VGR behörighetsportal, teknisk dokumentation v 1.0
Datum

Anslutningsdokument - active directory (AD)

Innehåll

Anslutningsdokument - active directory (AD) 1

Sammanfattning 3

Målgrupp och ansvar 3

Så här funkar det 4

Så här gör du – steg för steg 5

Steg 1 - Förberedelser 5

Steg 2 – Skapa beställning 6

Steg 3 – Vi sätter upp anslutningen 6

Steg 4 – Test och driftsättning 6

Testmiljö (RTC) 6

Det här behöver vi från dig 9

Det här får du automatiskt 10

Tekniska riktlinjer (kortversion) 10

Frågor och mer information 13

Teknisk kravbilaga – detaljerade specifikationer 13

Tilldelningspolicy (automatisk tilldelning) 16

VGR behörighetsportal (Omada Identity) hanterar tilldelning och borttag av behörigheter i verksamhetens IT-system. För de flesta applikationer sker detta genom koppling till Active Directory (AD) – den vanligaste och rekommenderade metoden. Denna vägledning beskriver hur du gör, vad vi behöver från dig, och vad du får automatiskt när din applikation ansluts till portalen via AD.

Syftet med detta dokument är att ge en enkel och tydlig vägledning för hur en applikation ansluts till VGR behörighetsportal via Active Directory, samt en teknisk kravbilaga för mer detaljerad information.

VGR behörighetsportal är Västra Götalandsregionens centrala plattform för styrning av identiteter och behörigheter och bygger på etablerade principer inom Identity Governance and Administration (IGA). För en övergripande beskrivning av plattformens arkitektur, begrepp och anslutningsmodeller, se dokumentet Inledning och generell beskrivning.

AD är i nuläget den rekommenderade anslutningsmodellen för applikationer som kan hantera behörigheter via gruppmedlemskap. Modellen bygger på att åtkomst till applikationer realiseras genom medlemskap i AD-grupper, vilket möjliggör en standardiserad, skalbar och förvaltningsbar integration.

Behörighetsstyrningen i VGR behörighetsportal utgår från applikationsroller, som representerar verksamhetsmässig åtkomst. Dessa roller kopplas till AD-grupper som används för att tekniskt realisera behörigheter i anslutna system. Denna uppdelning möjliggör en tydlig separation mellan verksamhetslogik och teknisk implementation.

Tilldelning av behörigheter sker i första hand automatiskt via tilldelningspolicyer. Policyer baseras på attribut från masterdata, där KIV utgör den primära källan för identitets- och organisationsinformation. Genom att använda policybaserad tilldelning kan behörigheter styras konsekvent utifrån exempelvis organisatorisk tillhörighet, uppdrag eller roll, vilket minskar behovet av manuell hantering och minimerar risken för felaktiga eller kvarhängande behörigheter.

Manuell beställning används som komplement i de fall där åtkomst inte kan styras fullt ut via policy eller där särskild prövning krävs.

Den övergripande målsättningen är att i så hög utsträckning som möjligt använda standardiserade och policybaserade mekanismer för tilldelning, samt att använda etablerade integrationsmönster, såsom AD-grupper, för att tekniskt realisera behörigheter i anslutna system.

Sammanfattning

- Vad & varför: Dokumentet beskriver hur en applikation ansluts till VGR behörighetsportal (Omada Identity) via Active Directory (AD) för att säkerställa enhetlig, spårbar och automatiserad tilldelning och borttag av behörigheter.
- Vem: Riktar sig till systemägare och berörda resursägare som ansvarar för applikationsroller och AD-grupper.
- Hur: Åtkomst modelleras som applikationsroller som kopplas till en eller flera AD-grupper. All tilldelning i VGR behörighetsportal sker via applikationsroller, medan AD-grupper används som teknisk implementation för att realisera behörigheter i anslutna system. Tilldelning sker automatiskt via policy (rekommenderat) eller manuellt via beställning med stöd för godkännandeflöden.
- När: Processen startar när du vill ansluta ett system till portalen och genomförs i fyra steg: Förberedelser → Beställning → Konfiguration → Test & driftsättning.
- Var: Beställning görs i Serviceportalen (KB0028399) med tillhörande Excel-underlag.
- Resultat: Du får automatiserad provisionering av AD-gruppmedlemskap, självservicebeställning, stöd för godkännanden, loggning, stöd för revision samt stöd för automatiserade avslut. Återkallelse vid uppdragsslut samt loggning och stöd för revision.

