Del 5 – Identitetshantering i Microsoft Entra ID

MFA och Villkorsstyrd Åtkomst – GreenTyre Recycling AB

Datum	2026-03-05
Upprättad av	Julian Rieger – IT-säkerhetskonsult
Kurs	IAM – Identity and Access Management
Tenant	julianflaggoronline.onmicrosoft.com

1. Inledning

Denna labb demonstrerar hur GreenTyre Recycling AB implementerar identitetshantering i molnet via Microsoft Entra ID (tidigare Azure Active Directory). Labben omfattar skapandet av användarkonton med tilldelade roller, aktivering av Multifaktorautentisering (MFA) samt en genomgång av Villkorsstyrd åtkomst (Conditional Access).

2. Labbmiljö

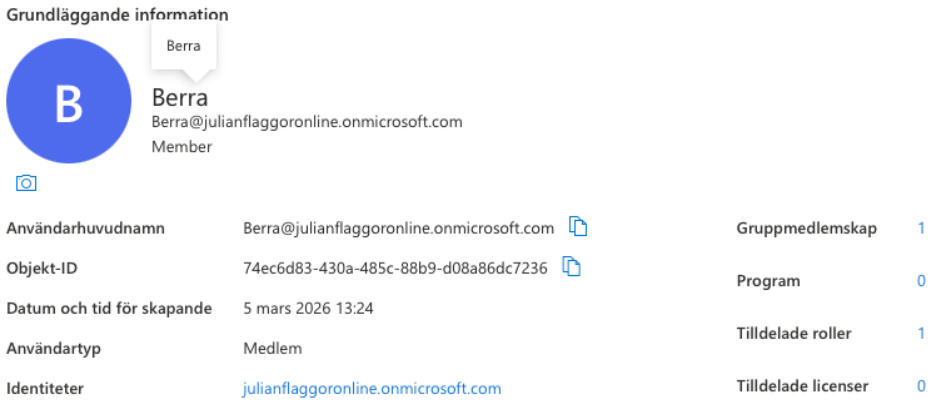
Komponent	Detaljer
Tenant	julianflaggoronline.onmicrosoft.com
Licens	Microsoft Entra ID Free (Azure-prenumeration 1)
Adminverktyg	Microsoft Entra-administratörscenter (entra.microsoft.com) + Azure CLI

3. Skapade användare

Tre interna användarkonton skapades i Entra ID-tenanten. Kontona representerar olika behörighetsnivåer i enlighet med principen om minsta privilegium.

Visningsnamn	UPN	Roll	Typ
DA_Admin	DA_Admin@julianflaggoronline.onmicrosoft.com	Global administratör	Medlem
Berra	Berra@julianflaggoronline.onmicrosoft.com	Skrivartekniker	Medlem
terminalator	terminalator@julianflaggoronline.onmicrosoft.com	Ingen (vanlig användare)	Medlem

