Vitec Identity

Identitets- och rollhantering i Vitec Bygg och Fastighet

2020-11-30

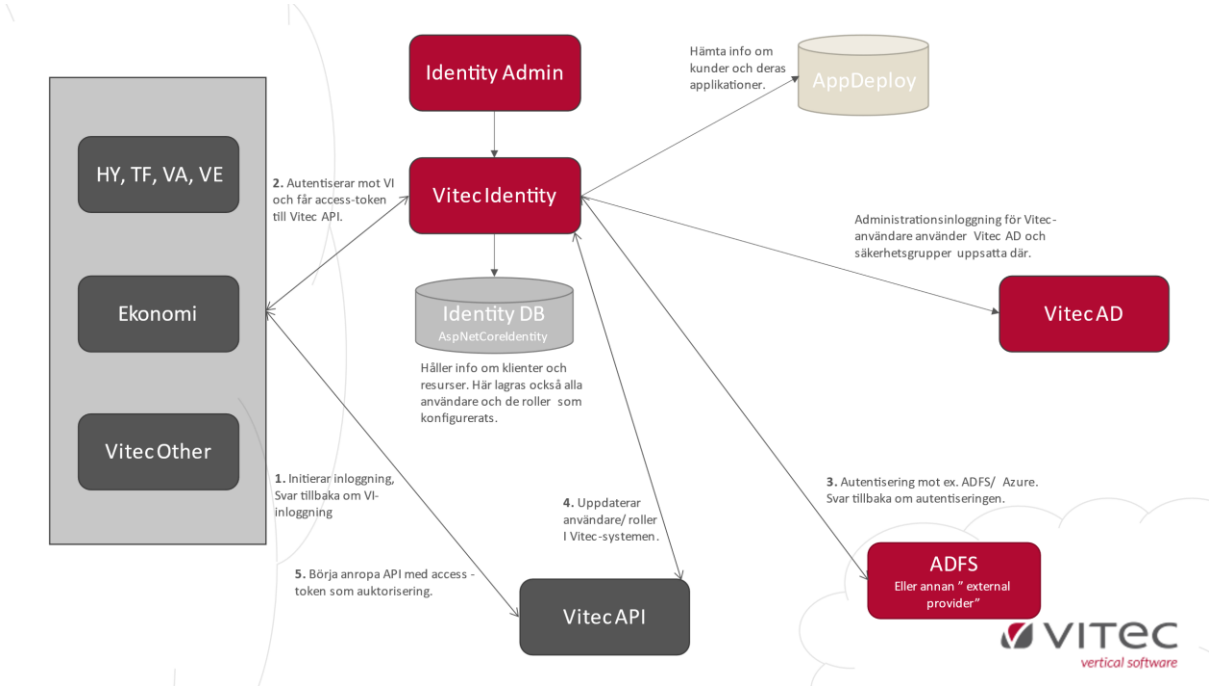
Table of Content

Vitec Identity

Vitec Identity möjliggör en gemensam autentisering och auktorisering för produkter i Vitec Bygg och Fastighet. Vitec Identity förkortas VI i detta dokument.

VI hanterar inloggning och identifikation av användare samt erbjuder möjligheten att koppla ihop roller i Vitec-systemen med säkerhetsgrupper i ert AD-system. VI bygger på standardiserade protokoll (OIDC och OAuth2) och moderna tekniker (AspNetCore) vilket ger ett framtidssäkert och robust sätt att logga in i och hantera era användares behörigheter i Vitec-systemen.

