



NetIQ® Identity Manager

Brugervejledning til Identity Applications

Maj 2024

Juridisk meddelelse

Copyright 2009-2024 Open Text.

De eneste garantier for produkter og tjenester, der gives af Open Text og Open Texts associerede selskaber og licensgivere ("Open Text"), er angivet i de garantier, der udleveres sammen med disse produkter og tjenester. Intet i nærværende dokument er udarbejdet med henblik på at udgøre en yderligere garanti. Open Text er ikke ansvarlig for tekniske eller redaktionelle fejl eller udeladelser heri. Oplysningerne i nærværende dokument kan ændres uden varsel.

Du kan finde flere oplysninger, f.eks. certificeringsrelaterede bemærkninger og varemærker, i <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).

Indhold

Om denne bog og biblioteket	7
Del I Velkommen til Identity Manager	9
1 Introduktion	11
Om roller og ressourcer	11
Om Identity Applications	11
Om Identity Manager Dashboard	11
Udforskning af dashboardet	12
Om siden Programmer	13
Om opgaver	14
Mest almindelige måder at bruge Identity Applications på	14
Sådan fungerer selvbetjening af id.	14
Sådan fungerer roller og ressourcer	14
Sådan fungerer procesanmodninger	16
Sådan fungerer helpdesk	16
2 Adgang til Identity Applications	19
Overvejelser i forbindelse med adgang til Identity Applications	19
Sådan logger du på første gang	20
Reaktion på kontrol af foretrukket landestandard	21
Fejlfinding af logonproblemer	21
Hvis du glemmer din adgangskode	21
Hvis du har problemer med at logge på	21
Hvis du bliver bedt om yderligere oplysninger	22
Sådan logger du af	22
Del II Tilpasning af dit dashboard	23
3 Administration af widgets og layout	25
Administration af det globale dashboard	26
Skift dashboardets layout	26
Tilføj en widget	27
Tilføj generelle widgets	28
Tilføj Identity Manager-widgets	29
Tilføj Identity Governance-widgets	30
Widget-indstillinger	30
Konfigurer en widget	31

Del III Administration af dine tilladelser og din identitetsprofil	33
4 Administration af anmodninger om tilladelser	35
Visning af dine tilladelser	35
Anmodning om tilladelser	37
Visning af anmodninger	37
Sporing af en anmodning	38
Annullering af en anmodning	38
Oprettelse af en helpdeskanmodning	39
Tilbagekaldelse af tilladelser	39
"Deep linking" til en anmodning	40
5 Administration af programmer	43
Oprettelse af foretrukne elementer	43
Tilføjelse af et program	43
Tilføjelse af en tilladelse	44
Tilføj, redigere eller slette en kategori	44
Tilføj en kategori	44
Redigere en kategori	44
Slette en kategori	45
6 Administration af dine opgaver	47
Visning af dine opgaver	47
Administration anmodninger om godkendelse eller afvisning	48
Administration af helpdeskopgaver	49
7 Sådan handler du på vegne af en anden	51
Visning af fuldmægtigtildelinger	51
Funktion som fuldmægtig	51
Administration af fuldmægtigtildelinger	51
8 Administration af uddelegeringer	53
9 Administration af din tilgængelighed	55
10 Administration af din profil	57
Opdatering af din profil	57
11 Administration af organisationsdiagrammet	59
Visning af et organisationsdiagram	59
Om organisationsdiagrammet	60
Arbejde med organisationsdiagrammet	61
Nulstille roden i visningen med organisationsdiagrammet	62
Skifte visningen med organisationsdiagrammet	62
Vælge en relation, du vil have vist	63
Navigere til næste niveau i relationshierarkiet	64

Sende e-mail til brugere fra organisationsdiagrammet	65
Få vist detaljerede oplysninger om en bruger	65
12 Administration af din adgangskode	67
Brug af selvbetjent styring af adgangskoder i Identity Manager.	67
Om challenge/response for adgangskode	68
Ændring af adgangskoden.	68
Status for adgangskodepolitik.	69
Brug af styring af gamle adgangskoder	69
Verificeringssvar til adgangskode	70
Ændring af adgangskodetip.	71
Skift adgangskode	71
Status for adgangskodepolitik.	72
Status for adgangskodesynkronisering.	72
Del IV Administration af brugere, grupper og teams	73
13 Administration af brugere	75
Oprettelse af en bruger	75
Redigering af brugeroplysninger	75
Visning af brugere	76
Søgning efter brugere	77
Sortering af brugere	78
14 Administration af teams	79
Få vist teams	79
Opret et team	80
Rediger et team	80
15 Håndtering af grupper	81
Oprettelse af en gruppe	81
Del V Appendiks	83
A Brug af godkendelsesapplikationen til Identity Manager	85
Produktkrav	85
Installere godkendelsesapplikationen	86
Konfigurere godkendelsesapplikationen	86
Anmode om mobiladgang via brugerprogrammet	86
Brug af et konfigurationslink eller en QR-kode	87
Konfigurere godkendelsesapplikationen manuelt	87
Oversigt over godkendelsesapplikationen	90
Opgavevisning	90
Detaljevisning	91
Massetilstand	91
Visning af afsluttede opgaver	91
Visningen Logonindstillinger	92

Visningen Avancerede indstillinger	92
Ændre visningsproget for godkendelsesapplikationen.	92

Om denne bog og biblioteket

I denne vejledning beskrives, hvordan slutbrugere og nogle administratorer kan bruge Identity Applications til NetIQ Identity Manager, med hovedvægt på dashboardet og brugerprogrammet.

Tiltænkt målgruppe

Denne bog indeholder oplysninger til de personer, der er ansvarlige for at forstå administrationskoncepter samt implementere en sikker, distribueret administrationsmodel.

Andre oplysninger i biblioteket

Du kan finde flere oplysninger om biblioteket til Identity Manager ved at gå til [webstedet med dokumentation til Identity Manager \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

Velkommen til Identity Manager

NetIQ Identity Manager er et systemsoftwareprodukt, som din organisation bruger til at administrere brugergruppens adgangsbehov på en sikker måde. Hvis du er medlem af denne brugergruppe, drager du fordel af Identity Manager på en række forskellige måder. Med Identity Manager kan organisationen f.eks.:

- ♦ Give brugere adgang til oplysninger (f.eks. gruppeorganisationsdiagrammer, afdelingers hvide sider eller opslag af medarbejdere) samt roller og ressourcer (f.eks. udstyr eller konti på interne systemer), som de har brug for, lige fra dag ét
- ♦ Synkronisere flere adgangskoder til et enkelt logon til alle systemer
- ♦ Ændre eller tilbagekalde adgangsrettigheder øjeblikkeligt, når det er nødvendigt (f.eks. når en person overføres til en anden gruppe eller forlader organisationen)
- ♦ Sikre overholdelse af offentlige regulativer

Læs først denne del for at få oplysninger om Identity Manager Identity Applications og om, hvordan du kommer i gang med at bruge dem. Denne vejledning er udviklet som en hjælp til følgende typer af onlineaktiviteter i din organisation:

- ♦ Administration af din onlineidentitet, der er knyttet til organisationsressourcer.
- ♦ Visning eller ændring af din adgang til organisationsroller og -ressourcer.
- ♦ Godkendelse af anmodninger om adgang til ressourcer og roller.
- ♦ Administration af tilladelser, der er knyttet til softwareprogrammer og andre ressourcer, som din organisation leverer til medlemmer af din organisation.

1 Introduktion

I dette afsnit beskrives det, hvordan du kommer i gang med at bruge Identity Applications. Emnerne omfatter:

- ♦ “Om roller og ressourcer” på side 11
- ♦ “Om Identity Applications” på side 11
- ♦ “Om Identity Manager Dashboard” på side 11
- ♦ “Udforskning af dashboardet” på side 12
- ♦ “Om opgaver” på side 14
- ♦ “Mest almindelige måder at bruge Identity Applications på” på side 14

Om roller og ressourcer

I Identity Applications repræsenterer en **tilladelse** den adgang, der er givet til en bruger eller en gruppe af brugere for en rolle eller en ressource. En **rolle** definerer et sæt tilladelser, der er relateret til et eller flere målsystemer eller -programmer. En brugeradministratorrolle kan f.eks. være godkendt til at nulstille en brugers adgangskode, mens en systemadministratorrolle kan være godkendt til at tildele en bruger til en bestemt server. En **ressource** er en vilkårlig digital enhed som f.eks. en brugerkonto, computer eller database, som en forretningsbruger har behov for at kunne få adgang til.

Om Identity Applications

Identity Manager Identity Applications er et sæt browserbaserede webprogrammer, der er forbundet til hinanden. De giver din organisation mulighed for at administrere de brugerkonti og tilladelser, der er knyttet til det store udvalg af roller og ressourcer, som er tilgængeligt for brugere. Du kan konfigurere Identity Applications, så de understøtter selvbetjening for dine brugere, f.eks. anmodning om roller eller ændring af adgangskoden. Du kan også konfigurere workflows, der skal forbedre effektiviteten i forbindelse med administration og tildeling af roller og ressourcer.

Om Identity Manager Dashboard

NetIQ Identity Manager Dashboard (dashboardet) fungerer som den primære indgangsportal til Identity Applications. Dashboardet kan have en eller flere widgets, der hjælper dig med at få hurtige oplysninger om en bestemt aktivitet. Fra dit dashboard kan du udføre følgende aktiviteter:

- ♦ Administrere dine profilindstillinger og din adgangskode.
- ♦ Se oplysninger i dit organisationsdiagram.
- ♦ Gennemse og fuldføre dine opgaver, f.eks. godkende brugers anmodninger om adgang.
- ♦ Anmode om tilladelse for roller, ressourcer eller processer.

- Gennemse status og historik for anmodningerne om tilladelse.
- Finde andre brugere i din organisation.
- Tilpasse dit dashboard, f.eks. tilføje widgets og ændre placeringen af dem baseret på dine interesser.
- Angive en hvilken som helst bruger som din proxy fra systemet.
- Uddelegere dine opgaver til andre brugere fra systemet.

Du kan udføre følgende opgaver med de rette **tilladelser**:

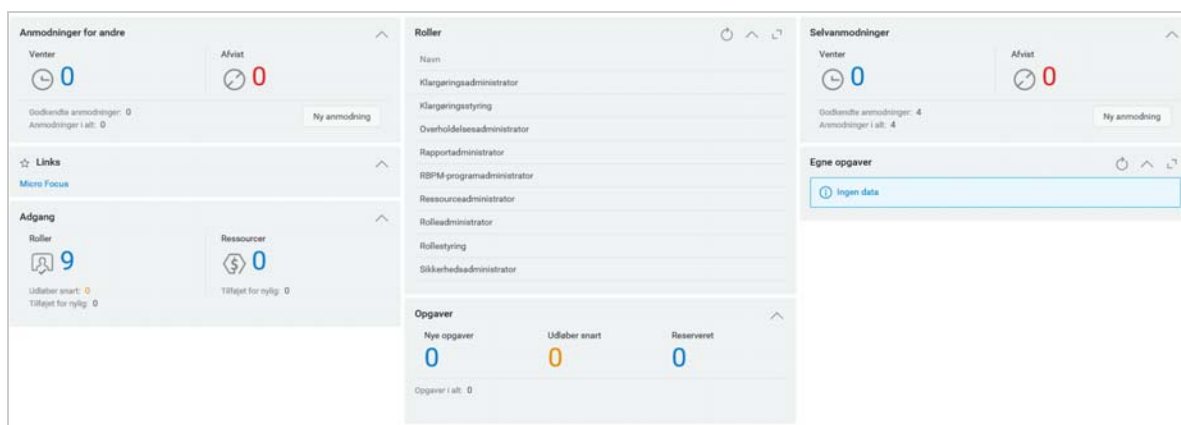
- Oprette og ændre brugerprofiler.
- Se oplysninger om andre brugere i organisationsdiagrammet.
- Oprette og ændre teams, der repræsenterer flere brugere og grupper, som kan udføre klargøringsanmodninger og godkendelsesopgaver, der er knyttet til disse teams.
- Anmode om tilladelser eller tilbagekalde tilladelser på vegne af andre brugere i organisationen.

Udforskning af dashboardet

Dashboardet leverer hurtige oplysninger om dine opgaver, dine tilladelser og anmodninger i form af widgets. Du kan navigere til bestemte sider eller programmer med et enkelt klik. Du kan desuden tilføje, fjerne, konfigurere og ændre placeringen af widgets på dit dashboard. Du kan finde flere oplysninger om tilpasning af dit dashboard i [Kapitel 3, "Administration af widgets og layout," på side 25](#).

I det følgende er der et eksempel, der beskriver standardindstillingerne for widgets i dashboardet.

Figur 1-1 Eksempel på personligt dashboard



I Identity Manager Dashboard kan du administrere forskellige aktiviteter i Identity Manager. På følgende sider kan du få hjælp til at administrere dine opgaver og aktiviteter:

Program

Viser en liste over alle de programmer, der er klargjort til dig. Det giver dig standardlinks til flere områder, hvor du kan strømline de grundlæggende opgaver, som du skal udføre i Identity Manager. Du kan finde yderligere oplysninger i ["Om siden Programmer" på side 13](#).

Opgaver

Viser alle dine opgaver, der afventer handling. Hvis du har den rette rolle, kan du se andres opgaver. For eksempel Teamleder.

Adgang

Giver dig tilladelse til at se tilladelser eller anmode om tilladelser. Hvis du vil se status for tilladelser, du har anmodet om, skal du gå til [Anmodningshistorik](#). På denne side vises alle dine anmodninger og deres status.

Personer

Giver dig tilladelse til at se andre brugere eller grupper i systemet og andre brugeres [organisationsdiagram](#). Det hjælper dem med at visualisere, hvordan disse brugere og grupper er indbyrdes relateret.

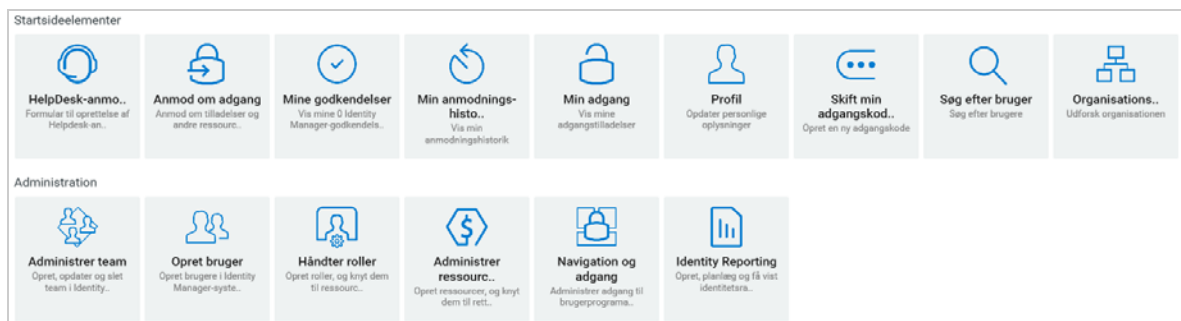
Administration

Giver dig tilladelse til at se og administrere roller, ressourcer, konsistenssikring af tilladelser, og hvordan de er konfigureret. Denne indstilling vises kun for administratorer. Du kan finde flere oplysninger om administrationsopgaver under [Identity Applications Administration](#) (Administration af Identity Applications) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Om siden Programmer

Den anden vigtige visning i dashboardet er siden **Programmer** ([Figur 1-2](#)), som indeholder standardlinks til flere områder for at strømline de grundlæggende opgaver, som slutbrugere og administratorer skal udføre i Identity Manager.

Figur 1-2 Eksempel på programsiden i dashboardet



Helpdeskanmodning vises som standard på siden **Programmer**. Denne indstilling giver dig mulighed for at sende en anmodning til helpdesk.

Din identitetsadministrator tilpasser siden **Programmer** til at indeholde felter med links til ressourcer eller programmer, der jævnligt anmodes om, og som brugere ofte åbner. Du kan konfigurere brugeradgang til disse felter, hvis du har den rette administrative rolle. Naviger til [Dit id > Indstillinger > Adgang](#) for at tilføje betroede for de påkrævede navigationselementer. Du kan få flere oplysninger om adgang til klargøring ved at se under [Managing User Access](#) (Administration af brugeradgang) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Nogle af felterne på denne side vises måske kun for brugere med en administrativ rolle i Identity Applications. En person, der kan oprette eller ændre roller, kan f.eks. se felterne **Opret bruger** og **Håndter roller**.

Du kan finde flere oplysninger om brug af dashboardet ved at klikke på  i dashboardet.

Om opgaver

På siden **Opgaver** kan du godkende eller afvise handlinger for de viste opgaver.

I Identity Manager Dashboard kan du administrere Identity Manager- og Identity Governance-opgaverne fra opgavesiden. Du kan nu se og godkende både Identity Manager- og Identity Governance-opgaver fra samme brugergrænseflade.

Mest almindelige måder at bruge Identity Applications på

Her er nogle eksempler på, hvordan personer typisk anvender Identity Applications i en organisation.

- ♦ [“Sådan fungerer selvbetjening af id” på side 14](#)
- ♦ [“Sådan fungerer roller og ressourcer” på side 14](#)
- ♦ [“Sådan fungerer procesanmodninger” på side 16](#)
- ♦ [“Sådan fungerer helpdesk” på side 16](#)

Sådan fungerer selvbetjening af id

- ♦ Ella (slutbruger) får sin glemte adgangskode tilbage via funktionerne til selvbetjening af identitetsinformation, når hun logger på.

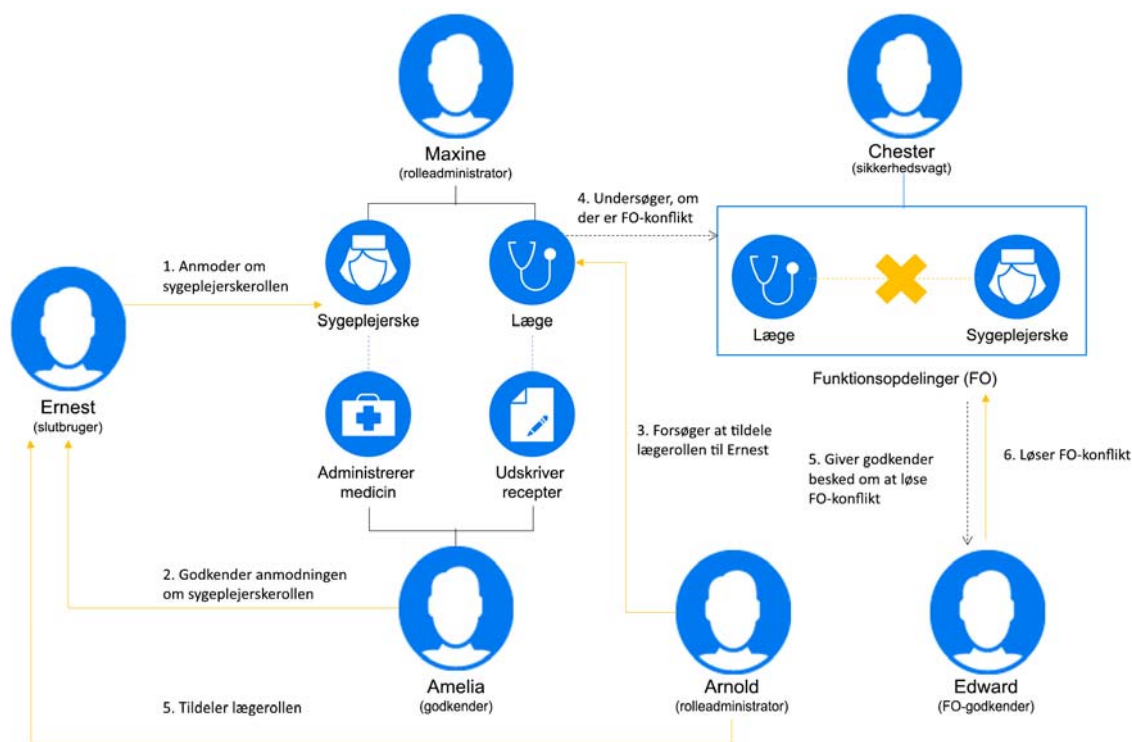
Identity Manager anvender som standard SSPR (Self Service Password Reset) til at give brugerne mulighed for at ændre deres adgangskoder. Identity Applications kan imidlertid bruge andre metoder til at styre glemte adgangskoder.

- ♦ Erik (slutbruger) foretager en søgning efter alle medarbejdere, som taler tysk på dette sted.
- ♦ Eduardo (slutbruger) gennemser organisationsdiagrammet, finder Ella og klikker på e-mail-ikonet for at sende en meddelelse til hende.

