś administratorem, zadania możesz też filtrować przy użyciu filtra **Przypisane do mnie, Odbiorca jako ja**.

- ♦ Jeżeli wyszukujesz zadania innych osób, możesz użyć filtra **Zwrócone zadania**, **Ponownie przypisane zadania** lub **Zadania delegowane**. Użycie filtra **Zadania delegowane** w pozycji **Inni** wyświetla wszystkie zadania, które oddelegowano do innych użytkowników w systemie.
- ♦ Możesz również uściślić wyszukiwanie zadań w oparciu o zadania, które pojawiły się w systemie:
 1. Wybierz .
 2. (Warunkowo) Aby wyświetlić zadania utworzone w określonym przedziale czasu, określ ten przedział w **Tygodniach**, **Dniach** lub **Godzinach**.
 3. (Warunkowo) Określ stan zadania, które chcesz przefiltrować.
 4. Kliknij **Filtruj**.
- ♦ Jeśli jesteś użytkownikiem stanowiska pomocy technicznej, możesz skorzystać z filtra **Zadania stanowiska pomocy technicznej**, aby wyświetlić odpowiednio dostosowaną listę. Informacje na temat zarządzania zadaniem stanowiska pomocy technicznej znajdują się w pomocy, która jest dostępna na pulpicie nawigacyjnym.

Jeśli zasady dotyczące żądania dostępu określają Cię jako zatwierdzającego żądania, czasami konieczne może być zatwierdzenie żądanych elementów. Te elementy wymagające zatwierdzenia znajdują się na liście na karcie **Zatwierdzenia**.

Zatwierdzenia IG: Ma zastosowanie, gdy opcja **Wyświetl zatwierdzenia IG na stronie zadań na stronie Konfiguracja > Identity Governance**.

Ta karta zawiera listę wszystkich oczekujących zadań zatwierdzenia w programie Identity Governance. Możesz ponownie przypisać zadania innym użytkownikom, korzystając z opcji **Przypisz ponownie**.

Zarządzanie zadaniami do zatwierdzenia lub odrzucenia

W niektórych organizacjach może istnieć grupa osób odpowiedzialnych za przegląd, zatwierdzanie i odrzucanie żądań dostępu. W takim przypadku każdy członek tej grupy otrzymuje te same żądania. Zespół obsługi IT może być na przykład odpowiedzialny za wszystkie żądania dotyczące telekomunikacji i sprzętu komputerowego. Kiedy nowy pracownik wysyła żądanie telefonu komórkowego, zostaje ono przypisane do wszystkich członków zespołu obsługi IT. Każdy członek tego zespołu może zająć się tym żądaniem.

Możesz wykonać dowolne z następujących czynności w odpowiedzi na żądanie:

Przyjmij żądanie

Możesz **przyjąć odpowiedzialność** za żądanie i zająć się jednośnym zadaniem niezwłocznie lub w późniejszym terminie. Niezależnie od tego, kiedy zajmiesz się zadaniem, nie będzie już ono widoczne dla innych członków Twojej grupy w ich **Zadaniach**.

Zwolnij żądanie

Jeżeli nie chcesz zająć się otrzymanym żądaniem, możesz je zwolnić.

Przypisz ponownie zadanie

Zadanie, które jest przypisane do Ciebie, może zostać przypisane do innego użytkownika w organizacji. Podczas ponownego przypisywania zadań należy uwzględnić poniższe kwestie:

- ♦ Jeśli nie jesteś w stanie wykonać zadania, możesz przypisać je do swojego menedżera. Zaznacz zadanie na karcie **Własne**, a następnie wybierz **Przypisz ponownie**. Zadanie zostanie automatycznie przypisane do Twojego menedżera.
- ♦ Jako menedżer zespołu możesz ponownie przypisywać tylko własne zadania do własnego menedżera. Chcąc jednak ponownie przypisać zadanie, które jest przydzielone do członka Twojego zespołu, możesz to zrobić na karcie **Inni**. Przejdź na kartę **Inni**, zaznacz pole wyboru wymaganego zadania i kliknij **Przypisz ponownie**. W menu rozwijanym **Przypisz do** wybierz członka zespołu, do którego chcesz ponownie przypisać zadanie, wprowadź komentarz dotyczący ponownego przypisania, a następnie kliknij **Przypisz ponownie**. Zadanie zostanie ponownie przypisane do wybranego członka zespołu.
- ♦ Jeśli w określonym przedziale czasu nie zostaną na zadaniu wykonane żadne działania, mogą wystąpić następujące sytuacje:
 - ♦ Administrator może ponownie przypisać zadanie do innego użytkownika. Administrator ma uprawnienia, aby ponownie przypisać zadanie do dowolnego użytkownika w organizacji.
 - ♦ Menedżer zespołu może ponownie przypisać zadanie do innego członka zespołu. Należy zapewnić, aby menedżer zespołu miał włączone uprawnienie Zarządzaj zadaniem adresata podczas tworzenia zespołu.

Dotyczy to tylko sytuacji, kiedy w celu dodania członków do zespołu podczas tworzenia zespołu użyto opcji **Członkowie**. Aby uzyskać więcej informacji, zobacz „[Tworzenie zespołu](#)” na stronie 84.

UWAGA: Jeśli do utworzenia zespołu używana jest opcja **Wszyscy użytkownicy** lub **Relacja**, menedżer zespołu nie może ponownie przypisywać zadań do innego członka zespołu.

- ♦ Użytkownik stanowiska pomocy technicznej może ponownie przypisać zadanie do Twojego menedżera aż do poziomu hierarchii zdefiniowanego na stronie **Ustawienia**. Hierarchia menedżerów jest konfigurowana przez administratora.

Jeśli zadanie zostało ponownie przypisane do Ciebie i nie jesteś w stanie go wykonać, możesz zwrócić je do użytkownika, który przypisał je do Ciebie.

Zwróć zadanie

Jeżeli nie chcesz zająć się zadaniem, które do Ciebie ponownie przypisano, możesz je zwrócić. Aplikacje do zarządzania tożsamością automatycznie przypisują zwrócone zadanie z powrotem do zatwierdzającego.

UWAGA: Można zwrócić wyłącznie ponownie przypisane zadanie.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Zarządzanie zadaniami stanowiska pomocy technicznej

Zadania stanowiska pomocy technicznej są tworzone dla każdego zgłoszenia pomocy technicznej w systemie. Zgodnie z przykładem w sekcji „[Działanie stanowiska pomocy technicznej](#)” na stronie 16 zgłoszenie Emili powoduje utworzenie zadania stanowiska pomocy technicznej na stronie **Zadania** Helen. Helen może podjąć odpowiednie działania związane z tym zadaniem stanowiska pomocy technicznej.

Jeśli jesteś użytkownikiem stanowiska pomocy technicznej, wybierz zgłoszenie pomocy technicznej, które wymaga Twojego działania. Wykonaj dowolne z następujących działań w odpowiedzi na wybrane zgłoszenie stanowiska pomocy technicznej:

Zaktualizuj

Aktualizuje zgłoszenie pomocy technicznej z odpowiednim komentarzem.

Zakończ

Kończy zgłoszenie pomocy technicznej z dołączonym komentarzem na temat rozstrzygnięcia.

Anuluj

Zamyka zgłoszenie pomocy technicznej z odpowiednim komentarzem.

UWAGA: Możesz **przyjąć** lub **zwolnić** zadanie stanowiska pomocy technicznej. Jeżeli przyjmiesz zgłoszenie pomocy technicznej z listy zadań, zgłoszenie pomocy technicznej będzie się wyświetlać w twoich zadaniach **własnych**.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

7 Działanie w imieniu innej osoby

W niektórych organizacjach możesz mieć możliwość wykonywania zadań jako pełnomocnik lub ustanawiania pełnomocnictwa na rzecz innej osoby. Asystent może na przykład działać w ramach pełnomocnictwa ustanowionego przez swojego szefa. Ponadto jeżeli na przykład współpracowniczka jest na urlopie macierzyńskim, możesz przez określony czas występować w jej imieniu.

- ♦ „Wyświetlanie przypisania pełnomocnictwa” na stronie 53
- ♦ „Występowanie w roli pełnomocnika” na stronie 53
- ♦ „Zarządzanie przypisaniami pełnomocnictwa” na stronie 53

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Wyświetlanie przypisania pełnomocnictwa

Aby wyświetlić przypisania pełnomocnictwa, wybierz na pulpicie nawigacyjnym opcję:

Dostęp > Przypisania pełnomocnictwa

Występowanie w roli pełnomocnika

Administrator może ustanowić Cię pełnomocnikiem innego użytkownika. Wówczas aplikacja dodaje opcję pełnomocnictwa do menu Twojego konta, w prawym górnym rogu.

Identyfikator użytkownika > Jako pełnomocnik

Na przykład Sara Smith może zarządzać relacjami z klientami. W aplikacjach do zarządzania tożsamością występuje zespół Relacje z klientami, którego menedżerem jest Sarah Smith. Może ona działać w imieniu Marii Belafonte, która jest członkiem jej zespołu. Wybiera na pulpicie nawigacyjnym **ssmith > Jako pełnomocnik**, a następnie wskazuje **mbelafonte**.

Zarządzanie przypisaniami pełnomocnictwa

Jako administrator lub menedżer zespołu możesz tworzyć, modyfikować i usuwać przypisania pełnomocnictwa. Skonfiguruj odpowiednio zespół, aby móc zarządzać przypisaniami pełnomocnictwa jako menedżer zespołu. Menedżer zespołu może przypisywać pełnomocnictwa wyłącznie członkom swojego zespołu.

8 Zarządzanie delegowaniami

W niektórych organizacjach dozwolone jest delegowanie zadań do innego użytkownika. Jeśli delegowano do Ciebie zadanie innego użytkownika lub Twoje zadania zostały delegowane do innych użytkowników w organizacji, informacje o delegowaniu możesz zobaczyć w opcji [Administrowanie > Delegowanie](#).

Delegowane zadania są wyświetlane na stronie [Zadania](#). Ikona  przy zadaniu wskazuje, że zadanie to zostało delegowane.

WAŻNE: Utworzenie przypisania delegowania wymaga również określenia szczegółów dostępności. Można podać szczegółowe informacje o dostępności podczas tworzenia przypisania delegowania lub utworzyć najpierw delegowanie, a potem określić szczegóły dostępności w osobnym działaniu. Zależy to od tego, czy administrator włączył wymagane uprawnienia. Gdy są włączone, na stronie [Utwórz przypisanie delegowania](#) widoczna jest opcja [Niedostępny od](#). Jeśli opcja [Niedostępny od](#) jest niewidoczna, szczegóły dostępności należy określić na stronie [Ustawienia dostępności](#) po utworzeniu przypisania delegowania. Dzięki temu delegowanie będzie działać zgodnie z oczekiwaniami. Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

9 Zarządzanie dostępnością

Użytkownik może wskazać, którymi żdaniami zasobów z przypisaniem delegowania nie może się zająć w danym okresie. Kiedy bieżący użytkownik jest niedostępny do obsługi konkretnego żądania w danym okresie, zadaniem może zająć się inny użytkownik oddelegowany do tego żądania.

Aby wyświetlić informacje o swojej dostępności, wybierz na pulpicie nawigacyjnym opcję

Osoby > Dostępność

Przed użyciem działania **Niedostępny od** należy skonfigurować co najmniej jedno przypisanie delegowania. Przypisania delegowania powinien utworzyć menedżer zespołu (lub administrator aplikacji zaopatrywania).