Figur 1 – Användarlista i Microsoft Entra ID med de skapade kontona

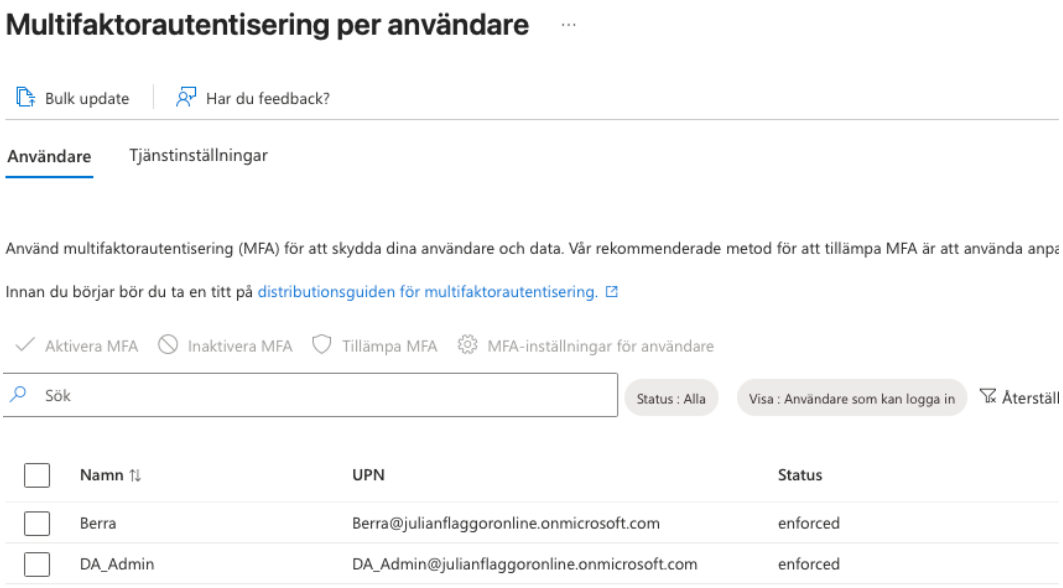


Figur 2 – Berras användarprofil med Skrivartekniker-rollen tilldelad

4. Multifaktorautentisering (MFA)

MFA aktiverades via "Multifaktorautentisering per användare" i Entra-administratörscentret. Metoden som konfigurerades är SMS och/eller Microsoft Authenticator-appen, i enlighet med labbinstruktionens rekommendation om Phone Authenticator.

Användare	MFA-status	Metod
DA_Admin	**Enforced**	Microsoft Authenticator / SMS
Berra	**Enforced**	Microsoft Authenticator / SMS
terminalator	**Enforced**	Microsoft Authenticator / SMS