Sådan fungerer roller og ressourcer

I følgende eksempel forklares arbejdsgangen for roller og ressourcer i systemet:

Figur 1-3 Eksempelscenarie for rolletildeling



- Maxine (rolleadministratør) opretter forretningsrollerne Sygeplejerske og Læge samt it-rollerne Administrer lægemidler og Skriv recepter. Maxine opretter flere ressourcer, som er nødvendige for disse roller, og knytter ressourcerne til rollerne.
- Maxine (rolleadministratør) definerer en relation mellem rollerne Sygeplejerske og Administrer lægemidler og angiver, at rollen Sygeplejerske indeholder rollen Administrer lægemidler. Maxine definerer også en relation mellem rollerne Skriv recepter og Læge og angiver, at rollen Læge indeholder rollen Skriv recepter.
- Chester (sikkerhedsmedarbejder) definerer en begrænsning i funktionsopdelinger, som angiver, at der foreligger en potentiel konflikt mellem rollerne Læge og Sygeplejerske. Det betyder, at den samme bruger almindeligvis ikke bør tildeles begge roller på samme tid. Under nogle omstændigheder kan en person, som anmoder om en rolletildeling, have brug for at tilsidesætte denne begrænsning. For at kunne definere en undtagelse til funktionsopdelinger skal den person, som anmoder om tildelingen, angive en berettigelse.
- Ernest (slutbruger) gennemser en liste over roller, der er tilgængelige for ham, og anmoder om tildeling af rollen Sygeplejerske.
- Amelia (godkender) modtager besked om en godkendelsesansøgning via e-mail (som indeholder en URL). Hun klikker på linket, får vist en godkendelsesformular og godkender den.
- Arnold (rolleadministratør) anmoder om, at Ernest får tildelt rollen Læge. Han får besked om, at der foreligger en potentiel konflikt mellem rollen Læge og rollen Sygeplejerske, som Ernest allerede er blevet tildelt. Han angiver en berettigelse for at gøre en undtagelse til begrænsningen i funktionsopdelinger.

- ♦ Edward (godkender af funktionsopdelinger) modtager besked om en konflikt i funktionsopdelinger via e-mail. Han godkender Arnolds anmodning om at tilsidesætte begrænsningen i funktionsopdelingerne.
- ♦ Amelia (godkender) modtager besked om en godkendelsesansøgning for rollen Læge via e-mail. Hun godkender Arnolds anmodning om at tildele Ernest rollen Læge.
- ♦ Bill (rollekontrollant) ser på FO-overtrædelserne og undtagelsesrapporten og ser, at Ernest er blevet tildelt både rollen Læge og Sygeplejerske. Han ser derudover, at Ernest er blevet tildelt de ressourcer, der er knyttet til disse roller.

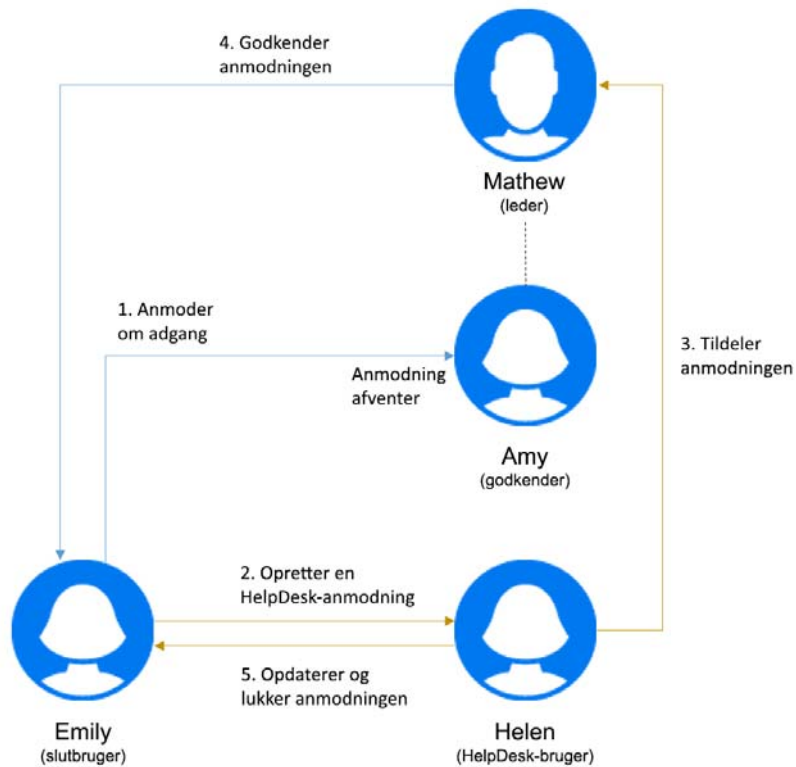
Sådan fungerer procesansøgninger

- ♦ Ernie (slutbruger) gennemser en liste over tilgængelige ressourcer og anmoder om adgang til Siebel*-systemet.
- ♦ Amy (godkender) modtager besked om en godkendelsesansøgning via e-mail (som indeholder en URL). Hun klikker på linket, får vist en godkendelsesformular og godkender den.
- ♦ Ernie kontrollerer status for sin tidligere anmodning om adgang til Siebel (som nu er sendt til en anden person med henblik på godkendelse). Han ser, at den stadig er i gang.
- ♦ Amy skal på ferie og angiver derfor, at hun midlertidigt ikke er til rådighed. Hun tildeles ikke nye godkendelsesopgaver, mens hun ikke er til rådighed.
- ♦ Amy åbner sin liste over godkendelsesopgaver, ser, at der er for mange til, at hun kan besvare dem i rette tid, og gentildeler flere af dem til kolleger.
- ♦ Pat (administrativ assistent, der fungerer som fuldmægtig for Amy) åbner Amys opgaveliste og udfører en godkendelsesopgave for hende.
- ♦ Max (leder) åbner opgavelisterne for medarbejdere i hans afdeling. Han ved, at Amy er på ferie, og gentildeler derfor opgaver til andre i afdelingen.
- ♦ Max starter en anmodning om en databasekonto for en medarbejder i sin afdeling, som rapporterer direkte til ham.
- ♦ Max tildeler Dan som autoriseret stedfortræder for Amy.
- ♦ Dan (nu delegeret godkender) modtager Amys opgaver, mens hun er væk.
- ♦ Max engagerer en ulønnet medarbejder, som ikke skal lægges ind i HR-systemet. Systemadministratoren opretter brugerposten for denne medarbejder og anmoder om, at vedkommende får adgang til Notes, Active Directory* og Oracle*.

Sådan fungerer helpdesk

I følgende eksempel forklares arbejdsgangen for helpdeskanmodninger i systemet:

Figur 1-4 Eksempel på helpdesk



- ♦ Emily (slutbruger) har anmodet om adgang til en printer på kontoret. Denne anmodning ventede i lang tid. Derfor oprettede hun en helpdeskanmodning.
- ♦ Helen (helpdeskbruger) modtager en meddelelse om helpdeskanmodningen på listen over opgaver.
- ♦ Helen analyserer problemet og finder ud af, at anmodningen er tildelt til Amy (godkender).
- ♦ Denne anmodning venter i systemet, fordi Amy ikke er til stede.
- ♦ Helen har tilladelse til at tildele opgaveanmodninger igen. Hun tildeler denne anmodning til Mathew (Amys chef).
- ♦ Mathew modtager anmodningen og godkender den. Emily har nu adgang til printerens på kontoret.
- ♦ Helen opdaterer og lukker helpdeskanmodningen.

2 Adgang til Identity Applications

Du kan få adgang til Identity Applications, f.eks. dashboardet, via en webbrowser. Identity Manager understøtter de fleste populære browserversioner. Kontakt systemadministratoren for at få en liste over understøttede browsere eller for at få hjælp til at installere en. Din organisation kan give dig den URL og de id-oplysninger, der kræves for at få adgang til programmerne.

- ♦ [“Overvejelser i forbindelse med adgang til Identity Applications” på side 19](#)
- ♦ [“Sådan logger du på første gang” på side 20](#)
- ♦ [“Reaktion på kontrol af foretrukket landestandard” på side 21](#)
- ♦ [“Fejlfinding af logonproblemer” på side 21](#)
- ♦ [“Sådan logger du af” på side 22](#)

Overvejelser i forbindelse med adgang til Identity Applications

Før du får adgang til dashboardet eller et af de andre Identity Applications, skal du overveje følgende:

- ♦ Du skal aktivere cookies og JavaScript* i din webbrowser.
- ♦ Når du bruger Internet Explorer, skal du som minimum angive niveauet for beskyttelse af personlige oplysninger **Mellem**. Du skal også vælge indstillingen **Hver gang jeg besøger webstedet** under **Funktioner > Internetindstillinger > Generelt, Browserdata > Indstillinger > Kontroller, om der er nye versioner af tidligere gemte sider**. Hvis denne indstilling ikke er valgt, vises nogle af knapperne muligvis ikke korrekt.
- ♦ Hvis du tidligere har haft adgang til Identity Manager-brugerprogrammet, kan du muligvis bruge det samme brugernavn og den samme adgangskode til at få adgang til dashboardet.
- ♦ Du kan ikke få adgang til Identity Applications ved hjælp af en konto, der indeholder følgende tegn i navnet:

\ / , * ? . \$ # +

- ♦ Hvis du ikke kan logge på, kan du klikke på **Glemmt adgangskode**. Du kan finde yderligere oplysninger i [“Hvis du glemmer din adgangskode” på side 21](#).
- ♦ Hvis du ser en anden første side, når du åbner Identity Manager-brugergrænsefladen, skyldes det typisk, at programmet er blevet tilpasset din organisation. Når du arbejder, vil du muligvis opdage, at andre funktioner i Identity Applications også er tilpasset.

Hvis det er tilfældet, kan du spørge systemadministratoren om, hvordan dine tilpassede Identity Applications adskiller sig fra den standardkonfiguration, der er beskrevet i denne vejledning.

Sådan logger du på første gang

Du skal være en godkendt bruger for at kunne logge på Identity Applications, f.eks. dashboardet. Hvis du har brug for hjælp til at få et brugernavn og en adgangskode for at kunne logge på, skal du kontakte systemadministratoren.

Første gang, du logger på Identity Applications, kræver Identity Manager, at du angiver sikkerhedsparametre for din konto, så du fremover kan nulstille din adgangskode. Hvis du glemmer din adgangskode og forsøger at nulstille den, stiller Identity Manager disse konfigurerede spørgsmål, næste gang du logger på, og beder dig om at angive det rigtige svar. Når svaret matcher det svar, du gemmer på denne side, kan du nulstille adgangskoden.

Sådan opretter du sikkerhedsspørgsmål, første gang du logger på:

- 1 Skriv dit brugernavn og din adgangskode, og klik derefter på **Logon**.
- 2 Logonsiden omdirigerer dig automatisk til siden til siden **Verificeringssvar**.
- 3 Angiv spørgsmålene og svarene til sikkerhedsspørgsmålene.

Angiv sikkerhedsspørgsmål

Hvis du glemmer din adgangskode, kan du få adgang til din konto ved at besvare dine sikkerhedsspørgsmål.

Vælg dine spørgsmål og svar, som kan bruges til at bekræfte din identitet, hvis du skulle glemme din adgangskode. Da disse svar kan bruges til at give dig adgang til din konto, skal du sørge for at angive svar, der ikke er nemme for andre at gætte eller finde ud af.

Skriv dine sikkerhedssvar

— Vælg et spørgsmål på listen —



— Vælg et spørgsmål på listen —



— Vælg et spørgsmål på listen —



— Vælg et spørgsmål på listen —



Gem svar

- 4 Klik på **Gem svar**. Derefter omdirigeres du til dashboardet.

Reaktion på kontrol af foretrukket landestandard

Hvis du modtager en prompt, hvor du bliver bedt om at vælge din egen foretrukne landestandard, når du logger på, har din administrator konfigureret Identity Applications til at udføre et sprogtek på brugernes browser. Det kan være nødvendigt for at sikre, at det indhold, du ser, vises på et understøttet sprog.

Når du bliver bedt om at tilføje en landestandard, skal du åbne listen **Understøttede landestandarder**, vælge en landestandard og klikke på **Tilføj**. Du kan finde flere oplysninger under [Tilføjelse af det nye sprog til Identity Applications](#).

Fejlfinding af logonproblemer

Dette afsnit indeholder løsninger til følgende typer af almindelige logonproblemer:

- ♦ [“Hvis du glemmer din adgangskode” på side 21](#)
- ♦ [“Hvis du har problemer med at logge på” på side 21](#)
- ♦ [“Hvis du bliver bedt om yderligere oplysninger” på side 22](#)

Hvis du glemmer din adgangskode

Hvis du ikke kan huske adgangskoden, kan du muligvis bruge linket **Glemmt adgangskode** for at få hjælp. Når du bliver bedt om at logge på, vises dette link som standard på siden. Du kan bruge dette link, hvis systemadministratoren har oprettet en adgangskodepolitik for dig.

- 1 Når du bliver bedt om at logge på, skal du klikke på linket **Glemmt adgangskode**.
- 2 Skriv brugernavnet, og klik på **Send**.
Hvis Identity Manager svarer, at der ikke blev fundet en adgangskodepolitik for dig, skal du kontakte systemadministratoren med henblik på assistance.
- 3 Svar på de verificeringsspørgsmål, der vises. Identity Manager beder dig om at besvare de konfigurerede spørgsmål. Når svaret matcher det svar, du har gemt tidligere, kan du nulstille adgangskoden. Klik på **Send**. For eksempel:

Besvar verificeringsspørgsmålene for at få hjælp til din adgangskode. Afhængigt af hvordan systemadministratoren har oprettet din adgangskodepolitik, kan du:

- ♦ Modtag en e-mail med din adgangskode om det
- ♦ Blive bedt om at nulstille adgangskoden

Hvis du har problemer med at logge på

Hvis du ikke kan logge på, skal du kontrollere, at du benytter det korrekte brugernavn og skriver adgangskoden korrekt (stavning, store og små bogstaver osv.). Kontakt systemadministratoren, hvis du stadig har problemer. Det er en fordel, hvis du kan give oplysninger om problemet (f.eks. fejlmeddelelser).

Hvis du bliver bedt om yderligere oplysninger

Du bliver måske bedt om at angive andre former for oplysninger, så snart du logger på. Det afhænger alt sammen af, hvordan systemadministratoren har oprettet din adgangskodepolitik (om nogen). For eksempel:

- ♦ Hvis dette er dit første logon, bliver du bedt om at definere dine verificeringsspørgsmål og -svar
- ♦ Hvis adgangskoden er udløbet, bliver du bedt om at nulstille den

Sådan logger du af

Når du er færdig med at arbejde i dashboardet eller andre Identity Applications, skal du logge af. I dashboardet skal du klikke på dit brugernavn i hjørnet øverst til højre og derefter vælge **Log af**.

|| Tilpasning af dit dashboard

Identity Applications indeholder mange indstillinger, som du kan bruge til at ændre visningen af dit *dashboard* og derefter gemme det som en tilpasset visning. Du kan f.eks. tilføje widgets og ændre placeringen af dem baseret på din interesse. Du kan også konfigurere widget-felterne og tilpasse dem. Dette dokument beskriver de forskellige indstillinger, du kan bruge til at tilpasse dit *dashboard*.

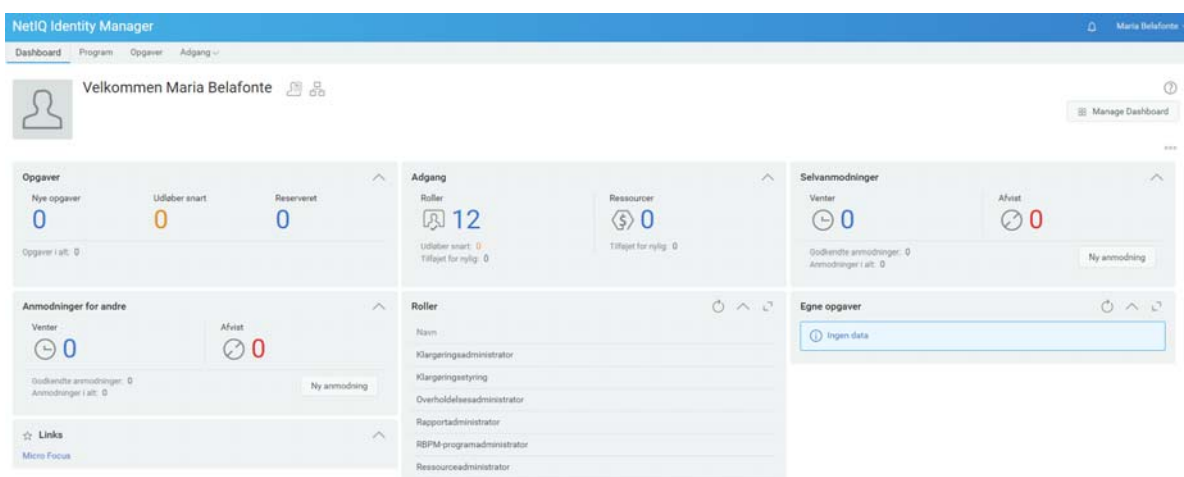
3 Administration af widgets og layout

Widgets er dashboardobjekter, som er designet til at give en bruger specifikke oplysninger om en bestemt aktivitet. Widgetten **Opgaver** giver f.eks. detaljer om nye opgaver, reservede opgaver eller opgaver, som forventes snart at udløbe. Tilsvarende kan der være mange andre widgets, som kan konfigureres, på dit dashboard.

Administratorer, som har adgang til siden **Indstillinger**, kan klargøre widgets for en bruger, gruppe, container eller rolle fra **Dit id > Indstillinger > Dashboardwidgets**.

Gå til dit **Dashboard**, og klik på **...** for at tilpasse det.

Figur 3-1 Tilpas dashboardet



Brug følgende indstillinger for at tilpasse dit dashboard:

Figur 3-2 Indstillinger for tilpasning



Widgets

Gør det muligt at føje widgets til dit dashboard. Se **“Tilføj en widget”** på side 27.

Layout

Gør det muligt at ændre dashboardets layout. Se **“Skift dashboardets layout”** på side 26.

Annuller

Annullerer alle ændringer, du har foretaget til dit dashboard.

Gem

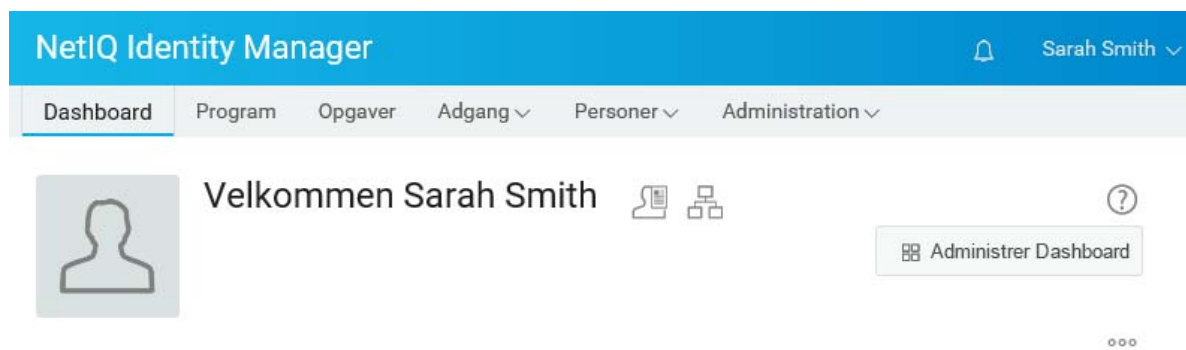
Gemmer dine ændringer og anvender dem til dit dashboard.

Administration af det globale dashboard

Det globale dashboard inkluderer et sæt widgets, der vises på dashboardet for de enkelte brugere i systemet. Brugere kan se disse widgets afhængigt af deres adgang, som er klargjort af en administrator. Indstillingen **Administrer dashboard** giver dig mulighed for at tilføje, ændre eller fjerne widgets fra det globale dashboard.

BEMÆRK: Du skal tilføjes som betroet bruger for at kunne bruge indstillingen **Administrer dashboard**.

Figur 3-3 Eksempel på globalt dashboard



Administratoren kan tilføje brugere, grupper, containere eller roller som en betroet enhed, der kan administrere det globale dashboard. Hvis du vil ændre de betroede, der kan administrere dashboardet, skal du gå til **Dit id > Indstillinger > Adgang** og klikke på **Globalt dashboard** på listen. Du kan finde flere oplysninger om konfigurationsadgang under [Managing Dashboard Widgets](#) (Administration af dashboardwidgets) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Skift dashboardets layout

Med Identity Applications kan du ændre layoutet af udseendet af widgets på dit dashboard.