Ustawienia globalne dotyczące delegowania opartego na dostępności są określone w opcji **Ustaw dostępność podczas tworzenia przypisania delegowania** w obszarze **Ustawienia > Dostosowywanie > Elementy nawigacyjne > Ogólne**. Jeśli wolisz nie określać swojej dostępności indywidualnie dla każdej definicji żądania, możesz wybrać ustawienie **Niedostępny** dla wszystkich żądań w sekcji **Zmień stan**.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

10 Zarządzanie profilem

Aplikacje do zarządzania tożsamością udostępniają wygodny sposób wyświetlania informacji o tożsamości i pracy z nimi. Zwiększają także elastyczność organizacji przez zapewnienie dostępu do informacji o innych użytkownikach zawsze, gdy są one potrzebne. Można na przykład wykonywać następujące działania:

- Bezpośrednie zarządzanie własnym kontem użytkownika.
- Wyszukiwanie innych użytkowników i grup w organizacji.
- Wizualizowanie relacji między użytkownikami i grupami.
- Wyświetlanie aplikacji powiązanych z użytkownikiem.

Konfigurowaniem zawartości aplikacji do zarządzania tożsamością na potrzeby użytkownika i innych osób w organizacji zajmuje się administrator systemu. Na karcie mogą być dostępne różne elementy w zależności od stanowiska pracownika i poziomu uprawnień.

Aktualizowanie profilu

Aby wyświetlić lub zaktualizować profil tożsamości, wybierz na pulpicie nawigacyjnym opcję:

[Twój identyfikator] > Mój profil

lub,

Kliknij ikonę  na pulpicie nawigacyjnym.

Na tej stronie wyświetlany jest Twój menedżer nadzorujący, role, zasoby i grupy. Aby zmodyfikować informacje na swój temat lub wyświetlić swój schemat organizacyjny, musisz mieć dostęp administracyjny.

Twój profil zawiera takie ustawienia, jak imię i nazwisko, adres e-mail oraz numer telefonu. Na tej stronie wyświetlane są także atrybuty użytkownika z włączonymi uprawnieniami **Wyszukiwanie** i **Odczyt**. Te właściwości dostępu można skonfigurować w warstwie abstrakcji katalogów (DAL). Więcej informacji znajduje się w sekcji **Właściwości atrybutów** w podręczniku *NetIQ Identity Manager — Przewodnik administratora po projektowaniu Identity Applications*. Organizacja decyduje o tym, które ustawienia użytkownik może modyfikować. Na przykład użytkownik może mieć możliwość zmiany numeru telefonu, ale nie swojego nazwiska.

11 Zarządzanie schematem organizacyjnym

Pulpit nawigacyjny aplikacji Identity Manager zapewnia wygodny sposób wyszukiwania encji w organizacji oraz wyświetlania schematu organizacyjnego (encją może być użytkownik, grupa lub encja niestandardowa zdefiniowana przez administratora). Schemat organizacyjny przedstawia hierarchię relacji, takich jak menedżer-pracownik, członkostwo w grupie lub grupy użytkowników, między encjami w organizacji.

Domyślnie na stronie **Schemat organizacyjny** pulpitu nawigacyjnego wyświetlane jest położenie encji użytkownika w ramach organizacji oraz jego hierarchia relacji z innymi encjami użytkowników na podstawie relacji schematu organizacyjnego ustawionej przez administratora. Więcej informacji na temat ustawień domyślnych strony schematu organizacyjnego można znaleźć w sekcji [Dostosowywanie widoków](#). Więcej informacji na temat sposobu wyświetlania encji schematu organizacyjnego innych niż encja użytkownika można znaleźć w sekcji [Wyświetlanie schematu organizacyjnego obiektu](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Schemat organizacyjny jest często nazywany w skrócie „schematem”. Oba te terminy mogą występować na pulpicie nawigacyjnym.

Wyświetlanie schematu organizacyjnego

W ustawieniu domyślnym Administrator zabezpieczeń i Administrator świadczenia usług może wyświetlić schemat organizacyjny przedstawiający wszystkie encje w systemie.

Po schemacie organizacyjnym encji użytkownika można się poruszać na jeden z następujących sposobów:

- Przejdź do strony **Osoby** > **Schemat organizacyjny**. Zobaczysz schemat organizacyjny zalogowanego użytkownika oparty na domyślnej relacji schematu organizacyjnego skonfigurowanej na stronie **Ustawienia**. Możesz również wyświetlić schemat organizacyjny za pomocą ikony  znajdujące się na stronach **Mój profil**, **Pulpit nawigacyjny** i **Aplikacje**.

Aby znaleźć schematy organizacyjne innych użytkowników w systemie, wpisz ich nazwy na pasku wyszukiwania znajdującym się na stronie **Schemat organizacyjny**.

- Przejdź do strony **Ludzie** > **Użytkownicy** i wybierz dowolnego użytkownika z listy, a następnie kliknij  obok nazwy użytkownika. Aby uzyskać więcej informacji, zobacz [Rozdział 13, „Zarządzanie użytkownikami”, na stronie 77](#).

UWAGA: Aby wyświetlić stronę **Schemat organizacyjny**, musisz mieć dostęp do wyświetlania schematu organizacyjnego. Skontaktuj się z administratorem, aby uzyskać ten dostęp. Więcej informacji znajduje się w sekcji **Ustawienia użytkownika** w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Informacje o schemacie organizacyjnym

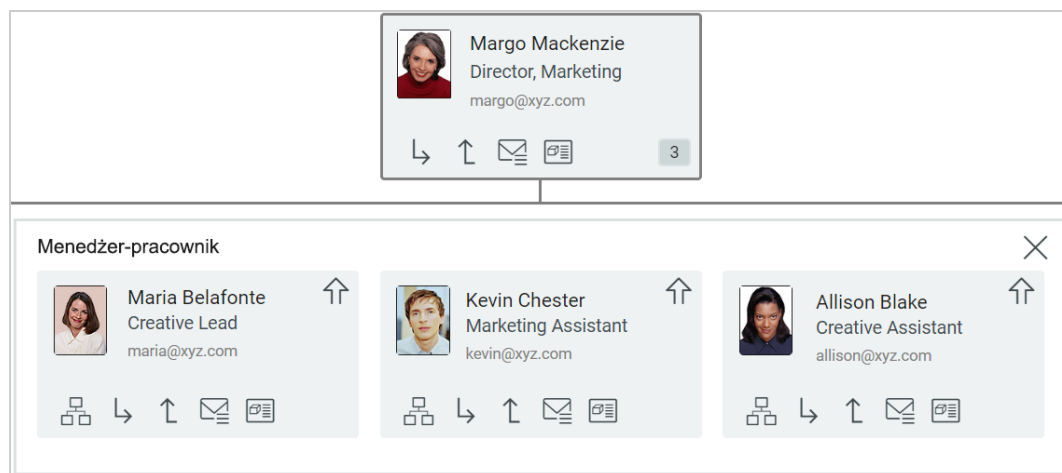
Na schemacie organizacyjnym informacje o encji są wyświetlane w formie karty. Karty te są uporządkowane w porządku hierarchicznym na podstawie domyślnej relacji schematu organizacyjnego skonfigurowanej przez administratora. Encja główna lub wybrana, która jest wyświetlana u góry, jest punktem początkowym lub punktem orientacyjnym w schemacie organizacyjnym, a encja podrzędna bezpośrednio pod główną jest wyświetlana u dołu na podstawie relacji domyślnej.

Każda karta zawiera informacje określone w oparciu o podstawowe i dodatkowe atrybuty zdefiniowane przez administratora. Więcej informacji na temat sposobu dostosowywania tych atrybutów można znaleźć w sekcji [Dostosowywanie widoku schematu organizacyjnego](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*. Na karcie encji użytkownika oprócz podstawowych i dodatkowych atrybutów zdefiniowanych przez administratora wyświetlane jest imię i nazwisko użytkownika. Dlatego jeśli administrator skonfiguruje imię i nazwisko jako atrybuty podstawowe, oba atrybuty mogą wystąpić dwukrotnie w **widoku karty** na stronie **Użytkownicy** w schemacie organizacyjnym.

UWAGA: Jeśli administrator nie zdefiniuje podstawowych i dodatkowych atrybutów encji w widoku schematu organizacyjnego, aplikacje do zarządzania tożsamością wyświetlają na stronie **Schemat organizacyjny** atrybut Nazwa zwykła (CN) encji.

Rysunek 11-1 przedstawia przykładowy schemat organizacyjny użytkownika *Margo Mackenzie*, w którym domyślną relacją schematu organizacyjnego jest Menedżer-pracownik.

Rysunek 11-1 Przykładowy schemat organizacyjny na pulpicie nawigacyjnym



W tym przykładzie użytkownik *Margo Mackenzie* jest menedżerem, a użytkownicy *Maria Belafonte*, *Kevin Chester* i *Allison Blake* są pracownikami, którzy bezpośrednio jej podlegają. U góry każdej karty wyświetlane jest imię i nazwisko użytkownika, w tym przypadku *Margo Mackenzie*, a po nich występuje rola w organizacji i adres e-mail, które zostały ustawione przez administratora jako atrybuty podstawowe i dodatkowe. Liczba znajdująca się w prawym dolnym rogu karty użytkownika *Margo Mackenzie* wskazuje liczbę pracowników, którzy jej bezpośrednio podlegają.

Praca ze schematem organizacyjnym

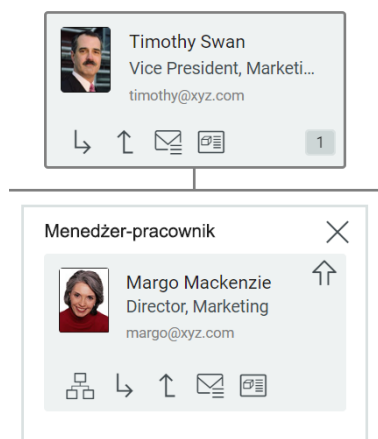
W zależności od wyszukiwania wykonanego na stronie **Schemat organizacyjny** na pulpicie nawigacyjnym wyświetlany jest schemat organizacyjny wyszukiwanej encji. Na tej stronie można wykonywać inne zadania, takie jak wyświetlanie innych relacji encji, zmiana encji głównej i wyświetlanie jej schematu organizacyjnego lub wyświetlanie schematu organizacyjnego encji znajdującej się na następnym poziomie w hierarchii relacji.

Aby dokładniej zapoznać się z zadaniami, które można wykonywać na stronie **Schemat organizacyjny**, rozważmy następujący przykład zespołu marketingowego w firmie XYZ:

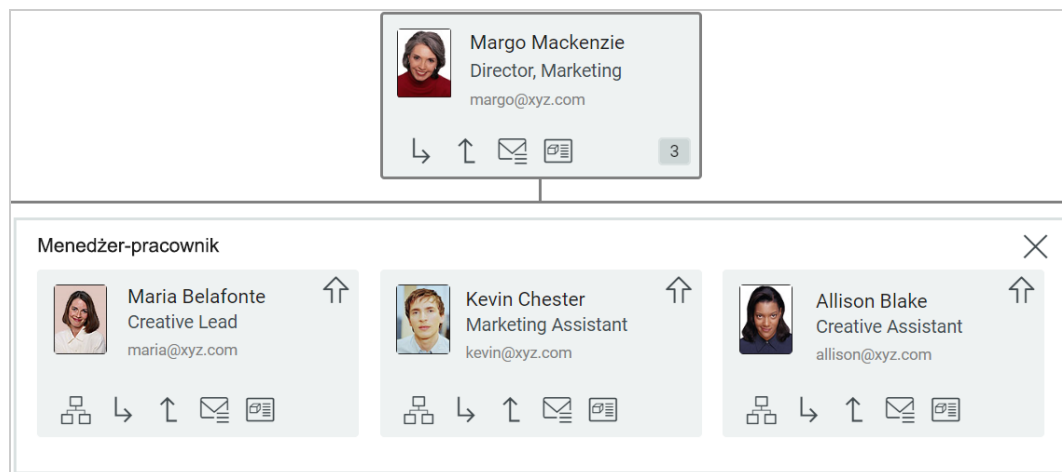
Margo Mackenzie jest dyrektorem w zespole marketingowym, a *Allison Blake*, *Kevin Chester* i *Maria Belafonte* są pracownikami, którzy bezpośrednio jej podlegają. Bezpośrednim przełożonym *Margo Mackenzie* jest *Timothy Swan* — wiceprezes zespołu marketingowego.