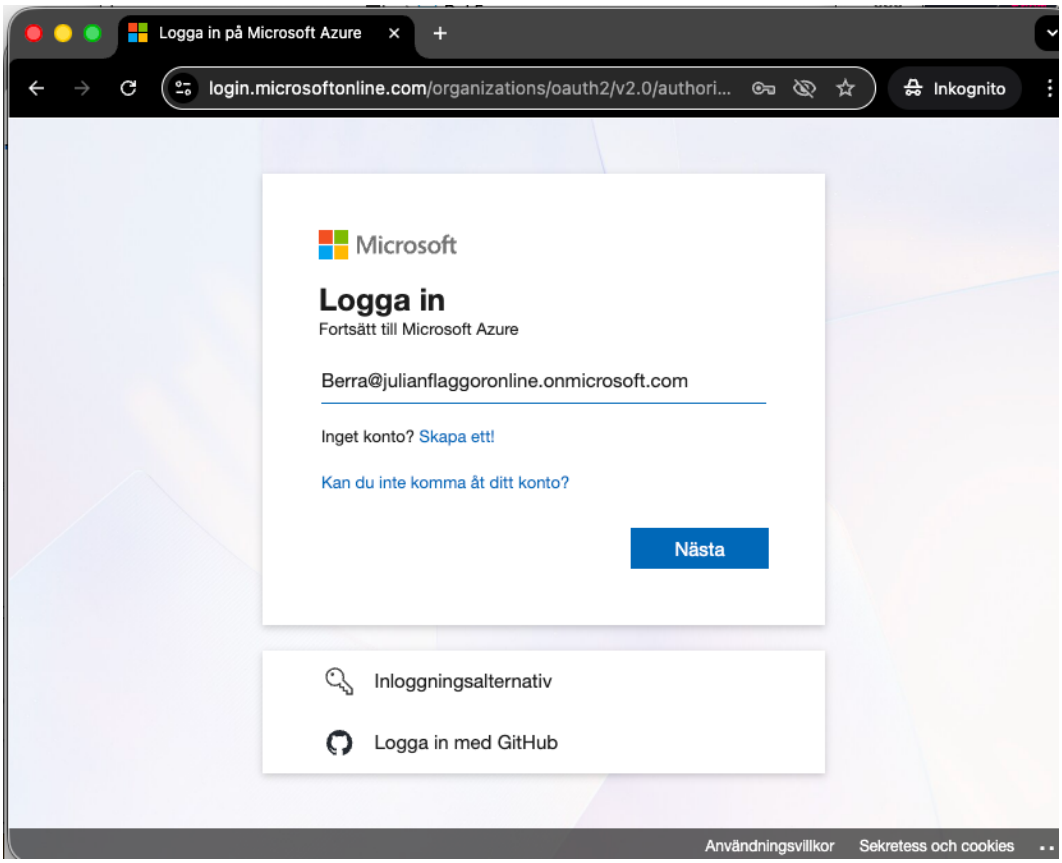


Figur 3 – MFA-status "enforced" för samtliga användare i Entra ID

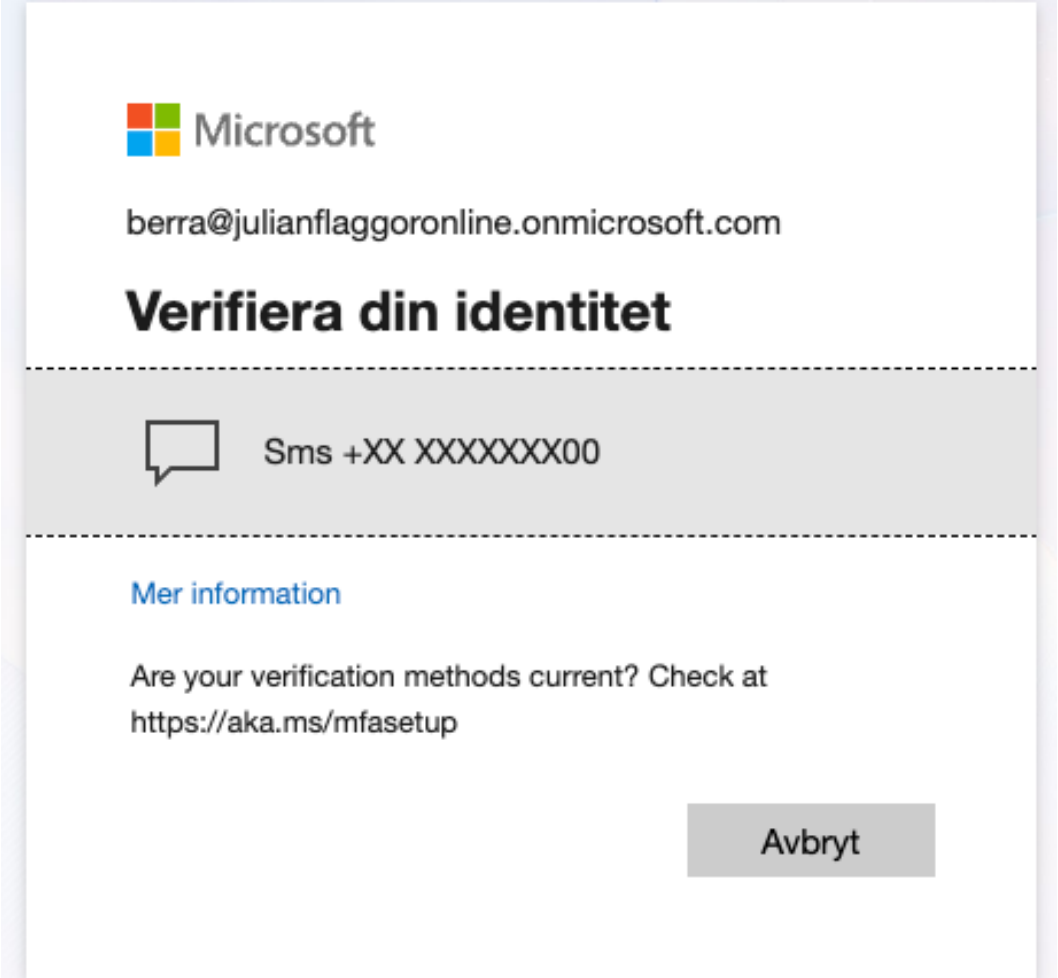
4.1 Test – MFA-inloggning som Berra

Ett inloggningstest genomfördes i inkognito-läge som Berra@julianflaggoronline.onmicrosoft.com. Testet visar att MFA-porten fungerar korrekt. Användaren blockeras och tvingas verifiera sin identitet via SMS innan åtkomst beviljas.