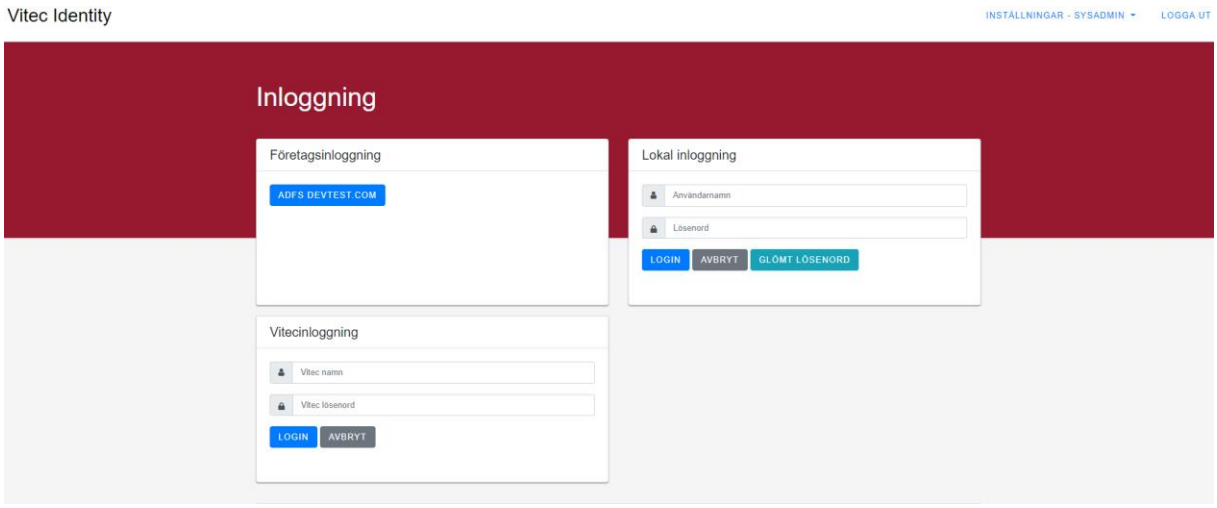
Vitec Identity – Systemöverblick och inloggningsflöde



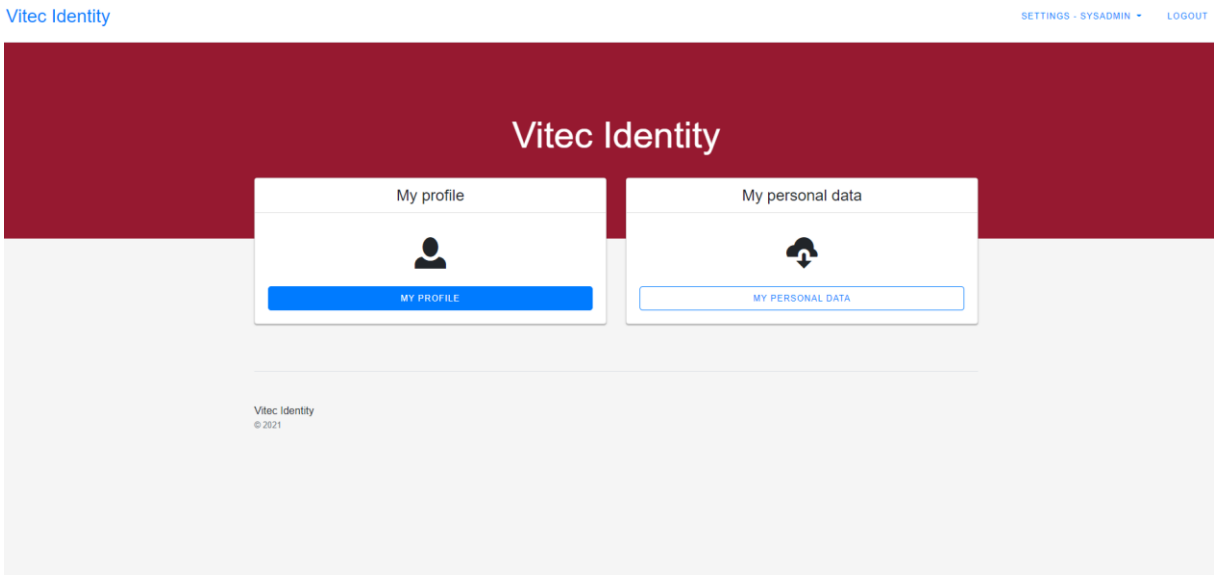
1. Vitec-klienter initierar en autentisering mot ett Vitec-API (resurs). När systemet är konfigurerat att använda VI så kommer inloggningen i klienten att styras dit.
2. Om en extern IdP används (ex. ADFS eller AzureAD) så skickar VI automatiskt vidare till denna IdP. Om användaren autentiseras får VI svar om den godkända inloggningen tillsammans med uppgifter om användaren (ex. vilka ”grupper” användaren har som senare kan kopplas till roller i Vitec).
3. Vid ok inloggning skapar sedan VI ett token som klienten kan skicka med till API-anropen som ”biljett” och efter API har validerat detta token mot VI tillåts klient kommunicera med API.
4. Om en användare inte finns sedan tidigare i den databas som hör till den startade klienten, så skapas den upp där med uppgifter från inloggningen.
5. Rollkopplingar uppsatta i VI Admin (säkerhetsgrupper i AD mot roller i de olika Vitec-systemen) kontrolleras och användaren får automatiskt roller i Vitec-systemen utifrån den satta roll-konfigurationen.

