ANTURA

Autentisering och Provisionering

Antura AB, www.antura.se

2608 (Augusti 2026)

Autentisering

Översikt

Autentisering avser kontroll av användarens uppgivna identitet i samband med inloggning. Antura stödjer både *formulärsbaserad autentisering* (dvs inloggning med användarnamn och lösenord) och *federerad autentisering* vilket innebär att autentisering görs via företagets IdP (Identity Provider). Federerad inloggning möjliggör även inloggning med Single Sign-On.

Formulärsbaserad inloggning

Formulärsbaserad inloggning är standardsättet att logga in i Antura. Alla användarkonton som har ett lösenord satt kan logga in i systemet genom att skriva in sitt användarnamn och lösenord på Antura inloggningssida.

Säkerhet

När formulärsinloggning används lagras användarinformation och lösenordshash i Anturas databas. Alla lösenord genomgår en hash via en stark hash-funktion och ett individuellt så kallat salt-värde. Inga lösenord sparas därmed i klartext och kan inte heller återläsas från hash-värdet.

Det finns också en lösenordspolicy som kan aktiveras i Antura för att konfigurera hur starka lösenord som ska krävas, hur ofta de ska bytas, hur länge de ska ligga i karantän etc. Lösenordspolicyn kan konfigureras av kunden själv via vyn *Administration – Systeminställningar – Inställningar för formulärsautentisering* i Antura-miljön (förutsatt att inställningen *Använd inställningar för formulärsautentisering* är aktiverad).

Tvåfaktorsautentisering

Tvåfaktorsautentisering innebär att man autentiserar sig genom att använda en kombination av *två* olika komponenter såsom genom ett bankkort/smartkort (något som användaren har) och en PIN-kod (något som användaren vet). Tvåfaktorsinloggning kan slås på i Antura via systeminställningen *Aktivera tvåfaktor* i inställningarna för formulärsautentisering. Väl påslagen kommer alla användare att behöva skapa en hemlighet genom att scanna en QR-kod med Google Authenticator. Authenticator-kontot namnges med både systemnamn och inloggning (till exempel **`Antura - Demo System:user@example.com`**), vilket gör posterna unika mellan olika Antura-system. Vid efterföljande inloggningar behöver användarna även ange en engångskod från appen,

tillsammans med användarnamn och lösenord. Om tvåfaktorsinloggning stängs av raderas samtliga hemligheter.

Inledning

Med 2-faktorautentisering aktiverat innebär det att inloggning inte sker enbart med lösenord, utan även med hjälp av “en andra faktor”. Antura har valt att för ändamålet bygga en lösning där en mobil enhet och en app används för att generera en kod som utgör den andra faktorn.

Stödet för tvåfaktorsautentisering riktar sig till de organisationer som använder det vi kallar “formulärsinloggning” vilket innebär de organisationer som inte har någon annan lösning för autentisering så som till exempel identitetsfederering eller AD-inloggning.

Inloggning med tvåfaktorsautentisering

När 2-faktorsautentisering är aktiverad (se avsnitt “Aktivera tvåfaktorsautentisering” nedan) så kommer följande dialog att visas för en användare första gången den loggar in med formulärsinloggning.

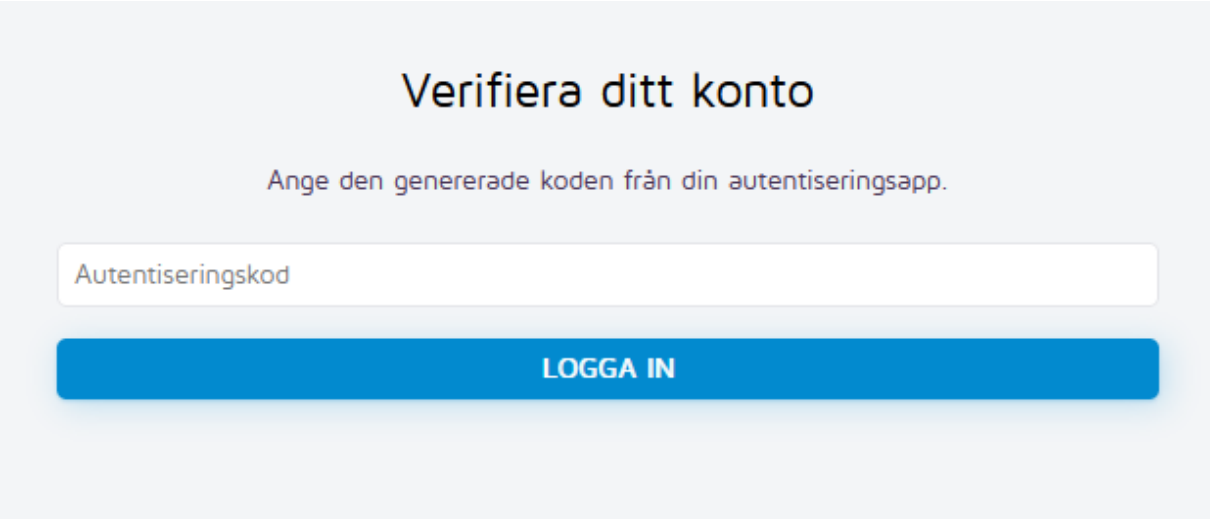
Figur 1 – Den första inloggningen

Användaren får en QR-kod presenterad för sig som skannas i Authenticator-appen.

I Authenticator-appen namnges kontot med både systemnamn och inloggning (till exempel **`Antura - Demo System:user@example.com`**). Det gör posterna unika när samma användare har åtkomst till flera Antura-system.

Efter att koden är skannad kommer en kod att genereras i Authenticator-appen. Efter att koden har matats in i formuläret så kommer användaren att skickas tillbaka till inloggningssidan.

För efterföljande inloggningar med formulärsinloggning så kommer användaren att få följande dialog istället. Användaren anger den genererade koden för att logga in i Antura.

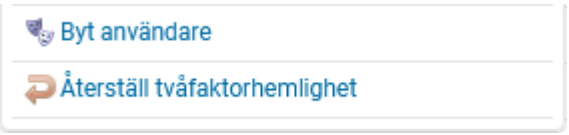


Figur 2 – Efterföljande inloggningar

Återställning av hemlighet

Om en användare av någon anledning förlorar sin andra faktor behöver den återställas av en användaradministratör innan användaren kan skapa en ny "hemlighet". Detta görs på användaren i vyn *Administration – Användare*.

Detta innebär att användaren kommer att behöva aktivera tvåfaktorsautentisering på nytt för att kunna logga in.



Figur 3 - Återställa hemlighet

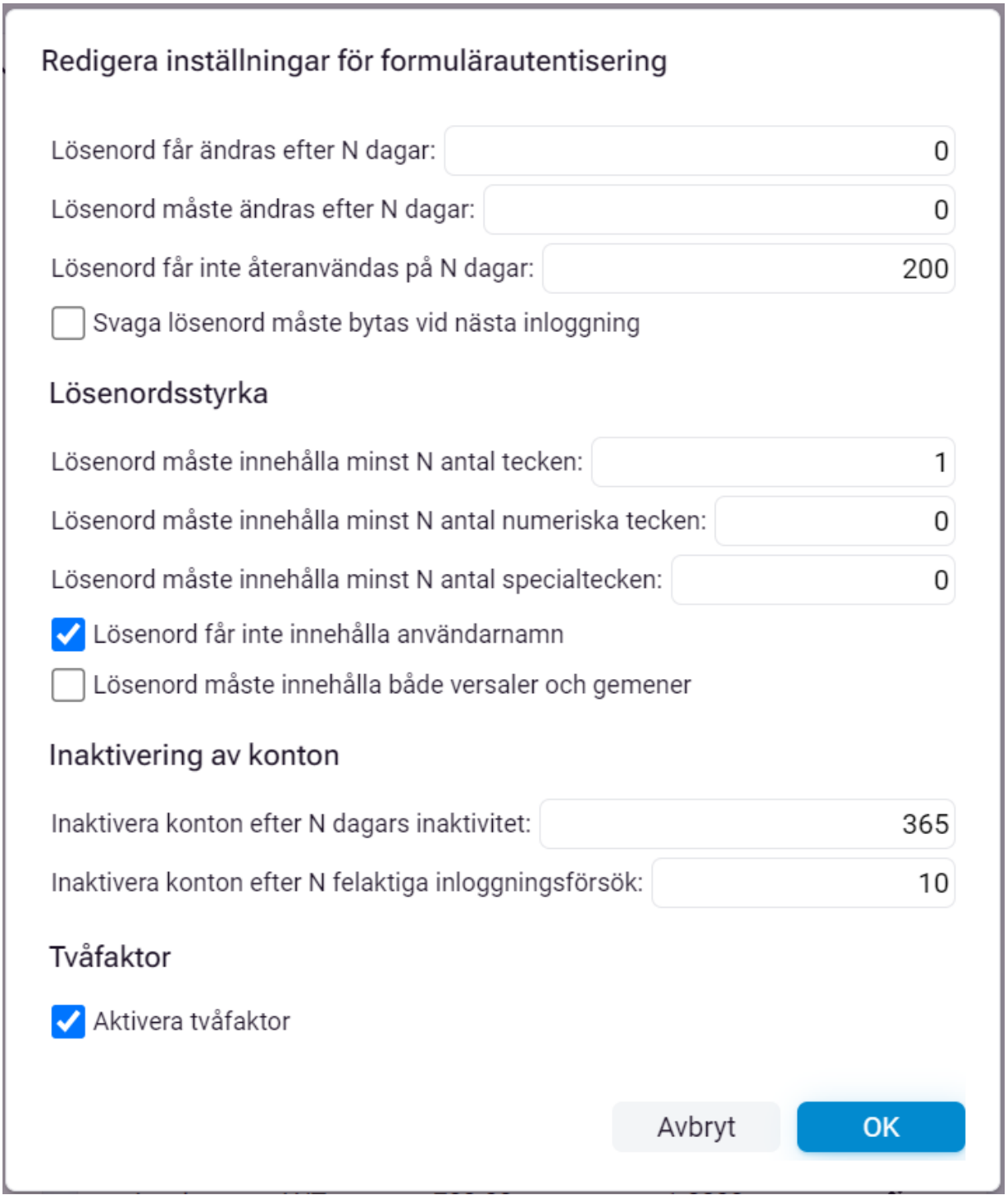
Authenticator-app

Det finns flera appar som går att använda för autentiseringen. Två vanligt förekommande appar är Microsoft Authenticator och Google Authenticator. Båda finns att ladda ned kostnadsfritt från Google Play Butik alternativt Apple App Store.

Aktivera tvåfaktorsautentisering

Stöd för tvåfaktorsautentisering aktiveras i vyn *Administration – Systeminställningar – Allmänt* under sektioner för "Inställningar för formulärautentisering".

1. Klicka i *Aktivera tvåfaktor*
2. Klicka på OK



Figur 4 – Aktivera tvåfaktorsautentisering

När inställningen är aktiverad så kommer användaren nästa gång att bli ombedd att sätta upp "hemligheten" som blir den andra faktorn vid inloggning.

Identitetsfederering

Identitetsfederering gör det enklare för användarna att logga in i Antura genom att använda företagets Identity Provider (IdP). Detta möjliggör också att användare kan logga in på flera olika applikationer med samma användarnamn och lösenord via så kallad single sign-on (SSO).

Lösning

Interna användare godkänns av kundens IdP och ansluter då till Antura med en giltig *token*. Kundens IdP godkänner användare om de är medlem i en eller flera utpekade grupper (denna administration sköts internt av kundens IT-avdelning). Om användarnamnet inte hittas i Antura nekas inloggningen. Antura gör således ingen kontroll på om användaren har behörighet att logga in, utan antagandet är att de användare som kundens Identity Provider autentiserar och släpper igenom också har tillgång till systemet.

Det går att hindra en användare från att logga in via federering genom att ta bort eller inaktivera användaren i Antura. Det finns också möjlighet att tillåta användare som inte finns i Antura att logga in via federering och då skapas automatiskt i Antura i samband med inloggning alternativt möjliggöra att inaktiverade användare aktiveras automatiskt i Antura (se avsnittet "Skapa användare automatiskt").

Externa användare (dvs användare som inte finns i kundens användarkatalog) kan fortsatt logga in i Antura även om identitetsfederering för interna användare är aktiverat, förutsatt att de inte är borttagna (se avsnittet "Mixed mode").

Användare kan även provisioneras, dvs användaruppgifter kan synkroniseras via kundens IdP till Antura se avsnitt "Provisionering".

Lagring av token och loggning

Vid inloggning sparas användartoken som utfärdas av externa Identity Providers i Anturas databas. Tokenvärdena krypteras med tvåvägs (reversibel) kryptering med **`Authentication:Secrets:UserTokenEncryptionKey`**, en krypteringsnyckel som kunden sätter i **`Application.config`**. Innehållet styrs av den externa Identity Providern och kan innehålla

personuppgifter, till exempel personnummer, om sådana värden finns i utfärdade token eller claims.

Loggning av claims kan konfigureras per autentiseringsprotokoll. **`Authentication:Protocols:<protocol>:Identity:Logging:ExternalClaim`** styr loggning av claims som tas emot från den externa Identity Providern, och **`Authentication:Protocols:<protocol>:Identity:Logging:InternalClaim`** styr loggning av de internt mappade claims som Antura använder. Om någon av inställningarna konfigureras med **`*`** loggar Antura alla claims i den kategorin vid inloggning. Kunder bör undvika att använda **`*`** om de inte har verifierat att claims inte innehåller känsliga personuppgifter, eftersom personnummer eller andra personuppgifter annars kan skrivas till loggar.