- 1 Gå til **Dashboard**, og klik på **...**.
- 2 Vælg **Layout**.
- 3 Vælg det layout, du vil have vist på dit dashboard.

Figur 3-4 Skift layout

REDIGER DASHBOARD ✕

Titel

Dashboard

Struktur

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

3-9 (12/6-6)

VIGTIGT: Klik på **Gem** for at anvende dine ændringer.

Tilføj en widget

Gå til **Dashboard**, klik på **☰**, og vælg **Widgets** for at føje en ny widget til dit dashboard, .

Figur 3-5 Tilføj widgets

TILFØJ NY WIDGET ✕

Generelt

IDM

IG

Tilføj generelle widgets

I kategorien **Generelt** kan du føje widgets til dit dashboard uden for standardwidgets i Identity Manager. Du kan angive REST API-URL'en til den påkrævede widget og vise de påkrævede oplysninger som kurve-, cirkel- eller tabeldiagrammer.

1 Vælg en af følgende widgettyper på listen:

- ♦ **Kurvediagram:** Viser de oplysninger, der er anmodet om for det valgte element, i form af et kurvediagram.
- ♦ **Links:** Giver dig mulighed for at angive et bogmærke for ofte anvendte links, så du hurtigere kan få adgang til dem.
- ♦ **Cirkeldiagram:** Viser de oplysninger, der er anmodet om for det valgte element, i form af et cirkeldiagram.
- ♦ **Tabel:** Viser de oplysninger, der er anmodet om for det valgte element, i tabelform.

2 Klik på  for at konfigurere den widget, der er tilføjet på dit dashboard.

3 (Betinget) For widgets af typerne **Kurvediagram**, **Cirkeldiagram** og **Tabel** skal du angive følgende oplysninger:

- ♦ **Titel:** Angiver det widgetnavn, der skal vises på dit dashboard.
- ♦ **URL:** Angiver REST API-URL'en for den påkrævede widget, som du vil vise på dit dashboard.
- ♦ **Rodelement:** Angiver elementet fra REST-API-koden, som du vil vise et diagram for. Der skelnes mellem store og små bogstaver i dette felt. Du skal indtaste nøjagtigt det samme navn, som er angivet i REST API-koden.
- ♦ **Kolonner:** Angiver de kolonner, som du vil vise på din widget. Du kan tilføje flere kolonner. **Titel** angiver det viste navn for en kolonne. **Sti** angiver kolonnenavnet, som angivet i REST API'en. Der skelnes mellem store og små bogstaver i feltet **Sti**. Du skal indtaste nøjagtigt den samme streng fra REST API-koden.

Følgende er et eksempel på en REST API-kode for siden **Roller**:

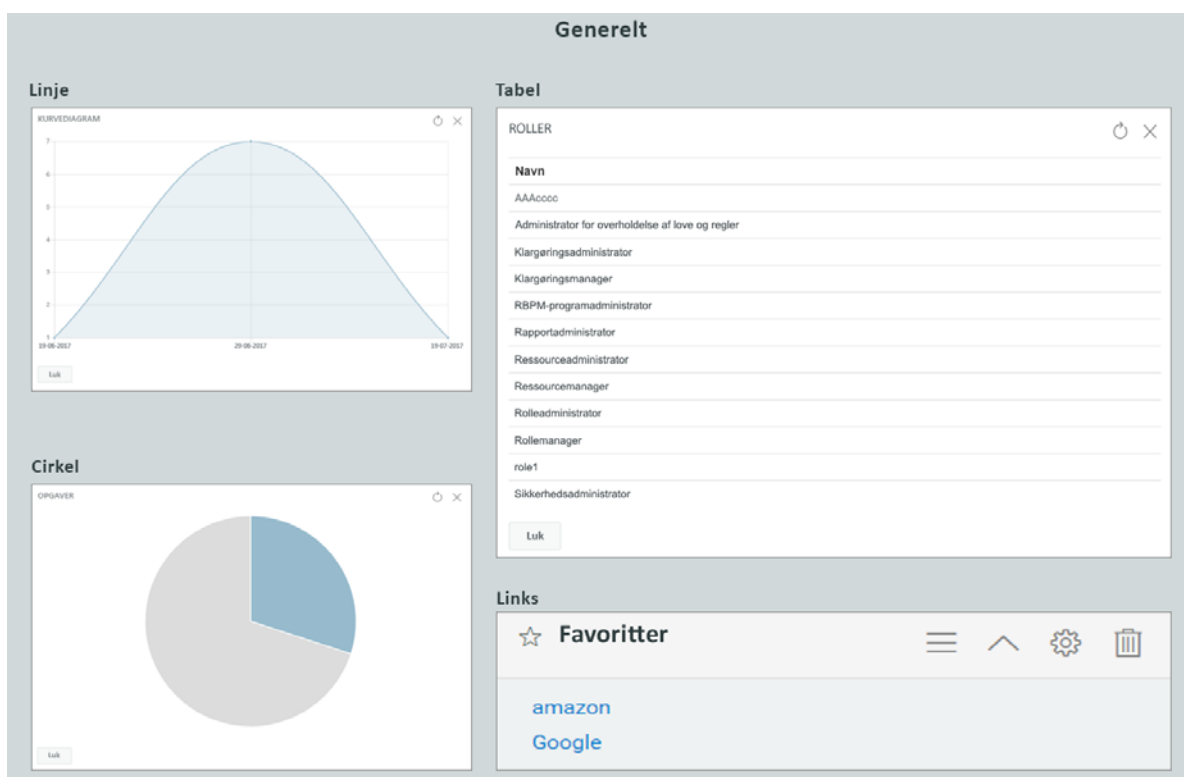
```
{
  "total": 12,
  "nextIndex": 0,
  "token": "60045d6be10f4419a2da9fa728683b06",
  "assignments": [
    {
      "id":
"cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
application driver,cn=driverset1,o=system",
      "name": "AAAcxxx",
      "description": "afasfdsf",
     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

I dette eksempel er tildelinger rodelementet, og navnet er den valgte kolonne, som skal vises på widgetten. Du kan også sætte et bogmærke for enhver URL, som du vil have adgang til fra dit dashboard

- 4 (Betinget) For widgets af typen **Links** skal du angive **Titel** for linkene og tilføje de link, som du vil have adgang til fra dashboardet.
- 5 Klik på **Gem** for at anvende dine ændringer.

Følgende er det eksempeldiagram og de link-widgets, som kan føjes til dit dashboard:

Figur 3-6 Eksempel på generelle widgets



Tilføj Identity Manager-widgets

Kategorien **IDM** giver dig mulighed for at føje Identity Manager-standardwidgets til dit dashboard.

For eksempel,

- ♦ **Adgang**: Viser antallet af roller og ressourcer og andre oplysninger om dem.
- ♦ **Anmodning for andre**: Viser antallet af ventende og afviste anmodninger for andre brugere og giver dig mulighed for at oprette en anmodning for disse brugere.
- ♦ **Selvanmodninger**: Viser antallet af ventende og afviste anmodninger og giver dig også mulighed for at oprette en ny anmodning.
- ♦ **Opgaver**: Viser antallet af nye eller ventende opgaver eller de opgaver, der snart udløber.

Hvis du vil konfigurere disse widgets, kan du gå til "[Konfigurer en widget](#)" på side 31.

VIGTIGT: Klik på **Gem** for at anvende dine ændringer.

Tilføj Identity Governance-widgets

Hvis du vil bruge Identity Governance-widgets, skal du installere og konfigurere Identity Governance med Identity Manager Dashboard.

Kategorien IG giver dig mulighed for at føje Identity Governance-standardwidgets til dit dashboard. For eksempel:

Udførelsesopgaver

Viser antallet af adgangsanmodninger, forretningsroller og fejl i tilladelsestildelinger i systemet.

Gennemsynsopgaver

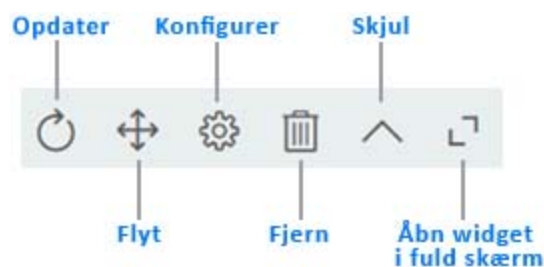
Viser antallet af ventende og fuldførte gennemsyn i systemet.

FO-overtrædelser

Viser antallet af ikke-gennemsete, godkendte eller løste FO-overtrædelser i systemet.

Widget-indstillinger

Du kan udføre følgende handlinger på widgets:



Opdater

Opdaterer widgetindholdet med de seneste oplysninger.

Flyt

Giver dig mulighed for at flytte widgetten på dashboardet.

Konfigurer

Giver dig mulighed for at konfigurere widgetegenskaberne. Du kan finde yderligere oplysninger i ["Konfigurer en widget" på side 31](#).

Fjern

Sletter widgetten fra dashboardet.

Skjul

Skjuler widgetoplysningerne og viser kun widgettens titel.

Åbn widget i fuld skærm

Viser widgetoplysningerne på fuld skærm.

BEMÆRK

- ♦ Indstillingerne **Opdater** og **Åbn widget i fuld skærm** vises kun for de widgets, der tilhører kategorien **Generelt**.
 - ♦ Klik på **Gem** for at anvende dine ændringer.
-

Konfigurer en widget

Du kan konfigurere enhver widget, som er føjet til dit dashboard. Du kan f.eks. aktivere eller deaktivere felterne for en widget eller ændre felternes visningsfarve.

1 Klik på  på den widget, du vil konfigurere.

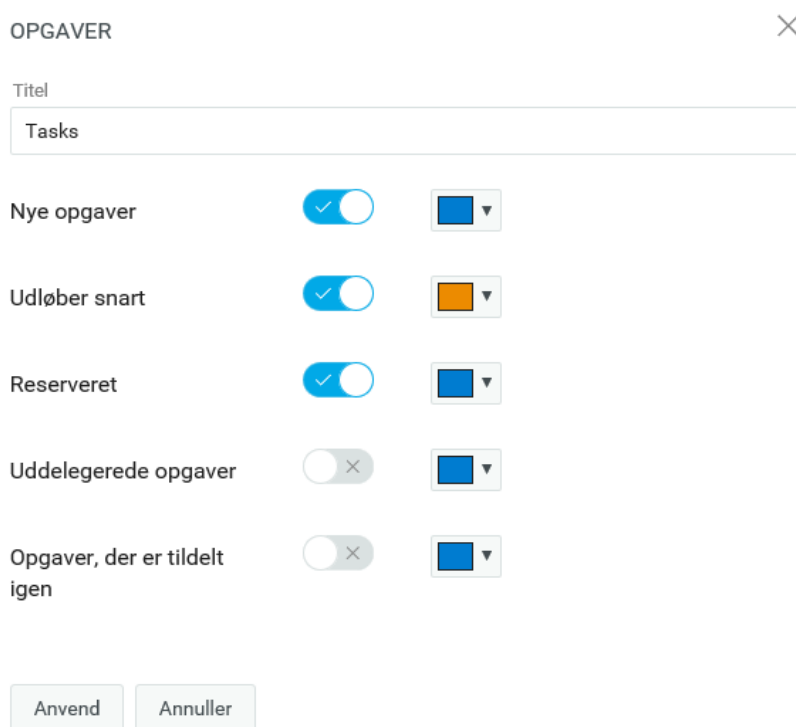
2 Rediger widgetegenskaberne.

Du kan f.eks. ændre titlen på en widget eller ændre farven på en etiket for et widgetfelt. Du kan også aktivere eller deaktivere et widgetfelt på egenskabssiden.

3 Klik på **Anvend** for at få vist ændringerne på dashboardet.

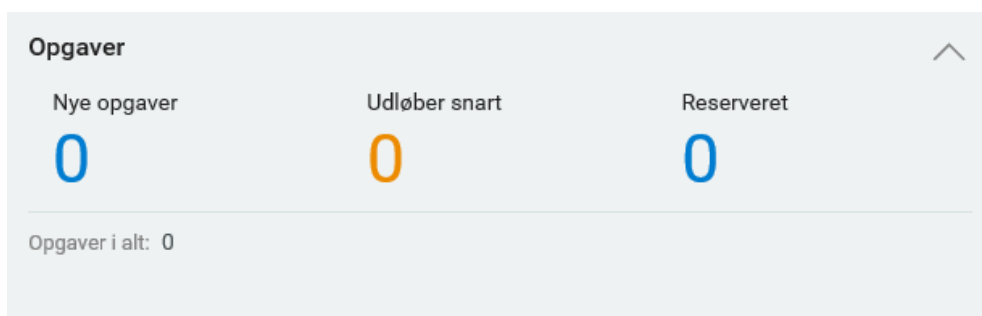
Du kan f.eks. redigere opgavewidgetten som vist nedenfor:

Figur 3-7 Eksempel på konfiguration af widget



OPGAVER	
Titel Tasks	
Nye opgaver	☒ 
Udløber snart	☒ 
Reserveret	☒ 
Uddelegerede opgaver	☐ 
Opgaver, der er tildelt igen	☐ 
Anvend Annuller	

Klik på **Anvend** for at få vist ændringerne på dashboardet.



Hvis du vil konfigurere generelle widgets, skal du ændre de indstillinger, som vises, mens du tilføjer widgets. Se [“Tilføj generelle widgets” på side 28](#).

VIGTIGT: Klik på **Gem** for at anvende dine ændringer.



Administration af dine tilladelser og din identitetsprofil

Identity Manager Dashboard hjælper dig med at anmode om adgang til de ressourcer og roller, som du skal have for at fuldføre dine daglige opgaver. Du kan også handle på opgaver, der er tildelt til dig i Identity Manager-miljøet, f.eks. godkendelse af anmodninger om adgang. Ejere af ressourcer og roller kan administrere processen.

Når du anmoder om tilladelse, starter Identity Manager en proces, hvor din anmodning gennemses effektivt, så du kan få den rolle eller ressource, du har brug for. Din manager modtager en notifikation enten via e-mail eller i dashboardet om at gennemse din anmodning. I visse tilfælde kan din anmodning også godkendes af andre personer i organisationen.

Nogle brugere kan oprette anmodninger på vegne af andre eller fungere som fuldmægtig for en anden bruger.

- ♦ [Kapitel 4, "Administration af anmodninger om tilladelser," på side 35](#)
- ♦ [Kapitel 5, "Administration af programmer," på side 43](#)
- ♦ [Kapitel 6, "Administration af dine opgaver," på side 47](#)
- ♦ [Kapitel 7, "Sådan handler du på vegne af en anden," på side 51](#)
- ♦ [Kapitel 8, "Administration af uddelegeringer," på side 53](#)
- ♦ [Kapitel 9, "Administration af din tilgængelighed," på side 55](#)
- ♦ [Kapitel 10, "Administration af din profil," på side 57](#)
- ♦ [Kapitel 11, "Administration af organisationsdiagrammet," på side 59](#)
- ♦ [Kapitel 12, "Administration af din adgangskode," på side 67](#)

4 Administration af anmodninger om tilladelser

Dette afsnit indeholder en vejledning til følgende aktiviteter:

- ♦ “Visning af dine tilladelser” på side 35
- ♦ “Anmodning om tilladelser” på side 37
- ♦ “Visning af anmodninger” på side 37
- ♦ “Tilbagekaldelse af tilladelser” på side 39
- ♦ ““Deep linking” til en anmodning” på side 40

Du kan også gennemse ⓘ for at få oplysninger om dashboardet for disse aktiviteter.

Visning af dine tilladelser

Tilladelser repræsenterer de konti, roller eller ressourcer, som er tilgængelige for dig. Tilladelser kan tildeles automatisk til dig af din organisation, eller du kan anmode om specifikke tilladelser. Du kan også arve nogle tilladelser indirekte via rollerelationer, eller hvis du er medlem af en gruppe eller en container.

Hvis du vil have vist de roller og ressourcer, som du har adgang til, skal du gå til dashboardet og vælge:

Adgang > Tilladelser

Du kan derefter vælge en bestemt tilladelse for at få yderligere oplysninger om den pågældende rolle eller ressource. Tilladelsen indeholder måske også oplysninger om årsagen til, at tilladelsen er tildelt. Du kan finde en bestemt tilladelse på en lang liste ved at skrive navnet, det almindelige navn eller en beskrivelse af tilladelsen i søgefeltet. Du kan også filtrere listen.

BEMÆRK:

- ♦ Du kan som standard se listerne over tilladelser, der er tildelt eller godkendt til dig direkte. Men det kan variere, afhængigt af hvordan administratoren har konfigureret indstillingerne for siden. Du kan få flere oplysninger ved at se under [Brugerindstillinger](#) i *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).
 - ♦ Hvis du vil se de underordnede tilladelser, der er knyttet til de tildelte eller godkendte tilladelser, skal du klikke på ⓘ.
-

Visning af tilladelsesdetaljer

Vælg den tilladelse, du vil have vist flere detaljer om. Følgende tabel indeholder de felter, der vises for de enkelte tilladelser:

Tabel 4-1 Tilladelsesfelter og en beskrivelse af dem

Felter	Beskrivelse
Beskrivelse	Beskrivelsen af rollen eller ressourcen.
Ikrafttrædelsesdato	Dato og klokkeslæt for tildeling af tilladelsen.
Udløbsdato	Den dato, hvor tilladelsen ikke længere vil være tildelt til brugeren. Den vises kun for tilladelser, hvor indstillingen for udløb er aktiveret.
Årsag	Angiver årsagen til, at tilladelsen er tildelt til brugeren.
Tildelt tilladelse via	Angiver, hvem der har tildelt tilladelsen til brugeren. Hvis en rolle tildeles til brugeren direkte via en godkendelsesproces, kan du se listen over den eller de godkendere, der har godkendt anmodningen om tildeling, under indstillingen Vis oplysninger om rollegodkendelse. Hvis en rolle arves af brugeren via medlemskab af en gruppe eller container, vises følgende oplysninger under indstillingen Vis oplysninger om tildeling af rolle til gruppe: ♦ Anmodet af: Angiver, hvem der har anmodet om tilladelsen. ♦ Beskrivelse af anmodning: Den beskrivelse, der angives, når der anmodes om tilladelsen. ♦ Godkendelsesdetaljer: Klik på linket for at se listen over godkendere, der har godkendt anmodningen om rolletildelingen.

Hvis du er Identity Applications-administrator, kan du se tilladelserne for dine teammedlemmer under fanen **Andre**. Gå til fanen **Andre**, og søg ved hjælp af brugernavn eller tilladelsesdetaljer.

- ♦ Hvis du søger efter bruger, vises alle de tildelte tilladelser for den pågældende bruger. Du kan derefter vælge en specifik tilladelse for at gennemse detaljerne, f.eks. datoen for tildeling, hvem der er tildelt tilladelsen, og om der er angivet en årsag til tildeling af tilladelsen. Du kan finde flere oplysninger i [Tabel 4-1 på side 36](#).
- ♦ Hvis du søger efter tilladelse, vises alle brugere, enkeltpersoner samt dem, der er medlem af en gruppe eller container, der er tildelt til den pågældende tilladelse.

BEMÆRK: Teamledere eller -supervisorer kan ikke søge ved hjælp af tilladelsesdetaljer. Men de kan se tilladelserne for deres teammedlemmer ved at søge efter navnet på eller en beskrivelse af teamet. Derudover kan der også søges ved hjælp af brugernavn på siden for at gøre det muligt at søge efter og se tilladelser for et specifikt teammedlem.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Anmodning om tilladelser

Hvis du vil anmode om roller og ressourcer, skal du klikke på [Adgang > Anmodninger](#)

Før du anmoder om tilladelser, skal du overveje følgende:

- Du kan måske anmode om adgang på vegne af en anden bruger. Hvis du f.eks. er teammanager, kan du som regel handle på vegne af gruppemedlemmerne. Processen er den samme med den undtagelse, at du skal angive, at anmodningen gælder for **Andre** i stedet for **Selv**.
- Undgå at bruge tegnsætning, når du angiver en tilladelse, som du vil anmode om. Hvis navnet på den tilladelse, som du vil anmode om, indeholder tegnsætning, skal du undgå at bruge det i din søgning.
- Forskellige tilladelser kræver forskellige oplysninger, afhængigt af hvordan administratoren har konfigureret tilladelsesformularen. Hvis tilladelsen kræver, at der angives detaljerede oplysninger, omdirigerer dashboardet dig til et separat vindue, når du vælger tilladelsen.
- Du kan anmode om flere tilladelser på én gang.

Men hvis tilladelsesformularen for en af anmodningerne kræver, at der angives særlige oplysninger, kan du måske ikke inkludere denne tilladelse i en anmodning om flere tilladelser. Hvis du vil anmode om flere tilladelser på én gang, må anmodningsformularerne for de forskellige anmodninger ikke kræve detaljerede oplysninger.

- Du kan angive udløbsdatoen, mens du anmoder om en ressource eller en rolle.

Sådan anmoder du om tilladelser til Identity Governance:

*Gælder kun for to forhold, nemlig når du har aktiveret indstillingen **Vil du vise IG-kataloget på anmodningssiden** på siden **Konfiguration > Identity Governance**, og når du har anmodet om tilladelse til **Selv**.*

- **IDM-kataloger:** Viser alle tilgængelige Identity Manager-roller, -ressourcer og -workflows.
- **IG-programmer:** Viser alle programmer, der indsamles i Identity Governance. Du kan derefter vælge de tilladelser, der er knyttet til det valgte program.
- **IG-tekniske roller:** Viser alle tekniske roller, der indsamles i Identity Governance. Vælg de IG-roller, som du vil anmode om, og angiv en årsag til at anmode om rollen.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Visning af anmodninger

Hvis du vil have vist status for en igangværende anmodning og afsluttede anmodninger, skal du gå til dashboardet og vælge:

[Adgang > Anmodningshistorik](#)

En teammanager eller supervisor kan se anmodningshistorikken for andre teammedlemmer under fanen **Andre**.

Du kan også oprette en helpdeskanmodning for dine ventende anmodninger.

- ♦ “Sporing af en anmodning” på side 38
- ♦ “Annullering af en anmodning” på side 38
- ♦ “Oprettelse af en helpdeskanmodning” på side 39

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

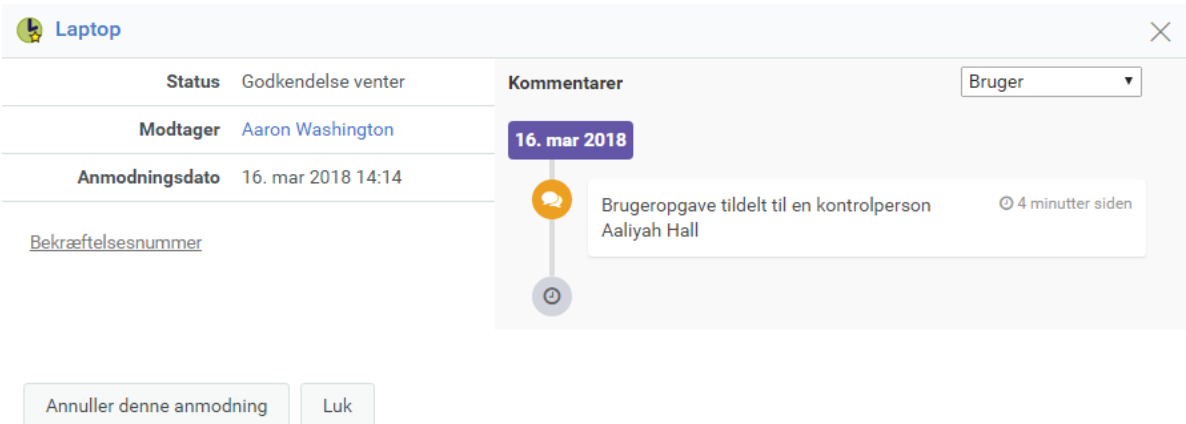
Sporing af en anmodning

For hver anmodning kan du ikke kun se dine handlinger, men også det workflow, der sker i forbindelse med godkendelse eller afvisning af din anmodning. De enkelte trin i processen har et tidsstempel.

BEMÆRK: Hvis du anmoder om programroller eller tekniske roller under fanerne **IG-programmer** eller **IG-tekniske roller**, kan de pågældende anmodninger ikke spores via siden **Anmodningshistorik**. Hvis du vil spore IG-anmodninger, kan du tilføje IG-historik-URL'en fra siden **Programmer** i dashboardet.

Du kan spore en anmodning, der er i kø, ved at vælge anmodningen og derefter ændre menuen øverst til højre til **Bruger og system**. Dashboardet viser anmodningens aktuelle tilstand i godkendelsesprocessen.

Figur 4-1 Sporing af en anmodning



Laptop ✕

Status	Godkendelse venter
Modtager	Aaron Washington
Anmodningsdato	16. mar 2018 14:14

[Bekræftelsesnummer](#)

Kommentarer Bruger ▼

16. mar 2018

 Brugeropgave tildelt til en kontrolperson ⌚ 4 minutter siden
Aaliyah Hall



Annuller denne anmodning Luk

Annullering af en anmodning

Du kan annullere en anmodning, der er i kø fra **Anmodningshistorik**. Vælg anmodningen på listen, og vælg derefter **Annuller denne anmodning** i det vindue, der åbnes.

Oprettelse af en helpdeskanmodning

Du kan kontakte Helpdesk, hvis du har brug for hjælp til anmodninger, der har været uovervåget i lang tid.

Du kan oprette en helpdeskanmodning følgende steder:

- ♦ **Adgang > Anmodning**, klik på **Helpdeskanmodning**.
- ♦ **Programmer**, og klik på **Helpdeskanmodning**.
- ♦ **Adgang > Anmodningshistorik**, klik på  i den anmodning, som du vil eskalere til en helpdeskanmodning.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Helpdeskmedlemmer modtager en meddelelse om helpdeskanmodningen. Du får besked om din anmodning, når anmodningen er løst eller lukket.

Tilbagekaldelse af tilladelser

Hvis du ikke længere har brug for at have adgang til en rolle eller ressource, kan du tilbagekalde tilladelsen til den pågældende rolle eller ressource. Hvis du vil tilbagekalde en tilladelse, skal du navigere til **Adgang > Tilladelser**, vælge den relevante tilladelse og angive en årsag til, at tilladelsen skal tilbagekaldes.

Du kan også tilbagekalde en tilladelse på vegne af andre brugere. Hvis dit teammedlem f.eks. er flyttet fra Afdeling 1 til Afdeling 2, og teammedlemmet ikke længere har brug for at have adgang til en bestemt ressource, kan du tilbagekalde tilladelsen for den pågældende bruger i Identity Manager. Hvis du vil tilbagekalde en tilladelse, skal du vælge **Andre** og fjerne tilladelsen. Du kan tilbagekalde flere tilladelser på én gang. Du kan føje disse tilladelser til en kø, så du kan gennemse dem, før du beslutter dig for at tilbagekalde dem.

Det er kun administratorer og teammanagers, der kan tilbagekalde tilladelser for andre brugere. En administrator kan tilbagekalde tilladelser for alle brugere i organisationen, mens en teammanager kun kan tilbagekalde tilladelser for egne teammedlemmer.

Du kan tilbagekalde tilladelser for andre brugere på følgende måder:



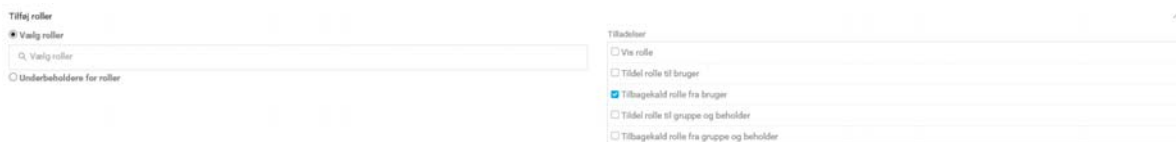
- ♦ **Søg efter brugere:** Giver dig mulighed for at søge efter en bruger og tilbagekalde tilladelser for den pågældende bruger. Du kan tilbagekalde en tilladelse direkte for brugeren eller føje tilladelsen til en kø. En kø er et permanent arbejdsområde, hvor du midlertidigt kan gemme tilladelser, som du kan gennemse og eventuelt tilbagekalde. Du kan derefter søge efter andre tilladelser, som du vil tilbagekalde for den pågældende bruger, og føje dem til køen. Det giver dig mulighed for at tilbagekalde alle tilladelser på én gang.

- ♦ **Søg efter tilladelser:** Giver dig mulighed for at søge efter en bestemt tilladelse. Hvis du vælger en tilladelse, vises alle de brugere, som har den pågældende tilladelse. Du kan tilbagekalde tilladelsen for den valgte bruger direkte eller føje denne tilladelse til en kø og tilbagekalde den pågældende tilladelse for flere brugere på én gang.

Teamleder: Hvis du er teamleder, kan du tilbagekalde tilladelser for dine teammedlemmer under fanen **Andre**. Kontroller, at du har de rette tilladelser til at tilbagekalde andres tilladelser.

Administrator: Hvis du er administrator, kan du tilføje tilbagekaldelsestilladelser for en teamleder. Hvis du f.eks. vil tilføje en tilbagekaldelsesrolle fra en brugertilladelse for en teamleder. Gå til **Personer > Teams**, og rediger teamtilladelser for at aktivere tilbagekaldelsestilladelser for en teamleder.

Figur 4-2 Eksempel på tilføjelse af en tilbagekaldelsestilladelse for en teamleder



Denne indstilling giver teamlederen tilladelse til at tilbagekalde den valgte rolle fra teammedlemmerne.

BEMÆRK: Hvis du tilbagekalder en tilladelse, afspejler dine liste over tilladelser måske ikke ændringen med det samme. Det kan skyldes, at tilladelsen er knyttet til en tilbagekaldelsesproces, der kan tage tid. Opdater listen for at se ændringerne.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

"Deep linking" til en anmodning

I Identity Applications kan du oprette dybe links til en specifik procesanmodning (også kaldet en klargøringsanmodning). Denne funktion giver en leder mulighed for at sende en specifik procesanmodnings-URL til en medarbejder, så denne medarbejder hurtigt kan anmode om processen uden at skulle gå via Identity Manager Dashboard. Når du opretter et dybt link til en procesanmodning, vises anmodningsformularen på sidens indhold sammen med sidehovedet for Identity Applications.

Når der anmodes om en tilladelse, vises anmodningen på siden **Adgang > Anmodningshistorik** for anmoderen, og den vises også på siden **Opgaver** for kontrolpersonen.

Den URL, der bruges til at oprette et direkte link til en procesanmodning, bruger følgende format:

- ♦ I forbindelse med ældre formularer

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

Her er et eksempel, der viser den URL-adresse, man kunne bruge til at linke direkte til en definition af klargøringsanmodning:

[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=&jas=%7B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22window.close%28%29%22%7D](https://testserver:8543/IDMProv/requestForm.do?uid=cn=request%20mobile%20approval%20app,cn=requestdefs,cn=appconfig,cn=user%20application%20driver,cn=driverset1,o=system&aqua=true&idmdash=true&recipient=&jas=%7B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22window.close%28%29%22%7D)