Målgrupp och ansvar

Detta dokument riktar sig till de roller som är involverade i anslutning av applikationer till VGR behörighetsportal via Active Directory (AD), samt i den löpande förvaltningen av behörigheter.

Följande roller är vanligt förekommande involverade:

Systemägare
Här avses rollen "Systemägare" i VGR behörighetsportal. Ansvarar för applikationen ur ett verksamhets- och säkerhetsperspektiv. Säkerställer att behörighetsmodellen är korrekt utformad och att rätt personer har rätt åtkomst. Systemägare fungerar ofta som beslutsfattare vid tilldelning av behörigheter och kan ingå i godkännandeflöden.

Applikationsansvarig / produktägare
Ansvarar för den operativa och tekniska hanteringen av applikationen. Tar fram underlag för anslutning, definierar hur applikationsroller kopplas till AD-grupper samt säkerställer att integration och behörighetstilldelning fungerar som avsett.

Informationsägare
Ansvarar för att åtkomst till informationstillgångar är korrekt utifrån verksamhetens krav och gällande regelverk. Säkerställer att behörighetsmodellen är förenlig med riktlinjer för informationssäkerhet och åtkomst.

Resursägare (valfritt beroende på upplägg)
Kan anges för applikationsroller och/eller AD-grupper och används främst i godkännandeflöden samt vid revision av behörigheter. Ansvarar för att ta ställning till tilldelning och fortsatt behov av åtkomst.

Systemägare ansvarar för vad åtkomst innebär och vem som ska ha den, medan applikationsansvarig ansvarar för hur detta implementeras och fungerar tekniskt.

Beroende på applikationens storlek och komplexitet kan en och samma person inneha flera av ovanstående roller.

Det är systemägarens ansvar att säkerställa att relevanta roller är identifierade inför anslutning samt att kontaktuppgifter hålls uppdaterade över tid.

Så här funkar det

När en applikation kopplas till behörighetsportalen via AD:

- Ett **logiskt system (applikation)** skapas i VGR behörighetsportal som representerar din applikation.

Du definierar **applikationsroller** som behörighetsteamet konfigurerar upp (exempel nedan för att hjälpa modelleringen):

- **Basanvändare** – normal åtkomst för dagligt arbete (läs/skriv i applikationens huvudflöden)
- **Läsbehörighet** – read-only åtkomst (granskning, revision, introduktion)

    - **Funktionsroll: Förskrivare/Beställare** – skapa/godkänna ordrar eller ärenden i systemet
    - **Systemadministratör** – full administrativ åtkomst för konfiguration och masterdata
    - **Rapportör/Analytiker** – åtkomst till rapport- och analysfunktioner
    - **Tillfällig/Projektroll** – tidsbegränsad åtkomst för projekt/trainee/vikarier
- Varje applikationsroll kopplas till en eller flera AD-grupper. Medlemskap i dessa grupper används för att realisera behörigheter i applikationen.
- När en användare får en applikationsroll tilldelad via VGR-behörighetsportal blir personen automatiskt medlem i rätt AD-grupp(er).

behörighetsportalen hanterar både **automatiska tilldelningar** (via policy) och **manuella beställningar** (med godkännande vid behov). För båda fallen tilldelas medlemskap automatiskt i rätt AD-grupper omedelbart.

Applikationsroller representerar verksamhetsmässig åtkomst och är det som exponeras i VGR behörighetsportal. Varje applikationsroll kopplas till en eller flera AD-grupper som används för att realisera åtkomsten tekniskt i applikationen.