Protokoll

Antura har stöd för följande protokoll för identitetsfederering:

- OpenID Connect (OIDC)
- SAML2 (SAML 2.0 tokens)
    - Kräver att kundens Identity Provider exponerar en metadata-endpoint
        - Stödjer SP-initierad SSO/SLO (stödjer ej IdP-initierad SSO/SLO)

OIDC är det modernaste alternativet och bör vara förstahandsvalet vid nya implementationer när kundens Identity Provider stödjer både OIDC och SAML2. SAML2 är fortsatt ett fullt supporterat alternativ för miljöer där det redan är etablerat eller annars är det mer praktiska valet.

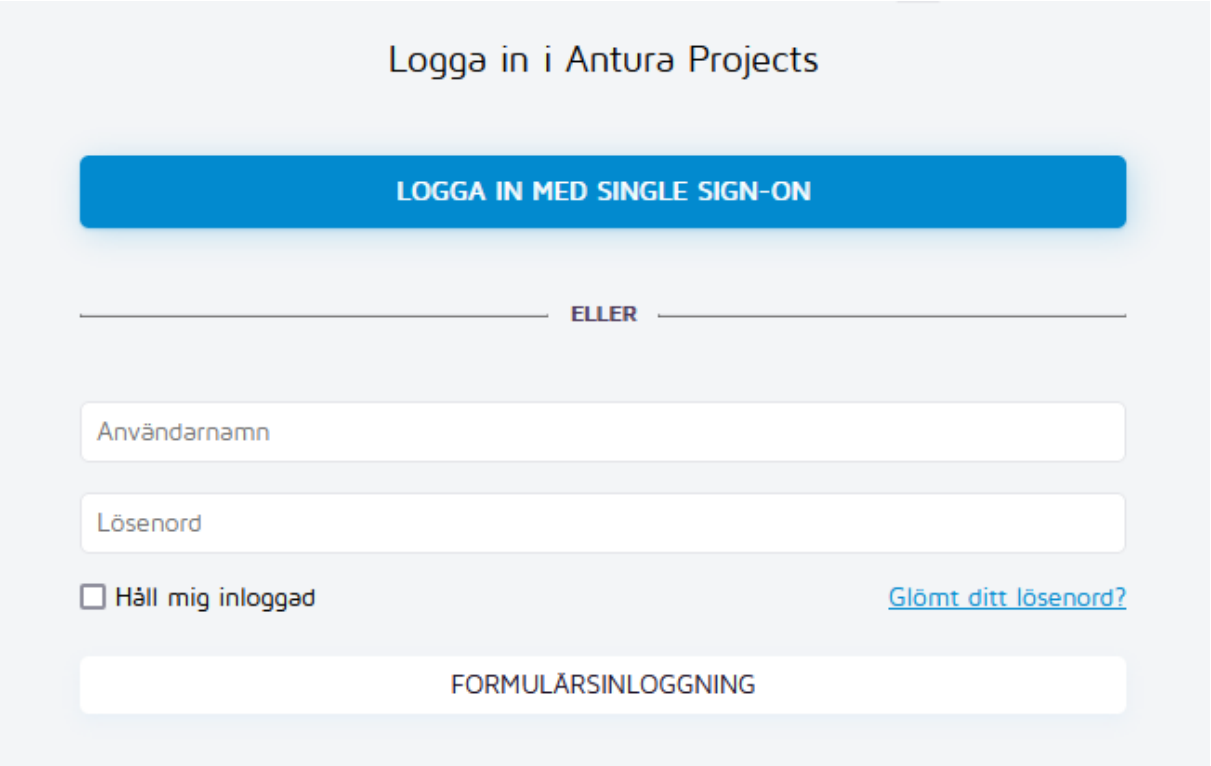
IBM Tivoli

Som standard skickar Tivoli tickets innehållandes ett Renewal-element. Antura kan inte hantera detta och kopplingen kommer inte att fungera. Renewal måste konfigureras bort i Tivoli.

Mixed mode

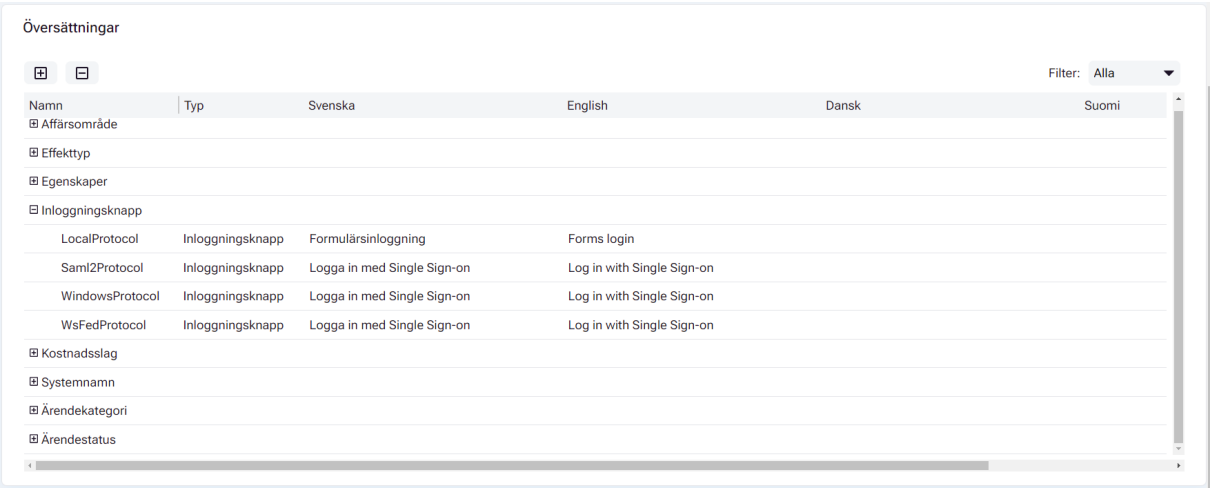
Det går att kombinera flera olika inloggningsförfaranden. Till exempel kan man ha formulärsinloggning påslaget avsett för externa användare, och ett identitetsfedereringsprotokoll såsom SAML2 påslaget avsett för interna användare.

I det fallet så kommer inloggningssidan se ut på följande vis:



De interna användarna loggar in genom att klicka på knappen “LOGGA IN MED SINGLE SIGN-ON”, medan de externa användarna loggar in med formuläret för formulärsinloggning.

Vilka texter som visas på knapparna går att ställa in via vyn *Administration – Språkinställningar – Översättningar*



Det går också att automatiskt sätta på olika protokoll baserat på vilket nätverk en användare befinner sig på. Detta gör det möjligt att till exempel dölja formulärsinloggningen för interna användare och identitetsfedereringsprotokoll för externa användare. Om bara ett identitetsfedereringsprotokoll är påslaget för en användare så kommer användaren att skickas vidare till protokollets login-sida per automatik.

Konvertering av befintliga användare

Inför att lösningen aktiveras i test- respektive produktionsmiljön behöver befintliga interna användare uppdateras så att deras användarnamn matchar det användarnamn som kundens Identity Provider skickar som ett claim. Externa användare kan bibehålla tidigare användarnamn. Antura kan hjälpa till att massuppdatera användare via en skriptkörning vid behov. Kunden behöver då bistå Antura med en Excel-fil som innehåller samtliga befintliga, respektive nya, användarnamn. Det kan även göras manuellt via vyn *Administration – Användare* i Antura-miljön.

Notera att en användare som är skapad manuellt i Antura och sedan loggar in via federering (med samma användarnamn) kommer konverteras till en federerad användare. Det betyder att användarens uppgifter skrivs över med information från kundens Identity Provider och användaren kommer inte längre kunna logga in på annat sätt än via federering.

Grundläggande behörigheter vid federerad inloggning

Alla användare som loggar in via SSO läggs automatiskt i en användargrupp så att en administratör enkelt kan sätta behörigheter för hela gruppen. Användargruppen skapas av systemet och heter “Interna användare”, men gruppens namn kan ändras efter att systemet har skapat den.

Denna grupp kan användas för att ge interna användare vissa grundläggande behörigheter i Antura. Utökade behörigheter kan hanteras manuellt i Antura.

Behörigheter för externa användare hanteras manuellt i Antura på sedvanligt vis genom att tilldela dessa användare till en användargrupp med konfigurerade behörigheter.

Aktivera identitetsfederering

För att aktivera identitetsfederering med SAML2 görs följande konfigurering:

1. Sätt inställningen *Authentication:Protocols:Saml2:Enabled* i filen Application.config till true för att aktivera identitetsfederering via SAML2.
2. I inställningen *Authentication:Protocols:Saml2:EnabledNetworks* i filen Application.config, ange de nätverk (IP-adresser) för användarna som ska komma åt inloggningssidan för SAML2. Om inget nätverk anges så kan alla användare komma åt inloggningssidan för SAML2.
3. Inställningen *Provisioning:SsoCreateNewUsersAutomatically* i filen Application.config sätts till true om kunden vill att synkroniserade användare skall skapas automatiskt i samband med inloggning via SSO.

Konfiguration av trust

Nedan följer instruktioner för hur man sätter upp ett federationsförtroende med Antura i Microsoft Entra ID.

1. Logga in i Microsoft Entra admin center (https://entra.microsoft.com/) med ditt Microsoft 365-konto.
2. Navigera till företagsprogram.
3. Klicka på “Nytt program”.
4. Klicka på “Skapa till ditt eget program”.
5. Skriv vad du vill döpa trustet till, vanligtvis sätter man upp ett trust för Antura-produktionsmiljön och ett trust för Antura-testmiljön. Ett förslag är att inkludera “Prod” eller “test” i programnamnet.
6. Välj “Non-gallery application” och klicka på “Skapa”.
7. När programmet är skapat, navigera till “Enkel inloggning”. Välj “SAML”.

Under “Identifierare (entitets-ID)” skriv in själva URL:en till Antura-siten: “https://customer.projects.se”. Under “Svars-URL” skriv in själva URL:en till Antura-siten: “https://customer.projects.se/oauth/Saml2”. 8. Antura behöver “URL för appfederationsmetadata”. 9. Navigera till “Användare och grupper”. Här kan vi välja vilka Microsoft Entra ID användare/grupper som ska få logga in mot Antura-produktionsmiljön/testmiljön.

Konfigurera claims

Användarnamn, förnamn, efternamn och e-post är obligatoriska fält som måste skickas med från en Identity Provider. Övriga fält uppdateras om de skickas från kundens IdP (se avsnittet “Konfigurera användaruppgifter via claims”) förutsatt att provisionering via claims är aktiverat (se avsnittet “Konfigurera provisionering via claims”).

Konfigurera provisionering via claims

För att aktivera provisionering av användaruppgifter via claims aktiveras inställning *Provisioning:UpdateUsersFromClaim*s i filen Application.config. Om denna är satt till true kommer användaruppgifterna att uppdateras automatiskt i samband med inloggning via SSO.

Konfigurera användaruppgifter via claims

Mappning av claims från en Identity Provider kan göras med inställningar som sätts i filen Application.config. Om inte respektive systeminställning för claimet är satt sätts defaultvärdet som listas i kolumnen “Default”.

Om claimet inte hittas får fältet ett tomt värde. Claims accepteras oavsett om stora eller små bokstäver används.

Inställning	Uppgift	Default
Authentication:Protocols:Saml2:ClaimTypes:Login	Användarnamn	http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
Authentication:Protocols:Saml2:ClaimTypes:FirstName	Förnamn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Authentication:Protocols:Saml2:ClaimTypes:LastName	Efternamn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Authentication:Protocols:Saml2:ClaimTypes:Initials	Initialer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/initials
Authentication:Protocols:Saml2:ClaimTypes:Email	E-post	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Authentication:Protocols:Saml2:ClaimTypes:Company	Företag	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company
Authentication:Protocols:Saml2:ClaimTypes:Department	Avdelning	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department
Authentication:Protocols:Saml2:ClaimTypes:StreetAddress	Adress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetadress
Authentication:Protocols:Saml2:ClaimTypes:PostalCode	Postkod	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode
Authentication:Protocols:Saml2:ClaimTypes:City	Postort	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/city

Inställning	Uppgift	Default
Authentication:Protocols:Saml2:ClaimTypes:Telephone	Telefon	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Authentication:Protocols:Saml2:ClaimTypes:MobilePhone	Mobil	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Authentication:Protocols:Saml2:ClaimTypes:Facsimile	Fax	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/facsimilieTelephoneNumber

Antura E-legitimation

Antura E-legitimation är en valfri tilläggsprodukt som utökar Antura med inloggning via e-legitimationsleverantörerna BankID och Freja eID. Tilläggsprodukten är avsedd att ge externa användare en enkel inloggningsmetod på tillitsnivå 3 (LoA3) utan att behöva hantera lösenord.

När tilläggsprodukten är aktiverad kan administratörer aktivera användare för e-legitimation istället för (eller parallellt med) formulärsinloggning, och användarna kan själva byta från lösenordsinloggning till e-legitimation. Formulärsinloggning kan fortsatt vara påslagen tillsammans med tilläggsprodukten, exempelvis för användare som inte har BankID.

Så fungerar det

Antura tillhandahåller inloggningsportalen och integrationen mot e-legitimationsleverantören (BankID eller Freja eID) som en komplett tjänst — kunden behöver inget eget avtal med en e-legitimationsleverantör och behöver inte sätta upp någon egen integration.

En användares identitet i Antura kopplas till användarens *personnummer*, som lagras i Anturas databas som en säker envägs-hash. Endast svenska personnummer stöds — danskt CPR-nummer och andra nationella id-nummer accepteras inte.

När en användare aktiveras för e-legitimation skickas ett e-postmeddelande med en länk som är giltig i 48 timmar där användaren anger sitt personnummer. Därefter loggar användaren in med sin e-legitimation — vägen via användarnamn och lösenord är avstängd för den användaren och funktionen “Glömt ditt lösenord?” har ingen effekt.