Przejdź do opcji **Osoby** > **Schemat organizacyjny** na pulpicie nawigacyjnym i wyszukaj użytkownika *Timothy Swan*, aby wyświetlić jego schemat organizacyjny. Podobnie wykonaj wyszukiwanie użytkownika *Margo Mackenzie*. **Rysunek 11-2** i **Rysunek 11-3** przedstawiają ich schematy organizacyjne na podstawie relacji Menedżer-pracownik.

Rysunek 11-2 Schemat organizacyjny użytkownika *Timothy Swan* w roli menedżera.



Rysunek 11-3 Schemat organizacyjny użytkownika *Margo Mackenzie* w roli menedżera.



Przyjrzyjmy się zadaniom, które można wykonywać na stronie **Schemat organizacyjny**, opierając się na powyższym przykładzie:

- „Resetowanie encji głównej w widoku schematu organizacyjnego” na stronie 64
- „Przełączanie widoku schematu organizacyjnego” na stronie 64
- „Wybór relacji do wyświetlenia” na stronie 65
- „Przechodzenie do następnego poziomu w hierarchii relacji” na stronie 66
- „Wysyłanie wiadomości e-mail do użytkowników ze schematu organizacyjnego” na stronie 67
- „Wyświetlanie szczegółowych informacji o użytkowniku” na stronie 67

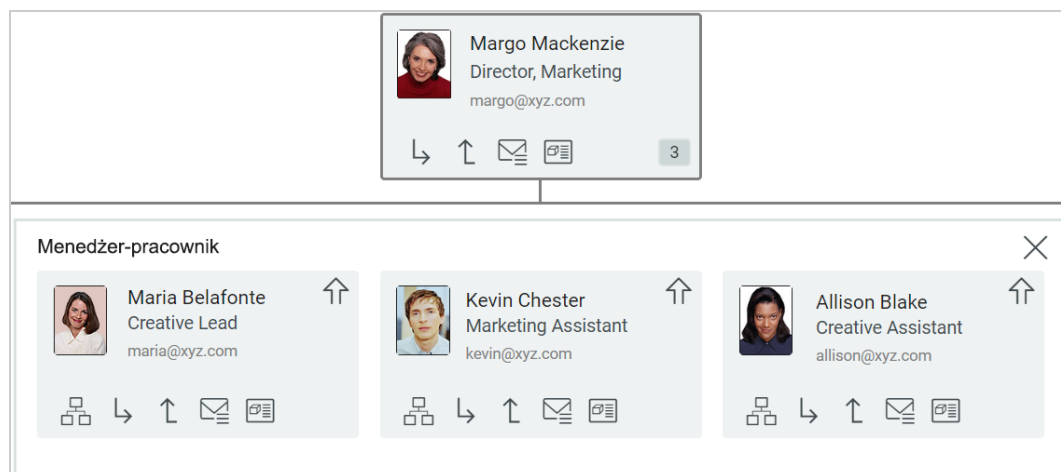
UWAGA: Powyższe zadania dotyczą zarówno encji użytkownika, jak i niestandardowych.

Resetowanie encji głównej w widoku schematu organizacyjnego

Aby zresetować głównego użytkownika w widoku schematu organizacyjnego, wykonaj następujące czynności:

- 1 Zidentyfikuj użytkownika, którego chcesz utworzyć jako nowego głównego użytkownika.
Przypuśćmy, że wyświetlany jest schemat organizacyjny, w którym *Timothy Swan* odgrywa rolę menedżera, a chcemy wyświetlić *Margo Mackenzie* jako nowego użytkownika głównego.
- 2 Przejdź do karty *Margo Mackenzie* i kliknij ikonę . Stanie się ona nowym użytkownikiem głównym i pojawi się u góry schematu organizacyjnego Menedżer-pracownik. Bezpośredni podwładni użytkownika *Margo Mackenzie* — czyli *Maria Belafonte*, *Kevin Chester* i *Allison Blake* — są wyświetlani pod nią.

Rysunek 11-4 *Margo Mackenzie jest nową encją główną w widoku schematu organizacyjnego*



Przełączanie widoku schematu organizacyjnego

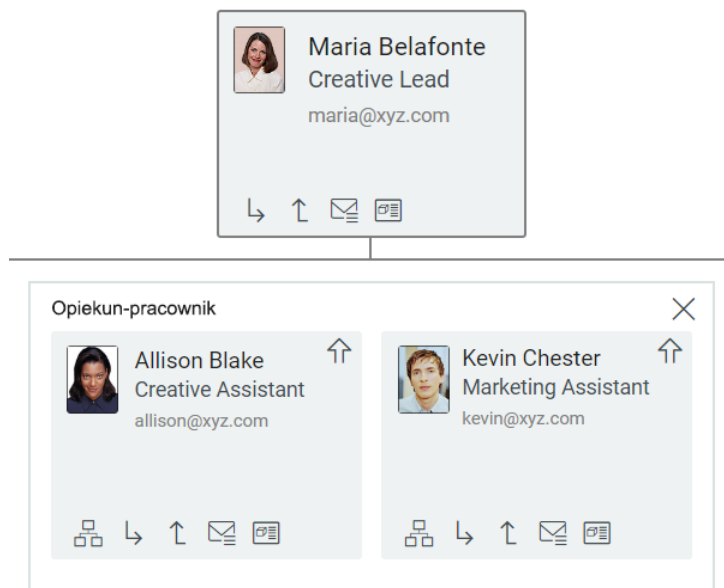
Aby zresetować użytkownika głównego i domyślną relację w widoku schematu organizacyjnego, wykonaj następujące czynności:

- 1 Zidentyfikuj użytkownika, którego schemat organizacyjny chcesz wyświetlić.

Przypuśćmy, że wyświetlany jest schemat organizacyjny, w którym *Margo Mackenzie* odgrywa rolę menedżera. *Maria Belafonte* — pracownik podlegający *Margo Mackenzie* — jest również opiekunem użytkowników *Kevin Chester* i *Allison Blake*. Chcesz wyświetlić relację Opiekun-pracownik *Maria Belafonte*.

- 2 Przejdź do karty użytkownika *Maria Belafonte* i kliknij ikonę .
- 3 Wybierz z menu rozwijanego relację **Opiekun-pracownik**. *Maria Belafonte* stanie się encją główną schematu organizacyjnego Opiekun-pracownik, a użytkownicy *Kevin Chester* i *Allison Blake* będą wyświetlani pod nią.

Rysunek 11-5 Schemat organizacyjny Marii Belfonte w roli opiekuna



Wybór relacji do wyświetlenia

Aby wyświetlić relacje użytkownika innego niż domyślny, wykonaj następujące czynności:

- 1 Zidentyfikuj użytkownika, którego relację chcesz wyświetlić.
Przypuśćmy, że wyświetlany jest schemat organizacyjny, w którym *Margo Mackenzie* odgrywa rolę menedżera. Chcesz wyświetlić relację grupy użytkowników *Marii Belafonte*, która należy do grupy Marketing.
- 2 Przejdź do karty użytkownika *Maria Belafonte* i kliknij ikonę .
- 3 Wybierz z menu rozwijanego relację **Grupy użytkowników**. Schemat przynależności do grupy użytkownika *Maria Belafonte* zostanie dodany do istniejącego widoku schematu organizacyjnego.

UWAGA: Maksymalny poziom, do którego można rozwinąć schemat organizacyjny użytkownika i wyświetlać wpłatane relacje, jest definiowany przez administratora. Domyślnie można rozwinąć maksymalnie do poziomu 3, przy czym poziom 1 jest zawsze przypisany do użytkownika głównego.

Przechodzenie do następnego poziomu w hierarchii relacji

Aby dokładnie zapoznać się z tym zadaniem, rozważmy drugi przykład, w którym *Edward Miller* jest dyrektorem w zespole sprzedaży. *Allison Blake* i *Filla Martell* są bezpośrednimi podwładnymi użytkownika *Edward Miller*. Jak widać, *Allison Blake* jest członkiem zespołów zarówno sprzedaży, jak i marketingu, a jej bezpośrednimi menedżerami są *Edward Miller* oraz *Margo Mackenzie*.

Aby przejść do następnego poziomu w drzewie relacji i rozwinąć go, wykonaj następujące czynności:

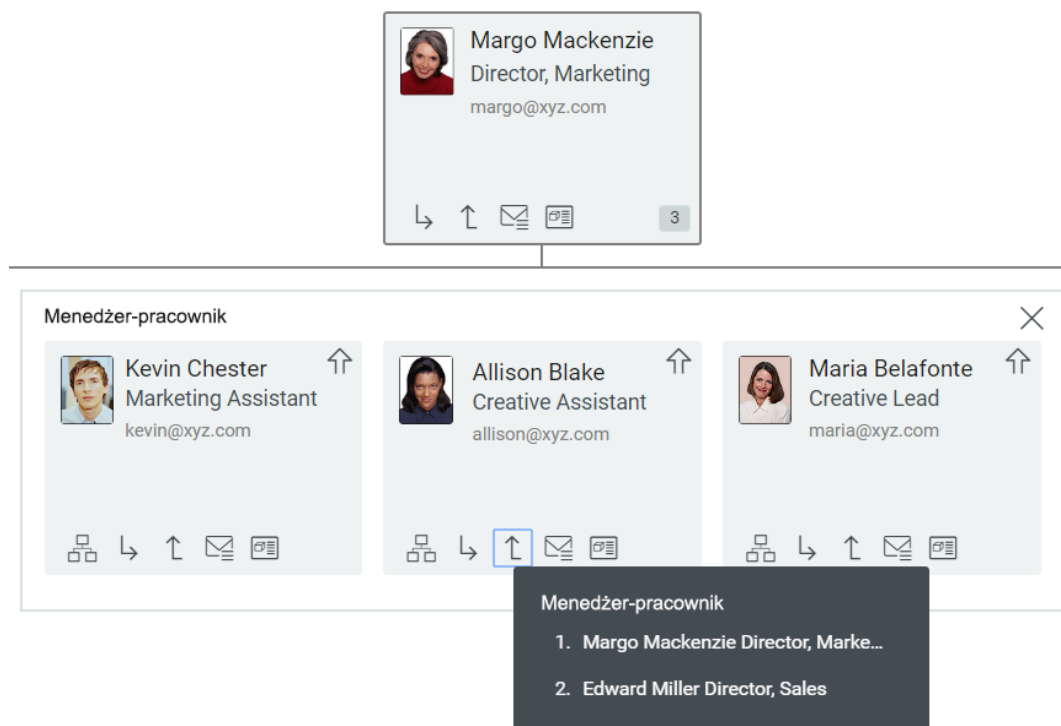
- 1 Zidentyfikuj użytkownika, dla którego chcesz wyświetlić następny poziom, i przejdź do następnego poziomu w hierarchii.