Så här gör du – steg för steg

Steg 1 - Förberedelser

- Identifiera **systemägare** och **resursägare** för applikationen (det kan vara samma person/personer om man vill, används bl.a. för olika typer av godkännandeflöden och revision).
- Definiera **applikationsroller** för applikationen och ange vilka **AD-grupper** som ska kopplas till respektive roll.
- Bestäm om tilldelningen ska ske **automatiskt** (policy) eller via **beställning** eller om båda ska användas.
- Fyll i underlaget ”Ansökan anslutning VGR behörighetsportal.xlsx” (AD-fliken), gäller båda

flikarna, ”Anslutning” & ”AD Grupper”. OBS! Läs hela detta dokument först inklusive den tekniska kravbilagan. Underlaget (Excel-filen) finnas att ladda ner via Serviceportalen som en bilaga till följande kunskapsartikel.

Steg 2 – Skapa beställning

- Gå till Serviceportalen och skapa en beställning enlig kunskapsartikel.
- Bifoga den ifyllda Excel-filen. Gäller båda flikarna, ”Anslutning” & ”AD Grupper”. Observera att i nuläget är det enbart universella grupper och personliga AD-konton som hanteras, mer detaljerad information finns i Teknisk kravbilaga – detaljerade specifikationer.
- Vi kontaktar dig för eventuell komplettering.

Steg 3 – Vi sätter upp anslutningen
Behörighetsteamet gör följande:

- Skapar applikationen i VGR behörighetsportal.
- Skapar applikationsroller och kopplar AD-grupper.
- Konfigurerar tilldelningspolicyer och godkännandeflöden.

Steg 4 – Test och driftsättning
När anslutningen är konfigurerad genomförs test och verifiering innan lösningen tas i drift i produktionsmiljö. Syftet är att säkerställa att behörighetsmodellen fungerar korrekt, att tilldelning och borttag av åtkomst sker som förväntat samt att applikationen konsumerar AD-gruppmedlemskap enligt avsett arbetssätt.

Testmiljö (RTC)

Test och verifiering genomförs i VGR:s gemensamma testmiljö RTC.

RTC omfattar:

- VGR behörighetsportal testinstans
- ett test-AD med fiktiva data
- ett test-KIV med fiktiv identitets- och organisationsdata

Detta möjliggör end-to-end-test av hela flödet, från identitetsdata och tilldelningslogik till faktisk åtkomst i applikationen.

Följande ska säkerställas inför test:

- applikationen är korrekt uppsatt i VGR behörighetsportal (RTC)
- applikationen är ansluten till test-AD i RTC
- relevanta AD-grupper finns tillgängliga i testmiljön
- applikationen kan läsa och tillämpa gruppmedlemskap från test-AD

Om applikationen har flera egna miljöer, till exempel QA eller motsvarande, bör dessa mappas mot RTC för test och motsvarande struktur säkerställas inför produktion.

Verifiering

Följande bör verifieras i RTC:

- att applikationsroller är korrekt uppsatta och kopplade till rätt AD-grupper
- att tilldelning av applikationsroller leder till korrekt medlemskap i AD-grupper i test-AD
- att borttag av applikationsroller tar bort medlemskap i AD-grupper
- att applikationen ger rätt åtkomst baserat på AD-gruppmedlemskap
- att manuella beställningar fungerar enligt konfigurerade godkännandeflöden
- att eventuella tilldelningspolicyer fungerar enligt definierad logik baserat på testdata i KIV

Verifieringen bör omfatta både teknisk funktion och att behörigheterna motsvarar verksamhetens behov.

Roller i test och verifiering

Test och verifiering genomförs i samverkan mellan:

- teamet för VGR behörighetsportal
- representanter för den anslutande applikationen, till exempel applikationsansvarig
- systemägare eller verksamhetsrepresentant för verifiering av åtkomst och behörighetsnivåer
- vid behov AD- eller infrastrukturresurser

Syftet är att säkerställa att både teknisk implementation och verksamhetskrav uppfylls.

Go-live-kriterier

Inför driftsättning i produktion ska de tester som parterna gemensamt har kommit överens om vara genomförda och godkända.