En användare kan återställas till lösenordsinloggning genom att rensa personnumret via massuppdatering i *Administration - Användare*, varefter användaren kan aktiveras för lösenord igen.

Aktivera tilläggsprodukten

Kontakta Antura för att beställa tilläggsprodukten Antura E-legitimation. Vi sköter hela uppsättningen — från integration mot e-legitimationsleverantören till konfiguration i er miljö — så att ni kan erbjuda era användare en modern inloggning på tillitsnivå 3 (LoA3) utan något tekniskt arbete hos er.

Integritet och loggning

Tilläggsprodukten hanterar personnumret som känsliga personuppgifter (PII). Konkret gäller följande:

- Personnumret lagras i Anturas databas som en säker envägs-hash — klartextvärdet behålls inte efter att användaren har angett det.
- Klartextpersonnumret visas endast på sidan där användaren anger det (som nås via den tidsbegränsade aktiveringslänken på 48 timmar). Det visas inte någonstans i administrationsgränssnittet, i exporter, i användaruppgifter eller i någon rapport. Detta innebär att en administratör inte kan se vilket personnummer en viss användare har registrerat.
- Personnumret som anges via Anturas aktiveringsflöde för e-legitimation skrivs inte till någon loggfil av det flödet.
- Värden på claims som tas emot från Identity Providern och mappas internt av Antura censureras i loggar som standard. Kundspecifika undantag för claim-loggning kan konfigureras; bred claim-loggning kan skriva personuppgifter till loggar om claims innehåller sådana uppgifter. Se avsnittet “Lagring av token och loggning”.

Vad som loggas

Följande aspekter av Antura E-legitimation loggas:

- **Revisionslogg**

PersonalIdentityNumberAdded – När ett personnummer sparas för en användare (via aktiveringslänken) registreras denna händelse i revisionsloggen.

PersonalIdentityNumberRemoved – När ett personnummer tas bort från en användare (t.ex. via massuppdatering) registreras denna händelse i revisionsloggen.

- **Åtkomstlogg**

TriedToSetSamePersonalIdentityNumber – Konflikt med personnummer. En användare skickade in en giltig registreringstoken för personnummer, men personnumret är redan kopplat till ett annat konto. Systemet avvisade begäran för att säkerställa att personnummer är unika och registrerade händelsen. Upprepade försök kan indikera ett försök till identitetskapning eller kontokoppling mot en annan användare.

PersonalIdentityNumberTokenExpired – Registreringstoken för personnummer har löpt ut. En begäran om att ange ett personnummer innehöll en token som tidigare varit giltig men vars giltighetstid har passerat. Systemet nekade begäran. Användaren måste begära en ny registreringstoken för att slutföra uppdateringen.

PersonalIdentityNumberTokenUnknown – Registreringstoken för personnummer känns inte igen. En begäran om att ange ett personnummer innehöll en token som inte matchar någon utfärdad post. Systemet nekade begäran och registrerade händelsen för att upptäcka försök att gissa eller återanvända tokenvärden.

Vad som INTE loggas

Följande känsliga information loggas INTE explicit av Anturas aktiveringsflöde för e-legitimation och förekommer inte i revisionshistorik eller loggar för det flödet:

Detta avsnitt beskriver endast loggning. Användartoken som utfärdas av externa Identity Providers kan innehålla personuppgifter och sparas i databasen med tvåvägskryptering; se avsnittet “Lagring av token och loggning”.

- **Klartextpersonnummer** - Det faktiska personnumret (siffrorna) som anges via Anturas aktiveringsflöde för e-legitimation skrivs inte till någon loggfil av det flödet. Detta omfattar inte kundaktiverad loggning av externa eller interna identitetsclaims; se avsnittet “Lagring av token och loggning”.
- **Hash av personnummer** - Envägs-hashen av personnumret loggas inte; den lagras endast i databasen.
- **Svar från e-legitimationsleverantören** - Svar från BankID eller Freja eID som innehåller personnummer eller verifieringsdetaljer censureras innan någon loggning sker.
- **Aktiveringslänk-token** - De 48-timmars-aktiveringslänkarna och deras token loggas inte.

Där personnummer visas i systemet

Personnummer som hanteras direkt av Antura E-legitimation visas på följande platser:

1. **Under användaraktivering** - På den temporära 48-timmars-aktiveringssidan anger användaren sitt personnummer direkt i ett inmatningsfält. Denna sida nås via e-postlänk och visas endast för den användare som aktiverar sitt konto.
2. **I databasen** - Lagrat som en säker envägs-hash i användartabellen. För detta flöde lagras klartextvärdet aldrig.

Provisionering

Översikt

Provisionering innebär synkronisering av användare och användaruppgifter. All information för användare uppdateras från företagets Identity Provider.

Det finns tre olika sätt att provisionera användare:

- Vid inloggning
- Automatiskt
- Manuellt

Provisionering i samband med inloggning innebär att användaruppgifterna uppdateras varje gång en användare loggar in i Antura via s.k. claims som skickas med från en Identity Provider. Nya användare kan skapas upp automatiskt i samband med inloggning till Antura.

Automatisk provisionering innebär att användaruppgifterna uppdateras löpande utifrån synkroniserade AD-grupper. Detta möjliggör att användaruppgifter och användarkonton kan skapas upp långt innan en användare loggar in första gången i Antura. Provisionering kan även köras på manuell begäran.

Provisionering i samband med inloggning

Användare som hittas i Antura-miljön kommer att loggas in automatiskt i Antura via SSO. Om användaren redan finns i Antura kan användaruppgifter som skickas med från en Identity Provider uppdateras när en användare loggar in i Antura. Hur användaruppgifterna skall mappas kan konfigureras i Antura. Om ingen konfigurering av synkroniserade användaruppgifter görs används en default-mappning (för mer detaljer se avsnitt “Konfigurera användaruppgifter via claims”).

Om användarinformation skall uppdateras i samband med inloggning styrs via en inställning som Anturas Support gör (för mer detaljer se avsnitt “Konfigurera provisionering via claims”).

Skapa användare automatiskt

Användare som tillåts logga in av företagets IdP kan antingen få sitt konto i Antura skapat automatiskt vid första inloggningen eller nekas inloggning om konto saknas. Konton får då skapas

manuellt via gränssnittet i Antura. Om kunden vill att användare skall skapas upp automatiskt eller inte styrs via en inställning (för mer detaljer se avsnitt “Aktivera identitetsfederering”).

Konfiguration per autentiseringsmetod

Huruvida en användare kan skapas eller aktiveras vid inloggning konfigureras per autentiseringsmetod, oberoende av om SCIM är aktiverat. Det möjliggör olika beteende för olika inloggningsprotokoll — till exempel kan SCIM hantera interna användare från Microsoft Entra ID samtidigt som en specifik OIDC- eller SAML2-integration styr om okända externa användare ska skapas automatiskt vid inloggning.

Automatisk provisionering

Automatisk provisionering från Active Directory samt Microsoft Entra ID tillhandahålls genom stödet för “Provisionering med Active Directory” (endast för on-prem) respektive “Provisionering med SCIM” enligt avsnitten nedan. Till skillnad från provisionering via inloggning skapas och uppdateras användare från synkroniserade AD-grupper som sker löpande eller automatiskt via ett nattligt jobb.

Provisionering med Active Directory

Med *Provisionering med Active Directory* är det möjligt att konfigurera provisionering av användare och grupper från Active Directory till Antura. Nya användare skapas och befintliga användare uppdateras från synkroniserade AD-grupper nattligen i Antura. Åtgärder för synkroniserade användare (såsom borttagna AD-användare, inaktiverade AD-användare, AD-användare som inte tillhör en synkroniserad grupp mm) styrs via synkroniseringsinställningar för användare i Antura. Lösningen innefattar även autentisering av användare.

Introduktion

Provisionering med Active Directory gör det möjligt för behöriga användare att automatiskt loggas in i systemet utan att behöva använda inloggningsrutan. Användaren loggas in automatiskt utan att behöva ange användarnamn och lösenord. Synkroniseringen görs genom att koppla samman en eller flera grupper i AD med samma antal systemgrupper i Antura.

Konfiguration

När användare ansluter till Antura verifieras det att användaren har behörighet. Beroende på vilka AD-grupper användaren tillhör så blir den medlem i motsvarande Antura-grupper och får därigenom angivna behörigheter. Om användaren inte är med i någon motsvarande Antura-grupp nekas inloggningen.

Behörighetsstyrning

Nedan visas två alternativ för konfiguration av AD-synkronisering i Antura:

1. Behörigheter administreras i Antura

En synkroniseringsgrupp används för att synkronisera samtliga användare från AD. Behörigheter för användare som synkroniseras hanteras med separata grupper i Antura.

Ex: En systemgrupp skapas i Antura med namnet "Synkroniseringsgrupp" och kopplas till AD med en gruppreferens. Systemgruppen tilldelas inga behörigheter. Istället tilldelas behörigheter genom att systemadministratören lägger till användare i ytterligare systemgrupper (som inte synkroniseras med AD).

2. Behörigheter administreras i AD

Flera synkroniseringsgrupper används för att synkronisera användare från AD. Behörigheter tilldelas direkt till synkroniseringsgrupperna i Antura.

Ex: Tre systemgrupper skapas i Antura: "Antura projektledare", "Antura administratörer" och "Antura användare". Dessa kopplas till tre olika gruppreferenser i AD. En systemadministratör tilldelar behörigheter till systemgrupperna och de synkroniserade användarna får behörigheter tilldelade beroende på vilken grupp de synkroniseras till.

Samma användare kan ingå i flera synkroniserade grupper, t ex både "IT" och "Ledning". Användaren får då behörigheter från båda grupperna.

Gruppstrukturer

Antura använder sig inte av en hierarkisk gruppstruktur (som kan användas i AD). Antura har dock stöd för att synkronisera användare mot en hierarkisk gruppstruktur i AD via en konfiguration per synkroniserad grupp.

Ex: Givet följande gruppstruktur i AD: "IT => Utveckling => .NET" (tre i trädstruktur). Om gruppen "IT" synkroniseras går det att välja huruvida endast direkta medlemmar till IT eller även undergrupper ska inkluderas (dvs Utveckling och .NET).

Nätverk och domäner

Om integration med AD skall användas bör webbservern som driver Antura vara med i den domän som ingår i företagets “forest”. Standardfallet är att synkroniseringen sker mot serverns domänkontrollant och att Antura autentiserar sig med den användaridentitet som är konfigurerad på applikationspoolen i webbservern (IIS).
Det går också att konfigurera adress, användarnamn och lösenord mot en eller flera specifika AD-servrar – detta kräver då att AD-kommunikation är öppen till dessa servrar. I det fallet behöver inte Antura-servern ingå i domänen.

Synkronisering av information

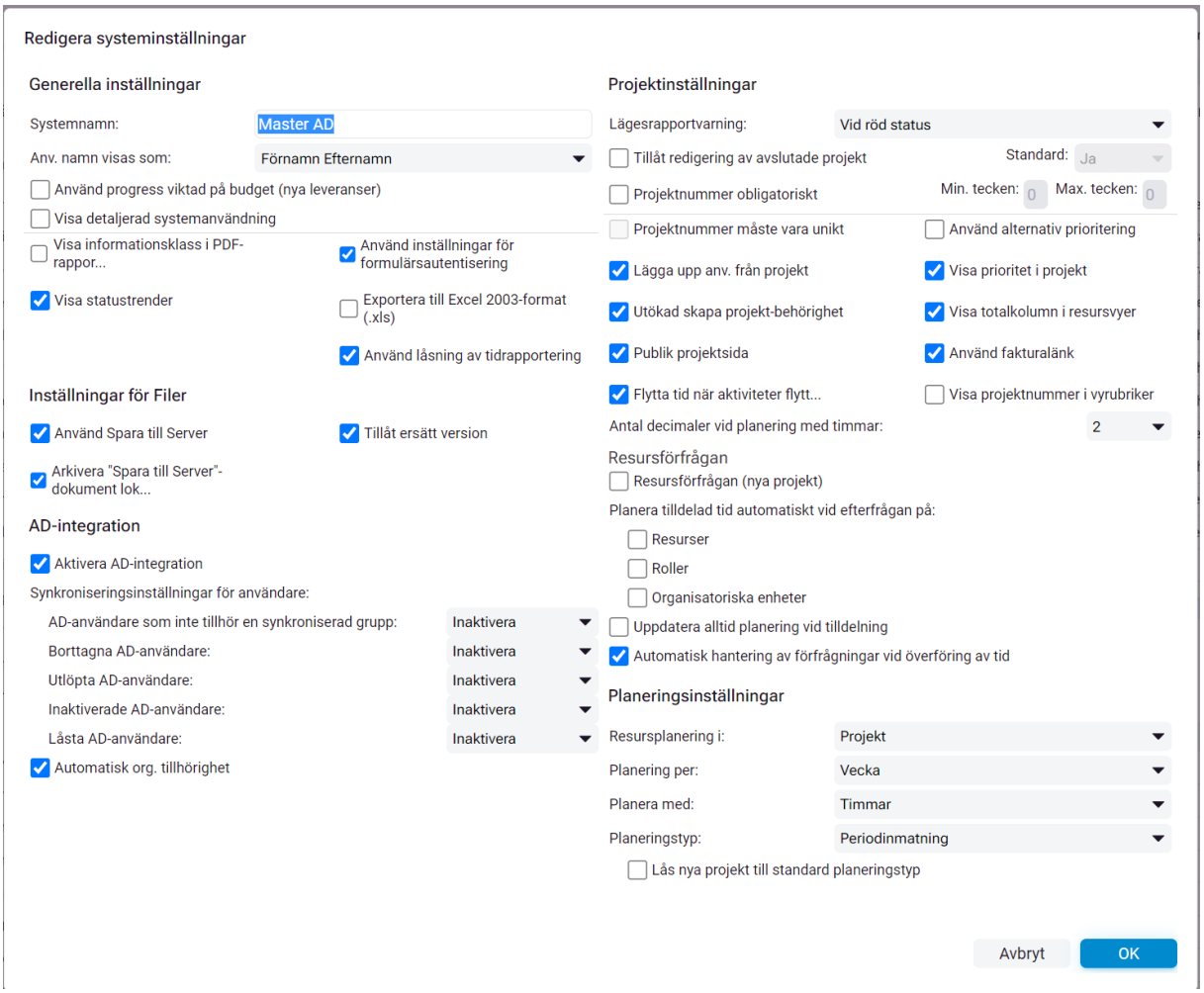
När en användare synkroniseras kopieras en del av informationen från AD till Antura.
Synkronisering sker per automatik en gång per dygn samt per användare vid inloggning.
Följande fält läses över från AD och uppdateras i Antura:

ADSI namn	Antura
givenName	Förnamn
sn	Efternamn
displayName	Visningsnamn
company	Företag
department	Avdelning
streetAddress	Adress
postalCode	(Postnummer) Första delen av postadress
mail	E-postadress
mobile	Mobilnummer
telephoneNumber	Telefonnummer
facsimileTelephoneNumber	Faxnummer

ADSI namn	Antura
L	(Stad) Andra delen av postadress

Automatisk organisationstillhörighet

För att automatiskt sätta en användares organisationstillhörighet klickas systeminställningen "Automatisk organisationstillhörighet" i (*Administration – System - Allmänt).*



När inställningen är aktiverad kopplas användaren till en organisatorisk enhet som har samma namn som texten i fältet "Avdelning" (dvs "department" i AD). Kopplingen till organisationstillhörighet sker vid varje synkronisering av användaren.