Vitec Identity

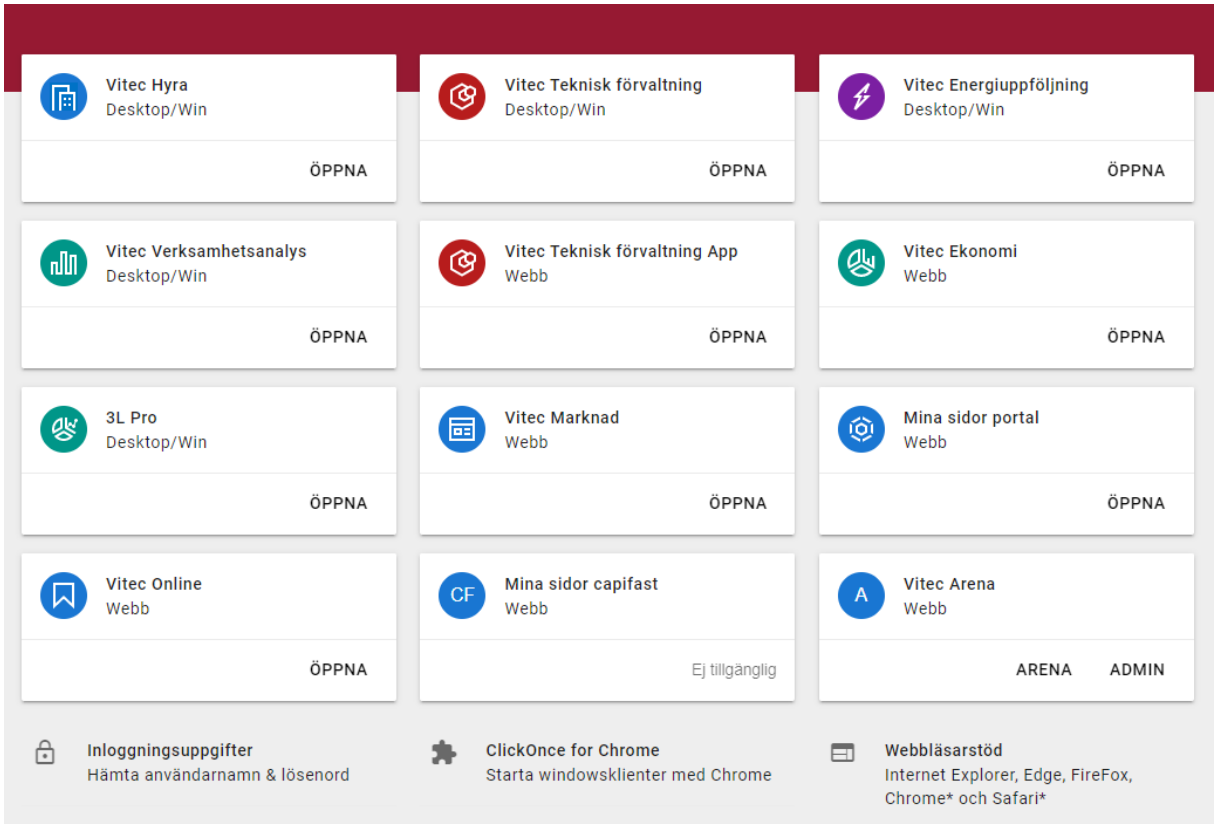
Gränssnittet i VI hanterar dels inloggningssidan, vars innehåll beror av konfiguration. Det en användare ser vid inloggning beror på flera saker, mer om det längre fram i dokumentet.