- ♦ I forbindelse med de nye JSON-formularer

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

Her er et eksempel, der viser den URL-adresse, man kunne bruge til at linke direkte til en definition af klargøringsanmodning:

<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%3Dhelp-deskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20driver,cn%3Ddriverset1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&formContainer=RequestForms&locale=en>

5 Administration af programmer

Som administrator for Identity Applications kan du redigere siden **Programmer**, så den viser alle de programmer, aktiviteter og tilladelser, som brugere skal have adgang til. Som standard indeholder Identity Applications kategorien **Standardsideelementer**, som ikke kan slettes.

Når du har gennemført dine ændringer, skal du klikke på **Redigering udført** for at vende tilbage til **Programmer**.

Oprettelse af foretrukne elementer

Du kan oprette lige så mange programmer og tilladelser, du vil, og tilføje dem til siden **Programmer**. Du behøver ikke at føje disse elementer til kategorien **Startsideelementer** eller andre **Programmer**-kategorier.

- 1 (Betinget) Hvis du vil oprette et nyt element, skal du klikke på + under fanen **Programmer** eller **Tilladelser**.
- 2 Udfyld formularen for et program eller en tilladelse. Se ["Tilføjelse af et program" på side 43](#) eller ["Tilføjelse af en tilladelse" på side 44](#).

BEMÆRK: Du skal angive en værdi for alle felter, der har en stjerne (*), f.eks. navnet på og beskrivelsen af et program.

- 3 (Valgfrit) Træk og slip det nye program eller den nye tilladelse til en kategori.
- 4 (Betinget) Hvis du vil redigere et eksisterende element, skal du vælge redigeringsikonet inde i feltet og derefter opdatere værdierne.

Tilføjelse af et program

Hvis du vil tilføje et program, skal du angive følgende oplysninger:

(Betinget) Føj til kategori

Angiver kategorien for dette program.

Navn

Angiver navnet på programmet.

Beskrivelse

Angiver typen af program.

(Valgfrit) Billede

Angiver et logo eller billede for et program.

Link

Angiver et link for dette program. Se [""Deep linking" til en anmodning" på side 40](#).

(Valgfrit) API-URL

Angiver URL'en til REST-slutpunktet med JSON-data, der giver flere detaljer, f.eks. værdien af parametre og et badge. Du kan finde flere oplysninger i dokumentationen.

Tilføjelse af en tilladelse

Hvis du vil tilføje en tilladelse, skal du angive følgende oplysninger:

Tilladelser

Angiver tilladelsen. Det kan være en rolle, en ressource eller en PRD.

(Betinget) Føj til kategori

Angiver kategorien for dette program.

(Valgfrit) Billede

Angiver et logo eller billede for et program.

Tilføje, redigere eller slette en kategori

Du kan organisere elementer i **Programmer** i logiske kategorier. Du kan oprette lige så mange kategorier, som din organisation har brug for. Du kan også omarrangere felterne i en kategori eller flytte felter til en anden kategori.

Tilføje en kategori

1 Vælg **Ny kategori**.

Identity Manager tilføjer kategorien i slutningen af kategorigrupperne. Det kan være nødvendigt at rulle ned for at vise den tilføjede kategori.

2 Angiv navnet på den nye kategori.

3 Klik på +, og vælg derefter **Program** eller **Tilladelse**.

4 Udfyld formularen til programmet eller tilladelsen.

BEMÆRK: Du skal angive en værdi for alle felter, der har en stjerne (*), f.eks. navnet på og beskrivelsen af et program.

5 Vælg **+Tilføj**.

Redigere en kategori

Du kan redigere en kategori på følgende måder:

- Tilføje felter til programmer og tilladelser ved at trække dem fra sektionen **Nye elementer** og **Tilladelser** og slippe dem til højre på siden
- Fjerne et program eller en tilladelse ved at vælge skraldespandsikonet i elementets felt
- Redigere indstillinger for et element

- ♦ Redigere navnet på kategorien
- ♦ Omarrangere elementerne inden for kategorien

Slette en kategori

Hvis du vil slette en kategori, skal du vælge skraldespandsikonet til højre for kategoriens navn.

6 Administration af dine opgaver

Hvis du har ansvaret for at godkende eller afvise tilladelser, der anmodes om i Identity Manager, kan du bruge dashboardet til at administrere dine opgaver, som du måske tidligere har gjort i brugerprogrammet. Du kan godkende eller afvise en anmodning ad gangen, eller du kan godkende eller afvise flere simple anmodninger, der ikke kræver detaljerede oplysninger, samlet.

Hvis du vil gennemse anmodninger i kø, skal du klikke på **Opgaver**.

Du kan også modtage en e-mailmeddelelse med et link, hvor du kan godkende eller afvise en anmodning i en svar-e-mail.

Før du handler på brugeranmodninger, skal du overveje følgende:

- Du kan vælge flere opgaver, så du kan godkende/afvise flere anmodninger.
- I forbindelse med en mere kompleks anmodning, der kræver detaljerede oplysninger, vises der ikke et afkrydsningsfelt i dashboardet. Du skal godkende eller afvise disse anmodninger ved at vælge de enkelte anmodninger og udfylde formularerne.
- Når du vælger en mere kompleks anmodning, der skal godkendes eller afvises, åbnes anmodningsformularen måske under en særskilt browserfane i dashboardet.
- Du skal som hovedregel skrive en kommentar, der forklarer, hvorfor du vil godkende eller afvise de valgte opgaver.

Visning af dine opgaver

For at håndtere dine opgaver skal du vælge **Opgaver**. Hvis du vil have vist opgaver, der er tildelt til andre, skal du klikke på **Andre**.

Hvis du fungerer som fuldmagtsgiver eller stedfortræder for andre opgaver, kan du afslutte opgaver, som er tildelt til andre. Du kan finde flere oplysninger om fuldmægtigtildelinger og delegeringstildelinger under **Funktion som fuldmægtig**.

IDM-godkendelser: *Gælder, hvis du har aktiveret indstillingen* **Vil du vise IG-godkendelser på opgavesiden på siden Konfiguration > Identity Governance**.

Under denne fane vises alle Identity Manager-opgaver. Den indeholder som standard alle **egne** opgaver. Hvis du vil have vist andre opgaver med en passende rolle, skal du klikke på **Andre**.

- Du kan søge efter dine opgaver ved at bruge filtrene **Opgaver, der er tildelt igen**, **Returnerede opgaver** eller **Uddelegerede opgaver**. Hvis du bruger filteret **Uddelegerede opgaver** for indstillingen **Selv**, vises kun de opgaver, der er delegeret til dig.
- Hvis du er administrator, kan du også filtrere opgaver ved at bruge filtrene **Tildelt til mig** eller **Modtager som mig**.
- Hvis du søger efter andre opgaver, kan du bruge filtrene **Returnerede opgaver**, **Opgaver, der er tildelt igen** eller **Delegerede opgaver**. Hvis du bruger filteret **Uddelegerede opgaver** for **Andre**, vises alle de opgaver, der er delegerede til andre brugere i systemet.

- Du kan også begrænse din opgavesøgning baseret på opgaver, som findes i systemet:
 1. Vælg .
 2. (Betinget) Angiv perioden i **Uger**, **Dage** eller **Timer** for at få vist opgaver, der er oprettet i en bestemt periode.
 3. (Betinget) Angiv den opgavestatus, som du vil filtrere på.
 4. Klik på **Filtrer**.
- Hvis du bruger helpdesk, kan du bruge filteret **HelpDesk-opgaver** til at se en begrænset liste. Hvis du vil administrere helpdeskopgaver, kan du gå til hjælpen til dashboard.

I visse tilfælde skal du muligvis godkende anmodede elementer, hvis politikken Adgangs-anmodning angiver dig som godkender af anmodninger. Disse elementer, der skal godkendes, vises under fanen **Godkendelser**.

IG-godkendelser: *Gælder, hvis du har aktiveret indstillingen Vil du vise IG-godkendelser på opgavesiden på siden Konfiguration > Identity Governance.*

Under denne fane vises alle ventende godkendelsesopgaver for Identity Governance. Du kan tildele opgaverne til andre ved hjælp af indstillingen **Tildel igen**.

Administration anmodninger om godkendelse eller afvisning

I nogle organisationer kan en gruppe personer være ansvarlige for at kontrollere, godkende eller afvise anmodninger om adgang. Når dette er tilfældet, modtager hvert medlem af gruppen den samme anmodning. IT-serviceteamet kan f.eks. være ansvarlig for alle anmodninger vedrørende telekommunikations- og computerudstyr. Når en ny medarbejder anmoder om en mobiltelefon, tildeles anmodningen til alle medlemmer af IT-serviceteamet. Alle i teamet kan fuldføre anmodningen.

Du kan udføre alle følgende opgaver på anmodningen:

Reservere anmodning

Du kan **reservere** en anmodning og handle på den påkrævede opgave med det samme eller senere. Uanset hvornår du handler på opgaven, kan de andre medlemmer af din gruppe ikke længere se den pågældende opgave i deres **opgaver**.

Frigive en anmodning

Hvis du ikke vil handle på den anmodning, du har reserveret, kan du frigive anmodningen.

Tildel en anmodning igen

En opgave, der er tildelt til dig, kan tildeles til en anden bruger i organisationen. Du skal gøre dig følgende overvejelser, når du tildeler opgaver til andre:

- Hvis du ikke kan fuldføre opgaven, kan du tildele den til din manager. Vælg anmodningen under fanen **Selv**, og vælg derefter **Tildel igen**. Opgaven tildeles automatisk til din leder.

- ♦ Som teamleder kan du kun gentildele egne opgaver til din egen leder. Men hvis du vil gentildele en opgave, der er tildelt til et medlem af dit team, kan du gøre det ved hjælp af fanen **Andre**. Gå til fanen **Andre**, markér afkrydsningsfelt for den ønskede opgave, og klik derefter på **Tildel igen**. I rullemenuen **Tildel til** skal du vælge det teammedlem, du vil tildele opgaven til, skrive en kommentar til den nye tildeling og klikke på **Tildel igen**. Opgaven tildeles igen til et teammedlem efter eget valg.
 - ♦ Hvis du ikke har handlet på opgaven i løbet af den angivne tidsramme, kan følgende handlinger indtræffe:
 - ♦ En administrator kan tildele opgaven til en anden bruger. En administrator har tilladelse til at tildele en opgave til en hvilken som helst bruger i organisationen.
 - ♦ Teamlederen kan tildele opgaven til et andet medlem af teamet. Sørg for, at teamlederen har tilladelsen Administrer adressatopgave på det tidspunkt, hvor teamet oprettes. Dette gælder kun, når indstillingen **Medlemmer** bruges til at føje medlemmer til teamet på det tidspunkt, hvor teamet oprettes. Yderligere oplysninger finder du i ["Opret et team" på side 80](#)
-
- BEMÆRK:** Hvis du bruger indstillingen **Alle brugere** eller **Relation** til at oprette et team, kan teamlederen ikke tildele opgaverne til et andet medlem af teamet.
-
- ♦ Helpdeskbrugeren kan tildele opgaven til din leder op til det hierarkiniveau, der er defineret på siden **Indstillinger**. Administratoren konfigurerer managerhierarkiet.

Hvis en opgave tildeles til dig igen, og du ikke kan tage dig af den, kan du sende opgaven tilbage til den bruger, der har tildelt opgaven til dig.

Sende anmodning tilbage

Hvis du ikke vil handle på en anmodning, der er reserveret til dig, kan du sende den pågældende anmodning tilbage. Id-programmerne tildeler automatisk den returnerede opgave til den oprindelige godkender igen.

BEMÆRK: Det er kun en gentildelt anmodning, der kan sendes tilbage.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Administration af helpdeskopgaver

Helpdesk-opgaver oprettes, når der oprettes en Helpdesk-anmodning i systemet. Ifølge eksemplet i ["Sådan fungerer helpdesk" på side 16](#) opretter Emilys anmodning en helpdeskopgave på Helens side med **opgaver**. Helen kan udføre de rette handlinger for denne helpdeskopgave.

Hvis du er helpdeskbruger, skal du vælge den helpdeskanmodning, der kræver din handling. Udfør en af følgende handlinger på den valgte helpdeskanmodning:

Opdater

Opdaterer helpdeskanmodningen med den rette kommentar.

Udført

Fuldfører helpdeskanmodningen og vedhæfter din kommentar til løsningen.

Annuler

Lukker helpdeskanmodningen med den rette kommentar.

BEMÆRK: Du kan **reservere** eller **frigive** en helpdeskopgave. Hvis du reserverer en helpdeskanmodning på listen over opgaver, vises helpdeskopgaven i dine **egne** opgaver.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

7 Sådan handler du på vegne af en anden

I visse organisationer er det måske tilladt at fuldføre opgaver som fuldmægtig eller stedfortræder for en anden. En personlig assistent kan f.eks. udføre handlinger med chefens fuldmagt. Eller hvis en kollega er på forældreorlov, kan du måske blive udnævnt til at handle på hendes vegne.

- ♦ [“Visning af fuldmægtigtildelinger” på side 51](#)
- ♦ [“Funktion som fuldmægtig” på side 51](#)
- ♦ [“Administration af fuldmægtigtildelinger” på side 51](#)

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Visning af fuldmægtigtildelinger

Hvis du vil se dine fuldmægtigtildelinger, skal du åbne dashboardet og vælge:

Adgang > **Fuldmagtstildelinger**

Funktion som fuldmægtig

En administrator kan udnævne dig til at fungere som fuldmægtig for en anden bruger. Når det sker, føjer programmer en fuldmægtigindstilling til din kontomenu i øverste højre hjørne.

Dit id > **Fuldmagt som**

Sarah Smith administrerer f.eks. Kunderelationer. Identity Applications indeholder gruppen Kunderelationer, hvor Sarah Smith er Teammanager. Hun kan handle på vegne af Maria Belafonte, der er medlem af gruppen. I dashboardet vælger hun **ssmith** > **Fuldmagt som** og angiver derefter **mbelafonte**.

Administration af fuldmægtigtildelinger

Som administrator eller teammanager kan du oprette, ændre og slette en tildeling. Hvis en teammanager skal administrere fuldmægtigtildelinger for en gruppe, skal du konfigurere gruppen til det. Teammanageren kan kun oprette tildelinger for gruppemedlemmer.

8 Administration af uddelegeringer

I nogle organisationer er det tilladt at uddelegere opgaver til en anden bruger. Hvis du uddelegerer andres opgaver, eller dine opgaver uddelegeres til andre brugere i organisationen, kan du se uddelegeringsoplysninger i **Administration > Delegering**.

Du kan se de uddelegerede opgaver på siden **Opgaver**. Opgaverne med ikonet  angiver, at opgaven er uddelegeret.

VIGTIGT: Hvis du opretter en stedfortrædertildeling, kræver det også, at du angiver dine tilgængelighedsdetaljer. Du kan enten angive dine tilgængelighedsdetaljer, når du opretter stedfortrædertildelingen, eller oprette delegeringen og derefter angive tilgængelighedsdetaljer i en særskilt handling. Det afhænger af, om administratoren har aktiveret de nødvendige indstillinger, så du kan se indstillingen **Ikke tilgængelig fra** på siden **Opret stedfortrædertildeling**. Men hvis du ikke kan se indstillingen **Ikke tilgængelig fra**, skal du angive dine tilgængelighedsdetaljer fra siden **Tilgængelighedsindstillinger**, når du har oprettet stedfortrædertildelingen. Derved sikres det, at delegeringen fungerer som forventet. Du kan finde flere oplysninger ved at klikke på  i dashboardet.

9 Administration af din tilgængelighed

Du kan angive, hvilke ressourceanmodninger med en stedfortrædertildeling du ikke er tilgængelig til at arbejde på i en bestemt periode. I den tidsperiode, hvor du ikke er tilgængelig for en bestemt anmodning, kan den bruger, der er delegeret til at handle på anmodningen, arbejde på den.

Hvis du vil se din tilgængelighed, skal du åbne dashboardet og vælge

Personer > Tilgængelighed

Før du bruger handlingen **Ikke tilgængelig fra**, skal du have mindst én stedfortrædertildeling at arbejde på. Du skal få din teamleder (eller administratoren af klargøringsprogrammer) til at oprette stedfortrædertildelinger for dig.

De globale indstillinger, der vedrører tilgængelighedsbaseret delegering, er angivet af **Angiv tilgængelighed under oprettelse af en stedfortrædertildeling** i **Indstillinger > Tilpasning > Navigationselementer > Generelt**. Hvis du foretrækker ikke at angive din tilgængelighed for hver anmodningsdefinition enkeltvist, kan du bruge **Ikke tilgængelig for nogen anmodninger fra handlingen Skift status**.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

10 Administration af din profil

I Identity Applications kan du nemt få vist og arbejde med dine identitetsoplysninger. De kan også være med til at øge effektiviteten i din organisation ved at give dig adgang til oplysningerne om andre brugere, som du skal bruge – når du har brug for det. Du vil f.eks. gøre følgende:

- ♦ Administrere din egen brugerkonto direkte
- ♦ Slå andre brugere og grupper i organisationen op efter behov
- ♦ Visualisere, hvordan disse brugere og grupper er indbyrdes relateret
- ♦ Angive programmer, som du er knyttet til

Systemadministratoren er ansvarlig for at konfigurere indholdet i Identity Applications for dig og andre i organisationen. Hvad du kan se og gøre, bestemmes typisk af dine jobkrav og dit tilladelsesniveau.

Opdatering af din profil

Hvis du vil se eller opdatere din identitetsprofil, skal du åbne dashboardet og vælge:

[\[dit id\]](#) > Profil

Eller

Klik på  i dit dashboard.

På denne side vises den leder, du rapporterer til, dine roller, dine ressourcer og din gruppe. Du skal have administratoradgang for at redigere dine oplysninger eller for at se organisationsdiagrammet.

Din profil indeholder indstillinger som dit navn, din e-mailadresse og dit telefonnummer. På denne side vises de brugerattributter, der aktiveres med adgangstilladelserne **Søg** og **Læs**. Disse adgangsegenskaber kan konfigureres i DAL (Directory Abstraction Layer). Du kan få flere oplysninger ved at se under [Attribute Properties](#) (Attributegenskaber) i [NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications). Din organisation bestemmer, hvilke indstillinger du kan ændre. Du kan f.eks. ændre dit telefonnummer, men ikke dit efternavn.

11 Administration af organisationsdiagrammet

I Identity Manager Dashboard er det nemt at søge efter en enhed i din organisation og at få vist organisationsdiagrammet (en enhed kan være en bruger, gruppe eller brugerdefineret enhed, der er konfigureret af din administrator). Et organisationsdiagram viser hierarkiet for relationer, f.eks. leder-medarbejder, gruppens medlemskab eller brugergrupper blandt enheder i din organisation.

Siden **Organisationsdiagram** i dashboardet viser som standard placeringen af en brugerenhed i organisationen og dens relationshierarki med andre brugerenheder baseret på relationen i organisationsdiagrammet, der er oprettet af administratoren. Du kan finde flere oplysninger om standardindstillingerne for siden med organisationsdiagrammet under [Customizing the Views](#) (Tilpasning af visningerne). Du kan finde flere oplysninger om, hvordan du kan få vist organisationsdiagrammer over andre enheder end brugerenheden, i [Viewing the Organization Chart of an Object](#) (Visning af organisationsdiagrammet for et objekt) i [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Organisationsdiagrammet kaldes ofte "organisationsdiagram". Begge disse begreber bruger i dashboardet.

Visning af et organisationsdiagram

Sikkerhedsadministratoren og klargøringsadministratoren kan som standard se organisationsdiagrammet for alle enheder i systemet.