Synkronisering av grupper (provisionering)

Varje natt synkroniseras de grupper i Antura som är kopplade till AD. Nya medlemmar i AD-grupperna skapas per automatik som användare i Antura. All information för existerande

användare uppdateras från AD. I de fall där en användare tagits bort ur AD-gruppen kommer användaren att inaktiveras i Antura (indikeras med röd statuslampa i Antura) och kommer inte längre kunna logga in. Om användaren läggs tillbaka i AD-gruppen kommer den att aktiveras igen (indikeras med grön statuslampa i Antura) vid nästa synkronisering.
Det går också att synkronisera grupperna manuellt vilket ger samma effekt som den automatiska synkroniseringen.

Åtkomst för nya användare

När nya användare har lagts till i någon av de AD-grupper som är synkroniserade kommer de att ges åtkomst på en gång. Användarna kommer kunna logga in i Antura. Ett användarobjekt kommer att skapas i Antura (eller uppdateras om användaren redan finns). Användare som har blivit tillagda i AD-gruppen, men inte har loggat in, kommer att bli skapade i Antura vid nästkommande synkronisering.

Upphävande av åtkomst

När användare har blivit borttagna från AD-grupper som synkroniserats kommer deras åtkomst att upphävas omedelbart. Användarna kommer inte att kunna logga in i Antura. Användarobjekten i Antura kommer bli inaktiverade. Användare som har tagits bort från AD-grupperna, men inte har försökt logga in, kommer bli inaktiverade vid nästkommande synkronisering.

Användare som inte finns i AD

I vissa fall behöver externa användare som inte har AD-konton kunna logga in i Antura-miljön (t ex konsulter). För att hantera detta finns ett stöd både AD- och formulärsinloggning parallellt (så kallat “Mixed Mode”).

Med mixed mode-autentisering kan AD-inloggning kombineras med formulärsinloggning. Detta kan användas om alla interna användare kommer från ett internt nät (t ex 192.168..) och externa användare kommer från andra nät. I det läget kan Antura konfigureras så externa användare presenteras med en inloggningsruta medan interna användare loggas in automatiskt med SSO (Single Sign-On). För mer information, se avsnittet “Mixed mode” ovan.

Aktivering av Active Directory-synkronisering med Antura

Förberedelser i AD

Kunden skapar en eller flera grupper i AD, beroende på vilken konfiguration som väljs i det tidigare avsnittet *"Konfiguration i Antura"*. De användare som ska ha tillgång till Antura kopplas till respektive grupp. Slutligen skickas fullständig sökväg till grupperna i DN-format (*"Distinguished Name"*) till Antura. Exempel på gruppreferens:
CN=AnturaProjectsSyncGroup,CN=Users,DC=antura,DC=se

Befintliga användare i Antura

I de fall som synkronisering med AD aktiveras då det redan finns befintliga användare i systemet behöver dessa mappas om till sina motsvarande användarnamn i AD. Antura förser kunden med en Excel-fil som innehåller samtliga användare i systemet tillsammans en tom kolumn vid respektive användare: *"Användarnamn i AD"* som kunden fyller i. *Ex: DOMÄN\användarnamn*. När filen är ifylld och skickats tillbaka ändras de befintliga användarna och därefter är de redo för synkronisering mot AD.

Aktivera Active Directory och initial synkronisering

När grupperna är skapade och Antura har fått gruppreferenserna samt eventuell mappningstabell är det klart för att aktivera AD-kopplingen. Detta görs av Antura och innebär en kortare nertid av systemet (ca 1 timme). I samband med aktiveringen skapas de nya systemgrupperna i Antura (för att synkronisera mot AD) och eventuella befintliga användare skrivs om till sina motsvarande användarnamn i AD (med hjälp av mappningstabellen). Efter att aktiveringen är klar öppnas miljön upp och då kommer användarna att automatiskt logga in i systemet, utan att behöva ange användarnamn och lösenord.

Ändringen görs först i **testmiljö** för att verifiera att allt fungerar korrekt samt att lösningen uppfyller förväntningarna. När synkroniseringen fungerar i test och godkänts görs samma ändring i produktionsmiljön.

Konfiguration av Mixed Mode

Om Mixed Mode-autentisering ska användas behöver en tekniker från Antura diskutera med en tekniker på kundsidan för att avgöra om man med hjälp av IP-adresser kan avgöra om en användare ska AD-autentiseras eller dirigeras till inloggningssidan (t ex om alla konsulter kommer via externa nät). Detta behöver inte göras separat som ett senare steg, efter att AD-synkroniseringen är klar.

Provisionering med SCIM

Med *Provisionering med SCIM* är det möjligt att konfigurera automatisk provisionering av användare och grupper från Microsoft Entra ID till Antura via SCIM. Nya användare skapas och befintliga användare uppdateras från synkroniserade AD-grupper löpande i Antura. Åtgärder för AD-användare (såsom nya, uppdaterade, borttagna AD-användare) styrs från Microsoft Entra ID.

Introduktion

Med *Provisionering med SCIM* är det möjligt att konfigurera automatisk provisionering av användare och grupper från identitetsleverantörer som Microsoft Entra ID och Okta till Antura, vilket underlättar hantering av nya användare och att hålla användare och grupper synkroniserade.

Provisionering med SCIM använder sig av SCIM-protokollet som är en standard för provisionering. Jämfört med AD-synkronisering kräver lösningen inte att AD:t är installerat på samma nätverk som Antura. När Provisionering med SCIM är installerad, finns det ett REST API i Antura som implementerar ett SCIM API enligt https://tools.ietf.org/html/rfc7644#section-3.2.

I Identitetsleverantören registreras Antura som en klientapplikation av administratören. Genom en attributmappning definieras vilka attribut i Identitetsleverantören som skall mappas mot vilka attribut i Antura. E-postadress, för- och efternamn måste finnas på användare för att nya användare ska kunna skapas i Antura.

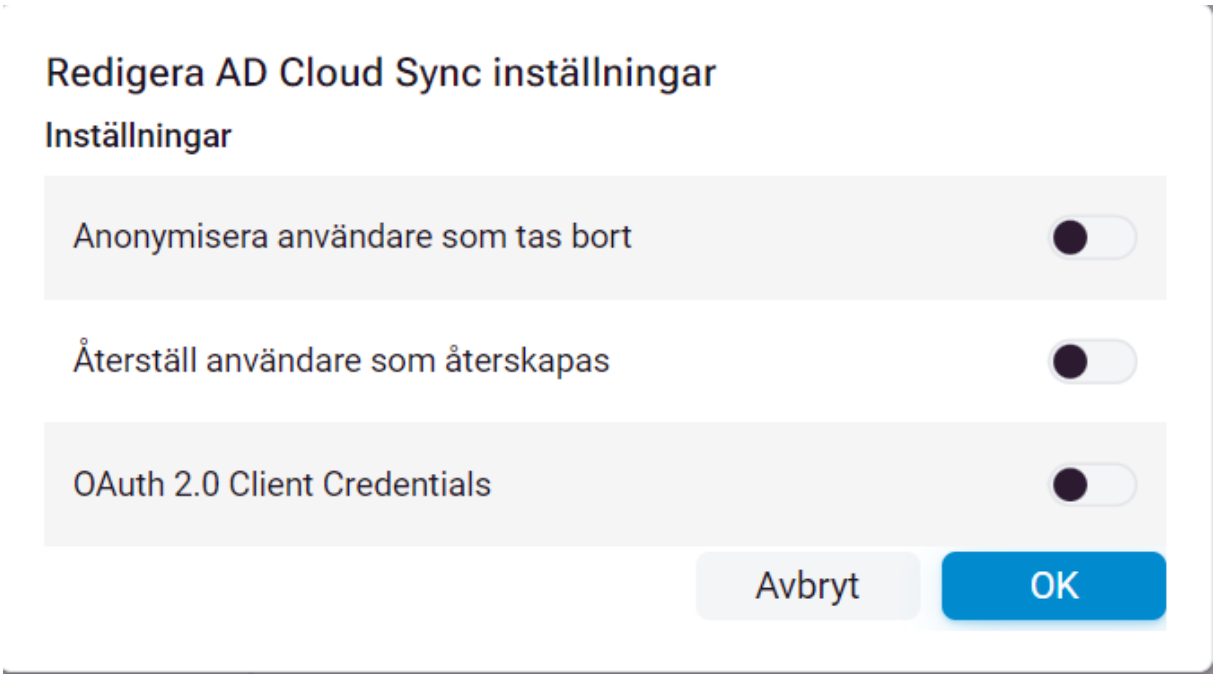
Omfattning för provisioneringen definieras i Identitetsleverantören genom att välja att alla användare och grupper ska provisioneras eller genom att peka ut vilka användare och grupper som skall inkluderas i provisioneringen till Antura.

Till skillnad från för användare finns det inte stöd för att *skapa* och *ta bort* grupper via SCIM.

För information avseende autentisering och inloggning via SSO, se avsnittet “Autentisering” ovan.

Inställningar

Det finns tre inställningar för Provisionering med SCIM; *Anonymisera användare som tas bort*, *Återställ användare som återskapas* samt *OAuth 2.0 Client Credentials*.



Aktivering av inställningen "*Anonymisera användare som tas bort*" medför att användare som tas bort i Identitetsleverantören anonymiseras i Antura. Detta innebär följande:

- Användarnamn, För-/Efternamn samt E-postadress sätts till slumpmässiga värden
- Företag, Avdelning, Gatuadress, Postadress, Telefon/Mobil/Fax blankas
- Eventuell profilbild tas bort
- Organisatorisk enhet sätts till "Ingen organisatorisk enhet"
- Användaregenskaper påverkas ej

Som standard är denna inställning aktiverad.

Aktivering av inställningen "*Återställ användare som återskapas*" medför att användare som återskapas i Identitetsleverantören aktiveras på nytt i Antura förutsatt att användaren kan identifieras, dvs en (och bara en) användare kan matchas via (i första hand) attribut "externalId" och (i andra hand) attribut "userName". Som standard är denna inställning inte aktiverad.

Observera att om båda dessa inställningar är aktiverade krävs att attributet "externalId" (se "SCIM-attributmappning") är mappat och synkas för att användaren skall kunna återskapas.

Aktivering av inställningen "*OAuth 2.0 Client Credentials*" medför att Identitetsleverantören kan kontakta Anturas REST API med OAuth 2.0 Client Credentials Grant istället för bara en token. Efter aktivering visas följande fält som krävs för att ansluta Identitetsleverantören:

- Klient-id
- Klient-scope

- Klientens callback-URL
- Hemlig token (om värdet är dolt är det värde som senast visades fortfarande giltigt)

Som standard är denna inställning inte aktiverad.

Provisionering från Microsoft Entra ID till Antura

Skapa användare

Om en användare i Microsoft Entra ID saknas i Antura, skapas användaren förutsatt att åtgärd "Skapa" är konfigurerat för användare i Microsoft Entra ID.

Aktivering och inaktivering av användare

För att en användare skall bli aktiv i Antura skall SCIM-attributet *active* sättas till true för användaren. Rekommenderat är att använda Microsoft Entra ID-attributet "isSoftDeleted" och sätta detta till false för att aktivera användaren, och till true för att inaktivera användaren (se SCIM-attributmappning för hur uttrycket ser ut i Microsoft Entra ID). Nya användare i Microsoft Entra ID kommer således att skapas som aktiva i Antura och användare som tas bort (utan att tas bort permanent) i Microsoft Entra ID kommer att inaktiveras i Antura.