Efter inloggning mot VI kan användaren, om man går till identity-sidan under er molninstallation, bland annat se de uppgifter som är lagrade för personen i fråga. Denna information är idag inte synkroniserad mot Vitec-systemen som användaren loggar in mot, men det planeras i framtiden.

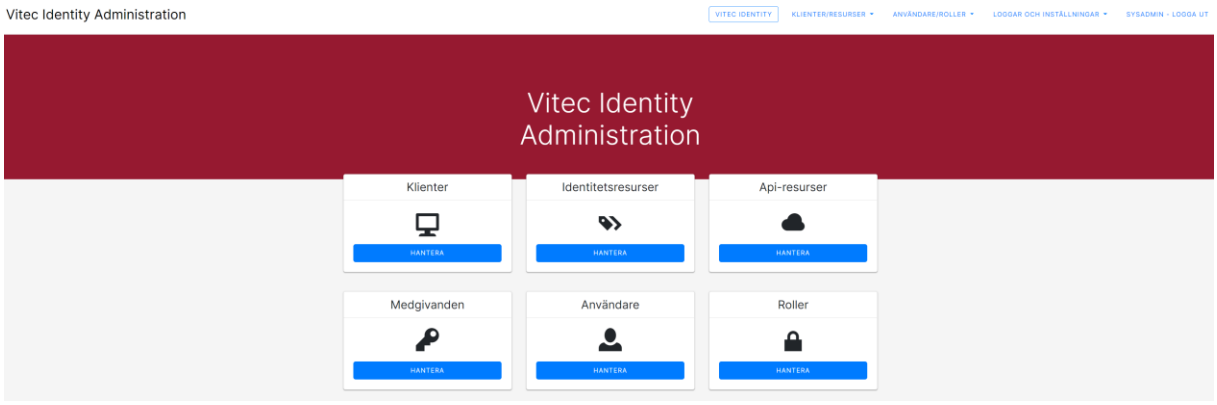


Efter utloggning från Vitec-systemen kommer en användare att dirigeras till er startsida i Vitec-molnet.



Vitec Identity Admin (VI Admin)

VI Admin är ett administrationsgränssnitt mot Vitec Identity som ger möjlighet att redigera användare/roller/klienter/resurser. Det är en administrations-site för att administrera era VI-inställningar. Vitec kan nå denna sida för att konfigurera er miljö samt utföra eventuell felsökning.



Kund-administratör – en anpassad roll

Det finns en fördefinierad roll för er i detta gränssnitt som når vissa utvalda delar av administrations-gränssnittet. Användare, roller, information om användarinloggningar samt loggar är åtkomligt för användare med denna roll, vilket gör att ”kund-administratörer” kan kontrollera och styra VI på de områden som rör era användare.

En administratör hos Vitec tilldelar denna behörighet till de användare hos er som ni önskar kunna nå detta. Längre fram i dokumentet visas kund-administratörens vyer i VI Admin.

Generell funktionalitet

Single Sign On (SSO)

Ett krav för SSO i VI är att användaren använder en och samma browser (Chromium-baserad rekommenderas), för att applikationerna ska kunna hitta den gemensamma inloggningen.
Efter inloggning i ett Vitec-system via VI kan andra system öppnas utan att behöva logga in på nytt. Först när inloggningens giltighet har gått ut krävs ny inloggning. Giltighetstid på SSO-sessionen är konfigurerbar både generellt och per klient i VI-Admin. Om inga särskilda förutsättningar finns rekommenderas att ha samma värde för alla klienter.

Två-faktorsautentisering (MFA)

Det är möjligt att använda tvåfaktor-autentisering för att öka säkerheten vid inloggning. Det finns stöd i VI, men det är inte verifierat i praktiken eftersom det då finns beroende mot externa mobil-appar. Men när behovet uppstår finns det möjlighet att inom en release stabilisera och verifiera flödet.