Du kan navigere til organisationsdiagrammet for en brugerenhed på en af følgende måder:

- ♦ Gå til **Personer** > **Organisationsdiagram**. På denne side vises organisationsdiagrammet for den bruger, der er logget på, baseret på den standardrelation for organisationsdiagrammer, der er konfigureret på siden **Indstillinger**. Du kan også se organisationsdiagrammet ved hjælp af ikonet , der findes under **Min profil**, **Dashboard** og på siderne **Programmer**.

Du kan finde organisationsdiagrammet for andre brugere i systemet ved at skrive navnet på de andre brugere på søgelinjen, der findes på siden **Organisationsdiagram**.

- ♦ Gå til **Personer** > **Brugere**, vælg en bruger på listen, og klik på  ud for brugerens navn. Du kan finde yderligere oplysninger i [Kapitel 13, "Administration af brugere,"](#) på side 75.

BEMÆRK: Du skal have adgangstilladelsen **Organisationsdiagram** for at få vist **organisationsdiagrammet**. Kontakt din administrator for at få denne adgang. Du kan få flere oplysninger ved at se under [Brugerindstillinger](#) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Om organisationsdiagrammet

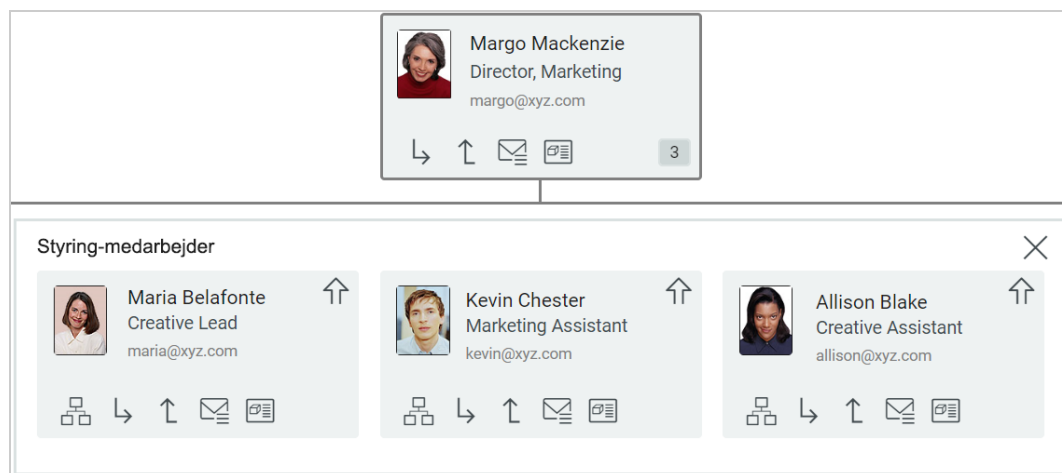
I organisationsdiagrammet vises enhedsoplysningerne i kortformat. Disse kort er arrangeret i hierarkisk rækkefølge baseret på den standardrelation for organisationsdiagrammer, der er konfigureret af administratoren. En rod eller valgt enhed, der vises øverst, er udgangspunktet eller retningspunktet i organisationsdiagrammet, og den underordnede enhed, der er direkte under rodenheden, vises nederst baseret på standardrelationen.

De enkelte kort viser oplysninger baseret på de primære og sekundære attributter, der er defineret af administratoren. Du kan finde flere oplysninger om, hvordan disse attributter kan tilpasses, i [Customizing the Organization Chart View](#) (Tilpasning af visningerne i organisationsdiagrammer) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications). Specifikt for en brugerenhed er kortet angivet til at vise brugerens fulde navn samt de primære og sekundære attributter, der er defineret af administratoren. Det betyder, at når administratoren konfigurerer fornavn og efternavn som primære attributter, vises brugerens fulde navn muligvis to gange i [Kortvisning](#) på siden [Brugere](#) og i organisationsdiagrammet.

BEMÆRK: Hvis de primære og sekundære attributter for en enhed ikke er defineret af administratoren i visningen med organisationsdiagrammer, viser Identity Applications CN-attributten for den pågældende enhed på siden [Organisationsdiagram](#).

[Figur 11-1](#) viser et eksempel på et organisationsdiagram for brugeren *Margo Mackenzie*, hvor standardrelationen for organisationsdiagrammer er angivet til Leder-medarbejder.

Figur 11-1 Eksempel på organisationsdiagrammet i dashboardet



I dette eksempel er *Margo Mackenzie* lederen, og *Maria Belafonte*, *Kevin Chester* og *Allison Blake* er medarbejdere, der rapporterer til hende. På hvert kort vises brugerens fulde navn øverst, hvilket i Margos tilfælde er *Margo Mackenzie*, efterfulgt af rollen i organisationen og e-mailadressen, der er angivet som primære og sekundære attributter af administratoren. Det tal, der vises i nederste højre hjørne af *Margo Mackenzies* kort, angiver det antal medarbejdere, der rapporterer til hende.

Arbejde med organisationsdiagrammet

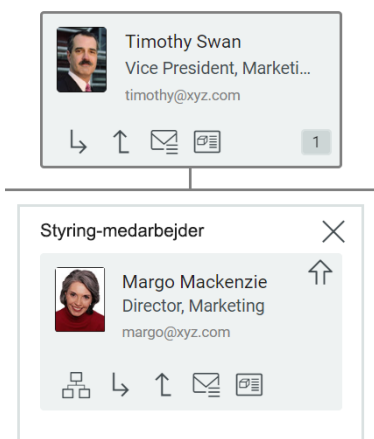
På baggrund af det søgeinput, der er angivet på siden **Organisationsdiagram**, viser dashboardet organisationsdiagrammet for enheden. Du kan udføre andre opgaver på siden, f.eks. se andre relationer for enheden, ændre rodenheden og se dens organisationsdiagram eller se organisationsdiagrammet for en enhed på næste niveau i relationshierarkiet.

For at du kan forstå mere om de opgaver, du kan udføre på siden **Organisationsdiagram**, vil vi kigge på følgende eksempel på et marketingteam i firmaet XYZ:

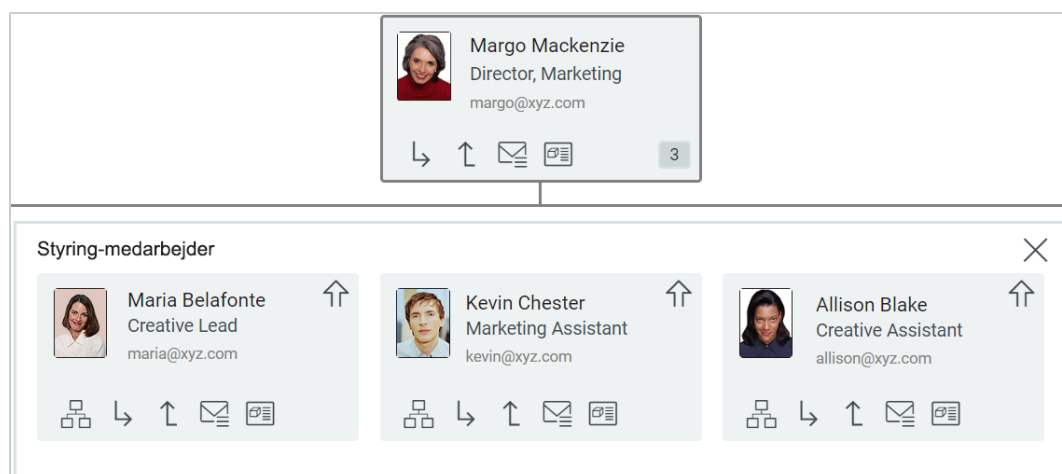
Margo Mackenzie er Director i marketingteamet, hvor *Allison Blake*, *Kevin Chester* og *Maria Belafonte* er medarbejdere, der rapporterer til hende. *Margo Mackenzie* rapporterer til *Timothy Swan*, Vice President i marketingteamet.

Gå til **Personer > Organisationsdiagram** i dashboardet, og søg efter *Timothy Swan* for at se hans organisationsdiagram. På samme måde kan du udføre en søgning efter *Margo Mackenzie*. [Figur 11-2](#) og [Figur 11-3](#) viser dig deres individuelle organisationsdiagrammer baseret på relationen Leder-medarbejder.

Figur 11-2 Organisationsdiagram for Timothy Swan i rollen som Leder.



Figur 11-3 Organisationsdiagram for Margo Mackenzie i rollen som Leder.



Lad os kigge på de opgaver, som du kan udføre på siden **Organisationsdiagram** baseret på eksemplet ovenfor:

- ♦ “Nulstille roden i visningen med organisationsdiagrammet” på side 62
- ♦ “Skifte visningen med organisationsdiagrammet” på side 62
- ♦ “Vælge en relation, du vil have vist” på side 63
- ♦ “Navigere til næste niveau i relationshierarkiet” på side 64
- ♦ “Sende e-mail til brugere fra organisationsdiagrammet” på side 65
- ♦ “Få vist detaljerede oplysninger om en bruger” på side 65

BEMÆRK: Opgaverne ovenfor gælder for både bruger- og kundeenheder.

Nulstille roden i visningen med organisationsdiagrammet

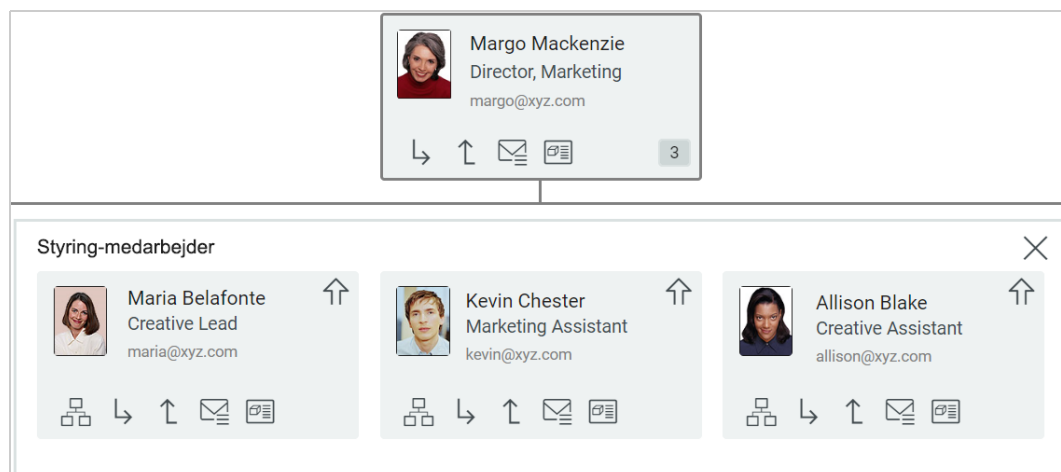
Sådan nulstiller du rodbrugeren i visningen med organisationsdiagrammet

- 1 Identificer den bruger, du vil anvende som den nye rod.

Antag, at du ser organisationsdiagrammet, hvor *Timothy Swan* har rollen som Leder, og du vil angive *Margo Mackenzie* som ny rod.

- 2 Gå til *Margo Mackenzies* kort, og klik på ikonet . Hun bliver den nye rod og er nu øverst i organisationsdiagrammet for Leder-medarbejder. De medarbejdere, der rapporterer til *Margo Mackenzie*, dvs. *Maria Belafonte*, *Kevin Chester* og *Allison Blake*, vises under hende.

Figur 11-4 *Margo Mackenzie som ny rod i visningen med organisationsdiagrammet*



Skifte visningen med organisationsdiagrammet

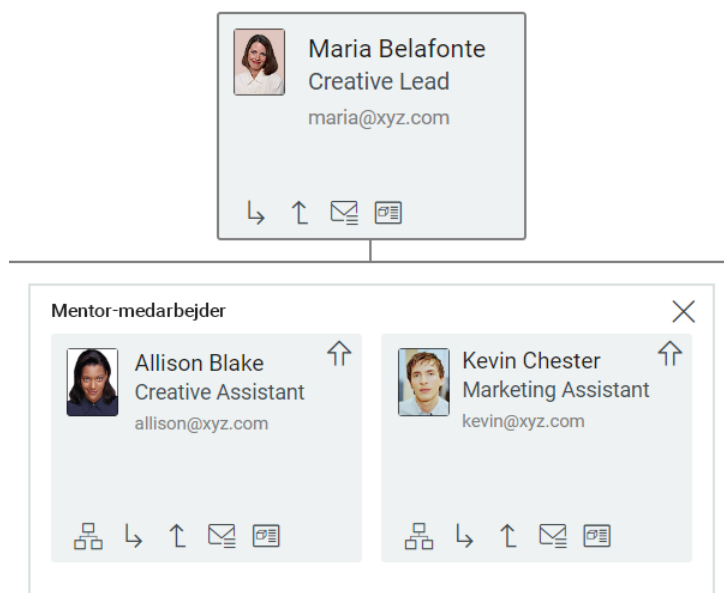
Hvis du vil nulstille rodbrugeren og standardrelationen i din visning med organisationsdiagrammet, skal du udføre følgende handlinger:

- 1 Identificer den bruger, hvis organisationsdiagram du vil have vist.

Antag, at du ser organisationsdiagrammet, hvor *Margo Mackenzie* har rollen som Leder. *Maria Belafonte*, medarbejderen under *Margo Mackenzie*, er også mentor for *Kevin Chester* og *Allison Blake*. Du ønsker at se relationen Mentor-medarbejder for *Maria Belafonte*.

- 2 Gå til *Maria Belafontes* kort, og klik på .
- 3 I rullemenuen skal du vælge relationen **Mentor-medarbejder**. *Maria Belafonte* bliver roden i organisationsdiagrammet for Mentor-medarbejder, og *Kevin Chester* og *Allison Blake* vises som medarbejdere under hende.

Figur 11-5 Organisationsdiagram for *Maria Belfonte* i rollen som Mentor



Vælge en relation, du vil have vist

Hvis du vil se relationen for en anden bruger end standarden, skal du udføre følgende handlinger:

- 1 Identificer den bruger, hvis relation du vil have vist.
Antag, at du ser organisationsdiagrammet, hvor *Margo Mackenzie* har rollen som Leder. Du ønsker at se brugergrupperelationen for *Maria Belafonte*, der er en del af marketinggruppen.
- 2 Gå til *Maria Belafontes* kort, og klik på .
- 3 I rullemenuen skal du vælge relationen **Brugergrupper**. Diagrammet over *Maria Belafontes* gruppemedlemskab tilføjes internt i den eksisterende visning med organisationsdiagrammet.

BEMÆRK: Det højeste niveau, du kan udvide organisationsdiagrammet til for en bruger og se relationen internt, defineres af administratoren. Du kan som standard udvide op til niveau 3, hvor niveau 1 altid er tildelt til rodbrugeren.

Navigere til næste niveau i relationshierarkiet

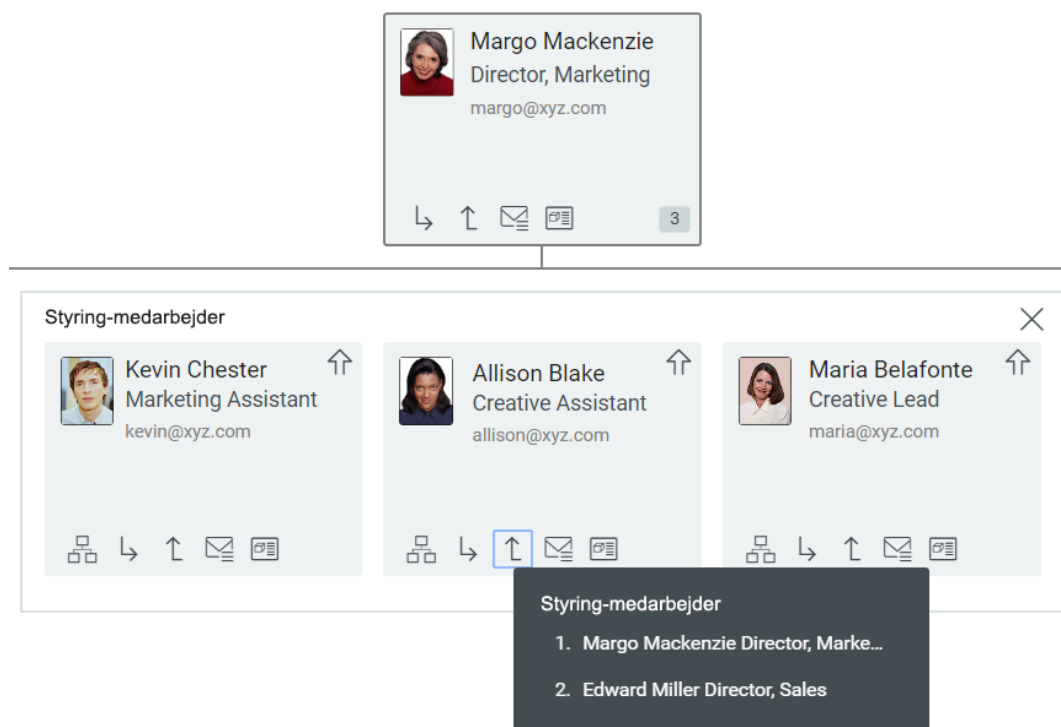
For at forstå denne opgave kan vi kigge på et andet eksempel med *Edward Miller*, der er Director i salgsteamet. *Allison Blake* og *Filla Martell* er direkte underordnede i forhold til *Edward Miller*. Som du kan se, er *Allison Blake* et almindeligt medlem af salgs- og marketingteamet og rapporterer til to ledere, nemlig *Edward Miller* og *Margo Mackenzie*.

Hvis du vil navigere til og udvide næste niveau i relationstræet, skal du udføre følgende handlinger:

- 1 Identificer den bruger, du vil have vist og navigere til næste niveau for i hierarkiet.
Antag, at du ser organisationsdiagrammet, hvor *Margo Mackenzie* har rollen som Leder, og du ønsker at se organisationsdiagrammet for *Allison Blake*.
- 2 Gå til *Allison Blakes* kort, klik på , og vælg den rekursive relation Leder-medarbejder på listen.
- 3 Klik på .

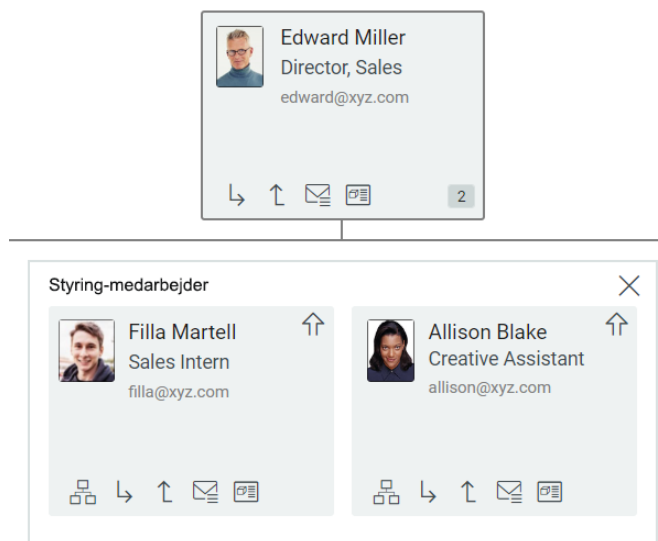
I rullemenuen Leder-medarbejder viser medarbejderen *Allison Blake* to ledere, nemlig *Margo Mackenzie* og *Edward Miller*, som hun rapporterer til.

Figur 11-6 Den rekursive relation Leder-medarbejder for *Allison Blake*



- 4 Vælg lederen, *Edward Miller*. Organisationsdiagrammet for *Allison Blake* vises.

Figur 11-7 Organisationsdiagram for Allison Blake



Sende e-mail til brugere fra organisationsdiagrammet

Ved hjælp af indstillingen  kan du:

- Sende en e-mail til den valgte bruger.
- Dele profillinket for en enhed via e-mail.
- (Valgfrit. Gælder kun for relationen Leder-medarbejder) Sende en e-mail til alle teammedlemmer under den valgte bruger.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

VIGTIGT:

- Før du sender en e-mail fra visningen med organisationsdiagrammet, skal du sikre dig, at der er konfigureret en standard-e-mailklient i dit system.
 - Du kan sikre, at indstillingerne **Ny e-mail** og **Send e-mail til team** fungerer, ved at konfigurere e-mailattributten som primær eller sekundær attribut på siden Indstillinger. Du kan få flere oplysninger ved at se under [Brugerindstillinger](#) i *NetIQ Identity Manager - Administrator's Guide to Identity Applications* (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).
-

Få vist detaljerede oplysninger om en bruger

- 1 Identificer den bruger, hvis oplysninger du vil have vist.

Antag, at du ser organisationsdiagrammet, hvor *Margo Mackenzie* har rollen som Leder, og du ønsker at se yderligere detaljer, f.eks. roller og ressourcer, der er tildelt til *Kevin Chester*.

- 2 Gå til *Kevin Chesters* kort, og klik på ikonet . Profilsiden viser detaljerede oplysninger, herunder de roller og ressourcer, der er tildelt til ham.

Hvis du ikke kan se ikonet  på en brugers kort, f.eks. *Jack Millers* kort, der er President i XYZ-organisationen, betyder det, at du ikke har de rette tilladelser til brugerkataloget og derfor ikke kan se hans profil. Kontakt din administrator, hvis du skal bruge den nødvendige adgang for at se en profil.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

12 Administration af din adgangskode

Identity Manager omfatter Self Service Password Reset (SSPR), der gør det muligt at administrere processen til ændring af adgangskoder og nulstille glemte adgangskoder. Under nulstilling af adgangskoden anvender SSPR en challenge/response-godkendelsesmetode til at godkende dig.

- ♦ [“Brug af selvbetjent styring af adgangskoder i Identity Manager” på side 67](#)
- ♦ [“Brug af styring af gamle adgangskoder” på side 69](#)

BEMÆRK: I dette afsnit beskrives standardfunktionerne til administration af din adgangskode. Du kan støde på nogle forskelle på grund af jobrolle, sikkerhedsniveau og tilpasninger, der er foretaget for organisationen. Kontakt systemadministratoren for at få yderligere oplysninger.

Brug af selvbetjent styring af adgangskoder i Identity Manager

SSPR integreres automatisk med processen til enkeltlogon for Identity Applications og identitetsrapportering. Det er standardprogrammet til styring af adgangskoder til Identity Manager. Når en bruger anmoder om nulstilling af en adgangskode, kræver SSPR, at brugeren skal besvare spørgsmålet i forbindelse med verificeringssvar. Hvis svarene er korrekte, reagerer SSPR på en af følgende måder:

- ♦ Giver brugere mulighed for at oprette en ny adgangskode
- ♦ Opretter en ny adgangskode og sender den til brugeren
- ♦ Opretter en ny adgangskode, sender den til brugeren, og markerer den gamle adgangskode som udløbet.

Du kan konfigurere dette svar i SSPR Configuration Editor. Når du har opgraderet til en ny version af Identity Manager, kan du konfigurere SSPR til at bruge den NMAS-metode, som Identity Manager traditionelt har brugt til adgangskodestyring. SSPR genkender dog ikke dine eksisterende adgangskodepolitikker til styring af glemte adgangskoder. Du kan også konfigurere SSPR til at bruge dets ophavsretligt beskyttede protokol i stedet for NMAS. Hvis du foretager denne ændring, kan du ikke gå tilbage til at bruge NMAS uden at nulstille dine adgangskodepolitikker.

Du kan bruge SSPR til at udføre de funktioner, der er angivet i [Tabel 12-2, “Funktioner i Adgangskodestyring,” på side 70](#):

Tabel 12-1 Funktioner i Adgangskodestyling

Med denne adgangskodestylingsside	Kan du
Verificeringssvar til adgangskode	Angive eller ændre følgende: ♦ Dine gyldige svar på administratordefinerede verificeringsspørgsmål ♦ Brugerdefinerede verificeringsspørgsmål og -svar
Skift adgangskode	Ændre (nulstille) din adgangskode i henhold til de regler, der er fastlagt af systemadministratoren
Status for adgangskodepolitik	Gennemgå kravene til adgangskodepolitik.

Om challenge/response for adgangskode

Verificeringsspørgsmål bruges til at bekræfte din identitet under logon, når du har glemt din adgangskode. Hvis systemadministratoren har oprettet en adgangskodepolitik, som aktiverer denne funktion for dig, kan du bruge siden Verificeringssvar til adgangskode til at:

- ♦ Angive svar, der er gyldige for dig ved besvarelse af administratordefinerede spørgsmål
- ♦ Angive dine egne spørgsmål og gyldige svar på dem (hvis adgangskodepolitikken giver mulighed for dette)

Logonsiden dirigerer dig automatisk til challenge/response-siden under logonprocessen. Du kan konfigurere svarene på verificeringsspørgsmålene på denne side. Yderligere oplysninger finder du i ["Hvis du glemmer din adgangskode" på side 21](#). Når du logger på igen og forsøger at nulstille den glemte adgangskode, stiller SSPR de konfigurerede spørgsmål og beder dig om at give det rigtige svar. Når svaret matcher det svar, du har gemt tidligere, gør SSPR det muligt at nulstille adgangskoden.

Ændring af adgangskoden

Du kan ændre adgangskoden (forudsat at systemadministratoren har givet dig tilladelse til dig).

- 1 I dashboardet skal du klikke på **Programmer > Skift min adgangskode**.
- 2 Skriv din nuværende adgangskode. Siden Skift adgangskode åbnes.



- 3 Skriv den nye adgangskode i tekstboksen **Ny adgangskode**.
- 4 Skriv den nye adgangskode igen i tekstboksen **Bekræft adgangskode**.
- 5 Klik på **Skift adgangskode**.

Hvis din nye adgangskode overtræder nogen af de adgangskoderegler, der er defineret i adgangskodepolitikken af administratoren, vises der en fejlmeddelelse på siden Skift adgangskode.

Denne side indeholder typisk oplysninger om, hvordan du angiver en adgangskode, der overholder de regelkrav, som din administrator har defineret. Gennemgå adgangskodereglerne, og prøv igen.

- 6 Klik på **Fortsæt**. Status for anmodningen vises. Hvis det lykkes, føres du tilbage til OSP-logonsiden.

Status for adgangskodepolitik

BEMÆRK: Denne funktion er kun tilgængelig for administratorer.

Du er tildelt en adgangskodepolitik af administratoren. Politikken fastlægger de sikkerhedsforanstaltninger, der er knyttet til din adgangskode. Du kan ikke kontrollere regelkravene i din adgangskode, medmindre brugerprogrammets administrator har givet dig rettigheder til at gøre dette. Administratoren af brugerprogrammet kan kontrollere statussen på adgangskodereglerne på Identity Manager-startsiden. Dette link findes ikke som standard. Du skal tilpasse startsiden, så det medtages. Hvis du vil tilpasse standardelementerne på Identity Manager-hjemmesiden, kan du se [Kapitel 5, "Administration af programmer," på side 43](#).

Klik på linket **Adgangskodestatus og -regler** på landingssiden. Siden **Adgangskodestatus og -politik** vises. Hvis du vil ændre din adgangskode til Identity Manager, skal du gå til Identity Manager-startsiden og vælge Skift adgangskode. Linket på Identity Manager-startsiden omdirigerer dig til området til skift af adgangskode i SSPR.

Brug af styring af gamle adgangskoder

I dette afsnit beskrives det, hvordan du bruger siderne til Adgangskodestyling under fanen **Selvbetjening af identitetsinformation** i Identity Manager-brugerprogrammet. Emnerne omfatter:

- ["Verificeringssvar til adgangskode" på side 70](#)
- ["Ændring af adgangskodetip" på side 71](#)
- ["Skift adgangskode" på side 71](#)
- ["Status for adgangskodepolitik" på side 72](#)
- ["Status for adgangskodesynkronisering" på side 72](#)

BEMÆRK: I dette afsnit beskrives standardfunktionerne på siderne til Adgangskodestyling. Du kan støde på nogle forskelle på grund af jobrolle, sikkerhedsniveau og tilpasninger, der er foretaget for organisationen. Kontakt systemadministratoren for at få yderligere oplysninger.

Mere generelle oplysninger om adgang til og arbejde med fanen **Selvbetjening af identitetsinformation** finder du i [Kapitel 10, "Administration af din profil," på side 57](#).

Du kan bruge siderne til Adgangskodestyling til at udføre de funktioner, der er angivet i [Tabel 12-2, "Funktioner i Adgangskodestyling," på side 70](#):

Tabel 12-2 Funktioner i Adgangskodestyling

Med denne adgangskodestylingsside	Kan du
Verificeringssvar til adgangskode	Angive eller ændre følgende: ♦ Dine gyldige svar på administratordefinerede verificeringsspørgsmål ♦ Brugerdefinerede verificeringsspørgsmål og -svar
Ændring af adgangskodetip	Angive eller ændre dit adgangskodetip
Skift adgangskode	Ændre (nulstille) din adgangskode i henhold til de regler, der er fastlagt af systemadministratoren
Status for adgangskodepolitik	Gennemgå kravene til adgangskodepolitik.
Status for adgangskodesynkronisering	Vise status for synkronisering af programadgangskoder med identitetsboksen BEMÆRK: Hvis programmer åbnes inden gennemførelse af synkronisering, medfører det problemer med programadgang.

Verificeringssvar til adgangskode

Verificeringsspørgsmål bruges til at bekræfte din identitet under logon, når du har glemt din adgangskode. Hvis systemadministratoren har oprettet en adgangskodepolitik, som aktiverer denne funktion for dig, kan du bruge siden Verificeringssvar til adgangskode til at:

- ♦ Angive svar, der er gyldige for dig ved besvarelse af administratordefinerede spørgsmål
- ♦ Angive dine egne spørgsmål og gyldige svar på dem (hvis adgangskodepolitikken giver mulighed for dette)

Sådan bruges siden Verificeringssvar til adgangskode:

- 1 Klik på **Verificeringssvar til adgangskode** i menuen (under **Adgangskodestyling**) under fanen **Selvbetjening af identitetsinformation**.

Siden Verificeringssvar til adgangskode åbnes.