Det går dock att implementera mer komplex logik för när användare skall anses bli aktiva. För mer detaljer kring hur man skriver dessa uttryck se https://learn.microsoft.com/en-us/entra/identity/app-provisioning/functions-for-customizing-application-data

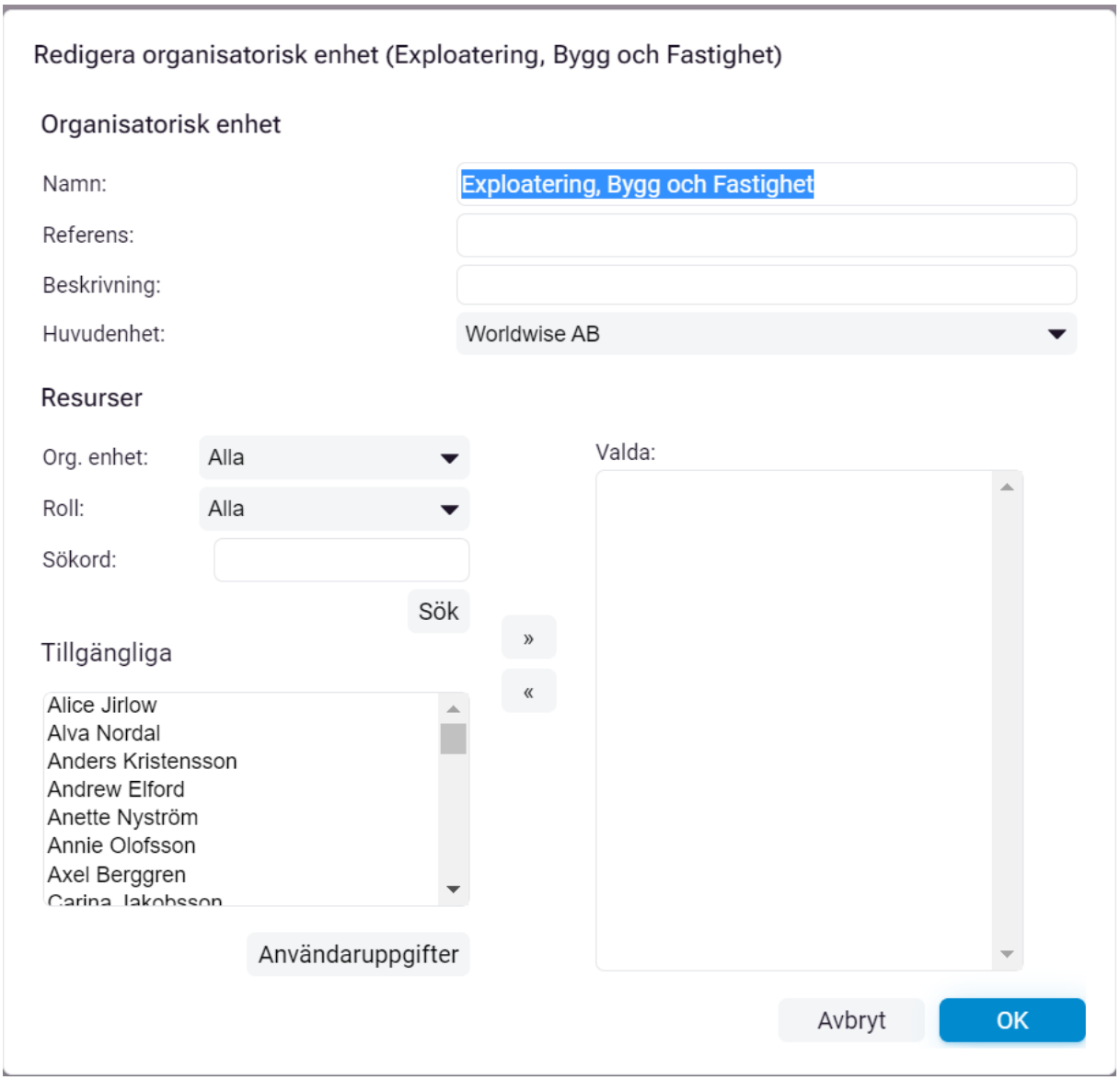
Borttagning av användare

Om en användare tas bort permanent i Microsoft Entra ID, tas användaren bort i Antura förutsatt att åtgärd "Ta bort" är konfigurerat för användare i Microsoft Entra ID. Eftersom användare inte kan tas bort permanent i Antura kommer en sk "soft delete" göras (dvs användaren markeras som borttagen). Det är konfigurerbart huruvida användare som tas bort skall anonymiseras eller ej (se avsnitt "Inställningar"). Om anonymisering är aktiverat kommer användarnamn, namn (förnamn, efternamn) och e-postadress uppdateras med slumpmässiga värden och andra uppgifter att blankas.

Om användare som återskapas i Microsoft Entra ID skall skapas upp på nytt i Antura eller återställas är också konfigurerbart (se avsnitt "Inställningar").

Organisationstillhörighet

Vilken organisatorisk enhet en användare tillhör avgörs genom en jämförelse av företagets namn i Microsoft Entra ID med värdet i fältet "Referens" som är satt på en organisatorisk enhet i Antura (Projektportfölj – Org.enheter – Projekt). *Notera att jämförelsen är skiftlägeskänslig.*

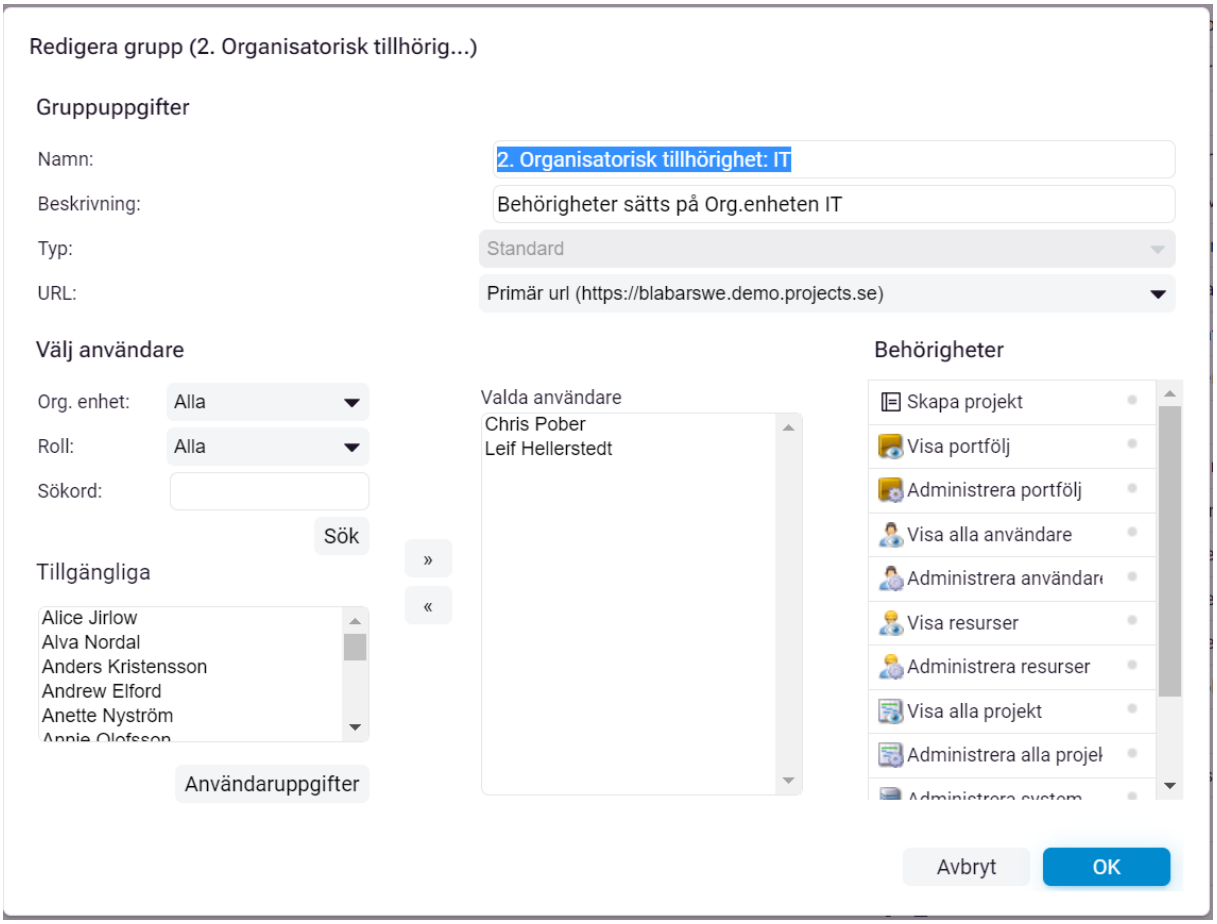


Om exakt en organisationsenhet matchar uppdateras användaren att tillhöra organisationsenheten i Antura. Om ingen eller flera organisationsenhet matchar uppdateras användaren utan organisationstillhörighet och en varning loggas.

Notera att provisionering av organisationstillhörighet styrs genom attributmappning i Microsoft Entra ID (se SCIM-attributmappning) och påverkas inte av vad systeminställningen "Automatisk organisationstillhörighet" (Administration – System - Allmänt) är satt till.

Grupptillhörighet

Vilken användargrupp en användare tillhör avgörs genom en jämförelse av gruppens namn i Microsoft Entra ID med värdet i fältet "Gruppreferens" som är satt på en grupp i Antura (Administration – Grupper). Fältet visas endast om Provisionering med SCIM är aktiverat (se avsnittet "Aktivera Provisionering med SCIM") och om gruppen är en standardgrupp (dvs fältet Typ = "Standard"). *Notera att jämförelsen inte är skiftlägeskänslig.*



Om gruppen matchar uppdateras användaren att tillhöra gruppen i Antura. Om en användare tas bort från en grupp i Microsoft Entra ID tas användaren bort från motsvarande grupp i Antura (förutsatt att gruppen matchar).

Multipla grupper

En användare kan tillhöra flera grupper i Microsoft Entra ID. Det kan innebära att användaren blir medlem av flera grupper i Antura.

Det är dock inte möjligt att ha flera Microsoft Entra ID-grupper som alla är mappade till samma grupp i Antura eller vice versa. Om samma gruppreferens anges för flera grupper kan detta resultera i ett odefinierat beteende.

Hierarkiska grupper

Microsoft Entra ID tillåter hierarkiska grupper, vilket inte stöds av Antura.

Om man väljer ut vilka användare och grupper som skall provisioneras fungerar det inte med hierarkiska grupper, dvs endast användare och grupper som ligger direkt mot utpekad grupp i Microsoft Entra ID kommer att synkroniseras till Antura (dvs för att få med alla användare i en viss trädstruktur av användare/grupper måste alla grupper utom lövnivån explicit väljas för provisionering).

Om man väljer att alla användare och grupper skall provisioneras kommer hierarkiska grupper och användare i en hierarkisk struktur provisioneras förutsatt att gruppen i Microsoft Entra ID matchar en grupp i Antura.

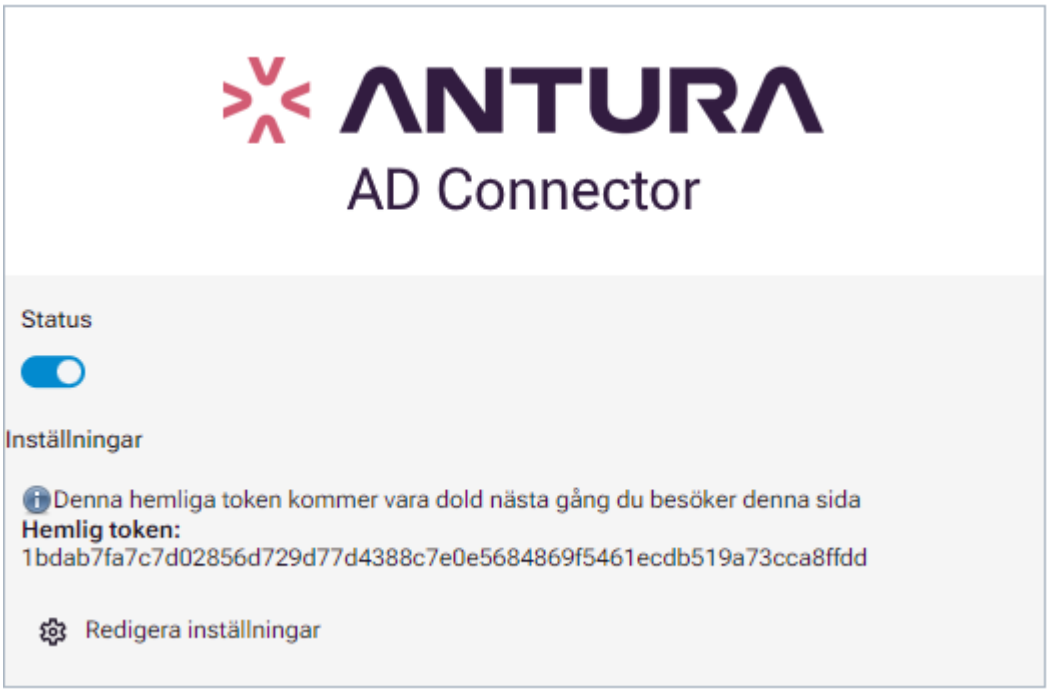
Installationsmanual för SCIM

Konfiguration i Antura

Aktivera Provisionering med SCIM

Provisionering med SCIM behöver aktiveras manuellt i administrationsgränssnittet. Aktivera Provisionering med SCIM via Status-knappen. Notera hemlig token som genereras och visas vid aktivering. Denna nyckel skall användas senare vid registrering av Antura som en klientapplikation i Microsoft Entra ID.

Microsoft Entra ID pratar med Antura via ett REST API och använder sig av OAuth 2.0 Client Credentials Grant för att autentisera sig. Microsoft Entra ID implementerar inte fullständigt stöd för Client Credentials Grant, utan konfigureras med en token istället. Antura genererar en token med oändlig livslängd. Detta är en begränsning i Microsoft Entra ID och inte i Antura.