VI Standalone

VI kan sättas upp utan att ni har ADFS/AzureAD. I detta läge agerar VI på liknande sätt som ex ADFS och ni kan hantera era användare och roller i VI.

Inloggning med organisations-konto mot ert AD.

Den ”claim-typ” som används av VI för att identifiera användare är **UPN**. Ert ADFS/AzureAD måste leverera detta claim för att VI ska fungera.

Om ADFS/AAD används i er organisation så kommer inloggning i Vitec-applikationer gå via VI som vidarebefordrar inloggningen till ADFS/AAD, dvs VI använder i detta läge ADFS/AAD för den faktiska autentiseringen. I slutändan är det dock alltid VI som ställer ut autentiseringen mot Vitec-applikationerna. Det blir alltså ingen skillnad för Vitec-applikationerna oavsett typ av extern IdP eller om ni kör lokal VI (VI Standalone).

Inloggning med extern IdP

För grundläggande flöden, se avsnitt ”Generell hantering av användare vid inloggning”.

När en användare loggar in i till exempel Hyra, där AD-användaren tillhör en AD-grupp ex. ”EkonomHosKundAB” som kopplats med motsvarande VI-roll ”Ekonom”, så kommer användaren att få den rollen i VI. Den VI-rollen kan i sin tur vara kopplad till roller i ett eller flera Vitec-system.
I detta exempel kan det motsvara rollen ”HyraEkonom” i Hyra. Inloggningsflödet tar hand om att skapa användaren i Hyra om den inte finns, samt kopplar i detta fall rollen ”HyraEkonom” till användaren. Hyra startar sedan med användaren och dennes behörigheter utifrån roller.

VI med Extern IdP - Windowsinloggning

Med Extern IdP uppsatt (AzureAD eller ADFS) så kan denna IdP konfigureras så att en inloggad användare i Windows på sin enhet (inloggad i ert AD) faller rakt in i applikationen utan att behöva genomföra en inloggning.

Användarfall vid inloggning

Vid inloggning mot VI kan användarens status och vad det medför vara något av följande:

1. Användaren finns i det underliggande systemets databas och har loggat in tidigare via VI (med eller utan extern IdP så som ADFS).
    a. Beroende på om användaren har en aktiv inloggning eller inte faller den antingen rakt in eller dirigeras till inloggning.
2. Användaren finns i det underliggande systemets databas men har inte loggat in via VI tidigare.
    a. Användaren dirigeras till inloggning och anger sina vanliga inloggningsuppgifter.
    b. VI ser att användaren inte finns i VI-databasen, verifierar inloggningen mot den underliggande systemdatabasen och om den är ok skapas användaren upp i VI med angivet användarnamn/lösenord.
    c. Användaren loggas därmed in utan att behöva registrera sig i VI.
3. Användaren finns i VI, dvs har loggat in tidigare, men inte mot/i det underliggande systemets databas.
    a. Om inloggningen godkänns i VI så skapar VI upp användaren i den underliggande databasen med de uppgifter som finns tillgängliga i VI alternativt extern IdP (ex. information i ADFS).
4. Användaren finns i extern IdP (ex. ADFS) men varken i VI eller underliggande system.
    a. Vid inloggning via extern IdP skapas användaren i VI och följer sedan flöde 3a.
5. Användaren finns inte registrerad alls.
    a. Om extern IdP används ska er systemadministratör lägga upp användaren där och sedan följer flöde 4.
    b. Om ni kör lokalt med VI ska VI erbjuda en registreringssida där användaren får ange användarnamn och lösenord för att då läggas upp i VI. Sedan följer flöde 3.