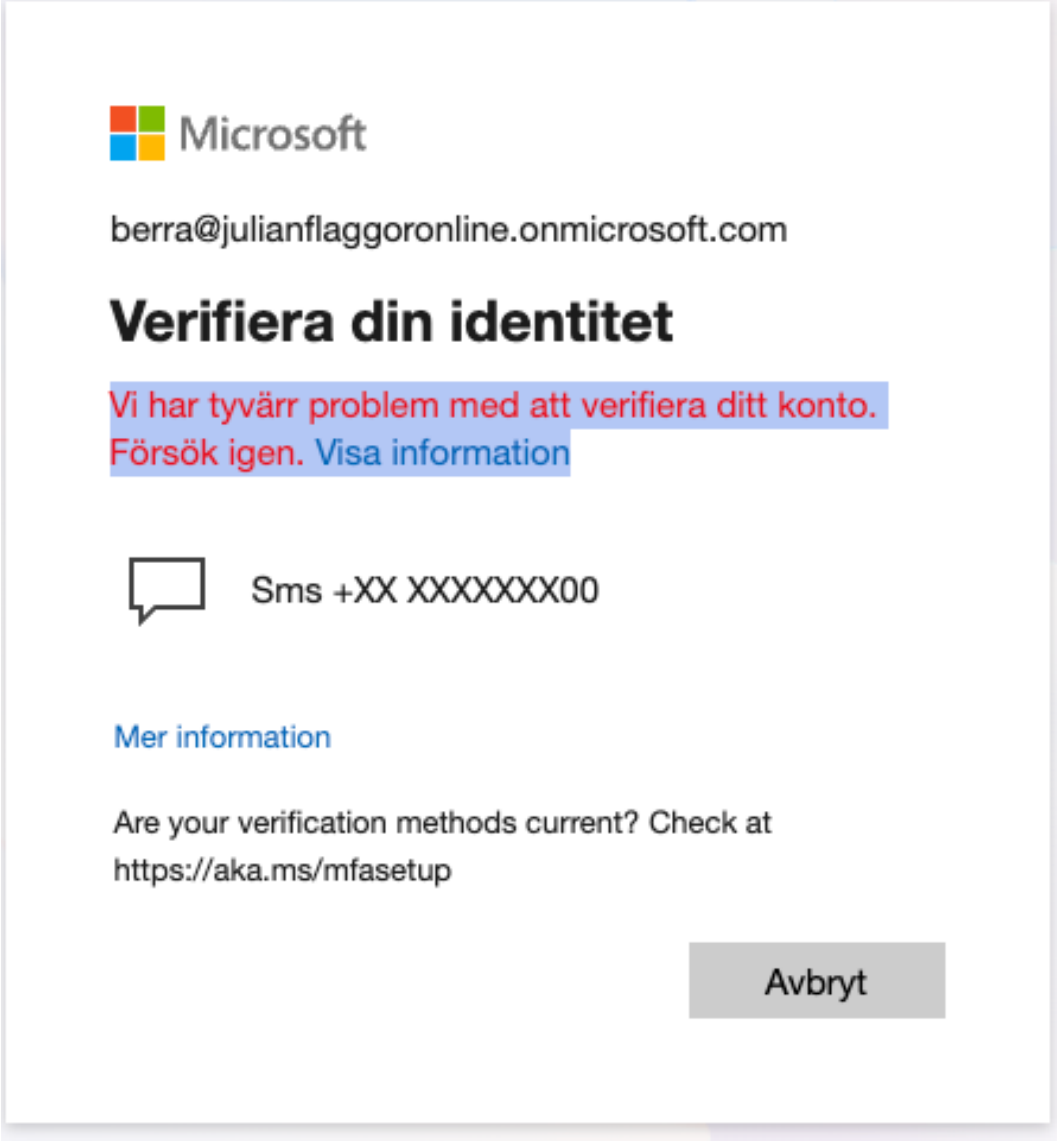
Microsoft kunde inte leverera SMS-koden under testet, vilket är en känd begränsning för nya konton i free-tier-tenanter utan aktiv P1/P2-licens. Felmeddelandet bekräftar dock att MFA är aktivt och att inloggning utan verifiering nekas.