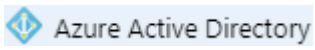


Konfiguration i Microsoft Entra ID

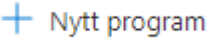
Integration mellan Provisionering med SCIM och Microsoft Entra ID kräver en konfiguration i Microsoft Entra ID. Denna konfiguration görs av Microsoft Entra ID administrator då den kräver Microsoft Entra ID-adminrättigheter.

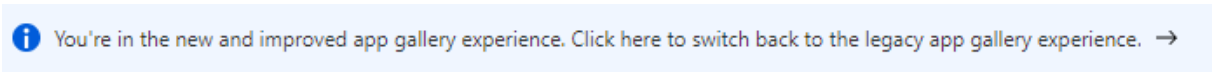
Registrera Antura som en klientapplikation i Microsoft Entra ID

För att Antura ska kunna ta emot provisioneringsdata från Microsoft Entra ID måste Antura manuellt registreras som en klientapplikation i Microsoft Entra ID.

1. Logga in på https://entra.microsoft.com/ (Microsoft Entra admin center) med ditt Microsoft 365-konto. Du kan även använda https://portal.azure.com om du föredrar det.
2. Klicka på tjänsten 

3. Klicka på 

4. Klicka på 

5. Klicka på


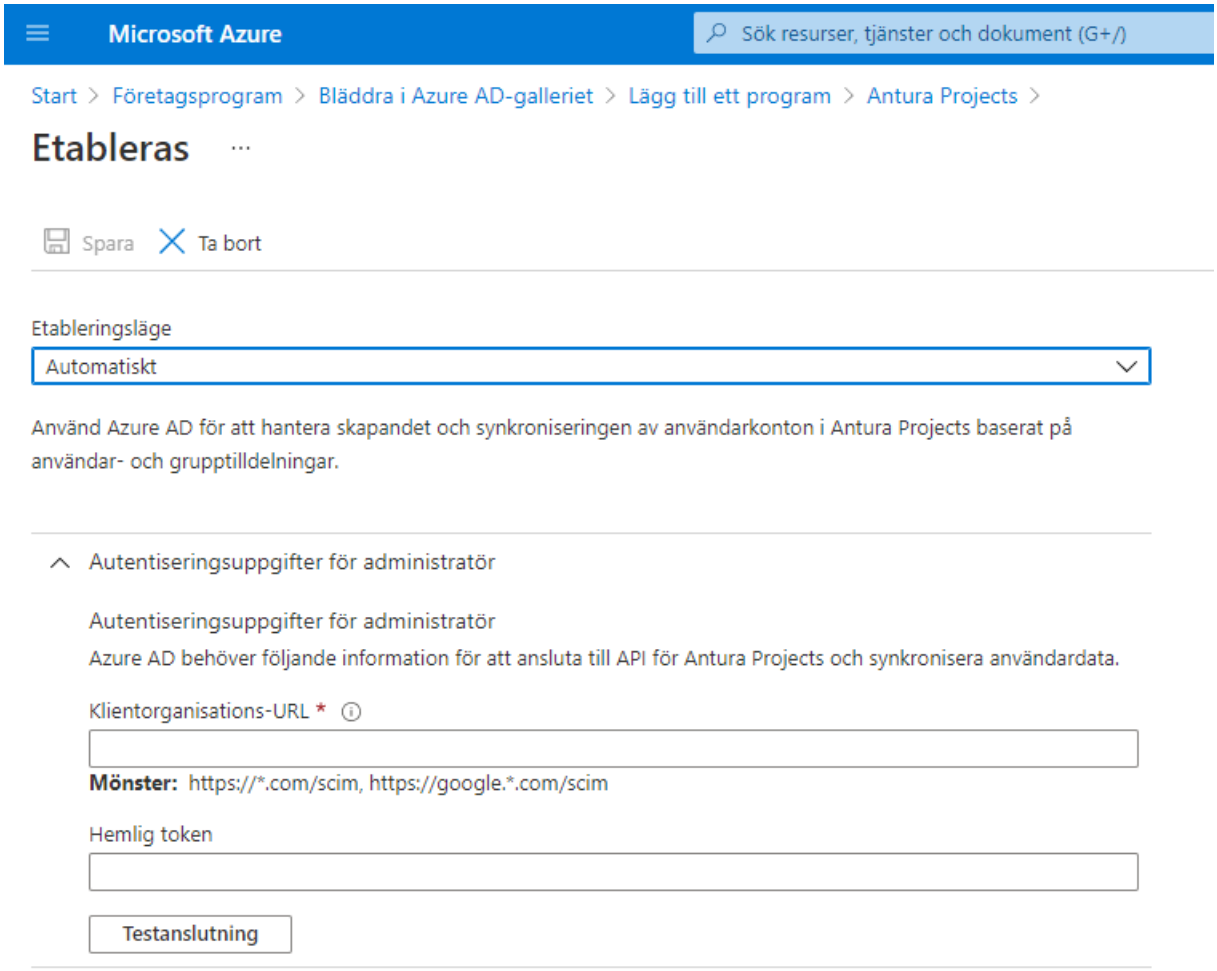
6. Klicka på 

7. Skriv in följande information:
    1. Namn - namnet på applikationen, kan vara vad som helst - till exempel “Antura”.

8. Klicka på “Lägg till”

Konfigurera automatisk provisionering med SCIM

1. Navigera till den nyligen skapade applikation och klicka på “Etableras” och därefter “Kom igång”. Välj “Automatisk” i dropdownen. Det innebär att informationen kommer att synkas automatiskt var 40:e minut.



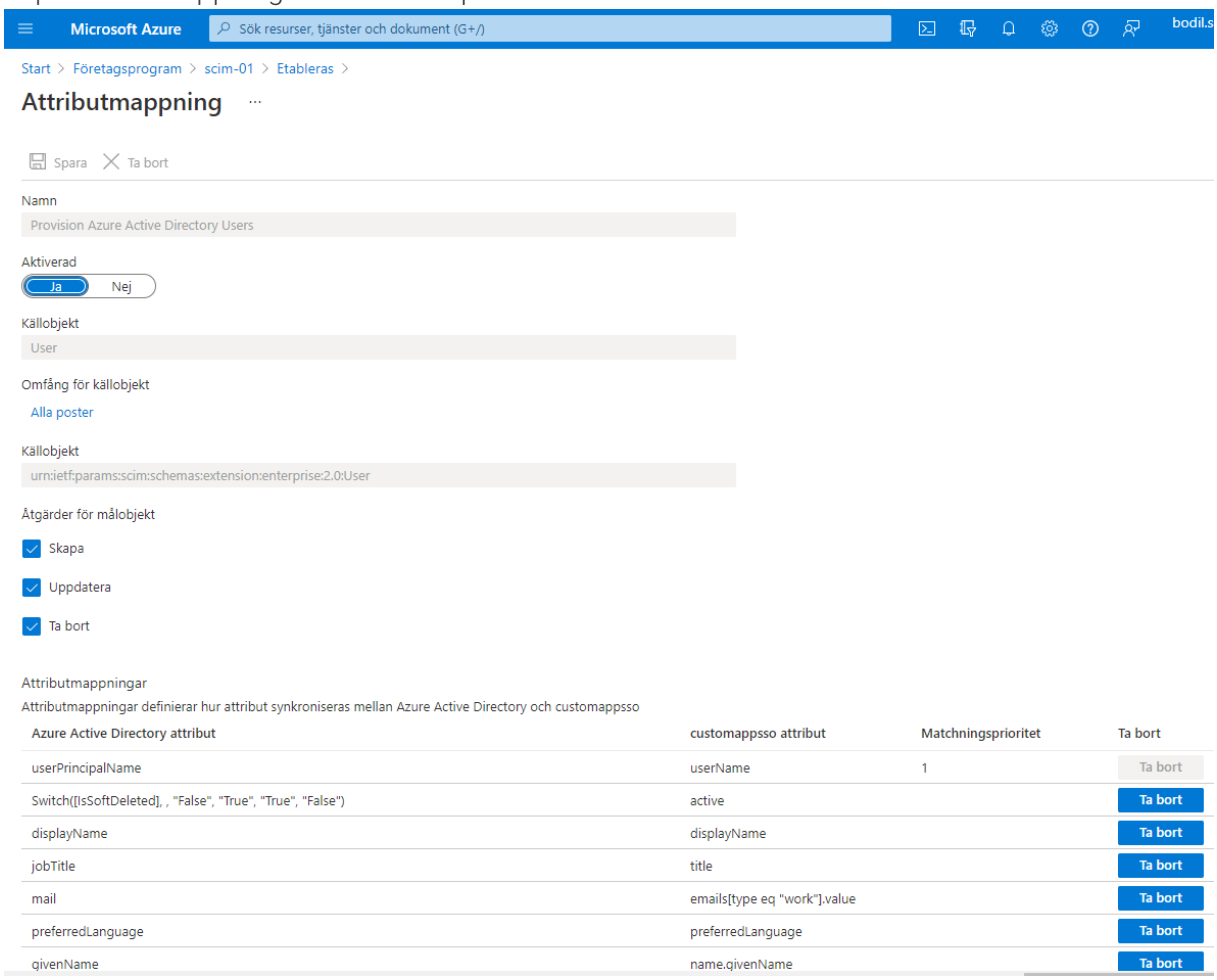
2. Expandera “Autentiseringsuppgifter för administratör” och skriv in bas-URL:en till Antura plus sökvägen till dess SCIM-API, till exempel *https://{customer}.projects.se/app/api/scim/v2/*, som *Klientorganisations-URL*.
3. Skriv in den hemliga token som är genererad av Antura. Det är en kryptografiskt unik nyckel som genereras vid aktivering av SCIM-provisioneringen (se avsnitt “Aktivera Provisionering med SCIM”).
4. Klicka på “Testanslutning” för att verifiera att inställningarna är rätt.
5. Klicka på Spara vilket kommer öppna ytterligare sektioner.
6. Expandera “Inställningar” och skriv in en e-postadress för var fel ska skickas.
7. Klicka i “Skicka ett e-postmeddelande när ett fel uppstår”.

8. Klicka på Spara

Konfigurera användarmappning

För att kunna provisionera användare måste man konfigurera mappning för provisioneringen.

1. Navigera till den nyligen skapade applikationen och klicka på “Etableras” och därefter “Redigera etablering”.
2. Expandera “Mappningar” och klicka på Provision Azure Active Directory Users



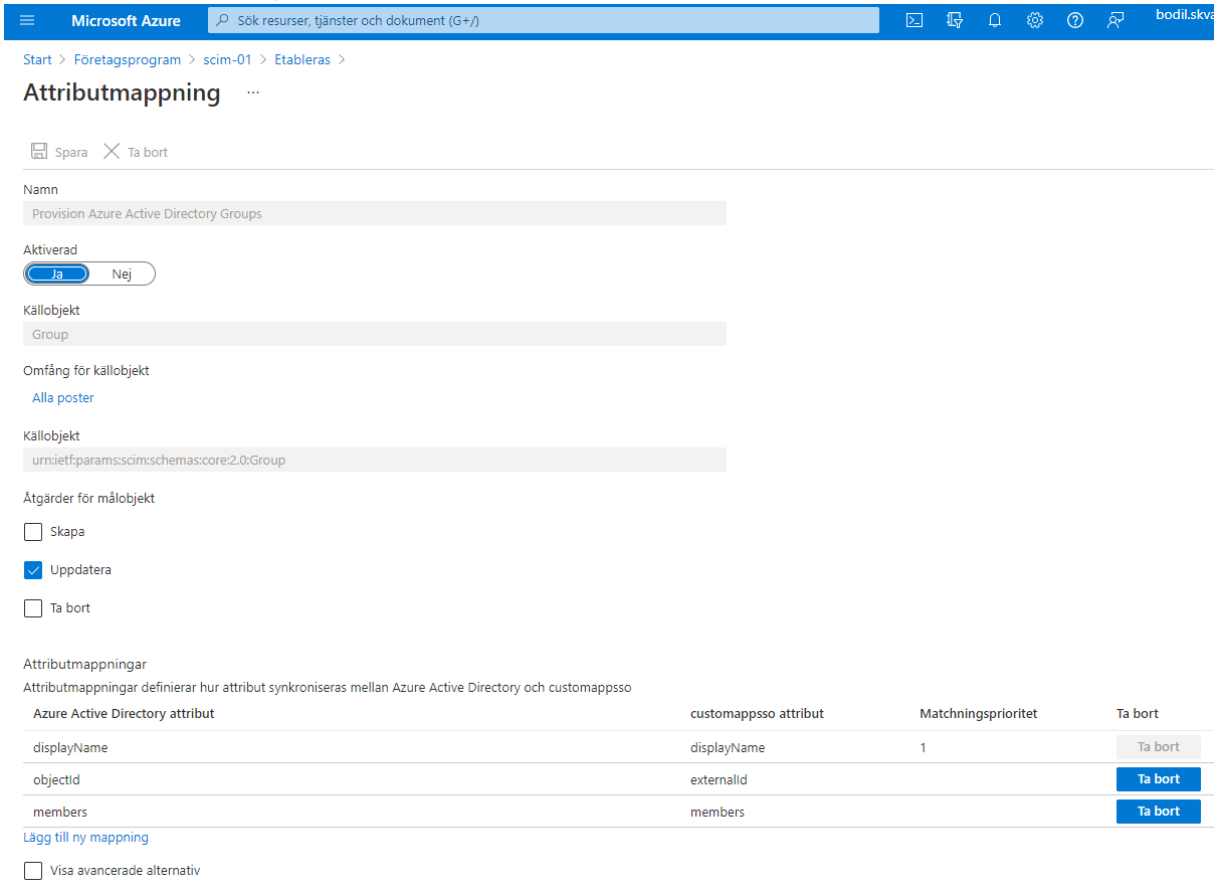
3. Klicka för vilka åtgärder som skall tas med i provisioneringen. Om nya användare inte skall skapas upp i Antura, klicka ur “Skapa”. Om användare inte skall tas bort i Antura, klicka ur “Ta bort”.
4. Mappa “userName” (i kolumnen som heter “customappsso Attribute”) till ett unikt attribut i Microsoft Entra ID (kolumnen heter “Microsoft Entra ID attribute” i portalen). **Viktigt! Använd samma mappning av userName som vid federering så att användare som skall provisioneras matchar eventuella befintliga användare i Antura, i annat fall kommer användaren inte kunna logga in. Om inte userName matchar kommer det inte att gå att autentisera användare.**

5. Dessa fält måste vara satta för att kunna skapa användare i Antura:
    1. emails[type eq “work”].value
    2. name.givenName
    3. name.familyName

Konfigurera gruppmappning

För att kunna provisionera grupper måste man konfigurera gruppmappning för provisioneringen.