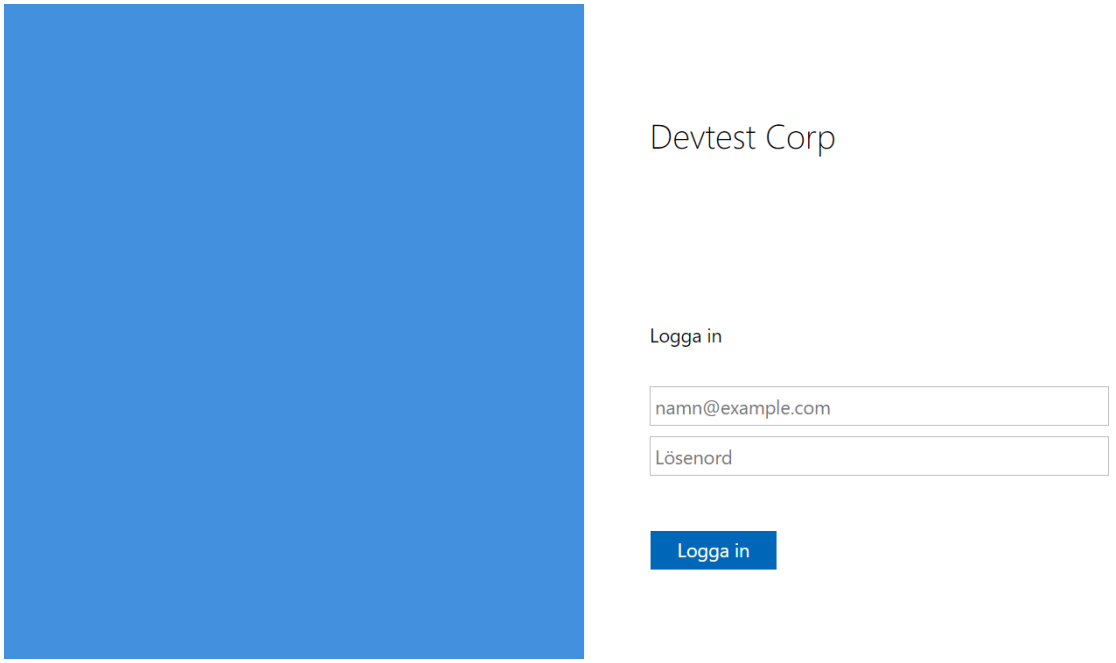
Inloggningsvyer

Det användaren ser vid inloggning i något av Vitec-systemen när VI används, beror på vilken klient det är och hur den är konfigurerad.

En användare som loggar in via ert ADFS/AzureAD i en klient som endast ska nås av era interna användare kan se:

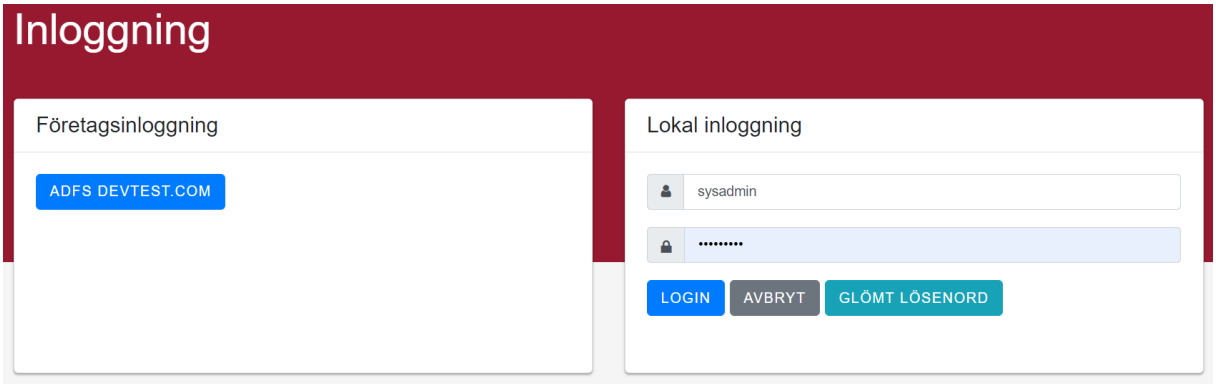
- Om ert ADFS/AzureAD är konfigurerad för att möjliggöra direktinloggning via enhetens/arbetsstationens inloggning, så ser användaren inget mer än att ett fönster blinkar till. Fönstret öppnas för att kommunicera inloggningen samt för att lagra inloggningsbiljetten (Single-Sign-On).