Detta inkluderar normalt att:

- applikationsroller och AD-grupper är verifierade
- godkännandeflöden är testade, vid manuell tilldelning
- tilldelningspolicyer är verifierade mot testdata i KIV, om sådana används
- berörda roller, till exempel systemägare och applikationsansvarig, har godkänt lösningen

Driftsättning i produktion

Efter godkänd test och verifiering i RTC genomförs driftsättning i produktionsmiljö.

Detta innebär att:

- applikationen konfigureras i VGR behörighetsportal (produktion)
- motsvarande applikationsroller och kopplingar till AD-grupper sätts upp i produktions-AD
- godkännandeflöden och policyer etableras enligt testad konfiguration

När detta är klart blir applikationsrollerna beställningsbara i VGR behörighetsportal och tilldelning av behörigheter sker för verkliga användare via AD-gruppmedlemskap.

Det här behöver vi från dig

För att kunna planera, modellera och sätta upp din anslutning smidigt behöver vi två typer av underlag:

1. **Systemunderlag** – beskriver applikationen, rollerna och hur åtkomst bör fungera ur verksamhetsperspektiv.
2. **Tekniskt underlag** – beskriver vilka AD-grupper som kopplas till respektive applikationsroll och hur dessa realiserar åtkomsten i applikationen.

Exakt vilken information vi behöver finns i underlaget som ska fyllas i (”*Ansökan anslutning VGR behörighetsportal.xlsx*”).

All tilldelning sker via applikationsroller. AD-grupper används för att tekniskt implementera dessa.

Tips på kvalitet i Excel-underlaget

- Använd beskrivande namn på applikationsrollerna som tydligt visar vad de innebär och komplettera även med mer omfattande beskrivningar. Bra namn på applikationsrollerna underlättar både att snabbt förstå vad applikationsrollens syfte är samt att det går att använda i sökningar när behörigheter beställs manuellt. Finns det enkla och bra sökord för användarna underlättar det väldigt mycket för användarna i beställningsprocessen.
- Använd en konsekvent namnsättning på applikationsrollerna för att göra det enhetligt.
- Lägg en **rad per miljö** om behörighet behöver finnas i flera miljöer.

Det här får du automatiskt

- Vid användning av tilldelningspolicys: automatisk tilldelning av applikationsroller (och då indirekt gruppmedlemskap) baserat på uppsatta kriterier.
- Självservicebeställning i portalen (vid manuell tilldelning).
- Automatisk provisionering av själva gruppmedlemskap till AD (gäller både policy och vid manuell tilldelning).
- Stöd för **godkännandeflöden** (linjechef, systemägare, resursägare)
- Automatisk **återkallelse** av manuellt tilldelade behörigheter när användares sista uppdrag på förvaltningen som den beställdes för upphör.
- Loggning, spårbarhet och stöd för revision.

Tekniska riktlinjer (kortversion)

Applikationsroller i VGR behörighetsportal är en kombination av en eller flera ingående AD-grupper (se nästa kapitel för beskrivning). När en användare tilldelas en applikationsroll (via policy eller manuellt via beställningsprocessen) får användaren automatiskt medlemskap i alla ingående AD-grupper. Applikationsrollerna ska ha beskrivande namn samt en tillhörande mer detaljerad beskrivning.

AD-grupper används som tekniska behörighetsresurser och kopplas alltid till applikationsroller. De exponeras inte direkt för beställning i VGR behörighetsportal. Här kommer en kortversion av nuvarande riktlinjer för AD-grupper som ska ingå i applikationsroller och hanteras via VGR behörighetsportal. Detta kommer att ändras framöver då VGR behörighetsportal utökar stöd för t.ex. fler kontotyper med mera.

- Endast **universella (U)** grupper används.
  - Gruppnamn ska börja med: .u.app., .u.sp., .u.as., eller .u.fs..
- Innehåll: **endast personkonton (VGR-ID)**, inga SA/KA- eller delade konton eller liknande.
- Ägarskap: minst en **resursägare** ska anges.
- Medlemskap hanteras **endast via VGR behörighetsportalen**.