1. Navigera till den nyligen skapade applikationen och klicka på “Etableras” och därefter “Redigera etablering”.
2. Expandera “Mappningar” och klicka på Provision Azure Active Directory Groups

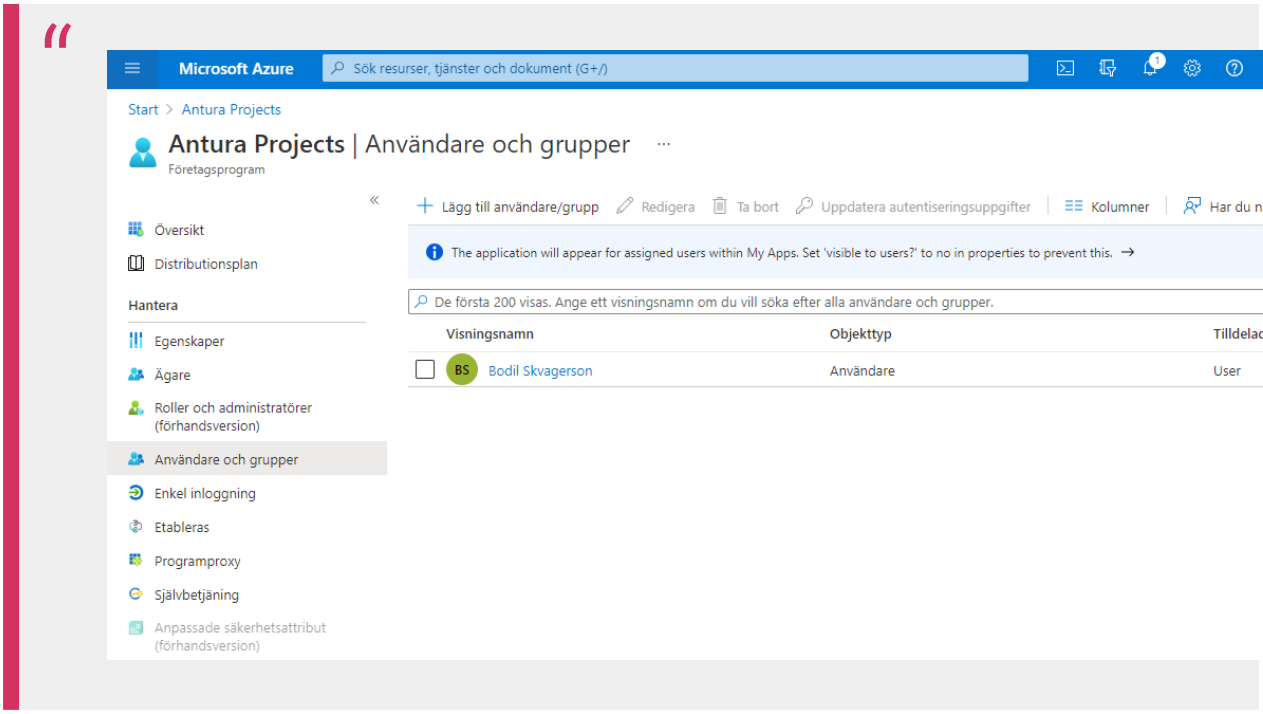


3. Klicka ur “Skapa” och “Ta bort” *Obs viktigt!* Antura har **inte** stöd för att skapa och ta bort grupper via SCIM.
4. Mappa “displayName” till ett unikt attribut i Microsoft Entra ID.
5. Mappa grupper i Microsoft Entra ID till grupper i Antura genom att ange namnet på Microsoft Entra ID-gruppen som en gruppreferens i Antura. *Notera att denna mappning är avsedd att vara en-till-en. Det finns alltså inte stöd för att mappa en grupp i Microsoft Entra ID till flera grupper i Antura.*

Konfigurera användare och grupper som skall inkluderas i provisioneringen

För att provisionera rätt användare måste man konfigurera vilka användare som ska inkluderas i provisioneringen. Om alla användare och grupper skall provisioneras gå vidare till avsnittet “Konfigurera omfång”.

1. Navigera till den nyligen skapade applikationen och klicka på “Användare och grupper”.
2. Tilldela användare och grupper till applikationen genom att klicka på “Lägg till användare/grupp” och söka på relevanta användare och grupper.



Konfigurera omfång

1. Navigera till applikationen och tryck på “Etableras” och därefter “Redigera etablering”.
2. Expandera “Inställningar”. I “Omfång”-dropdownen, välj “Synkronisera enbart tilldelade användare och grupper” eller “Synkronisera alla användare och grupper”.
   Observera att om man väljer “Synkronisera enbart tilldelade användare och grupper” måste man välja ut vilka användare och grupper som skall provisioneras, se tidigare avsnitt “Konfigurera användare och grupper som skall inkluderas i provisioneringen”.

Införande-process

Ett införande följer i stora drag processen nedan:

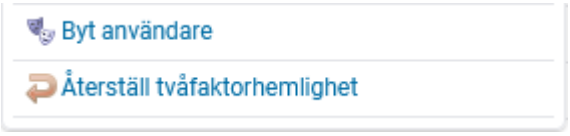
1. Kund och Antura kommer överens om den konfiguration som ska användas. T.ex. vilket protokoll som ska användas och vilka claims som ska skickas.
2. Båda sidor förbereder för införandet genom att konfigurera sina system (Antura och IdP).
3. Ett datum bestäms då införandet ska genomföras.
4. På utsatt datum aktiveras federeringen och befintliga användare konverteras om det skulle behövas.

Felsökning

Tvåfaktorsautentisering

Om det inte fungerar att logga in med autentiseringskoden så kan det bero på att telefonens tidsinställningar inte är synkroniserat. Det innebär att autentiseringskoden man ser i appen (Google Authenticator eller Microsoft Authenticator) aldrig är giltig. Prova att slå av/på synkroniseringen av tid i telefonen och testa sedan igen.

Om det fortfarande inte fungerar kan man återställa användarens tvåfaktorshemlighet via vyn *Administration – Användare*:



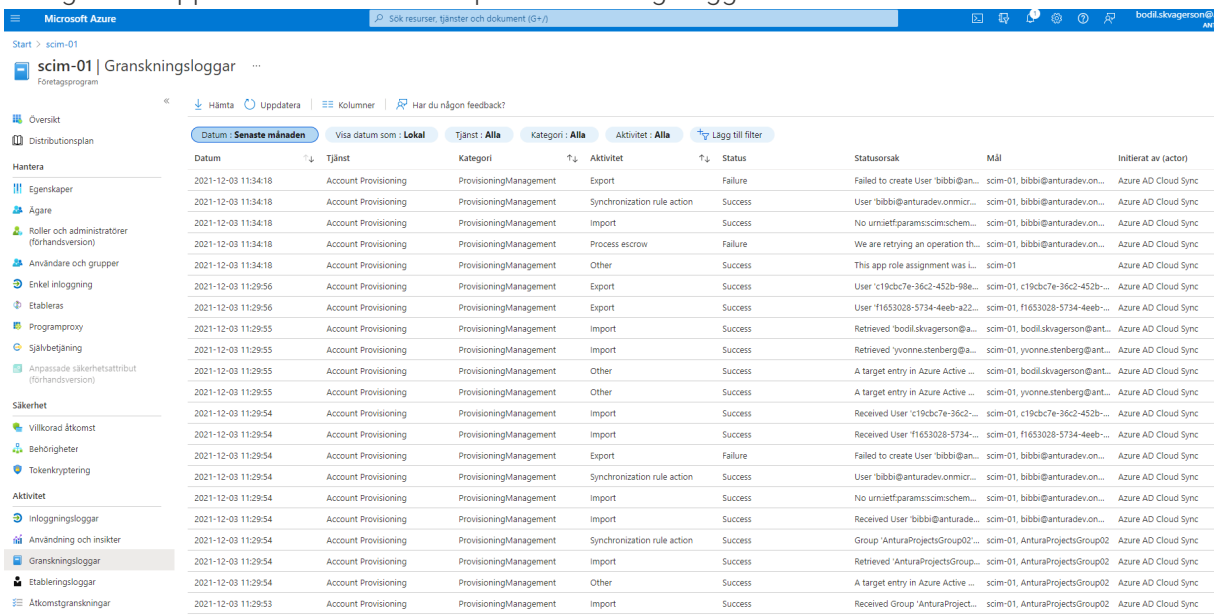
Figur 5 - Återställa hemlighet

SCIM-felsökning

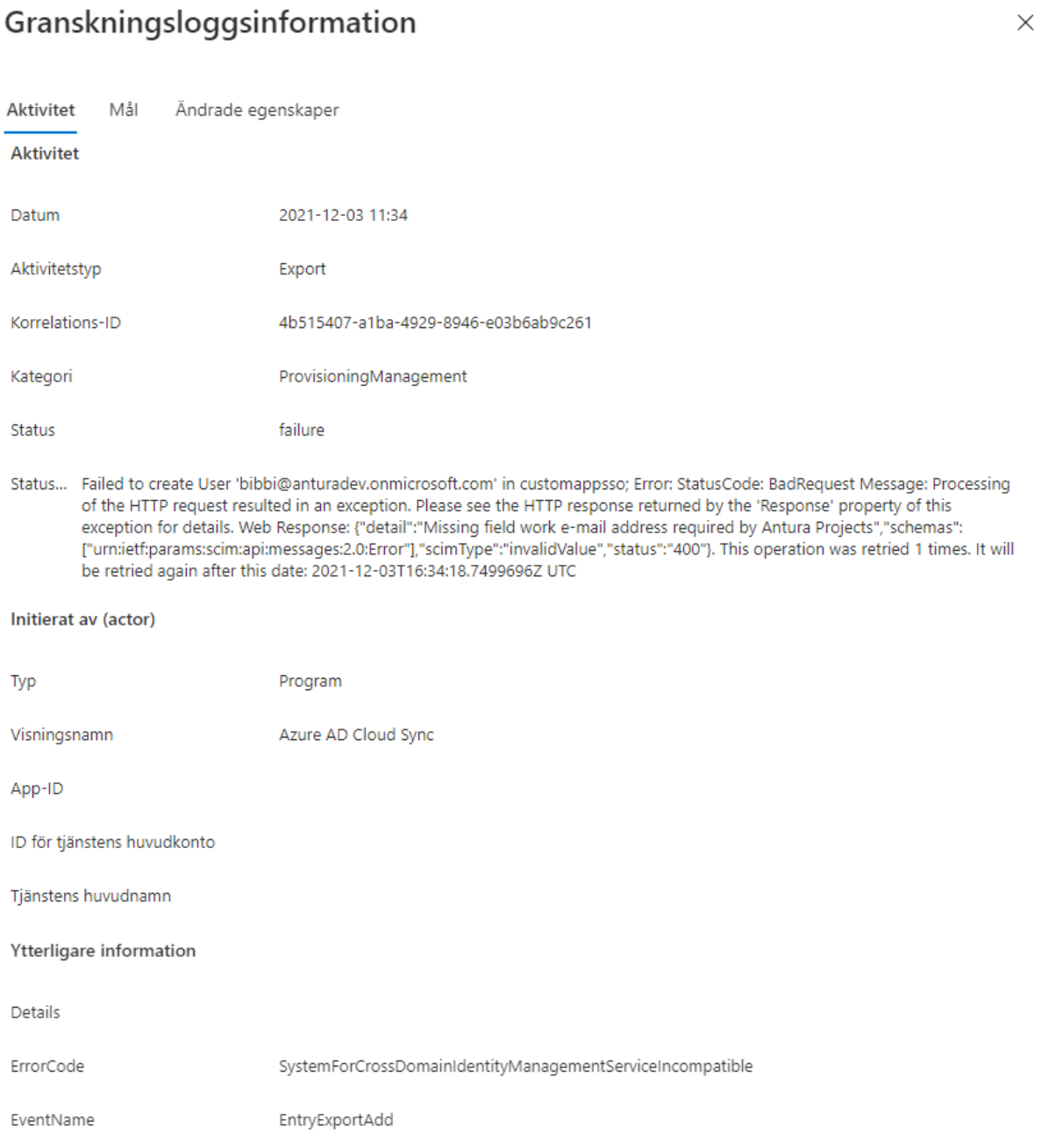
Om något går fel vid provisionering i Microsoft Entra ID kommer ett mail skickas till den e-postadress som angivits för notifieringar, förutsatt att kryssrutan “Skicka ett e-postmeddelande när ett fel uppstår” har klickats i (se avsnitt “Registrera Antura som en klientapplikation i Microsoft Entra ID”).

Det går också att se etableringsloggar i Microsoft Entra ID för mer information.