Przypuśćmy, że wyświetlany jest schemat organizacyjny, w którym *Margo Mackenzie* pełni rolę menedżera, a chcemy wyświetlić schemat organizacyjny użytkownika *Allison Blake*.

- 2 Przejdź do karty użytkownika *Allison Blake*, kliknij ikonę ↘ i wybierz z listy rekurencyjną relację Menedżer-pracownik.
- 3 Kliknij ikonę ↗.

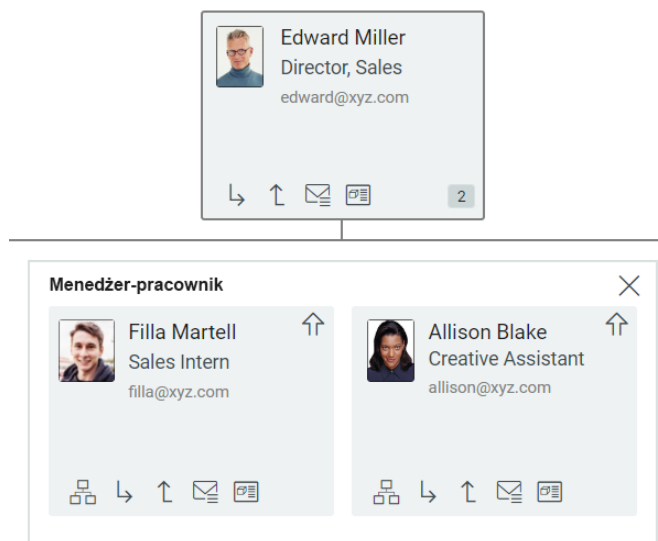
W menu rozwijanym Menedżer-pracownik użytkownika *Allison Blake* wyświetlanych jest dwoje jej bezpośrednich menedżerów: *Margo Mackenzie* oraz *Edward Miller*.

Rysunek 11-6 Rekurencyjna relacja Menedżer-pracownik użytkownika *Allison Blake*



- 4 Wybierz menedżera *Edward Miller*. Zostanie wyświetlony schemat organizacyjny użytkownika *Allison Blake*.

Rysunek 11-7 Schemat organizacyjny użytkownika Allison Blake



Wysyłanie wiadomości e-mail do użytkowników ze schematu organizacyjnego

Opcja  umożliwia wykonywanie następujących czynności:

- Wysyłanie wiadomości e-mail do wybranego użytkownika.
- Udostępnianie łącza do profilu encji w wiadomości e-mail.
- (Opcjonalne, dotyczy jedynie relacji Menedżer-pracownik) Wysyłanie wiadomości e-mail do wszystkich członków zespołu wybranego użytkownika.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

WAŻNE:

- Przed wysłaniem wiadomości e-mail z widoku schematu organizacyjnego należy się upewnić, że w systemie jest skonfigurowany domyślny klient poczty e-mail.
- Aby zapewnić, że opcje **Nowa wiadomość e-mail** i **Zespół ds. poczty elektronicznej** działają, należy skonfigurować atrybut Poczta elektroniczna jako atrybut podstawowy lub dodatkowy na stronie Ustawienia. Więcej informacji znajduje się w sekcji [Ustawienia użytkownika](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Wyświetlanie szczegółowych informacji o użytkowniku

- 1 Zidentyfikuj użytkownika, o którym informacje chcesz wyświetlić.

Przypuśćmy, że wyświetlany jest schemat organizacyjny, w którym *Margo Mackenzie* odgrywa rolę menedżera, a chcemy wyświetlić dodatkowe szczegóły, takie jak role i zasoby przypisane do użytkownika *Kevin Chester*.

- 2 Przejdź do karty użytkownika *Kevin Chester* i kliknij ikonę . Na stronie profilu wyświetlone zostaną szczegółowe informacje, w tym role i zasoby przypisane do tego użytkownika.

Jeśli nie widzisz ikony  na karcie użytkownika, na przykład na karcie użytkownika *Jack Miller*, który jest prezesem organizacji XYZ, oznacza to, że nie masz odpowiednich uprawnień do katalogu użytkowników, dlatego nie możesz wyświetlać jego profilu. Skontaktuj się z administratorem, jeśli musisz mieć niezbędne uprawnienia do wyświetlania profilu.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

12 Zarządzanie hasłami

Aplikacja Identity Manager udostępnia funkcję Self Service Password Reset (SSPR), która ułatwia zarządzanie procesem zmieniania haseł i resetowania zapomnianych haseł. Podczas resetowania hasła SSPR uwierzytelnia użytkownika z użyciem metody uwierzytelniania typu wezwanie-odpowieź.

- ♦ „Korzystanie z samoobsługowego zarządzania hasłem w programie Identity Manager” na stronie 69
- ♦ „Korzystanie ze starszej wersji zarządzania hasłami” na stronie 71

UWAGA: W tym rozdziale omówiono domyślne funkcje zarządzania hasłami. Niektóre informacje mogą się różnić ze względu na pełnioną przez użytkownika rolę, poziom uprawnień i dostosowania wprowadzone na potrzeby organizacji. Więcej informacji można uzyskać od administratora systemu.

Korzystanie z samoobsługowego zarządzania hasłem w programie Identity Manager

SSPR automatycznie integruje się z procesem jednokrotnego logowania na potrzeby aplikacji do zarządzania tożsamością i programu Identity Reporting. Jest to domyślny program do zarządzania hasłami programu Identity Manager. Gdy użytkownik przesyła żądanie zresetowania hasła, SSPR wymaga od użytkownika, aby odpowiedział na pytanie zabezpieczające. Jeśli odpowiedzi są poprawne, SSPR reaguje w jeden z następujących sposobów:

- ♦ Umożliwia użytkownikowi utworzenie nowego hasła.
- ♦ Tworzy nowe hasło i wysyła je do użytkownika.
- ♦ Tworzy nowe hasło, wysyła je do użytkownika i oznacza stare hasło jako wygasłe.

Odpowiedź tę można skonfigurować w edytorze konfiguracji SSPR. Po aktualizacji do nowej wersji programu Identity Manager można skonfigurować w SSPR użycie metody NMAS, która jest tradycyjnie wykorzystywana w programie Identity Manager do zarządzania hasłami. Jednak SSPR nie rozpoznaje istniejących założeń haseł w przypadku zarządzania zapomnianymi hasłami. W SSPR można również skonfigurować użycie jej zastrzeżonego protokołu zamiast NMAS. Jeśli dokonasz tej zmiany, nie możesz powrócić do użycia protokołu NMAS bez zresetowania założeń haseł.

Za pomocą SSPR można wykonywać wszystkie funkcje wymienione w tabeli [Tabela 12-2, „Funkcje stron Zarządzanie hasłami”](#), na stronie 72:

Tabela 12-1 Funkcje stron Zarządzanie hasłami

Ta strona Zarządzanie hasłami	Umożliwia
Odzew dla hasła	Ustawienie lub zmianę poniższych elementów: ♦ Prawidłowe odzewy na określone przez administratora pytania dotyczące odzewu. ♦ Pytania dotyczące odzewu zdefiniowane przez użytkownika oraz odpowiedzi.
Zmień hasło	Zmiana (zresetowanie) hasła według założeń określonych przez administratora systemu.
Stan założeń haseł	Sprawdzenie wymagań dotyczących założeń haseł.

Informacje o odzwie dla hasła

Pytania służące do uwierzytelnienia są używane w celu sprawdzenia tożsamości użytkownika podczas logowania w przypadku zapomnienia hasła. Jeśli administrator systemu skonfigurował założenia dotyczące haseł, które udostępniają tę funkcję, można użyć strony Odzew dla hasła w następujących celach:

- ♦ Określenie poprawnych odzewów na zdefiniowane przez administratora pytania.
- ♦ Określenie własnych pytań i poprawnych odzewów (jeśli umożliwiają to założenia haseł).

Podczas procesu logowania strona logowania automatycznie przekierowuje użytkownika do strony Odzew. Na tej stronie konfiguruje się odpowiedzi na pytania o odzew. Więcej informacji znajduje się w „Jeśli zapomnisz hasła” na stronie 22. Podczas ponownego logowania przy próbie zresetowania hasła SSPR zadaje skonfigurowane pytania i prosi o podanie poprawnej odpowiedzi. SSPR umożliwia zresetowanie hasła, gdy odpowiedź jest zgodna z zapisaną wcześniej.

Zmiana hasła

Swoje hasło można zmienić (pod warunkiem, że umożliwił to administrator systemu).

- 1 Na pulpicie nawigacyjnym kliknij **Aplikacje > Zmień moje hasło**.
- 2 Wpisz swoje bieżące hasło. Zostanie wyświetlona strona Zmień hasło.

- 3 Wpisz nowe hasło w polu tekstowym **Nowe hasło**.

4 Wpisz ponownie nowe hasło w polu tekstowym **Potwierdź hasło**.

5 Kliknij przycisk **Zmień hasło**.

Jeśli nowe hasło narusza dowolną z reguł dotyczących haseł zdefiniowanych w założeniach haseł przez administratora, na stronie Zmień hasło zostanie wyświetlony komunikat o błędzie.

Na tej stronie zazwyczaj znajdują się informacje o zdefiniowanych przez administratora wymaganiach, jakie powinno spełniać hasło. Przejrzyj reguły dotyczące haseł i spróbuj ponownie.

6 Kliknij przycisk **Kontynuuj**. Zostanie wyświetlony stan żądania. W przypadku powodzenia następuje przejście do strony logowania OSP.

Stan założeń haseł

UWAGA: Ta funkcja jest dostępna tylko dla administratorów.

Administrator przypisał użytkownikowi założenia haseł. Określają one poziom zabezpieczeń hasła użytkownika. Użytkownik nie może sprawdzić wymagań założeń haseł, jeśli administrator aplikacji użytkownika nie przyzna mu do tego prawa. Administrator aplikacji użytkownika może sprawdzić stan założeń haseł na stronie głównej programu Identity Manager. Domyślnie łącze to nie istnieje. Aby je dodać, należy dostosować stronę główną. Informacje na temat dostosowywania elementów strony głównej programu Identity Manager zawiera dokument [Rozdział 5, „Zarządzanie aplikacjami”, na stronie 45](#).

Na stronie docelowej kliknij łącze **Stan hasła i zasady**. Zostanie wyświetlona strona **Stan założeń haseł i założenia**. Aby zmienić hasło do programu Identity Manager, przejdź na stronę główną aplikacji i wybierz opcję Zmień moje hasło. Łącze na stronie głównej programu Identity Manager przekierowuje użytkownika do obszaru SSPR Zmień hasło.

Korzystanie ze starszej wersji zarządzania hasłami

W tym rozdziale omówiono korzystanie ze stron Zarządzanie hasłami na karcie **Samobsługa tożsamości** w aplikacji Identity Manager. Tematy obejmują następujące zagadnienia:

- ♦ „Odzew dla hasła” na stronie 72
- ♦ „Zmiana wskazówki do hasła” na stronie 73
- ♦ „Zmień hasło” na stronie 73
- ♦ „Stan założeń haseł” na stronie 74
- ♦ „Stan synchronizacji hasła” na stronie 74

UWAGA: W tym rozdziale omówiono domyślne funkcje stron Zarządzanie hasłami. Niektóre informacje mogą się różnić ze względu na pełnioną przez użytkownika rolę, poziom uprawnień i dostosowania wprowadzone na potrzeby organizacji. Więcej informacji można uzyskać od administratora systemu.