Figur 4 – Inloggningssida för Berra i inkognito-läge



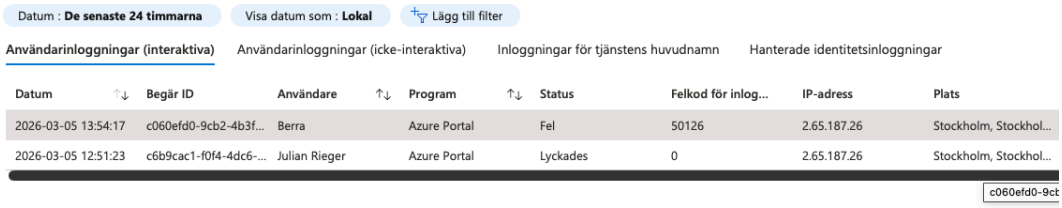
Figur 5 – MFA-prompt: Berra uppmanas verifiera sin identitet via SMS



Figur 6 – MFA blockerar inloggning: SMS-leverans misslyckades (free-tier-begränsning)

4.2 Inloggningsloggar i Entra ID

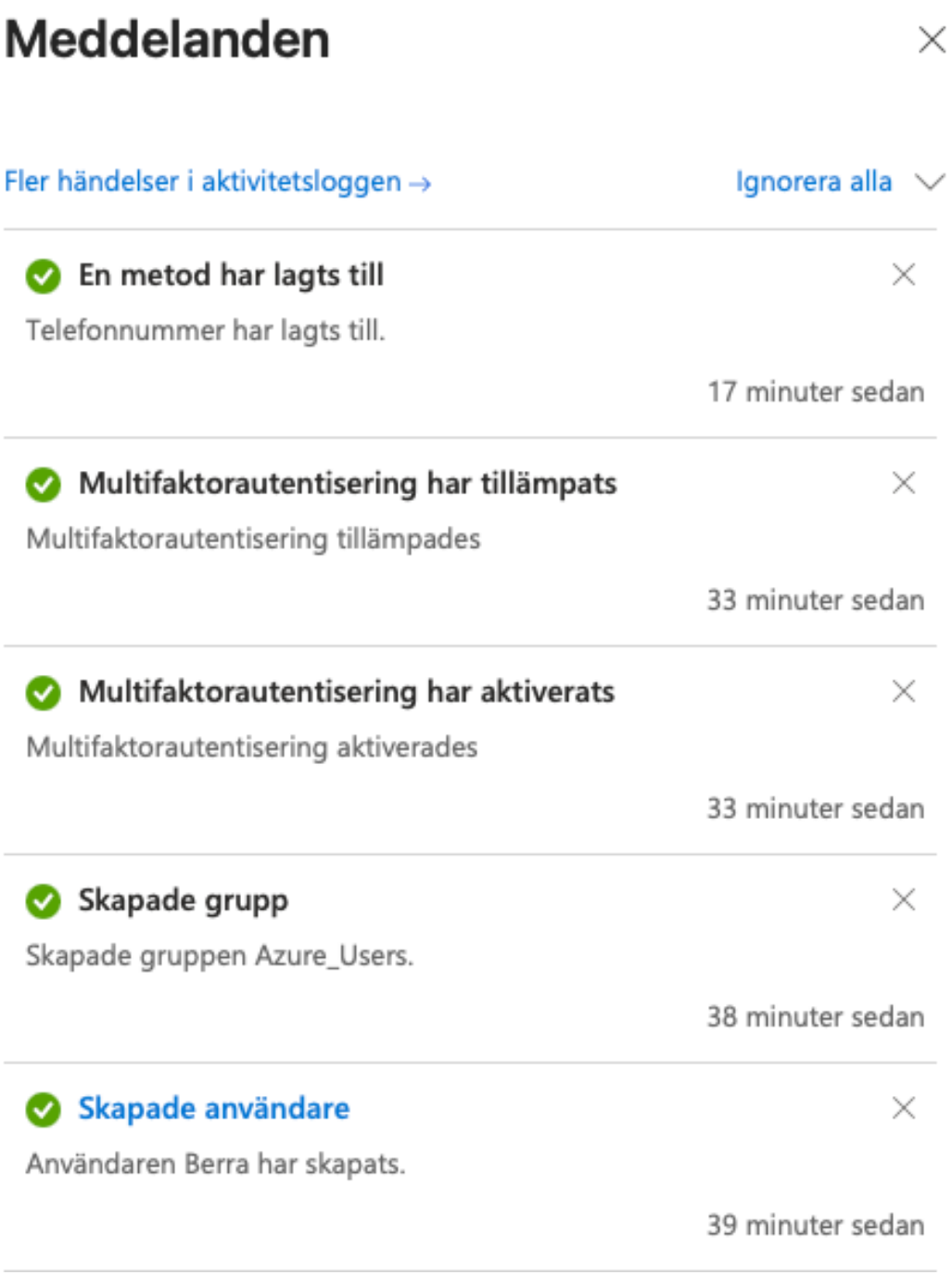
Inloggningsloggarna i Entra-administratörscentret bekräftar MFA-aktiviteten. Loggen nedan visar Berras inloggningsförsök (felkod 50126 – MFA-verifiering misslyckades) samt en lyckad inloggning för administratörskontot från samma IP-adress i Stockholm.