- 2 Skriv et korrekt svar i hver tekstboks til **Svar** (de er alle obligatoriske), eller brug dine tidligere gemte svar. Verificeringssvarene, herunder etiketterne, vises ikke, når **Brug lagret svar** er markeret. Derudover er brugerdefinerede verificeringsspørgsmål deaktiveret.

Sørg for at angive svar, du kan huske senere.

- 3 Angiv eller rediger brugerdefinerede spørgsmål, der er obligatoriske. Du må ikke bruge det samme spørgsmål mere end én gang.

- 4 Klik på **Send**.

Når du har gemt verificeringssvarene, viser brugerprogrammet en meddelelse om, at verificeringssvarene blev gemt, og skærmen med verificeringssvar åbnes igen med "Brug lagret svar?" markeret.

Ændring af adgangskodetip

Et adgangskodetip bruges under logon som hjælp til at huske din adgangskode, når du har glemt den. Brug siden Ændring af adgangskodetip til at angive eller ændre adgangskodetippet.

- 1 Klik på **Ændring af adgangskodetip** i menuen (under **Adgangskodestyring**) under fanen **Selvbetjening af identitetsinformation**.

Siden Definer adgangskodetip åbnes.

- 2 Skriv den nye tekst til tippet.

Adgangskoden kan ikke vises i teksten til tippet.

- 3 Klik på **Send**.

Status for anmodningen vises.

Skift adgangskode

Du kan bruge denne side, når det er nødvendigt at ændre adgangskoden (forudsat at systemadministratoren har gjort det muligt).

- 1 Klik på **Skift adgangskode** i menuen (under **Adgangskodestyring**) under fanen **Selvbetjening af identitetsinformation**.

Siden Skift adgangskode åbnes. Hvis systemadministratoren har oprettet en adgangskodepolitik for dig, indeholder siden Skift adgangskode typisk oplysninger om, hvordan der angives en adgangskode, som opfylder politikens krav. For eksempel:

Hvis der ikke anvendes nogen adgangskodepolitik, vil du se den grundlæggende Skift adgangskode-side, som blot indeholder felter til at ændre din adgangskode.

Brugerprogrammet understøtter følgende syntakstyper til adgangskoder:

- ♦ Microsoft-kompleksitetspolitik

Denne syntakstype til adgangskoder anvendes til bagudkompatibilitet med Active Directory 2003.

- ♦ Microsoft Server 2008-adgangskodepolitik

Dette er en ny syntakstype til adgangskoder, der er føjet til eDirectory 8.8.7 for at understøtte Active Directory 2008.

Følgende indstillinger understøttes med Microsoft Server 2008-adgangskodepolitik:

- ♦ Brug Microsoft Server 2008-adgangskodepolitik
- ♦ Maksimalt antal overtrædelser af kompleksitetspolitikken i adgangskode (0-5)

- ♦ Novell-syntaks

Følgende nye indstillinger understøttes med Novell-syntaksen:

- ♦ Mindste antal ikke-alfabetiske tegn (1-512)
- ♦ Højeste antal ikke-alfabetiske tegn (1-512)

Brugerprogrammet understøtter følgende funktioner for alle tre typer syntaks for adgangskoder:

- ♦ Antal tegn, der er forskellige fra den aktuelle adgangskode og adgangskoder fra historikken (0-6)
- ♦ Antal adgangskoder fra historikken, hvor tegn skal udelades (0-10)

Hvis din administrator har aktiveret regelsyntaksen for Microsoft Server 2008, skal følgende felter udfyldes på siden **Skift adgangskode**:

- 2 Skriv den nuværende adgangskode i tekstboksen **Gammel adgangskode**.
- 3 Skriv den nye adgangskode i tekstboksen **Ny adgangskode**.
- 4 Skriv den nye adgangskode igen i tekstboksen **Indtast adgangskode igen**.
- 5 Klik på **Send**.

Hvis din nye adgangskode overtræder nogen af de adgangskoderegler, der er defineret af administratoren, vises der en fejlmeddelelse på siden **Skift adgangskode**. Hvis du bruger Microsoft Server 2008-politik, og din adgangskode ikke overholder reglerne, vises denne meddelelsen øverst på siden:

Password AD2008 complexity policy violation.

Hvis din nye adgangskode ikke overholder reglerne, skal du gennemgå de adgangskoderegler, der er defineret af administratoren, og prøve igen.

- 6 Du kan blive bedt om at angive et adgangskodetip, hvis administratoren har konfigureret sikkerhedspolitikken til det. Se i så fald "[Ændring af adgangskodetip](#)" på side 71.
- 7 Status for anmodningen vises.

Status for adgangskodepolitik

Du er tildelt en adgangskodepolitik af administratoren. Politikken fastlægger de sikkerhedsforanstaltninger, der er knyttet til din adgangskode. Du kan kontrollere adgangskodepolitikens krav som følger:

- 1 Klik på **Status for adgangskodepolitik** i menuen (under **Adgangskodestyring**) under fanen **Selvbetjening af identitetsinformation**. Siden **Status for adgangskodepolitik** åbnes.

Du kan ikke ændre elementer, der er angivet som ugyldige.

Status for adgangskodesynkronisering

Brug siden Status for adgangskodesynkronisering til at fastlægge, om din adgangskode er blevet synkroniseret på tværs af programmer. Prøv kun at få adgang til et andet program, når adgangskoden er synkroniseret. Hvis programmer åbnes inden gennemførelse af synkronisering, medfører det problemer med programadgang.

- 1 Klik på **Status for adgangskodesynkronisering** i menuen (under **Adgangskodestyring**) under fanen **Selvbetjening af identitetsinformation**. Siden **Status for adgangskodesynkronisering** åbnes. Ikoner med normale farver angiver programmer, som adgangskoden er synkroniseret for. Nedtonede ikoner angiver programmer, som endnu ikke er synkroniseret.

BEMÆRK: Kun administratoren kan se boksen **Vælg bruger**.

IV Administration af brugere, grupper og teams

Hvis du har den rette rolle i Identity Applications, kan du oprette og administrere brugere, grupper og teams. Du kan oprette brugere og teams i dashboardet og brugerprogrammet. Du kan oprette og administrere grupper i brugerprogrammet.

Systemadministratorer kan oprette brugere og grupper. Systemadministratoren kan give andre (typisk udvalgte personer i administrations- eller ledelsesstillinger) adgang til denne funktion.

Du kan støde på nogle forskelle fra funktioner, der er dokumenteret i dette afsnit, på grund af din jobrolle, dit sikkerhedsniveau og tilpasninger, der er foretaget for organisationen. Kontakt systemadministratoren for at få oplysninger.

Et team repræsenterer brugere, grupper eller brugere og grupper, der kan udføre klargøringsanmodninger og godkendelsesopgaver, der er knyttet til teamet. Selv om et team matcher en gruppe, der findes i brugerbiblioteket, er teams ikke det samme som grupper. Dvs. at en gruppe eller et medlem af en gruppe ikke kan udføre teamfunktioner, medmindre de er tildelt til et team. Se [Kapitel 14, "Administration af teams," på side 79](#).

13 Administration af brugere

I dette afsnit beskrives, hvordan du kan oprette brugere og grupper i dashboardet og brugerprogrammet. Emnerne omfatter:

- ♦ “Oprettelse af en bruger” på side 75
- ♦ “Redigering af brugeroplysninger” på side 75
- ♦ “Visning af brugere” på side 76
- ♦ “Søgning efter brugere” på side 77
- ♦ “Sortering af brugere” på side 78

Oprettelse af en bruger

På siden **Opret bruger** vises de brugerattributter, der aktiveres med adgangstilladelserne **Søg** og **Læs**. Disse adgangsegenskaber kan konfigureres i DAL (Directory Abstraction Layer). Du kan få flere oplysninger ved at se under [Attribute Properties](#) (Attributegenskaber) i [NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Hvis du vil oprette en bruger, skal du åbne dashboardet og vælge:

Personer > Brugere > +

Identitetsadministratoren definerer de værdier, som du kan angive for brugeren. Og når du opretter en bruger, kan du se brugerens **container**, men du kan ikke ændre værdien. Denne begrænsning sikrer, at alle brugere gemmes i den samme container.

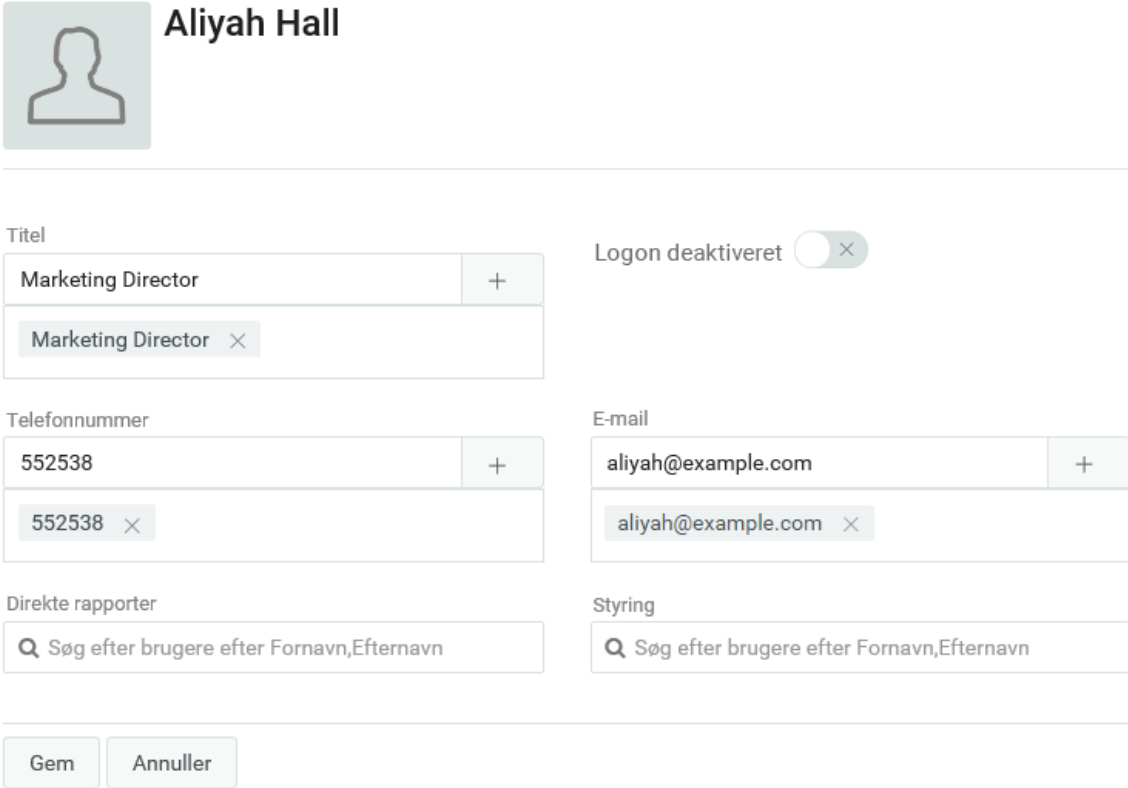
Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Redigering af brugeroplysninger

Vælg en bruger i en listevisning, og klik på  for at redigere brugeroplysningerne, f.eks. titel, e-mail, telefonnummer, leder osv. Du har tilladelse til at redigere de brugerattributter, som er indstillet af din administrator. Du kan finde flere oplysninger om konfiguration af brugerattributter under [Customizing the Views](#) (Tilpasning af visningerne) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications). Du kan slette brugere i visningen **Administrer brugere**.

Her er et eksempel på redigering af brugeroplysninger:

Figur 13-1 Redigering af brugeroplysninger



The image shows a user profile editing interface for a user named Aliyah Hall. At the top left is a placeholder for a profile picture. To the right of the picture is the name 'Aliyah Hall'. Below this, there are several sections for editing user information:

- Titel**: A text input field containing 'Marketing Director' with a '+' button to the right. Below it is a dropdown menu showing 'Marketing Director' with a close button (X).
- Logon deaktiveret**: A toggle switch that is currently turned off (grey).
- Telefonnummer**: A text input field containing '552538' with a '+' button to the right. Below it is a dropdown menu showing '552538' with a close button (X).
- E-mail**: A text input field containing 'aliyah@example.com' with a '+' button to the right. Below it is a dropdown menu showing 'aliyah@example.com' with a close button (X).
- Direkte rapporter**: A search bar with the placeholder text 'Søg efter brugere efter Fornavn,Efternavn'.
- Styring**: A search bar with the placeholder text 'Søg efter brugere efter Fornavn,Efternavn'.

At the bottom of the form are two buttons: 'Gem' (Save) and 'Annuller' (Cancel).

BEMÆRK: Til/fra-knappen **Logon deaktiveret** kan bruges til at deaktivere en brugerkonto. Knappen er kun synlig, hvis administratoren tilføjer attributten **Logon deaktiveret** i Kortvisning og Redigerbare attributter under **Indstillinger** > siden **Tilpasning**. Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Visning af brugere

Du kan få vist brugere i id-programmer på følgende måder:

- **Listevisning:** Hvis du vil have vist brugerne i listeformat, skal du klikke på . Derved vises der brugeroplysninger i højre side. Hvis du vil redigere brugeroplysninger, f.eks. Telefonnummer, E-mail, Manager m.m., skal du klikke på . Hvis du vil have vist organisationsdiagrammet for en bestemt bruger, skal du klikke på .
- **Kortvisning:** Hvis du vil have vist brugerne i kortformat, skal du klikke på . Derved vises der grundlæggende oplysninger på kortene. Administratoren kan konfigurere, hvilke oplysninger der skal vises på brugerens kort. Du kan få flere oplysninger ved at se under [Customizing the Views](#) (Tilpasning af visningerne) i [NetIQ Identity Manager - Administrator's Guide to Identity Applications](#) (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications). Klik på  for at redigere brugeroplysningerne, f.eks. **Telefonnummer**, **E-mail**, **Leder** og andre attributter. Hvis du vil se organisationsdiagrammet for en bestemt bruger, skal du klikke på .

- ♦ **Visningen Administrer brugere:** Hvis du vil have vist brugerne i tabelformat, skal du klikke på . Viser brugerne i en tabelvisning. I denne visning kan du sortere brugere i overensstemmelse med brugerattributter, f.eks. telefonnummer, e-mail, afdeling osv. Du kan tilpasse, hvilke kolonner der skal vises i denne visning. Du kan finde flere oplysninger om tilpasning af kolonner ved at klikke på  i dashboardet.

I denne visning kan du også slette brugere fra systemet. Sådan sletter du brugere:

1. Vælg en bruger, du vil slette.
2. Klik på .

Søgning efter brugere

Du kan søge efter brugere i id-programmer på følgende måder:

- ♦ **Lynsøgning:** Angiver brugerattributter og viser brugerne afhængigt af de valgte filtre. Sådan ændrer du filterindstillinger:

1. Klik på .
2. Vælg filterindstillinger for at søge efter brugere.

Her er et eksempel på de valgte brugerattributter for en lynsøgning:



☒	Fornavn
☒	Efternavn
☐	Titel
☐	Afdeling
☐	Region
☒	E-mail
☒	Telefonnummer

3. Klik på **Filtrer**.

Hvis du f.eks. vil søge efter en bruger med navnet Smith, hvor filtrene Fornavn og Efternavn er valgt. Lynsøgning viser alle brugere, der har Smith som fornavn og efternavn.

- ♦ **Avanceret søgning:** Denne indstilling henter en mere begrænset liste over brugere end lynsøgning. Du kan søge efter en bruger med de definerede brugerattributter. Sådan bruger du avanceret søgning:

1. Klik på .
2. Angiv de nøjagtige brugeroplysninger for de enkelte brugerattributter.

Her er et eksempel på de angivne brugerattributter for en avanceret søgning:

AVANCERET SØGNING



Søg efter

Fornavn	▼	Emily	×
Efternavn	▼	Cameron	×
E-mail	▼	emily.cameron@example.com	×
Telefonnummer	▼	5552368	×
+ Tilføj			

3. Klik på **Filtrer**.

Hvis du f.eks. vil søge efter en bruger, hvor **Fornavn** er Aliyah, **Efternavn** er Hall, og **Titel** er Director. Du kan angive disse attributter i den avancerede søgning for at søge efter en bruger, der har præcist dette sæt attributter.

Du kan også konfigurere søgeresultaterne på en side ved at angive indekset nederst. Et dashboard bruger VLV-styring (Virtual List View), der kører på LDAP OID 2.16.840.1.113730.3.4. Dette fungerer i kombination med sorteringsstyring.

Identity Manager Dashboard viser to forskellige optællinger, når resultaterne vises:

- ♦ **Samlet antal:** Det er det samlede antal brugere, der er fundet i systemet.
- ♦ **Antal brugere efter søgning:** Det er antallet af brugere, der vises for en bestemt søgning.

Sortering af brugere

I visningen Administrer brugere kan du sortere brugere efter deres attributter. Administratoren skal konfigurere sammensatte indekser for brugerattributterne for at aktivere sortering. Du kan finde flere oplysninger om sammensatte indekser under [Creating Compound Indexes](#) (Oprettelse af sammensatte indekser) i [NetIQ Identity Manager Install and Upgrade Guide for Windows](#) (NetIQ Identity Manager – Installations- og opgraderingsvejledning til Windows).

BEMÆRK: Hvis du ikke kan sortere brugere ved hjælp attributter, kan du kontakte din administrator for at få konfigureret sammensatte indekser for den påkrævede attribut, så du kan sortere brugere.

14 Administration af teams

Et team består af to typer brugere:

Anmoder

Foretager anmodninger om tilladelser på vegne af andre teammedlemmer (modtagerne). Afhængigt af hvordan teamet er konfigureret, kan en anmoder handle på en individuel klargøringsanmodning, en eller flere kategorier af anmodninger eller alle anmodninger. Administrerer også fuldmagtstildelingerne til teammedlemmer.

Modtager

Medlem af det team, som anmodere kan handle på vegne af.

Teammodtagere kan være brugere eller grupper inden for biblioteket. Eller de kan være afledt gennem biblioteksrelationer. Medlemslisten kan f.eks. være afledt af forholdet mellem leder og medarbejder i organisationen. I dette tilfælde vil teammodtagerne være alle brugere, der rapporterer til teamlederen.

BEMÆRK: Administratoren af klargøring kan konfigurere DAL (Directory Abstraction Layer) til at understøtte overlappende relationer, så flere niveauer inden for en organisation kan inkluderes i et team. Hvor mange niveauer der skal inkluderes, kan konfigureres af administratoren.

Hvis du vil udføre en af følgende aktiviteter, skal du gå til **Personer > Teams**:

- ♦ ["Få vist teams" på side 79](#)
- ♦ ["Opret et team" på side 80](#)
- ♦ ["Rediger et team" på side 80](#)

Få vist teams

Siden **Teams** viser alle de teams, du har tilladelser til at vise. Du kan være medlem af alle de viste teams. Du kan dog også være administrator med tilladelser til at vise, redigere eller slette bestemte teams, selv om du ikke er medlem.

Som teammedlem kan du være **anmoder** og foretage anmodninger på vegne af andre teammedlemmer. Andre i teamet kan også være i stand til at udføre disse handlinger for dig, som **modtager**. Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Opret et team

Som administrator kan du oprette teams. Et **team** repræsenterer brugere, grupper eller brugere og grupper, der kan udføre klargøringsanmodninger og godkendelsesopgaver, der er knyttet til teamet.

For hvert team angiver du de teammedlemmer (**Modtagere**), der modtager teamets tilladelser, og dem, der kan handle på modtageres vegne (**Anmodere**). Når du har oprettet et team, kan du angive de **Tilladelser** (definitioner af ressourcer og klargøringsanmodninger), der gælder for teammedlemmer. Du kan f.eks. tilføje en laptopressource, som teammedlemmer kan blive bedt om at have.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

Rediger et team

Som administrator kan du redigere og slette teams. Du kan redigere følgende aspekter af et team:

- ♦ Ændre navn og beskrivelse af teamet.
- ♦ Ændre anmodere for teamet.
- ♦ Tilføje eller fjerne teammedlemmer.
- ♦ Tilføje eller fjerne tilladelser for en teamleder.

Du kan finde flere oplysninger ved at klikke på  i dashboardet.

15 Håndtering af grupper

En gruppe består af brugere og andre konti, der har fælles egenskaber. Økonomigruppen består f.eks. af alle medarbejdere i økonomiafdelingen.

Der kan søges efter grupper ud fra beskrivelsen. Men administratorer, der har adgang til siden **Indstillinger**, kan tilpasse attributterne, og ud fra dem kan der søges i en gruppeenhed. Det betyder, at når du søger efter en bestemt gruppe, mens du tildeler en rolle til en gruppe, gør en gruppe til ejer af en ressource eller udfører en simpel søgning på siden **Grupper**, returnerer programmet navnene i gruppen som et resultat, der opfylder søgekriterierne. Du kan få flere oplysninger ved at se under **Entity Settings** (Enhedsindstillinger) i *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager – Administratorvejledning i design af Identity Applications).

Oprettelse af en gruppe

Hvis du har en administrativ rolle i Identity Applications, kan du oprette en gruppe.

- 1 Gå til **Personer > Grupper** i Identity Manager Dashboard.
- 2 Klik på +.
- 3 Angiv værdier for følgende obligatoriske attributter:

Attribut	Angiv følgende
Navn	Gruppenavnet på denne nye gruppe. VIGTIGT: Brug ikke følgende specialtegn i feltet Navn : < ; \ " + # / * ~
Beskrivelse	En beskrivelse af denne nye gruppe. Beskrivelsen bruges som gruppesøgekriterie i dashboardet. VIGTIGT: Brug ikke følgende specialtegn i feltet Beskrivelse : ~
Beholder	En organisationsenhed i den identitetsboks, hvor den nye gruppe skal lagres (f.eks. en OU med navnet Grupper). For eksempel: ou=groups,ou=MyUnit,o=MyOrg Oplysninger om at bruge de viste knapper til at angive en beholder findes i "Oprettelse af en bruger" på side 75 . BEMÆRK: Du bliver ikke bedt om Beholder , hvis systemadministratoren har fastlagt en standardoprettelsesbeholder til denne objekttype.

- 4 Klik på **Opret**.

Når gruppen er oprettet, vises panelet **Gruppemedlemmer**, hvor du kan føje brugerne til den gruppe, der netop er oprettet.

- 5 Hvis du vil føje brugere til gruppen, skal du klikke på ikonet + ud for gruppemedlemmerne.
- 6 Vælg de ønskede brugere i modalvinduet.
- 7 Klik på **Tilføj**.

V Appendiks

Følgende appendiks indeholder yderligere referenceoplysninger og avancerede emner til Identity Manager-brugerprogrammet.

A Brug af godkendelsesapplikationen til Identity Manager

Ud over den brugergrænseflade, der anvendes af Identity Manager-kunderne, kan du nu bruge en ny iOS-app, der giver Identity Manager-brugere mulighed for at fjerngodkende eller -afvise anmodninger via modulet til rollebaseret klargøring til Identity Manager.