Więcej informacji o uzyskiwaniu dostępu do karty **Samobsługa tożsamości** i korzystaniu z niej zawiera [Rozdział 10, „Zarządzanie profilem”, na stronie 59](#).

Stron Zarządzanie hasłami można używać do wykonywania czynności, które zawiera [Tabela 12-2](#), „Funkcje stron Zarządzanie hasłami”, na stronie 72.

Tabela 12-2 Funkcje stron Zarządzanie hasłami

Ta strona Zarządzanie hasłami	Umożliwia
Odzew dla hasła	Ustawienie lub zmianę poniższych elementów: ♦ Prawidłowe odzewy na określone przez administratora pytania dotyczące odzewu. ♦ Pytania dotyczące odzewu zdefiniowane przez użytkownika oraz odpowiedzi.
Zmiana wskazówki do hasła	Ustawienie lub zmiana wskazówki do hasła.
Zmień hasło	Zmiana (zresetowanie) hasła według założeń określonych przez administratora systemu.
Stan założeń haseł	Sprawdzenie wymagań dotyczących założeń haseł.
Stan synchronizacji hasła	Wyświetlenie stanu synchronizacji haseł aplikacji z magazynem tożsamości. UWAGA: Uruchamianie aplikacji przed zakończeniem synchronizacji może spowodować wystąpienie błędów dotyczących dostępu.

Odzew dla hasła

Pytania służące do uwierzytelnienia są używane w celu sprawdzenia tożsamości użytkownika podczas logowania w przypadku zapomnienia hasła. Jeśli administrator systemu skonfigurował założenia dotyczące haseł, które udostępniają tę funkcję, można użyć strony Odzew dla hasła w następujących celach:

- ♦ Określenie poprawnych odzewów na zdefiniowane przez administratora pytania.
- ♦ Określenie własnych pytań i poprawnych odzewów (jeśli umożliwiają to założenia haseł).

Aby korzystać ze strony Odzew dla hasła:

- 1 Na karcie **Samoobsługa tożsamości** kliknij opcję **Odzew dla hasła** w menu (w sekcji **Zarządzanie hasłami**).
Zostanie otwarta strona Odzew dla hasła.
- 2 Wprowadź odpowiedni odzew w każdym polu tekstowym **Odzew** (wszystkie są wymagane) lub użyj poprzednio zapisanych odzewów. Jeśli została wybrana opcja **Użyj zapisanej odpowiedzi**, odzewy, w tym etykiety, nie są wyświetlane. Ponadto zdefiniowane przez użytkownika pytania o odzew są wyłączone.
Upewnij się, że wprowadzone odzewy są łatwe do zapamiętania.
- 3 Określ lub zmień zdefiniowane przez użytkownika pytania wymagane. Każdego pytania można użyć tylko raz.

4 Kliknij przycisk **Prześlij**.

Po zapisaniu odpowiedzi aplikacja użytkownika wyświetla komunikat informujący, że odpowiedzi zostały zapisane, i ponownie pokazuje ekran odpowiedzi z wybraną opcją „Użyć zapisanej odpowiedzi?”.

Zmiana wskazówki do hasła

Wskazówka do hasła jest używana podczas logowania w celu przypomnienia hasła w razie jego zapomnienia. Wskazówkę do hasła można ustawić lub zmienić na stronie Zmiana wskazówki do hasła.

1 Na karcie **Samoobsługa tożsamości** kliknij opcję **Zmiana wskazówki do hasła** w menu (w sekcji **Zarządzanie hasłami**).

Zostanie wyświetlona strona Zdefiniuj wskazówkę hasła.

2 Wprowadź nowy tekst wskazówki.

Wskazówka nie może zawierać hasła.

3 Kliknij przycisk **Prześlij**.

Zostanie wyświetlony stan żądania.

Zmień hasło

Tej strony można użyć w celu zmiany hasła (jeśli umożliwił to administrator systemu).

1 Na karcie **Samoobsługa tożsamości** kliknij opcję **Zmień hasło** w menu (w sekcji **Zarządzanie hasłami**).

Zostanie wyświetlona strona Zmień hasło. Jeśli administrator systemu określił założenia hasła dla użytkownika, strona Zmień hasło będzie najczęściej zawierać informacje o ustawianiu hasła zgodnego z tymi założeniami. Na przykład:

Jeśli nie mają zastosowania żadne założenia haseł, pojawi się podstawowa strona Zmień hasło, która udostępnia jedynie pola zmiany hasła.

Aplikacja użytkownika obsługuje następujące rodzaje składni hasła:

- ♦ Zasady złożoności Microsoft

Ten rodzaj składni haseł jest używany w celu zapewnienia wstecznej zgodności z usługą Active Directory 2003.

- ♦ Zasady haseł Microsoft Server 2008

To nowy rodzaj składni haseł, który został dodany do eDirectory 8.8.7, aby zapewnić obsługę Active Directory 2008.

Zasada haseł Microsoft Server 2008 obsługuje następujące ustawienia:

- ♦ Użycie zasady haseł Microsoft Server 2008
- ♦ Maksymalna liczba naruszeń zasad złożoności hasła (0–5)

- ♦ Składnia Novell

W składni Novell są obsługiwane następujące nowe ustawienia:

- ♦ Minimalna liczba znaków niealfabetycznych (1–512)
- ♦ Maksymalna liczba znaków niealfabetycznych (1–512)

We wszystkich trzech rodzajach składni haseł aplikacja użytkownika obsługuje następujące funkcje:

- ♦ Liczba znaków innych niż w bieżącym haśle i hasłach z historii (0–6)
- ♦ Liczba haseł w historii uwzględnianych przy wykluczaniu znaków (0–10)

Jeśli administrator włączył składnię zasady Microsoft Server 2008, wypełnij następujące pola na stronie **Zmień hasło**:

- 2 Wpisz bieżące hasło w polu tekstowym **Stare hasło**.
- 3 Wpisz nowe hasło w polu tekstowym **Nowe hasło**.
- 4 Wpisz ponownie nowe hasło w polu tekstowym **Wpisz ponownie hasło**.
- 5 Kliknij przycisk **Prześlij**.

Jeśli nowe hasło narusza dowolną z reguł dotyczących haseł zdefiniowanych przez administratora, na stronie **Zmień hasło** zostanie wyświetlony komunikat o błędzie. Jeśli używana jest zasada Microsoft Windows Server 2008 i hasło ją narusza, w górnej części strony interfejsu użytkownika zostanie wyświetlony ten komunikat:

```
Password AD2008 complexity policy violation.
```

Jeśli nowe hasło narusza założenia, zapoznaj się z regułami haseł zdefiniowanymi przez administratora i spróbuj ponownie.

- 6 Może zostać wyświetlony monit o podanie wskazówki do hasła, jeśli administrator skonfigurował w ten sposób założenia zabezpieczeń. Aby uzyskać więcej informacji na ten temat, zobacz „[Zmiana wskazówki do hasła](#)” na stronie 73.
- 7 Zostanie wyświetlony stan żądania.

Stan założeń haseł

Administrator przypisał użytkownikowi założenia haseł. Określają one poziom zabezpieczeń hasła użytkownika. Aby sprawdzić wymagania dotyczące założeń haseł:

- 1 Na karcie **Samoobsługa tożsamości** kliknij opcję **Stan założeń haseł** w menu (w sekcji **Zarządzanie hasłami**). Zostanie wyświetlona strona **Stan założeń haseł**.

Elementów oznaczonych jako nieprawidłowe nie można zmienić.

Stan synchronizacji hasła

Strona Stan synchronizacji hasła umożliwia rozpoznanie, czy hasło użytkownika zostało zsynchronizowane z innymi aplikacjami. Inne aplikacje należy uruchamiać dopiero po zsynchronizowaniu hasła. Uruchamianie aplikacji przed zakończeniem synchronizacji może spowodować wystąpienie błędów dotyczących dostępu.

- 1 Na karcie **Samoobsługa tożsamości** kliknij opcję **Stan synchronizacji hasła** w menu (w sekcji **Zarządzanie hasłami**). Zostanie wyświetlona strona **Stan synchronizacji hasła**. Ikony w jednolitym kolorze oznaczają aplikacje ze zsynchronizowanymi hasłami. Przyciemnione ikony wskazują aplikacje, w przypadku których hasło nie zostało jeszcze zsynchronizowane.

UWAGA: Pole **Wybierz użytkownika** jest widoczne tylko dla administratora.

IV Zarządzanie użytkownikami, grupami i zespołami

Użytkownik mający przypisaną odpowiednią rolę w aplikacjach do zarządzania tożsamością może tworzyć użytkowników, grupy i zespoły oraz nimi zarządzać. Użytkowników i zespoły można tworzyć na pulpicie nawigacyjnym i w aplikacji użytkownika. Grupy tworzy się i zarządza nimi w aplikacji użytkownika.

Administratorzy systemu mogą tworzyć użytkowników i grupy. Administrator systemu może zapewnić innym osobom (zwykle z administracji lub kierownictwa) dostęp do tej funkcji.

Niektóre funkcje omówione w tej sekcji mogą się różnić w zależności od stanowiska użytkownika, poziomu uprawnień i dostosowań wprowadzonych w organizacji. Aby uzyskać więcej informacji, należy skontaktować się z administratorem systemu.

Zespół jest zbiorem użytkowników, grup lub użytkowników i grup mogących realizować żądania świadczenia usług i zadania zatwierdzenia przypisane do zespołu. Zespoły to nie to samo co grupy, choć zespół może odpowiadać grupie istniejącej w katalogu użytkownika. Grupa ani członek grupy nie mogą realizować funkcji zespołu, chyba że zostaną przypisani do zespołu. Patrz [Rozdział 14](#), „Zarządzanie zespołami”, na stronie 83.

13 Zarządzanie użytkownikami

W tej sekcji opisano sposób tworzenia użytkowników i grup na pulpicie nawigacyjnym i w aplikacji użytkownika. Tematy obejmują następujące zagadnienia:

- „Tworzenie użytkownika” na stronie 77
- „Edytowanie informacji o użytkowniku” na stronie 77
- „Wyświetlanie listy użytkowników” na stronie 78
- „Wyszukiwanie użytkowników” na stronie 79
- „Sortowanie użytkowników” na stronie 81

Tworzenie użytkownika

Na stronie **Utwórz użytkownika** wyświetlane są także atrybuty użytkownika z włączonymi uprawnieniami **Wyszukiwanie** i **Odczyt**. Te właściwości dostępu można skonfigurować w warstwie abstrakcji katalogów (DAL). Więcej informacji znajduje się w sekcji **Właściwości atrybutów** w podręczniku *NetIQ Identity Manager — Przewodnik administratora po projektowaniu Identity Applications*.

Aby utworzyć użytkownika, wybierz na pulpicie nawigacyjnym opcję:

Osoby > Użytkownicy > +

Wartości, które można określić dla użytkownika, są definiowane przez administratora tożsamości. Ponadto podczas tworzenia użytkownika wyświetlany jest **Kontener** użytkownika, ale tej wartości nie można zmienić. Dzięki temu ograniczeniu wszyscy użytkownicy są przechowywani w tym samym kontenerze.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Edytowanie informacji o użytkowniku

Wybierz użytkownika z widoku listy i kliknij ikonę , aby zmodyfikować takie informacje o użytkowniku, jak Tytuł, Adres e-mail, Numer telefonu, Menedżer itd. Dozwolone jest modyfikowanie atrybutów użytkownika, które zostały ustawione przez administratora. Więcej informacji o konfigurowaniu atrybutów użytkownika znajduje się w sekcji **Dostosowywanie widoków** w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*. Użytkowników można usuwać w widoku **Zarządzaj użytkownikami**.