- När konfigurationen hos er kräver en explicit inloggning kommer VI att dirigera användaren till er AD-inloggningssida



En användare som loggar in via ert ADFS/AzureAD i en klient som kan nås av både interna och externa användare:

- Här kommer användaren att se inloggningssidan i VI eftersom vi idet här läget inte vet vem som loggar in. En extern användare kan in logga in via ert AD och väljer därför lokal inloggning. En intern användare klickar på knappen för AD-inloggning. Under inloggningsbiljettens livstid (konfigurerbart men ofta 30 dagar) behöver era användare inte välja på nytt eftersom biljetten finns utställd redan. Först vid ny inloggning krävs valet på nytt.



Inloggning - rollnivåer

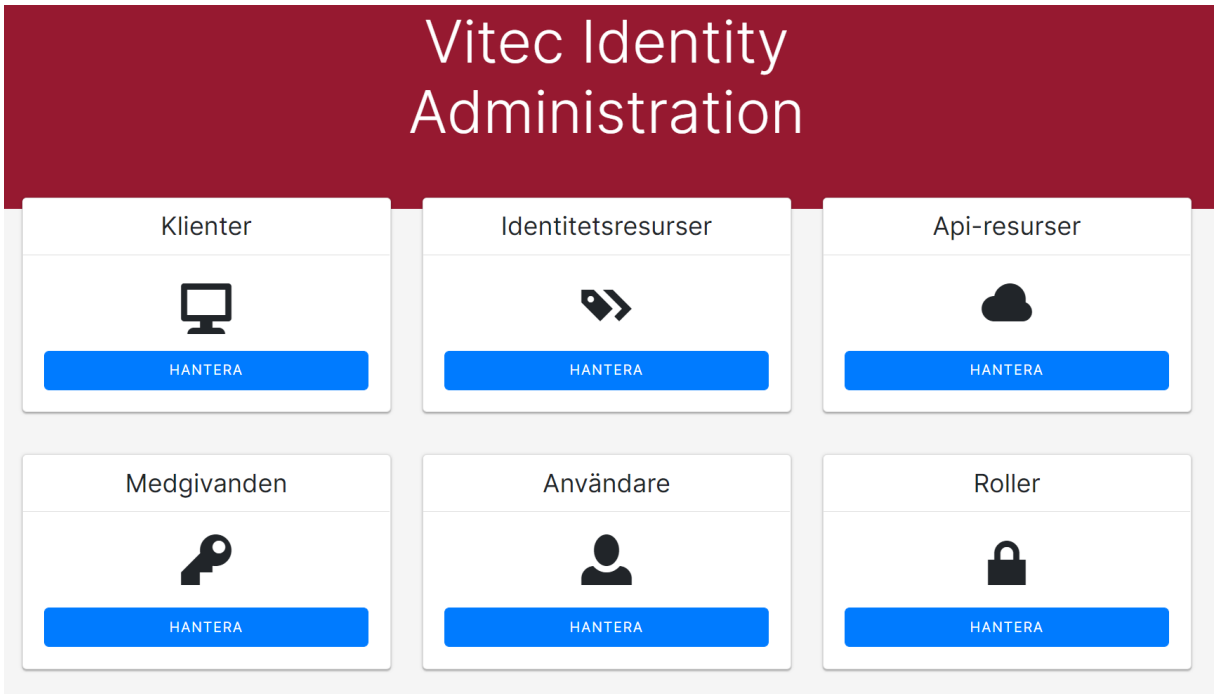
Vid inloggning i eller via VI kan en användare tillhöra en grupp/nivå utifrån sina roller.

Vitec Admin-inloggning

Vitec-inloggning gäller för Vitec-personal som har behörighet att logga in via VI mot ert Vitec i molnet.

En administratör från Vitec kan arbeta med alla kunder och deras uppsättningar via VI.