Tilldelning av applikationsroller i VGR behörighetsportal kan ske på två huvudsakliga sätt: automatisk tilldelning via policy eller manuell beställning. Båda sätten kan användas parallellt beroende på applikationens och verksamhetens behov.

Automatisk tilldelning, via policy, används när det finns tydliga och stabila regler för vilka personer som ska ha en viss åtkomst. Tilldelningen baseras på attribut från masterdata, till exempel organisatorisk tillhörighet, uppdrag eller roll.

- Tilldelning och borttag sker automatiskt utan manuella steg
- Ingen godkännandeprocess används
- Rekommenderas som förstahandsval där det är möjligt

Exempel:
Alla användare med ett visst uppdrag eller inom en viss enhet tilldelas automatiskt en basroll i applikationen.

Manuell beställning används när tilldelning inte kan styras fullt ut via regler eller när åtkomst kräver individuell prövning.

- Beställning sker via VGR behörighetsportal
- Tilldelning föregås av ett eller flera godkännandesteg
- Lämplig för känsliga, avvikande eller tidsbegränsade behörigheter

Exempel:
En användare behöver tillfällig administrativ åtkomst som kräver godkännande från systemägare.

Det är vanligt att kombinera automatisk tilldelning och manuell beställning inom samma applikation.

- Grundläggande behörigheter tilldelas via policy
- Utökade eller avvikande behörigheter hanteras via manuell beställning

Detta möjliggör en effektiv hantering med hög grad av automatisering, samtidigt som kontroll bibehålls där det behövs.

Godkännadeflöden

Vid manuell tilldelning av applikationsroller används godkännandeflöden för att säkerställa att åtkomst tilldelas med rätt kontroll och ansvar. Val av godkännandeflöde görs per applikation och baseras på verksamhetens behov samt vilken typ av åtkomst som tilldelas.

Det är möjligt att använda ett enskilt godkännandesteg eller kombinera flera steg i sekvens, till exempel att en beställning först godkänns av linjechef och därefter av systemägare.

Tillgängliga godkännandeflöden

Följande typer av godkännanden kan användas:

Linjechef
Avser den närmaste chefen för den person som beställningen gäller, baserat på information i KIV. Detta godkännande används för att säkerställa att åtkomsten är motiverad utifrån individens arbetsuppgifter.

- Livscykelhantering: hanteras automatiskt via KIV
- Lämplig när: åtkomst ska kopplas till individens uppdrag eller organisatoriska tillhörighet

Resursägare
Avser ansvarig för en applikationsroll eller underliggande behörighetsresurs. Används för att säkerställa att åtkomst till en specifik funktion eller resurs är korrekt.

- Livscykelhantering: kan vara manuell, beroende på hur resursägare sätts upp
- Lämplig när: åtkomst är känslig, systemkritisk eller kräver särskild kontroll

Systemägare
Avser ansvarig för applikationen. Används för att säkerställa att tilldelning av behörighet är förenlig med applikationens syfte och behörighetsmodell.

- Livscykelhantering: manuell uppdatering vid förändringar
- Lämplig när: åtkomst har stor påverkan på systemet eller kräver övergripande godkännande

Kombination av godkännandeflöden

Godkännandeflöden kan kombineras i flera steg, till exempel:

- Linjechef → Resursägare
- Linjechef → Systemägare
- Resursägare → Systemägare

Val av kombination beror på:

- hur känslig åtkomsten är
- om både verksamhets- och systemperspektiv behöver beaktas
- krav på spårbarhet och kontroll

Godkännandeflöden används endast vid manuell tilldelning. Vid automatisk tilldelning via policy sker ingen godkännandeprocess.

Återcertifiering

Att genomföra revisioner av manuellt beställda behörighetstilldelningar, dvs att utpekade personer får en uppgift att ta beslut om en behörighetstilldelning (i detta fall en tilldelning av en applikationsroll) ska vara kvar eller tas bort går att sätta upp i VGR behörighetsportal. Kontakta behörighetsteamet (behorighetsportal@vgregion.se) för detta.