Når du har installeret og konfigureret godkendelsesapplikationen, kan du se de samme godkendelsesopgaver i applikationen, som du normalt ville se på grænsefladen i brugerprogrammet. Alle ændringer synkroniseres mellem godkendelsesapplikationen og brugerprogrammet.

Du kan også arbejde offline, når forbindelsen til Identity Managers rollebaserede klargøringsmodulserver er afbrudt. Så synkroniserer godkendelsesapplikationen automatisk ændringerne, når forbindelsen genoprettes.

Dette appendiks indeholder oplysninger om, hvordan du installerer og bruger den nye godkendelsesapplikation. Du kan finde oplysninger om, hvordan Identity Manager-administratorer kan konfigurere deres miljø, så brugerne kan anvende applikationen, under [“Configuring the Identity Manager Approvals App”](#) (Konfigurere Identity Manager-godkendelsesapplikation) i *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications* (NetIQ Identity Manager – Administrationsvejledning til Identity Applications).

Du kan få mere detaljerede oplysninger om godkendelsesapplikationen i følgende afsnit:

- ♦ [“Produktkrav” på side 85](#)
- ♦ [“Installere godkendelsesapplikationen” på side 86](#)
- ♦ [“Konfigurere godkendelsesapplikationen” på side 86](#)
- ♦ [“Oversigt over godkendelsesapplikationen” på side 90](#)
- ♦ [“Ændre visningssproget for godkendelsesapplikationen” på side 92](#)

Produktkrav

Godkendelsesappen kræver en Apple iPhone eller iPad med Apple iOS 6 eller iOS 7 installeret eller en enhed med Android 5.0 eller nyere.

BEMÆRK: Hvis din administrator ikke har givet mulighed for brug af godkendelsesapplikationen, kan du muligvis ikke konfigurere applikationen efter installationen. Du kan finde oplysninger om, hvordan administratorer kan konfigurere Identity Manager-miljøet, så det er muligt at bruge godkendelsesprogrammet, under [“Configuring the Identity Manager Approvals App”](#) (Konfiguration af Identity Manager-godkendelsesprogrammet) i *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications* (NetIQ Identity Manager – Administrationsvejledning i design af Identity Applications).

Installere godkendelsesapplikationen

Du kan installere NetIQ Identity Manager-godkendelsesapplikationen fra siden til [godkendelsesapplikationen](#) i Apple App Store på din enhed.

Når du har installeret godkendelsesapplikationen, skal du derefter konfigurere den til at oprette forbindelse til din rollebaserede klargøringsmodulserver.

BEMÆRK: Hvis din adgangskode til brugerprogrammet er udløbet, anbefaler vi, at du udskifter din adgangskode, før du installerer og konfigurerer godkendelsesapplikationen. Hvis adgangskodepolitikken i dit miljø tillader et begrænset antal logonforsøg, når en adgangskode udløber, kan godkendelsesapplikationen bruge alle disse logons i et forsøg på at synkronisere dine Identity Manager med din enhed.

Konfigurere godkendelsesapplikationen

Du kan konfigurere NetIQ Identity Manager-godkendelsesapplikationen på flere måder, afhængigt af hvad dit miljø kræver, og den måde, din administrator har konfigureret Identity Manager på:

- ♦ Foretag en anmodning i brugerprogrammets grænseflade for at få adgang til godkendelsesapplikationen, og start derefter applikationen på din enhed via det e-maillink, du har fået af din Identity Manager-administrator. Linket indeholder alle de krævede konfigurationsoplysninger.
- ♦ Klik på et konfigurationslink, eller scan en konfigurations-QR-kode ved at bruge din enhed, hvor link eller QR-kode enten angiver alle de krævede konfigurationsoplysninger eller generaliserede konfigurationsoplysninger for din virksomhed.
- ♦ Angiv konfigurationsoplysningerne for dit miljø manuelt i selve applikationen.

VIGTIGT: For at brugerne automatisk kan konfigurere godkendelsesapplikationen ved brug af enten et link eller en QR-kode, skal administratoren af Identity Manager-miljøet først aktivere linket eller QR-koden.

Anmode om mobiladgang via brugerprogrammet

Hvis din administrator har konfigureret det, kan du anmode om adgang til godkendelsesapplikationen via brugerprogrammet. Identity Manager sender derefter en e-mail, der indeholder et tilpasset link, du kan åbne på din enhed, for automatisk at konfigurere applikationen med dine oplysninger.

Sådan anmoder du om mobiladgang via brugerprogrammet:

- 1 Log på Identity Manager-brugerprogrammet i en webbrowser ved hjælp af HTTPS-protokollen (<https://>).

BEMÆRK: Hvis du vil bede om adgang til godkendelsesapplikationen, skal du logge på brugerprogrammet ved hjælp af HTTPS-protokollen.

- 2 Klik på [Foretag en procesanmodning](#).

- 3 Klik på rullemenuen Procesanmodning, og vælg **Konti**.
- 4 Klik på **Fortsæt**.
- 5 Klik på **Anmod om mobil godkendelsesapplikation**.

BEMÆRK: Navn og kategori for procesanmodningen kan variere, afhængigt af hvordan din administrator har konfigureret anmodningsprocessen for godkendelsesapplikationen.

- 6 Angiv de krævede oplysninger i procesanmodningsformularen, og klik på **Send**.
- 7 Når du modtager en e-mail fra din Identity Manager-administrator, skal du åbne den på din enhed og klikke på det angivne link for at oprette forbindelse mellem din enhed og din rollebaserede klargøringsmodulserver.

BEMÆRK: Hvis du tidligere har installeret applikationen, kan den vise en advarselsmeddelelse om, at eksisterende indstillinger kan blive overskrevet. Sørg for, at det værtsnavn, der vises i advarselsmeddelelsen, er den samme vært som den, du havde adgang til, da du bad om adgang til applikationen. Hvis du er i tvivl, skal du ikke klikke på linket. Kontakt i stedet din administrator.

Hvis værtsnavnet er korrekt, skal du klikke på **Accepter** for at overskrive dine eksisterende indstillinger.

- 8 Når applikationen startes, skal du angive din adgangskode og klikke på ikonet Test forbindelse  for at bekræfte dine indstillinger.

Brug af et konfigurationslink eller en QR-kode

Din Identity Manager-administrator kan angive et konfigurationslink til at konfigurere din godkendelsesapplikation. Åbn linket i en browser på din enhed for automatisk at konfigurere applikationen.

Dette link kan dog kun angive nogle af de krævede indstillinger. Et link eller en kode kan typisk kun give den rollebaserede klargøringsmodulserver de oplysninger, der er nødvendige for, at godkendelsesapplikationen fungerer. Når du klikker på linket, skal du manuelt konfigurere dine indstillinger for Brugernavn og Adgangskode samt andre indstillinger, der ikke er indstillet automatisk.

I visse miljøer har du muligvis ikke adgang til dine e-mails på din enhed. Hvis du ikke kan modtage e-mail på din enhed, kan du i stedet bruge din enhed til at scanne en personligt tilpasset QR-kode, som du får fra Identity Manager-administratoren.

Vis om nødvendigt den QR-kode, du har fået, på din computer eller en udskreven side, og scan koden ved hjælp af en QR-kodelæser på din enhed. Når QR-koden automatisk har konfigureret godkendelsesapplikationen til dit miljø, skal du manuelt konfigurere dine indstillinger for Brugernavn og Adgangskode.

Konfigurere godkendelsesapplikationen manuelt

Hvis administratoren af dit Identity Manager-miljø ikke angiver et link eller en QR-kode, du kan bruge, når du skal konfigurere godkendelsesapplikationen, kan du også konfigurere de nødvendige konfigurationsindstillinger manuelt.

ADVARSEL: Da en manuel konfiguration af applikationen på din enhed kræver dybdegående viden om Identity Manager-komponenter, anbefaler vi, at det kun er superbrugere med viden om det rollebaserede klargøringsmodul og brugerprogrammiljøet i din virksomhed, der kan konfigurere applikationsindstillingerne manuelt. Andre brugere bør kontakte deres Identity Manager-administrator for at få oplysninger om, hvordan de konfigurerer applikationen.

Klik på indstillingsikonet  i applikationen, angiv de krævede indstillinger og klik derefter på ikonet Test forbindelse  for at bekræfte dine indstillinger.

Godkendelsesapplikationen kræver følgende indstillinger:

Navn på logonindstilling	Beskrivelse af logonindstilling
Brugernavn	Angiver det brugernavn, du bruger til at få adgang til den rollebaserede klargøringsmodulserver.
Adgangskode	Angiver den adgangskode, du bruger til at få adgang til den rollebaserede klargøringsmodulserver.
Datasykronisering	Angiver, om applikationen aktivt skal synkronisere data med den rollebaserede klargøringsmodulserver.
Avanceret > Serveroplysninger > Server	Angiver det fulde domænenavn eller IP-adressen på den rollebaserede klargøringsmodulserver.
Avanceret > Serveroplysninger > Sikker port	Angiver den HTTPS-port, som applikationen bruger til at oprette forbindelse til serveren.
Avanceret > Serveroplysninger > Kontekst	Angiver den kontekst, der bruges, når brugerprogrammets WAR-fil installeres. Standardværdien er IDMProv.
Avanceret > Serveroplysninger > Brugerbeholder	Angiver det fulde DN for den Identity Vault-beholder, der gemmer brugeroplysninger.
Avanceret > Serveroplysninger > Timeout	Angiver det antal sekunder, applikationen venter, under forsøg på at oprette forbindelse til serveren, før forbindelsen annulleres. Standardværdien er 5 sekunder.
Avanceret > Datadefinitionsindstillinger > Brugerenhed	Angiver den LDAP-enhed, der repræsenterer en bruger i Identity Vault. Standardværdien er user.
Avanceret > Datadefinitionsindstillinger > Navneformat	Angiver den DAL-attributrepræsentation, som applikationen bruger til at formatere en brugers fulde navn. Standardværdien er FirstName LastName.
Avanceret > Datadefinitionsindstillinger > Attributten Fornavn	Angiver det navn på DAL-attributten, der repræsenterer en brugers fornavn. Standardværdien er FirstName.
Avanceret > Datadefinitionsindstillinger > Attributten Efternavn	Angiver det navn på DAL-attributten, der repræsenterer en brugers efternavn. Standardværdien er LastName.

Navn på logonindstilling	Beskrivelse af logonindstilling
Avanceret > Datadefinitionsindstillinger > Attributten Brugerfoto	Angiver det navn på DAL-attributten, der indeholder en brugers foto. Standardværdien er <code>UserPhoto</code>. BEMÆRK: Hvis du ikke har konfigureret et billede i Identity Manager eller har konfigureret indstillingerne i Identity Manager til ikke at vise et billede, viser applikationen i stedet et generisk billede.
Avanceret > Datadefinitionsindstillinger > Attributten Arbejdstelefon	Angiver det navn på DAL-attributten, der repræsenterer en brugers arbejdstelefonnummer. Standardværdien er <code>TelephoneNumber</code> .
Avanceret > Datadefinitionsindstillinger > Attributten Mobiltelefon	Angiver det navn på DAL-attributten, der repræsenterer en brugers mobilnummer. Standardværdien er <code>mobile</code> .
Avanceret > Datadefinitionsindstillinger > Attributten E-mail	Angiver det navn på DAL-attributten, der repræsenterer en brugers e-mailadresse. Standardværdien er <code>Email</code> .
Avanceret > Datadefinitionsindstillinger > Attributten Foto-LDAP	Angiv navnet på den LDAP-attribut, der indeholder brugerens foto. Standardværdien er <code>photo</code> .
Avanceret > Datadefinitionsindstillinger > Navneattribut	Angiver den DAL-attribut for navngivning, der bruges i Identity Vault til at beskrive et navn. Standardværdien er <code>cn</code> .
Avanceret > Datadefinitionsindstillinger > Klargøringsadministrator	Angiver, om du er en klargøringsadministrator for den rollebaserede klargøringsmodulserver.
Avanceret > Accepterede certifikater	Angiver eventuelle ugyldige eller selvsignerede certifikater fra den rollebaserede klargøringsmodulserver, som du tillader, at godkendelsesapplikationen kan acceptere. Når godkendelsesapplikationen detekterer et selvsigneret eller ugyldigt certifikat, beder applikationen om at acceptere eller afvise certifikatet. Hvis du accepterer certifikatet, føjer applikationen certifikatet til listen over accepterede certifikater. Du kan fjerne et certifikat fra listen over accepterede certifikater ved at klikke på navnet på certifikatet og genstarten applikationen. BEMÆRK: Hvis certifikatet til den rollebaserede klargøringsmodulserver er gyldigt, føjer applikationen ikke certifikatet til listen over accepterede certifikater. Applikationen accepterer som standard gyldige certifikater.

Navn på logonindstilling	Beskrivelse af logonindstilling
Avanceret > Afviste certifikater	Angiver eventuelle ugyldige eller selvsignerede certifikater fra den rollebaserede klargøringsmodulserver, som du ikke tillader, at godkendelsesapplikationen kan acceptere. Når godkendelsesapplikationen detekterer et selvsigneret eller ugyldigt certifikat, beder applikationen om at acceptere eller afvise certifikatet. Hvis du afviser certifikatet, føjer applikationen certifikatet til listen over afviste certifikater. Hvis serveren derefter viser et afvist certifikat, kan applikationen ikke oprette forbindelse til serveren. Du kan fjerne et certifikat fra listen over afviste certifikater ved at klikke på navnet på certifikatet.

Oversigt over godkendelsesapplikationen

Dette afsnit indeholder en oversigt over brugergrænsefladen til NetIQ Identity Manager-godkendelsesapplikationen. Emnerne omfatter:

- ♦ [“Opgavevisning” på side 90](#)
- ♦ [“Detaljevisning” på side 91](#)
- ♦ [“Massetilstand” på side 91](#)
- ♦ [“Visning af afsluttede opgaver” på side 91](#)
- ♦ [“Visningen Logonindstillinger” på side 92](#)
- ♦ [“Visningen Avancerede indstillinger” på side 92](#)

Opgavevisning

Godkendelsesapplikationens standardvisning er i opgavevisningen. Denne visning viser alle de opgaver, der i øjeblikket er tildelt til eller krævet af dig, med opgavens titel og navnet og billedet på opgavemodtageren. Visningen angiver opgaver efter udløbsdato, viser de opgaver, der snarest forfalder, og opgaver uden forfaldsdato nederst.

BEMÆRK

- ♦ Hvis en bruger ikke har konfigureret et billede i Identity Manager eller har konfigureret indstillingerne i Identity Manager til ikke at vise et billede, viser applikationen i stedet et generisk billede.
- ♦ Hvis du bruger godkendelsesappen, kan du ikke godkende eller afvise opgaver, der bruger komplekse formularer.
- ♦ Godkendelsesappen understøtter i øjeblikket ikke nye JSON-formularer på både iOS- og Android-plattformen. Derfor modtager du muligvis en fejlmeddelelse, eller du kan måske ikke se opgavedetaljerne.

Hvis du vil godkende eller afvise en anmodning, eller hvis du vil vise detaljerne for en bestemt opgave, skal du klikke på opgaven eller navnet på modtageren af opgaven. Hvis du vil kontakte en opgavemodtager, skal du klikke på modtagerens billede.

Detaljevisning

Detaljevisningen angiver detaljer for en bestemt opgave, du er blevet tildelt. Felterne varierer afhængigt af anmodningen.

Hvis du vil godkende eller afvise en opgave, skal du angive eventuelle nødvendige oplysninger og klikke på enten **Godkend** eller **Afvis**.

Massetilstand

Hvis det er nødvendigt at godkende eller afvise et stort antal lignende opgaver, kan du skifte fra standardtilstanden til enkeltopgaver til massetilstanden i opgavevisningen.

BEMÆRK: Du kan ikke godkende alle opgaver i massetilstanden. Når det gælder mere komplekse opgaver som f.eks. attesteringer, skal du godkende hver enkelt attesteringsopgave separat i enkeltopgavetilstanden. Når du klikker på ikonet for massetilstand, viser applikationen kun de opgaver på listen, der kan godkendes i massetilstand.

Sådan godkendes eller afvises flere opgaver:

- 1 Klik på ikonet for massetilstand i opgavevisningen .
- 2 Vælg de opgaver, du vil godkende eller afvise. Du kan ikke godkende nogle opgaver og afvise andre på samme tid.
- 3 (Valgfrit) Hvis du vil godkende eller afvise alle opgaver, skal du klikke på **Alle**.
- 4 (Valgfrit) Hvis du skifter mening og ikke vil godkende eller afvise nogen opgaver, skal du klikke på ikonet for enkeltopgavetilstand .
- 5 Klik på **Godkend** eller **Afvis**.
- 6 (Valgfrit) Angiv en kommentar om massehandlingen.
- 7 Klik på **Bekræft**.

Visning af afsluttede opgaver

Du kan få vist dine afsluttede opgaver ved at klikke på ikonet for afsluttede opgaver . Visningen viser den afsluttede opgave samt det tidspunkt, hvor opgaven blev godkendt eller afvist. Du kan klikke på en afsluttet opgave for at få vist detaljerne for hver enkelt opgave. Når det gælder mere komplekse opgaver, kan du klikke på **Formularværdier** for at få vist specifikke oplysninger om anmodningen.

Hvis det er nødvendigt, kan du slette en eller flere af dine afsluttede opgaver i visningen af afsluttede opgaver. Hvis du vil slette opgaver, skal du klikke på ikonet for massetilstand , vælge de opgaver, du vil slette, og klikke på **Slet**.

BEMÆRK: Visningen af afsluttede opgaver viser kun opgaver, der er afsluttet på din enhed. Du kan ikke få vist opgaver, der er afsluttet i brugerprogrammet eller på en anden enhed, hvor godkendelsesapplikationen er installeret.

Visningen Logonindstillinger

Visningen Logonindstillinger gør det muligt at få vist eller ændre dine logonindstillinger.

ADVARSEL: Hvis din Identity Manager-administrator har angivet et link eller en QR-kode, så dine applikationsindstillinger kan konfigureres automatisk, anbefaler vi, at du ikke ændrer disse standardindstillinger, medmindre din administrator beder dig om at gøre dette.

Visningen Avancerede indstillinger

Visningen Avancerede indstillinger gør det muligt at få vist eller ændre avancerede indstillinger, der bestemmer, hvordan du modtager data fra den rollebaserede klargøringsmodulserver.

ADVARSEL: Hvis din Identity Manager-administrator har angivet et link eller en QR-kode, så dine applikationsindstillinger kan konfigureres automatisk, anbefaler vi, at du ikke ændrer disse standardindstillinger, medmindre din administrator beder dig om at gøre dette.

Hvis du ved et uheld ændrer datadefinitionsindstillingerne i visningen Avancerede indstillinger, skal du klikke på **Gendan standardindstillinger** for at gendanne de standardindstillinger, som Identity Manager har angivet. **Gen standardindstillinger** ændrer ikke dit brugernavn, din adgangskode eller nogen af serverdetaljeoplysningerne.

Ændre visningssproget for godkendelsesapplikationen

Godkendelsesapplikationen indeholder lokaliserede strenge på flere sprog. Hvis du vil ændre det sprog, som godkendelsesapplikationen anvender, skal du ændre indstillingerne for sprog- og områdeformatet på din iOS-enhed. Indstillingerne for områdeformatet konfigurerer, hvordan datoer, tidspunkter og telefonnumre vises på enheden.

Sådan ændrer du indstillinger for sprog og område:

- 1 Klik på **Indstillinger** på din iOS-enhed.
- 2 Klik på **Generelt**.
- 3 Klik på **International**.
- 4 (Valgfrit) Hvis du vil ændre det sprog, som anvendes af din enhed, skal du klikke på **Sprog**, vælge det sprog, du vil bruge, og derefter klikke på **Udfør**.
- 5 (Valgfrit) Hvis du vil ændre det områdeformat, din enhed bruger til datoer og tidspunkter, skal du klikke på **Områdeformat**, vælge det format, du vil bruge, og klikke på **International**.
- 6 Gå tilbage til enhedens startside.