1. Navigera till applikationen och klicka på “Granskningsloggar”. >



2. Klicka på raden som har Failure som Status för att se felorsak.



Granskningsloggsinformation

Aktivitet Mål Ändrade egenskaper

Aktivitet

Datum	2021-12-03 11:34
Aktivitetstyp	Export
Korrelations-ID	4b515407-a1ba-4929-8946-e03b6ab9c261
Kategori	ProvisioningManagement
Status	failure
Status...	Failed to create User 'bibbi@anturadev.onmicrosoft.com' in customappsso; Error: StatusCode: BadRequest Message: Processing of the HTTP request resulted in an exception. Please see the HTTP response returned by the 'Response' property of this exception for details. Web Response: {"detail":"Missing field work e-mail address required by Antura Projects","schemas":["urn:ietf:params:scim:api:messages:2.0:Error"],"scimType":"invalidValue","status":"400"}. This operation was retried 1 times. It will be retried again after this date: 2021-12-03T16:34:18.7499696Z UTC

Initierat av (actor)

Typ	Program
Visningsnamn	Azure AD Cloud Sync
App-ID	
ID för tjänstens huvudkonto	
Tjänstens huvudnamn	

Ytterligare information

Details	
ErrorCode	SystemForCrossDomainIdentityManagementServiceIncompatible
EventName	EntryExportAdd

SCIM-attributmappning

Användarattribut

Denna tabell beskriver hur användarinformation i Microsoft Entra ID mappas mot användarinformation i Antura (AP) via SCIM (se https://tools.ietf.org/html/rfc7643#section-4.1 och https://tools.ietf.org/html/rfc7643#section-4.3).

Observera att mappning av andra fält än dem som omnämns nedan inte känns igen av Antura och kommer därför att generera fel vid provisionering.

Microsoft Entra ID (default)	SCIM	Antura
userPrincipalName	userName	Username (User.Login)
Switch([IsSoftDeleted], , “False”, “True”, “True”, “False”)	active (User.	Status – Activated/ Deactivated Active)
displayName	displayName	Only used by SCIM (User.ExternalDisplayName)
jobTitle	title	Only used by SCIM (User.ExternalTitle)
mail	emails[type eq “work”].value E-	mail (User.Email1)
preferredLanguage	preferredLanguage	*Ignored*
givenName	name.givenName	First name (User.FirstName)
surname	name.familyName	Last name (User.LastName)
Join(“ “, [givenName], [surname]) na	me.formatted *I	gnored, does not exist in Antura*
physicalDeliveryOfficeName	addresses[type eq “work”].formatted *I	gnored*
streetAddress	addresses[type eq “work”]. St streetAddress	reet address (User.StreetAddress)

Microsoft Entra ID (default)	SCIM	Antura
city	addresses[type eq “work”].locality *S	ee postalCode below*
state	addresses[type eq “work”].region *I	gnored, does not exist in Antura*
postalCode	addresses[type eq “work”]. Po postalCode	stal address (User.Address gets the value “{postalCode}, {locality}[, {country}]”)
country	addresses[type eq “work”].country *S	ee postalCode above*
telephoneNumber	phoneNumbers[type eq “work”].value Ph	one (User.Telephone)
mobile	phoneNumbers[type eq “mobile”]. Mo value	bile (User.MobilePhone)
facsimileTelephoneNumber	phoneNumbers[type eq “fax”].value Fa	x (User.Facsimile)
mailNickname	externalId	Only used by SCIM (User.ExternalId)
employeeId	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: employeeNumber	*Ignored*
department	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: department	Department (User.Department)
manager	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: manager	*Ignored, does not exist in Antura*

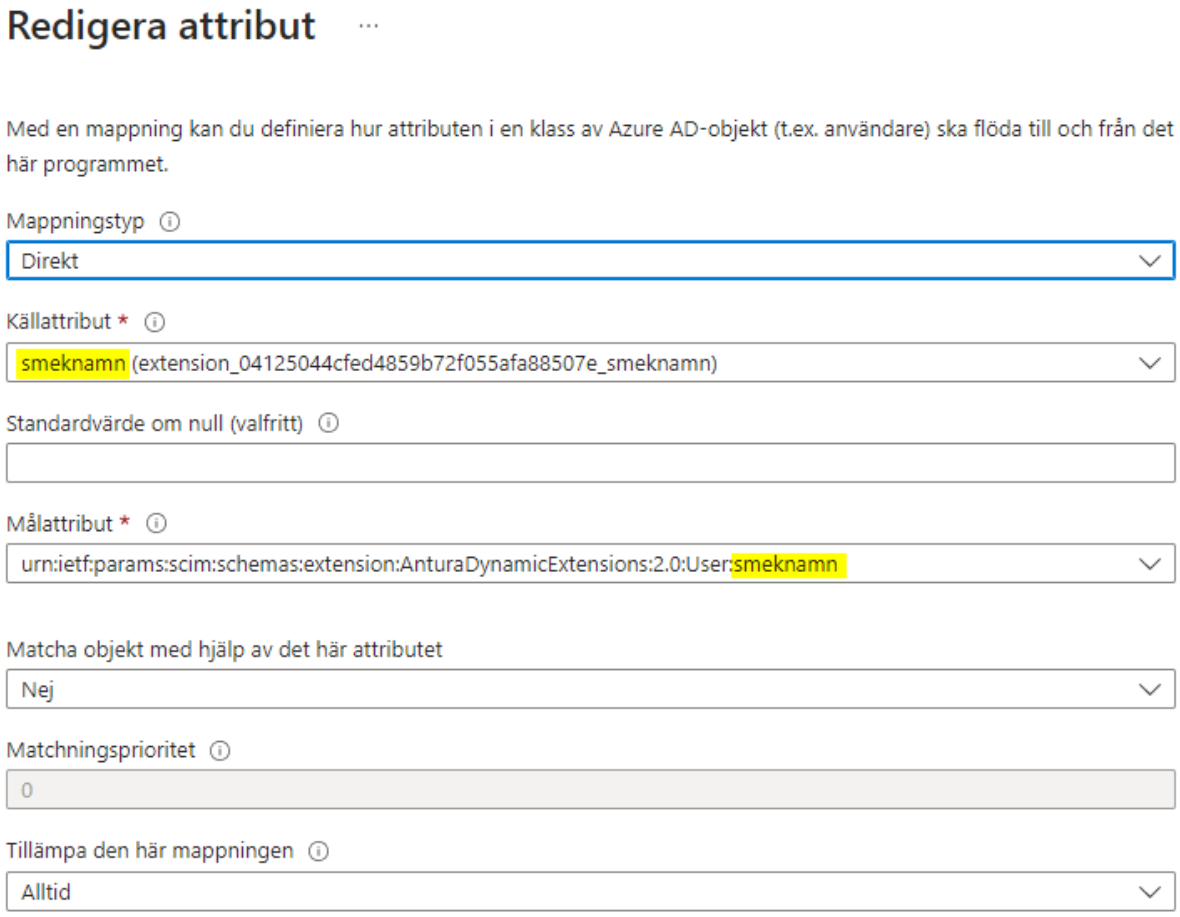
Microsoft Entra ID (default)	SCIM	Antura
companyName	urn:ietf:params:scim:schemas:extension:AnturaFixedExtensions:2.0:User:company. For mapping of companyName to work the companyName needs to be manually mapped to this schema [1].	Company (User.Company)
Note that default is missing in Microsoft Entra ID for organizational unit. For mapping of org unit to work, the org unit needs to be mapped to a field in Microsoft Entra ID such as companyName.[2]	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	Org. unit (mapped through the field “Reference” on organizational unit)
	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:costCenter	*Ignored*
	nickName	*Ignored, does not exist in Antura*
	profileUrl	*Ignored, does not exist in Antura*
	userType	*Ignored, does not exist in Antura*
	locale	*Ignored*
	timezone	*Ignored, does not exist in Antura*

Användaregenskaper

Använd Microsoft Graph PowerShell-cmdlet **`New-MgApplicationExtensionProperty`** (i modulen **`Microsoft.Graph.Applications`**) för att skapa en ny användaregenskap i Microsoft Entra ID.

Mappa användaregenskapen till ett SCIM-attribut i Microsoft Entra ID

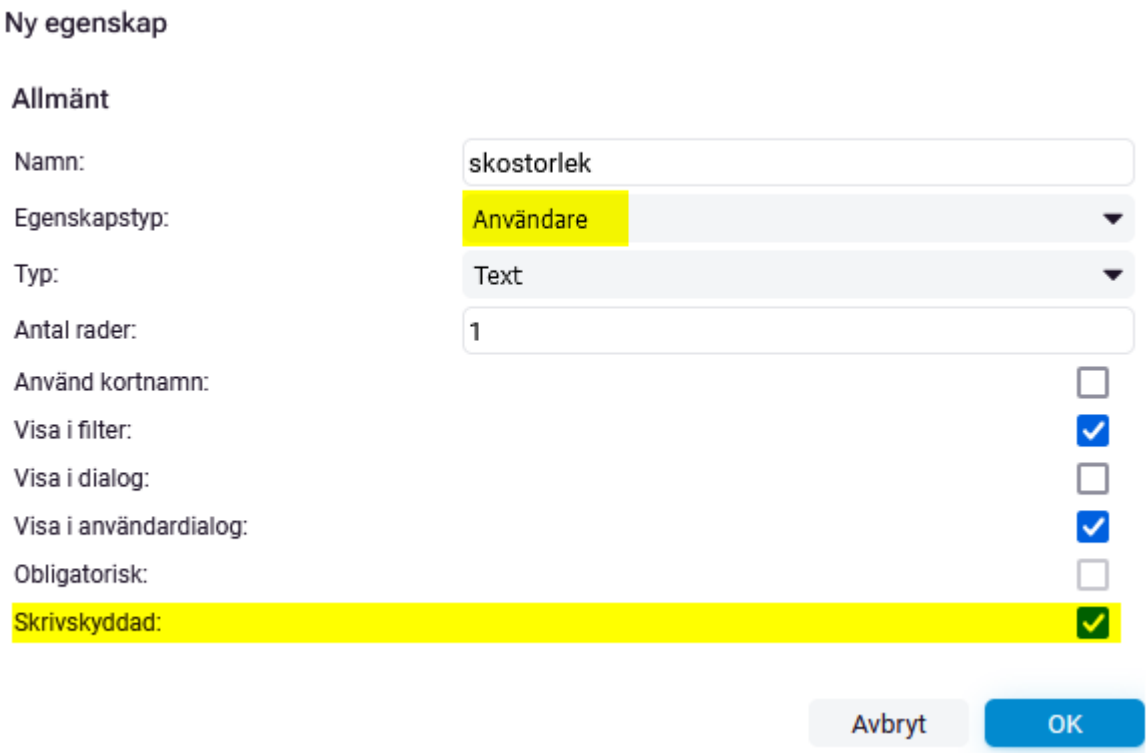
1. Navigera till applikation i Microsoft Entra ID och klicka på “Etableras” och därefter “Redigera Etablering”. Klicka “Mappningar” och välj “Provision Microsoft Entra ID Users”.
2. Klicka på “Visa avancerade alternativ” längst ner på sidan och välj “Redigera attribut lista för customappsso”.
3. Lägg till ett attribut med prefixet “urn:ietf:params:scim:schemas:extension:AnturaDynamicExtensions:2.0:User:”. *Notera att enbart text och numeriska typer är tillåtna för användaregenskaper. För att mappa numeriska typer till Antura måste typen i Microsoft Entra ID vara “text”, exempel på giltiga numeriska värden är “-4”, “42” och “33.5”.*
4. Spara ändringarna och gå till föregående sida “Attributmappning”.
5. Klicka på “lägg till ny mappning” längst ner på sidan. Exempel med ett attribut som kallas för “smeknamn”.



Skapa användaregenskapen i Antura

1. Navigera till sidan *Systemegenskaper* i Administration – System.

2. Skapa en ny egenskap med samma namn och typ (text eller numerisk) som egenskapen i Microsoft Entra ID. Välj egenskapstypen “Användare”. Egenskapen måste vara skrivskyddad eftersom Microsoft Entra ID skriver över alla värden i Antura. Exempel med ett attribut som kallas för “skostorlek”.



Notera:

- Mappning av användaregenskaper stöds enbart för egenskaper med ett **unikt namn** i Antura. Jämförelsen är inte skiftlägeskänslig.
- Att **ta bort ett användaregenskapsvärde** i Microsoft Entra ID provisioneras inte till Antura. Detta beror på att Microsoft Entra ID inte provisionerar tomma värden.
- Det rekommenderas att ha de synkroniserade värdena som **skrivskyddade** i Antura, eftersom förändringar kommer att skrivas över vid nästa synkronisering.

Gruppattribut

Denna tabell beskriver hur gruppinformation i Microsoft Entra ID mappas mot gruppinformation i Antura via SCIM (se https://tools.ietf.org/html/rfc7643#section-4.2).

Microsoft Entra ID (default)	SCIM attribute	Antura
displayName	displayName	Group (mapped through field “Group reference” on the group)
objectId	externalId	Only used by SCIM (Group.ExternalId)
members	members	Members of the group (SystemRoleService.GetMembers)

Synkronisering av tilläggsattribut

För användare i Active Directory **on-prem** måste du synkronisera användarna till Microsoft Entra ID. Microsoft Entra ID Connect synkroniserar automatiskt vissa attribut till Microsoft Entra ID, men inte alla attribut. Dessutom kan vissa attribut (så som SAMAccountName) som är synkroniserade som standard inte exponeras med Graph API. I dessa fall kan du använda en funktion i Microsoft Entra ID Connect för att synkronisera attributet till Microsoft Entra ID. På så sätt kommer attributet att vara synligt för Graph API och Microsoft Entra ID provisioning-tjänsten. För mer information se use the Microsoft Entra ID Connect directory extension feature to synchronize the attribute to Microsoft Entra ID.

---

1. Om ingen mappning av attributet görs kommer fältet inte att synkas.↩
2. Om ingen mappning av attributet görs kommer fältet inte att synkas.↩