Exklusiv hantering av grupper

Alla grupper som är anslutna till VGR behörighetsportal hanteras **uteslutande via VGR behörighetsportal** – inga manuella ändringar i AD. Detta säkerställer spårbarhet samt säkerställer att enbart medlemskap med godkänd anledning finns för dessa grupper.

Frågor och mer information

- **Beställning:** KB0028399 – VGR behörighetsportal – ansökan om anslutning
- **Excel-underlag:** Ansökan anslutning VGR behörighetsportal.xlsx (finns under bifogade filer i KB0028399)
- **Kontakt:** behorighetsportal@vgregion.se
- https://insidan.vgregion.se/forvaltningar/koncernkontoret/stod-och-tjanster/system-a-o/vgr-behorighetsportal/
- **Fördjupning:** se nedan – *Teknisk kravbilaga*

Teknisk kravbilaga – detaljerade specifikationer

Identitets- och organisationsdata

KIV är masterkälla för identitets- och organisationsinformation i VGR och utgör grunden för styrning av behörigheter i VGR behörighetsportal.

Tilldelningspolicyer baseras på attribut från KIV, vilket möjliggör automatisk tilldelning och återkallelse av behörigheter utifrån exempelvis organisatorisk tillhörighet, uppdrag eller roll. Korrekt och uppdaterad information i KIV är en förutsättning för att policybaserad tilldelning ska fungera på ett tillförlitligt sätt.

De attribut som används i tilldelningspolicyer motsvarar de som är inlästa i VGR behörighetsportal och tillgängliga i plattformens regelmotor. I praktiken innebär detta att policyer kan baseras på både identitetsattribut och organisatoriska tillhörigheter.

Tabellen nedan visar exempel på vanligt förekommande och praktiskt använda attribut vid utformning av tilldelningspolicyer. Tabellen är inte uttömmande.

Attribut för tilldelningspolicyer

Typ	***Exempelattribut***	***Beskrivning***
Organisation	Förvaltning (HSA-id)	Används för att styra behörighet på övergripande nivå, t.ex. hela Sahlgrenska Universitetssjukhuset
Organisation	Enhet (Organizational Unit)	Används för att styra behörighet på enhetsnivå
Organisation	Kostnadsställe	Ekonomisk indelning som kan användas för styrning
Anställning	Anställningsform	T.ex. tillsvidareanställd, visstid, konsult eller hyrpersonal
Roll / uppdrag	Uppdragsroll	Verksamhetsroll kopplad till individens uppdrag
Roll / uppdrag	Särskilt uppdrag	T.ex. IT-beställare, säkerhetsombud
Befattning	Befattning / AID-kod	Yrkesroll eller funktion, t.ex. sjuksköterska
Klassificering	Kategorikod	Klassificering av identitet som kan användas för filtrering

Klassificering	Chefskod	Anger chefsnivå eller chefsansvar
Identitet	Identitet	Identitet

Rekommenderad användning

I praktiken bör tilldelningspolicyer i första hand baseras på ett begränsat antal stabila och verksamhetsnära attribut, såsom:

- organisatorisk tillhörighet (förvaltning eller enhet)
- befattning / AID-kod
- uppdragsroller
- anställningsform

Detta ger en lösning som är enklare att förstå, implementera och förvalta över tid.

Exempel:

En tilldelningspolicy kan baseras på:

- Förvaltning = Sahlgrenska Universitetssjukhuset
- Befattning = Sjuksköterska

Detta kan automatiskt tilldela applikationsrollen *"Vårdsystem – Basanvändare"*. Om användaren byter befattning eller organisation tas tilldelningen bort automatiskt.

Kontakt

Vid behov av ytterligare attribut eller rådgivning kring tilldelningspolicyer, kontakta behörighetsteamet via: behorighetsportal@vgregion.se

Applikationsroller i VGR behörighetsportal

Varje applikation som ansluts till VGR behörighetsportal definieras med en eller flera applikationsroller. Applikationsroller representerar verksamhetsmässig åtkomst och är det som används för att tilldela behörighet till användare.