Figur 7 – Inloggningsloggar i Entra ID: Berra (Fel/50126) och Julian Rieger (Lyckades)

4.3 Aktivitetslogg – granskningslogg

Aktivitetsloggen i Entra ID bekräftar hela konfigurationskedjan i kronologisk ordning: användaren Berra skapades, gruppen Azure_Users skapades, MFA aktiverades och tillämpades, samt att ett telefonnummer registrerades som autentiseringsmetod.



Figur 8 – Aktivitetslogg: skapande av Berra, MFA-aktivering och telefonnummer tillagt

5. Villkorsstyrd åtkomst (Conditional Access)

Labbinstruktionen för Conditional Access innehåller följande notering: "You can do this LAB IF you could do so, taking licensing into account." Villkorsstyrd åtkomst kräver minst Microsoft Entra ID P1-licens.

Tenanten som användes i denna labb är ett eget free tier-konto. Kursen är kopplad till ett Lernia-studentkonto (julian.rieger@lerniastudent.se) från en tidigare DevOps-utbildning 2023, men de Microsoft Azure-krediter som tilldelades då tog slut och fylldes aldrig på inför denna kurs. Därmed genomfördes labben på det egna free tier-kontot, vilket saknar P1/P2-licens.

Nedan dokumenteras de steg som skulle ha genomförts med P1-licens:

Steg	Åtgärd
Steg 1	Skapa CA-princip från mallen "Kräv MFA för administratörer"
Steg 2	Exkludera administratörskontot från principen för att undvika utelåsning
Steg 3	Lägg till molnappar: Key Vault och Storage
Steg 4	Konfigurera plats: Sverige (standard-IP)
Steg 5	Bevilja åtkomst med krav: Multifaktorautentisering
Steg 6	Aktivera principen i läget "På"

Notering: Denna del av labben kunde inte genomföras praktiskt på grund av licensbegränsning i tenanten. Dokumentationen ovan beskriver de steg som skulle genomföras i en produktionsmiljö med Entra ID P1/P2.

6. Koppling till NIS2 och ISO 27002:2022

Krav/Kontroll	Källa	Hur labben uppfyller kravet
Art. 21.2(a) – Åtkomstkontroll	NIS2	Användare tilldelas roller efter minsta privilegium; DA_Admin är enda Global Admin
Art. 21.2(b) – Stark autentisering	NIS2	MFA enforced på samtliga konton – autentisering kräver två faktorer
Kontroll 8.2 – Privilegierad åtkomst	ISO 27002:2022	DA_Admin separerad som dedikerat administratörskonto
Kontroll 5.17 – Autentisering	ISO 27002:2022	MFA via SMS/Authenticator säkerställer att lösenord ensamt ej räcker

7. Slutsats och reflektion

Labben visar hur grundläggande IAM-principer implementeras i Microsoft Entra ID. Tre användarkonton skapades med tydlig rollseparation: en Global administratör (DA_Admin), en teknikroll (Berra – Skrivartekniker) och en standardanvändare (terminalator). MFA aktiverades i

Enforced-läge för samtliga konton, vilket innebär att inloggning alltid kräver en andra faktor utöver lösenordet.

Conditional Access-delen kunde inte genomföras praktiskt på grund av att Entra ID P1-licensen inte var aktiv i tenanten. Stegens dokumentation visar dock att principen "Kräv MFA för administratörer" med koppling till Key Vault och Storage samt platsbegränsning till Sverige.

- Rollseparation: DA_Admin är Global Admin, Berra är Skrivartekniker och terminalator är standardanvändare
- MFA Enforced: Samtliga konton kräver stark autentisering vid inloggning
- Conditional Access: Dokumenterat men ej genomfört praktiskt – kräver Entra ID P1
- NIS2-efterlevnad: Uppfyller krav på åtkomstkontroll och stark autentisering