Poniżej przedstawiono przykład edytowania informacji o użytkowniku:

✕



Aliyah Hall

Tytuł

Marketing Director +

Marketing Director ✕

Logowanie wyłączone ☒

Numer telefonu

552538 +

552538 ✕

Adres e-mail

aliyah@example.com +

aliyah@example.com ✕

Pracownicy podlegli

🔍 Wyszukaj użytkowników według imien...

Menedżer

🔍 Wyszukaj użytkowników według imien...

Zapisz

Anuluj

UWAGA: Przełącznik **Logowanie wyłączone** umożliwia wyłączenie konta użytkownika. Ten przełącznik jest widoczny tylko wtedy, gdy administrator doda atrybut **Logowanie wyłączone** w widoku karty i opcji **Atrybuty edytowalne** na stronie **Ustawienia > Dostosowywanie**. Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Wyświetlanie listy użytkowników

Poniżej przedstawiono różne sposoby wyświetlania listy użytkowników w aplikacjach do zarządzania tożsamością:

- ♦ **Widok listy:** Aby wyświetlić użytkowników w postaci listy, kliknij ikonę . Powoduje to wyświetlenie informacji o użytkowniku po prawej stronie. Aby zmodyfikować informacje, takie jak numer telefonu, adres e-mail, menedżer itd., kliknij ikonę . Aby wyświetlić schemat organizacyjny konkretnego użytkownika, kliknij ikonę .

- ♦ **Widok karty:** Aby wyświetlić użytkowników w postaci kart, kliknij ikonę . Powoduje to wyświetlenie podstawowych informacji o użytkownikach na kartach. Administrator może skonfigurować informacje, które są wyświetlane na karcie użytkownika. Więcej informacji znajduje się w sekcji [Dostosowywanie widoków](#) w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*. Kliknij ikonę , aby zmodyfikować informacje, takie jak **Numer telefonu**, **Adres e-mail**, **Menedżer** i inne atrybuty. Aby wyświetlić schemat organizacyjny konkretnego użytkownika, kliknij ikonę .
- ♦ **Widok zarządzania użytkownikami:** Aby wyświetlić użytkowników w postaci tabelarycznej, kliknij ikonę . Powoduje to wyświetlenie użytkowników w widoku tabelarycznym. Ten widok umożliwia sortowanie użytkowników według ich atrybutów, takich jak numer telefonu, adres e-mail, dział i innych. Kolumny wyświetlane w tym widoku można dostosować. Aby uzyskać więcej informacji na temat dostosowywania kolumn, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Ten widok umożliwia także usuwanie użytkowników z systemu. Aby usunąć użytkowników:

1. Zaznacz użytkownika, którego chcesz usunąć.
2. Kliknij ikonę .

Wyszukiwanie użytkowników

Poniżej przedstawiono różne sposoby wyszukiwania użytkowników w aplikacjach do zarządzania tożsamością:

- ♦ **Szybkie wyszukiwanie:** Określa atrybut użytkownika i wyświetla listę użytkowników na podstawie wybranych filtrów. Aby zmodyfikować opcje filtru:
 1. Kliknij ikonę .
 2. Wybierz opcje filtru wyszukiwania użytkowników.

Poniżej przedstawiono przykładowe wybrane atrybuty użytkownika do szybkiego wyszukiwania:

- ☒ Imię
- ☒ Nazwisko
- ☐ Tytuł
- ☐ Dział
- ☐ Region
- ☒ Adres e-mail
- ☒ Numer telefonu

3. Kliknij **Filtruj**.

Aby na przykład wyszukać użytkownika nazywającego się Smith, gdy zostały wybrane filtry Imię i Nazwisko. Szybkie wyszukiwanie wyświetla listę wszystkich użytkowników z ciągiem znaków Smith w polu Imię lub Nazwisko.

- ♦ **Wyszukiwanie zaawansowane:** Ta opcja umożliwia pobranie bardziej precyzyjnej listy użytkowników niż w przypadku szybkiego wyszukiwania. Można wyszukać użytkownika ze zdefiniowanymi atrybutami. Aby użyć wyszukiwania zaawansowanego:

1. Kliknij ikonę 🔍.

2. Podaj dokładne informacje o poszczególnych atrybutach użytkownika.

Poniżej przedstawiono przykład atrybutów użytkownika podanych na potrzeby wyszukiwania zaawansowanego:

WYSZUKIWANIE ZAAWANSOWANE

Wyszukaj według

Imię ▼	Emily	×
Nazwisko ▼	Cameron	×
Adres e-mail ▼	emily.cameron@example.com	×
Numer telefonu ▼	5552368	×
+ Dodaj		

3. Kliknij **Filtruj**.

Można na przykład wyszukać użytkownika, którego **Imię** to Aliyah, **Nazwisko** to Hall, a **Tytuł** to Dyrektor. Można podać te atrybuty w opcji Wyszukiwanie zaawansowane, aby znaleźć użytkownika mającego dokładnie ten zestaw atrybutów.

Można również skonfigurować wyniki wyszukiwania na stronie przez ustawienie indeksu u dołu. Pulpit nawigacyjny korzysta z elementu sterującego Widok listy wirtualnej (VLV), który ma w LDAP identyfikator OID 2.16.840.1.113730.3.4. Działa on w połączeniu z elementem sterującym sortowania.

Podczas wyświetlania wyników na pulpicie programu Identity Manager wyświetlane są dwie różne liczby:

- ♦ **Łączna liczba:** Jest to łączna liczba użytkowników znalezionych w systemie.
- ♦ **Liczba wyszukiwania:** Jest to liczba użytkowników wyświetlanych dla konkretnego wyszukiwania.

Sortowanie użytkowników

W widoku zarządzania użytkownikami można ich sortować według atrybutów. Aby umożliwić sortowanie, administrator musi skonfigurować indeksy złożone dla atrybutów użytkowników. Więcej informacji na temat indeksów złożonych zawiera sekcja [Tworzenie indeksów złożonych](#) w podręczniku *NetIQ Identity Manager — Podręcznik instalowania i aktualizowania dla systemu Windows*.

UWAGA: Jeśli nie można sortować użytkowników przy użyciu żadnych ich atrybutów, należy skontaktować się z administratorem w sprawie skonfigurowania indeksu złożonego dla atrybutu wymaganego do sortowania użytkowników.

14 Zarządzanie zespołami

Zespół składa się z dwóch rodzajów użytkowników:

Żądający

Przygotowuje żądania uprawnień w imieniu innych członków zespołu (odbiorców). Żądający może wykonywać czynności w odniesieniu do własnych żądań przydzielenia, jednej lub kilku kategorii żądań lub wszystkich żądań, w zależności od konfiguracji zespołu.

Zarządza on również przypisaniami pełnomocnictwa do członków zespołu.

Odbiorca

Członek zespołu, którego mogą reprezentować żądający.

Odbiorcy w zespole mogą być użytkownikami lub grupami w katalogu. Mogą oni również wywodzić się z relacji katalogów. Lista członków może wywodzić się na przykład z relacji menedżer-pracownik w organizacji. W takim przypadku odbiorcy w zespole są wszystkimi użytkownikami, którzy podlegają menedżerowi zespołu.

UWAGA: Administrator świadczenia usług w ramach aplikacji może skonfigurować poziom abstrakcji katalogu pod kątem obsługi relacji kaskadowych, tak aby można było uwzględnić w zespole wiele poziomów istniejących w organizacji. Liczba zawartych poziomów jest konfigurowana przez administratora.

Aby wykonać dowolne z poniższych działań, przejdź na stronę **Osoby > Zespoły**:

- ♦ „Wyświetlanie zespołów” na stronie 83
- ♦ „Tworzenie zespołu” na stronie 84
- ♦ „Modyfikowanie zespołu” na stronie 84

Wyświetlanie zespołów

Na stronie **Zespoły** wyświetlają się wszystkie zespoły, które możesz wyświetlać. Możesz być członkiem wszystkich wyświetlonych zespołów. Możesz być też administratorem z uprawnieniami do wyświetlania, modyfikacji lub usuwania określonych zespołów, do których nie należysz.

Jako członek zespołu możesz być **żądającym**, który może wystosowywać żądania w imieniu innych członków zespołu. Inni członkowie zespołu mogą być również uprawnieni do wykonywania tych czynności w twoim imieniu, a wówczas będziesz **odbiorcą**. Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Tworzenie zespołu

Jako administrator możesz tworzyć zespoły. **Zespół** jest zbiorem użytkowników, grup lub użytkowników i grup mogących realizować żądania świadczenia usług i zadania zatwierdzenia przypisane do zespołu.

Do każdego zespołu przypisujesz członków zespołu (**Odbiorcy**), którzy będą dysponować uprawnieniami zespołu i którzy mogą podejmować działania w imieniu odbiorcy (**Żądający**). Po utworzeniu zespołu możesz wskazać **Uprawnienia** (zasoby i definicje żądań zaopatrywania), które znajdują zastosowanie do członków zespołu. Możesz na przykład dodać zasób w postaci komputera przenośnego, który może być potrzebny członkom zespołu.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

Modyfikowanie zespołu

Jako administrator możesz zmieniać lub usuwać zespoły. Możesz zmieniać następujące aspekty zespołu:

- ♦ Zmieniać nazwę i opis zespołu.
- ♦ Modyfikować żądających zespołu.
- ♦ Dodawać lub usuwać członków zespołu.
- ♦ Dodawać lub usuwać uprawnienia menedżera zespołu.

Aby uzyskać więcej informacji, należy kliknąć ikonę  na pulpicie nawigacyjnym.

15 Zarządzanie grupami

Grupa składa się z użytkowników i innych kont o takiej samej charakterystyce. Na przykład grupa **Finanse** obejmuje wszystkich pracowników działu finansów.

Grupy można wyszukiwać na podstawie opisu. Jednak administratorzy z dostępem do strony **Ustawienia** mogą dostosować atrybuty, według których można wyszukiwać encję grupy. Oznacza to, że podczas wyszukiwania konkretnej grupy w celu przypisania do niej roli, ustawienia grupy jako właściciela zasobu lub wykonania prostego wyszukiwania na stronie **Grupy** aplikacja zwraca nazwy grup zgodnych z wyszukiwanym atrybutem. Więcej informacji znajduje się w sekcji **Ustawienia encji** w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Tworzenie grupy

Grupę może utworzyć użytkownik o przypisanej roli administracyjnej w aplikacjach do zarządzania tożsamością.

- 1 Na pulpicie programu Identity Manager przejdź do opcji **Osoby > Grupy**.
- 2 Kliknij ikonę **+**.
- 3 Określ wartości następujących wymaganych atrybutów:

Atrybut	Co określić
Nazwa	Nazwa nowej grupy. WAŻNE: W polu Nazwa nie należy używać następujących znaków specjalnych: < ; \ " + # / * ~
Opis	Opis nowej grupy. Opis jest używany jako kryteria wyszukiwania grup na pulpicie nawigacyjnym. WAŻNE: W polu Opis nie należy używać następujących znaków specjalnych: ~
Kontener	Jednostka organizacyjna w magazynie tożsamości, w której ma zostać zapisana nowa grupa (grupy nazwane w zależności od jednostki). Na przykład: <code>ou=groups,ou=MyUnit,o=MyOrg</code> Aby uzyskać więcej informacji o używaniu przycisków w celu określenia kontenera, patrz „ Tworzenie użytkownika ” na stronie 77. UWAGA: Jeśli administrator systemu określił domyślny kontener dla nowo utworzonych obiektów tego typu, nie zostanie wyświetlony monit dotyczący kontenera .