Varje applikationsroll kopplas till en eller flera underliggande AD-grupper. AD-grupperna används för att tekniskt realisera behörigheten i den anslutna applikationen.

All tilldelning i VGR behörighetsportal sker via applikationsroller, antingen automatiskt via tilldelningspolicy eller manuellt via beställning. När en applikationsroll tilldelas får användarens AD-konto ett medlemskap i de AD-grupper som är kopplade till rollen.

Syftet med applikationsroller är att skapa en tydlig separation mellan verksamhetslogik och teknisk implementation. Applikationsroller är utformade för att vara begripliga och användbara i beställningsprocessen, medan AD-grupper hanteras som en underliggande teknisk struktur.

Detta innebär flera fördelar:

- flera AD-grupper kan grupperas i en och samma roll
- roller får tydliga och beskrivande namn som är enkla att förstå
- underliggande AD-grupper kan ändras utan att påverka befintliga tilldelningar

Exempel

En applikation kan ha en applikationsroll med namnet:

Ekonomisystem – Attestant

Denna roll kan vara kopplad till följande AD-grupper:

- .u.app.ekonomi.attest
- .u.app.ekonomi.read

När en användare tilldelas rollen *Ekonomisystem – Attestant* får användaren automatiskt medlemskap i båda dessa AD-grupper, vilket ger rätt behörighet i applikationen.

Konton

- Endast personliga AD-konton (VGR-ID) hanteras.
- Ej stöd: SA/KA-konton, delade konton, tjänstekonton osv
- Roadmap: stöd för andra typer av konton t.ex. privilegierade konton planeras framöver.

Tilldelningspolicy (automatisk tilldelning)
Automatisk tilldelning via tilldelningspolicyer är förstahandsval för att styra behörigheter i VGR behörighetsportal. När tydliga och stabila regler finns för vilka personer som ska ha åtkomst kan behörigheter tilldelas och tas bort automatiskt utan manuell hantering.

Detta minskar behovet av manuella beställningar, ökar kvaliteten i behörighetstilldelningen och minskar risken för felaktiga eller kvarhängande behörigheter.

Grundprinciper

Tilldelningspolicyer i VGR behörighetsportal:

- bygger på identitets- och organisationsdata från KIV
- gäller alltid utan godkännande och utan undantag
- ska ha dokumenterad målpopulation, logik och ansvarig ägare

Tilldelning sker alltid av applikationsroller. För AD-anslutna applikationer innebär detta att användaren indirekt får medlemskap i de AD-grupper som ingår i rollen.

Hur policys fungerar

En tilldelningspolicy består av två huvudsakliga delar:

1. Scope (vilka som omfattas)
Bestämmer vilka personer som ska få en viss behörighet.

Detta baseras på:

- **Identitetsvy** – attribut från KIV, till exempel:
    - organisatorisk tillhörighet
    - uppdrag eller roll
    - arbetsplatskoppling
- **Kontext** – tillhörigheter i VGR behörighetsportal, till exempel:
    - förvaltning
    - organisatorisk gruppering i portalen

Scope kan definieras baserat på:

- enbart identitetsvy
- enbart kontext
- en kombination av båda

2. Tilldelning (vad som tilldelas)
Bestämmer vilka resurser som ska tilldelas.

För AD-anslutna applikationer innebär detta att:

- en eller flera applikationsroller tilldelas
- vilket i sin tur ger medlemskap i kopplade AD-grupper

Exempel:

En tilldelningspolicy kan definieras enligt följande:

- Scope: alla användare med uppdrag *"Sjuksköterska"* inom en viss förvaltning
- Tilldelning: applikationsrollen *"Vårdsystem – Basanvändare"*

När en användare uppfyller kriterierna tilldelas rollen automatiskt, vilket ger medlemskap i de AD-grupper som krävs för åtkomst till systemet. Om förutsättningarna ändras, till exempel vid byte av uppdrag, tas behörigheten bort automatiskt.