- 4 Kliknij przycisk **Create**.

Po pomyślnym utworzeniu grupy zostaje wyświetlony panel **Członkowie grupy** umożliwiający dodawanie użytkowników do nowo utworzonej grupy.

- 5 Aby dodać użytkowników do grupy, kliknij ikonę **+** znajdującą się obok członków grupy.
- 6 Wybierz wymaganych użytkowników w oknie modalnym.
- 7 Kliknij przycisk **Dodaj**.

V Załącznik

Poniższy załącznik zawiera dodatkowe informacje i tematy zaawansowane dotyczące aplikacji użytkownika Identity Manager.

A Korzystanie z programu Identity Manager Approvals

Oprócz używanego przez klientów interfejsu użytkownika programu Identity Manager można teraz używać nowego programu dla systemu iOS, który umożliwia użytkownikom programu Identity Manager zdalne zatwierdzanie i odrzucanie żądań za pomocą modułu zaopatrywania opartego na rolach Identity Manager.

Gdy zainstalujesz i skonfigurujesz aplikację Approvals, będą w niej wyświetlane te same zadania zatwierdzania, które są normalnie widoczne w interfejsie aplikacji użytkownika. Wszystkie zmiany są synchronizowane między aplikacją Approvals i aplikacją użytkownika.

Można również pracować w trybie offline przy braku połączenia z serwerem modułu zaopatrywania opartego na rolach programu Identity Manager. Aplikacja Approvals automatycznie synchronizuje zmiany po przywróceniu połączenia.

W tym dodatku przedstawiono informacje na temat instalowania i używania nowej aplikacji Approvals. Informacje na temat konfigurowania przez administratorów programu Identity Manager środowiska w sposób umożliwiający użytkownikom korzystanie z tej aplikacji można znaleźć w sekcji „[Konfigurowanie aplikacji Identity Manager Approvals](#)” w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Bardziej szczegółowe informacje na temat aplikacji Zatwierdzenia można znaleźć w następujących sekcjach:

- ♦ „Wymagania dotyczące produktu” na stronie 89
- ♦ „Instalowanie aplikacji Approvals” na stronie 90
- ♦ „Konfigurowanie aplikacji Approvals” na stronie 90
- ♦ „Przegląd aplikacji Approvals” na stronie 94
- ♦ „Zmiana języka wyświetlania aplikacji Approvals” na stronie 97

Wymagania dotyczące produktu

Aplikacja Approvals wymaga urządzenia Apple iPhone lub iPad z zainstalowanym systemem Apple iOS 6 bądź iOS 7 lub dowolnego urządzenia z systemem Android 5.0 lub nowszym.

UWAGA: Jeśli administrator nie umożliwił korzystania z aplikacji Approvals, jej skonfigurowanie po instalacji może być niemożliwe. Informacje na temat konfigurowania przez administratorów środowiska programu Identity Manager w sposób umożliwiający użytkownikom korzystanie z aplikacji Approvals można znaleźć w sekcji „[Konfigurowanie aplikacji Identity Manager Approvals](#)” w podręczniku *NetIQ Identity Manager — Podręcznik administratora aplikacji do zarządzania tożsamością*.

Instalowanie aplikacji Approvals

Aplikację NetIQ Identity Manager Approvals można zainstalować ze [strony aplikacji Approvals](#) w sklepie Apple App Store na urządzeniu.

Po zainstalowaniu aplikacji Approvals należy ją skonfigurować, aby umożliwić nawiązywanie połączenia z serwerem modułu zaopatrywania opartego na rolach.

UWAGA: Jeśli hasło aplikacji użytkownika utraciło ważność, zalecamy zmianę hasła przed zainstalowaniem i skonfigurowaniem aplikacji Approvals. Jeśli założenia haseł w środowisku pozwalają na ograniczoną liczbę dodatkowych logowań po wygaśnięciu hasła, aplikacja Approvals może wykorzystać wszystkie te logowania, próbując zsynchronizować zadania programu Identity Manager z urządzeniem.

Konfigurowanie aplikacji Approvals

Aplikację NetIQ Identity Manager Approvals można skonfigurować na kilka sposobów w zależności od potrzeb danego środowiska i sposobu, w jaki administrator skonfigurował program Identity Manager:

- ♦ Prześlij w interfejsie aplikacji użytkownika żądanie dostępu do aplikacji Approvals, a następnie uruchom tę aplikację na swoim urządzeniu, korzystając z łącza w wiadomości e-mail udostępnionego przez administratora programu Identity Manager. Łącze zawiera wszystkie wymagane informacje o konfiguracji.
- ♦ Kliknij łącze do konfiguracji lub zeskanuj kod QR przy użyciu urządzenia. Łącze i kod QR udostępniają wszystkie wymagane informacje o konfiguracji lub uogólnione informacje o konfiguracji dla firmy.
- ♦ Wprowadź ręcznie w aplikacji informacje o konfiguracji dla danego środowiska.

WAŻNE: Aby użytkownicy mogli automatycznie skonfigurować aplikację Approvals za pomocą łącza lub kodu QR, administrator środowiska programu Identity Manager musi najpierw włączyć łącze lub kod QR.

Zgłaszanie żądania dostępu mobilnego za pośrednictwem aplikacji użytkownika

Jeśli administrator skonfigurował taką możliwość, można zgłaszać żądania dostępu do aplikacji Approvals przy użyciu aplikacji użytkownika. Program Identity Manager wysyła następnie wiadomość e-mail zawierającą dostosowane łącze, które można otworzyć na urządzeniu, aby automatycznie skonfigurować aplikację, korzystając z odpowiednich informacji.

Aby zgłosić żądanie dostępu mobilnego za pośrednictwem aplikacji użytkownika:

- 1 W przeglądarce internetowej zaloguj się do aplikacji użytkownika Identity Manager przy użyciu protokołu HTTPS (<https://>).

UWAGA: Aby zażądać dostępu do aplikacji Approvals, należy zalogować się do aplikacji użytkownika z użyciem protokołu HTTPS.

- 2 Kliknij opcję **Wykonaj żądanie przetwarzania**.
 - 3 Kliknij menu rozwijane Kategoria żądania przetwarzania i wybierz **Konta**.
 - 4 Kliknij przycisk **Kontynuuj**.
 - 5 Kliknij opcję **Zażądaj aplikacji mobilnej Approval**.
-

UWAGA: Kategoria żądań przetwarzania i nazwa mogą się różnić w zależności od sposobu, w jaki administrator skonfigurował przetwarzanie żądania aplikacji Approvals.

- 6 Podaj wymagane informacje w formularzu żądania przetwarzania i kliknij przycisk **Prześlij**.
 - 7 Po otrzymaniu wiadomości e-mail od administratora aplikacji Identity Manager otwórz wiadomość e-mail na urządzeniu i kliknij udostępnione łącze, aby połączyć urządzenie z serwerem modułu zaopatrywania opartego na rolach.
-

UWAGA: Jeśli aplikacja została zainstalowana wcześniej, może się wyświetlić komunikat ostrzegawczy, że istniejące ustawienia zostaną zastąpione. Upewnij się, że nazwa hosta wyświetlana w komunikacie ostrzegawczym jest taka sama jak nazwa hosta, do którego użytkownik miał dostęp, żądając dostępu do aplikacji. W razie wątpliwości nie należy klikać łącza, tylko skontaktować się z administratorem.

Jeśli nazwa hosta jest poprawna, kliknij przycisk **Akceptuj**, aby zastąpić istniejące ustawienia.

- 8 Podczas uruchamiania aplikacji wprowadź hasło i kliknij ikonę Testuj połączenie , aby zweryfikować ustawienia.

Korzystanie z łącza do konfiguracji lub kodu QR

Administrator programu Identity Manager może udostępnić łącze do konfiguracji umożliwiające skonfigurowanie aplikacji Approvals. Otwórz łącze w przeglądarce na urządzeniu, aby automatycznie skonfigurować aplikację.

Łącze to udostępnia jednak jedynie niektóre wymagane ustawienia. Zazwyczaj łącze lub kod może udostępnić jedynie szczegółowe informacje o serwerze modułu zaopatrywania opartego na rolach niezbędne do działania aplikacji Approvals. Po kliknięciu łącza należy ręcznie skonfigurować ustawienia **Nazwa użytkownika i Hasło**, a także wszystkie inne ustawienia, które nie zostały skonfigurowane automatycznie.

W niektórych środowiskach może nie być możliwe uzyskanie dostępu do poczty elektronicznej z urządzenia. Jeśli nie możesz odbierać wiadomości e-mail na swoim urządzeniu, możesz użyć urządzenia do zeskanowania spersonalizowanego kodu QR, udostępnionego przez administratora programu Identity Manager.

Wyświetl podany kod QR na komputerze lub na wydrukowanej kartce, jeśli to konieczne, i zeskanuj przy użyciu czytnika kodów QR na urządzeniu. Gdy kod QR automatycznie skonfiguruje aplikację Approvals dla środowiska, należy ręcznie skonfigurować ustawienia **Nazwa użytkownika i Hasło**.

Ręczne konfigurowanie aplikacji Approvals

Jeśli administrator środowiska programu Identity Manager nie udostępnił łącza ani kodu QR umożliwiających skonfigurowanie aplikacji Approvals, można skonfigurować wymagane ustawienia ręcznie.

OSTRZEŻENIE: Ponieważ ręczne konfigurowanie aplikacji na urządzeniu wymaga dogłębnej znajomości komponentów programu Identity Manager, zaleca się, aby tylko zaawansowani użytkownicy dysponujący wiedzą na temat modułu zaopatrywania opartego na rolach i środowiska aplikacji użytkownika w firmie konfigurowali ustawienia aplikacji ręcznie. Inni użytkownicy powinni skontaktować się z administratorem programu Identity Manager, aby uzyskać informacje na temat konfigurowania aplikacji.

Kliknij w aplikacji ikonę Ustawienia , podaj wymagane ustawienia, a następnie kliknij ikonę Testuj połączenie , aby je zweryfikować.

Aplikacja Approvals wymaga następujących ustawień:

Nazwa ustawienia logowania	Opis ustawienia logowania
Nazwa użytkownika	Określa nazwę użytkownika używaną do uzyskania dostępu do serwera modułu zaopatrywania opartego na rolach.
Hasło	Określa hasło używane do uzyskania dostępu do serwera modułu zaopatrywania opartego na rolach.
Synchronizacja danych	Wskazuje, czy użytkownik chce, aby aplikacja aktywnie synchronizowała dane z serwerem modułu zaopatrywania opartego na rolach.
Zaawansowane > Szczegóły serwera > Serwer	Określa pełną nazwę domeny lub adres IP serwera modułu zaopatrywania opartego na rolach.
Zaawansowane > Szczegóły serwera > Bezpieczny port	Określa port HTTPS używany przez aplikację do nawiązywania połączenia z serwerem.
Zaawansowane > Szczegóły serwera > Kontekst	Określa kontekst używany podczas instalowania pliku WAR aplikacji użytkownika. Wartość domyślna to <code>IDMProv</code> .
Zaawansowane > Szczegóły serwera > Kontener użytkownika	Określa pełną nazwę wyróżniającą kontenera magazynu tożsamości, w którym przechowywane są informacje o użytkownikach.
Zaawansowane > Szczegóły serwera > Limit czasu	Określa liczbę sekund oczekiwania aplikacji podczas próby nawiązania połączenia z serwerem przed anulowaniem połączenia. Wartość domyślna to 5 sekund.
Zaawansowane > Ustawienia definicji danych > Encja użytkownika	Określa encję LDAP reprezentującą użytkownika w magazynie tożsamości. Wartość domyślna to <code>user</code> .

Nazwa ustawienia logowania	Opis ustawienia logowania
Zaawansowane > Ustawienia definicji danych > Format nazw	Określa reprezentację atrybutu DAL używaną w aplikacji do formatowania pełnej nazwy użytkownika. Wartość domyślna to <code>FirstName LastName</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut imienia	Określa nazwę atrybutu DAL reprezentującego imię użytkownika. Wartość domyślna to <code>FirstName</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut nazwiska	Określa nazwę atrybutu DAL reprezentującego nazwisko użytkownika. Wartość domyślna to <code>LastName</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut zdjęcia użytkownika	Określa nazwę atrybutu DAL zawierającego zdjęcie użytkownika. Wartość domyślna to <code>UserPhoto</code> . UWAGA: Jeśli w programie Identity Manager nie skonfigurowano zdjęć lub skonfigurowano w niej niewyświetlanie zdjęć, aplikacja wyświetla zamiast niego ogólny obraz.
Zaawansowane > Ustawienia definicji danych > Atrybut telefonu do pracy	Określa nazwę atrybutu DAL reprezentującego numer służbowego telefonu użytkownika. Wartość domyślna to <code>TelephoneNumber</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut telefonu komórkowego	Określa nazwę atrybutu DAL reprezentującego numer telefonu komórkowego użytkownika. Wartość domyślna to <code>mobile</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut adresu e-mail	Określa nazwę atrybutu DAL reprezentującego adres e-mail użytkownika. Wartość domyślna to <code>Email</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut LDAP zdjęcia	Określa nazwę atrybutu LDAP zawierającego zdjęcie użytkownika. Wartość domyślna to <code>photo</code> .
Zaawansowane > Ustawienia definicji danych > Atrybut nazwy	Określa atrybut DAL nazwy używany w magazynie tożsamości do opisu nazwy. Wartość domyślna to <code>cn</code> .
Zaawansowane > Ustawienia definicji danych > Administrator zaopatrywania	Wskazuje, czy użytkownik jest administratorem zaopatrywania na serwerze modułu zaopatrywania opartego na rolach.

Nazwa ustawienia logowania	Opis ustawienia logowania
Zaawansowane > Zaakceptowane certyfikaty	Określa dowolne nieważne lub samopodpisane certyfikaty z serwera modułu zaopatrywania opartego na rolach, które może akceptować aplikacja Approvals. Gdy aplikacja Approvals wykryje samopodpisany lub nieważny certyfikat, wyświetli monit o jego zaakceptowanie lub odrzucenie. Jeśli certyfikat zostanie zaakceptowany, aplikacja doda go do listy zaakceptowanych certyfikatów. Możesz usunąć certyfikat z listy zaakceptowanych certyfikatów, klikając jego nazwę i restartując aplikację. UWAGA: Jeśli certyfikat serwera modułu zaopatrywania opartego na rolach jest ważny, aplikacja nie dodaje go do listy zaakceptowanych certyfikatów. Aplikacja domyślnie akceptuje ważne certyfikaty.
Zaawansowane > Odrzucone certyfikaty	Określa dowolne nieważne lub samopodpisane certyfikaty z serwera modułu zaopatrywania opartego na rolach, których nie powinna akceptować aplikacja Approvals. Gdy aplikacja Approvals wykryje samopodpisany lub nieważny certyfikat, wyświetli monit o jego zaakceptowanie lub odrzucenie. Jeśli certyfikat zostanie odrzucony, aplikacja doda go do listy odrzuconych certyfikatów. Jeśli serwer przedstawi później odrzucony certyfikat, aplikacja nie będzie mogła utworzyć połączenia z tym serwerem. Możesz usunąć certyfikat z listy odrzuconych certyfikatów, klikając jego nazwę.

Przegląd aplikacji Approvals

Ta sekcja zawiera przegląd interfejsu użytkownika aplikacji NetIQ Identity Manager Approvals. Tematy obejmują następujące zagadnienia:

- ♦ „Widok Zadania” na stronie 95
- ♦ „Widok szczegółowy” na stronie 95
- ♦ „Tryb zbiorczy” na stronie 95
- ♦ „Widok Zakończone zadania” na stronie 96
- ♦ „Widok Ustawienia logowania” na stronie 96
- ♦ „Widok Ustawienia zaawansowane” na stronie 96

Widok Zadania

Domyślnym widokiem aplikacji Approvals jest widok Zadania. W tym widoku wyświetlane są wszystkie zadania aktualnie przypisane do użytkownika lub przez niego przyjęte wraz z tytułem zadania oraz imieniem, nazwiskiem i zdjęciem odbiorcy zadania. Lista zadań w widoku jest uporządkowana według daty wygaśnięcia, przy czym na samej górze wyświetlane są zadania, które mają zostać wykonane najwcześniej, a zadania bez daty wygaśnięcia znajdują się na dole.

UWAGA

- Jeśli w programie Identity Manager nie skonfigurowano zdjęcia lub skonfigurowano niewyświetlanie zdjęć, wyświetlany jest ogólny obraz.
- Za pomocą aplikacji Approvals nie można zatwierdzać ani odrzucać zadań, w których używane są złożone formularze.
- Obecnie aplikacja Approvals nie obsługuje nowych formularzy w formacie JSON na platformach iOS i Android. W rezultacie może pojawić się komunikat o błędzie lub wyświetlenie szczegółów zadania może być niemożliwe.

Aby zatwierdzić lub odrzucić żądanie albo wyświetlić szczegóły konkretnego zadania, kliknij to zadanie lub nazwę / nazwisko odbiorcy zadania. Jeśli chcesz skontaktować się z odbiorcą zadania, kliknij jego zdjęcie.

Widok szczegółowy

Widok Szczegóły zawiera szczegóły konkretnego zadania przypisanego do użytkownika. W zależności od zadania wyświetlane pola mogą być różne.

Aby zatwierdzić lub odrzucić zadanie, podaj niezbędne informacje i kliknij **Zatwierdź** albo **Odmowa**.

Tryb zbiorczy

Jeśli potrzebujesz zatwierdzić lub odrzucić dużą liczbę podobnych zadań, możesz przełączyć się w widoku Zadania z domyślnego trybu pojedynczego zadania w tryb zbiorczy.

UWAGA: W trybie zbiorczym nie można zatwierdzić wszystkich zadań. W przypadku bardziej złożonych zadań, takich jak zadania atestacji, należy zatwierdzić każde zadanie atestacji osobno w trybie pojedynczego zadania. Po kliknięciu ikony Tryb zbiorczy na liście w aplikacji wyświetlane są tylko te zadania, które można zatwierdzić w trybie zbiorczym.

Aby zatwierdzić lub odrzucić wiele zadań:

- 1 W widoku Zadania kliknij ikonę Tryb zbiorczy .
- 2 Wybierz zadania, które chcesz zatwierdzić lub odrzucić. Nie można w tym samym czasie jednych zadań zatwierdzić, a inne odrzucić.
- 3 (Opcjonalnie) Aby zatwierdzić lub odrzucić wszystkie zadania, kliknij **Wszystko**.
- 4 (Opcjonalnie) Jeśli zmienisz zdanie i zrezygnujesz z zatwierdzenia lub odrzucenia niektórych zadań, kliknij ikonę trybu pojedynczego zadania .

- 5 Kliknij **Zatwierdź** lub **Odmowa**.
- 6 (Opcjonalnie) Dodaj komentarz dotyczący operacji zbiorczej.
- 7 Kliknij **Potwierdź**.

Widok Zakończone zadania

Aby wyświetlić zakończone zadania, kliknij ikonę Zakończone zadania . Widok zawiera zakończone zadania, a także czas zatwierdzenia lub odrzucenia zadania. Kliknięcie zakończonego zadania powoduje wyświetlenie jego szczegółów. W przypadku bardziej złożonych żądań można kliknąć **Wartości z formularza**, aby wyświetlić konkretne informacje dotyczące żądania.

W razie potrzeby można w widoku Zakończone zadania usunąć jedno lub większą liczbę

zakończonych zadań. Aby usunąć zadania, kliknij ikonę Tryb zbiorczy , wybierz zadania, które chcesz usunąć, i kliknij **Usuń**.

UWAGA: W widoku Zakończone zadania wyświetlane są tylko zadania zakończone na urządzeniu użytkownika. Nie można wyświetlać zadań zakończonych w aplikacji użytkownika ani na innym urządzeniu z zainstalowaną aplikacją Approvals.

Widok Ustawienia logowania

Widok Ustawienia logowania umożliwia wyświetlanie i modyfikowanie ustawień logowania.

OSTRZEŻENIE: Jeśli administrator programu Identity Manager udostępnił łącze lub kod QR do automatycznego konfigurowania ustawień aplikacji, zalecamy, aby nie modyfikować tych ustawień domyślnych, chyba że administrator poprosi, aby to zrobić.

Widok Ustawienia zaawansowane

Widok Ustawienia zaawansowane umożliwia wyświetlanie i modyfikowanie ustawień zaawansowanych, które określają sposób odbierania danych z serwera modułu zaopatrywania opartego na rolach.

OSTRZEŻENIE: Jeśli administrator programu Identity Manager udostępnił łącze lub kod QR do automatycznego konfigurowania ustawień aplikacji, zalecamy, aby nie modyfikować tych ustawień domyślnych, chyba że administrator poprosi, aby to zrobić.

W razie przypadkowej zmiany ustawień definicji danych w widoku Ustawienia zaawansowane należy kliknąć przycisk **Przywróć wartości domyślne**, aby przywrócić domyślne ustawienia programu Identity Manager. Opcja **Przywróć wartości domyślne** nie powoduje zmiany nazwy użytkownika, jego hasła ani żadnych ustawień szczegółów serwera.

Zmiana języka wyświetlania aplikacji Approvals

W aplikacji Approvals wyświetlane są ciągi tekstowe przetłumaczone na wiele języków. Aby zmienić język używany w aplikacji Approvals, zmień ustawienia Język i Format regionu na urządzeniu z systemem iOS. Ustawienia Format regionu określają sposób wyświetlania dat, godzin i numerów telefonu na urządzeniu.

Aby zmodyfikować ustawienia języka i regionu:

- 1 Na urządzeniu z systemem iOS kliknij **Ustawienia**.
- 2 Kliknij opcję **Ogólne**.
- 3 Kliknij opcję **Międzynarodowy**.
- 4 (Opcjonalnie) Aby zmienić język urządzenia, kliknij opcję **Język**, wybierz język, który ma być używany, a następnie kliknij opcję **Gotowe**.
- 5 (Opcjonalnie) Aby zmienić format regionu używany na urządzeniu w przypadku dat i godzin, kliknij opcję **Format regionu**, wybierz format, który ma być używany, a następnie kliknij opcję **Międzynarodowy**.
- 6 Wróć na ekran główny urządzenia.