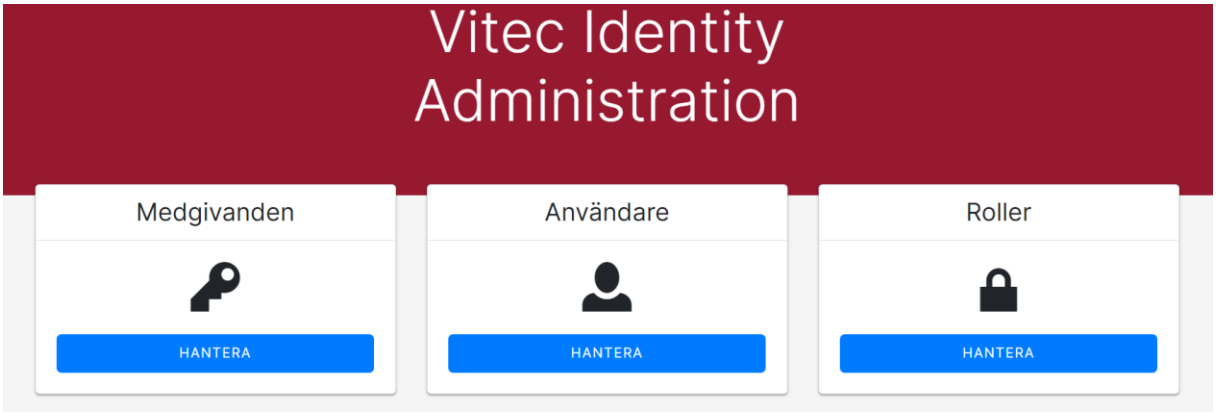
- Logga in som Vitec-administratör, går endast att nå inifrån Vitecs nät. Dvs det inloggningsvalet visas bara då samt om användaren har rätt behörighet hos Vitec.
- Spårbar inloggning, ni kan alltid se vem från Vitec som har varit inloggad i era Vitec-system samt vad denne har gjort.
- Kan logga in i alla system hos alla kunder (om rätt behörighet hos Vitec).
- Loggas alltid ut, dvs sessions-baserad inloggning för kundmiljöns säkerhet.
- Skapa/ändra/ta bort användare/roller/resurser/klienter etc.
- Ändra generell VI-konfiguration som ex. livslängd på token.



Kund-Administratörer

En kund-administratör kan administrera användare och roller för sitt eget Vitec Identity, samt se loggar.

- Logga in i VI-Admin med behörighetsnivå kund-administratör.
- Logga in i era Vitec-system med högsta behörighetsnivå.
- Skapa/ändra/ta bort användare/roller i VI.
- Om en kund-administratör vill ta bort en användare så stängs användaren av i AD eller tas bort från grupp i AD och detta slår igenom direkt i VI eftersom inloggningen går via ADFS i det fallet. För lokal installation tas användaren bort eller låses i VI. *OBS! För tillfället kräver detta antingen att applikationsbehörigheter används och att den behörigheten tas bort, eller att full rollsynkning är påslaget. Framöver kommer integration mot AD-systemet att förbättras.*



Era användare

- Kan logga in i de system som användaren har behörighet till. Detta styrs via roller i VI som kopplas mot roller i våra underliggande system. Rollerna i VI kan hos er kopplas mot säkerhetsgrupper så att ni kan styra era användares behörigheter i Vitec-systemen.
- Användaren kan ändra sina egna personliga uppgifter i VI. *(Framöver kommer användarens uppgifter att i högre grad synkroniseras ned i Vitec-systemen)*
- Om en användare inte längre är behörig att använda ett system pga. avsaknad grupptillhörighet i AD ska användaren inte kunna logga in i det specifika undersystemet. Styrs i VI via de s.k. applikationsrollerna.
- En användares roller synkroniseras ned till Vitec-systemen utifrån de säkerhetsgrupper som användaren tillhör. Default läggs roller till, men när ni har uppdaterat alla användare så att ert AD stämmer med den behörighet ni vill att användarna ska ha kan full synkning slås på. I detta läge kommer användaren bara ha de roller som ert AD säger att de ska ha.

Resursinloggning i TF

- En extern resurs (som inte finns i ert AD) kan logga in med sin användare genom att ”Lokal inloggning” har aktiverats i VI på den klient som det gäller (ex. TF-appen). Användaren anger användarnamn och lösenord och dessa kontrolleras mot det underliggande Vitec-systemet och om inloggningen godkänns där skapas användaren upp automatiskt i VI. På så vis kan efterföljande inloggningar autentiseras direkt mot VI istället.

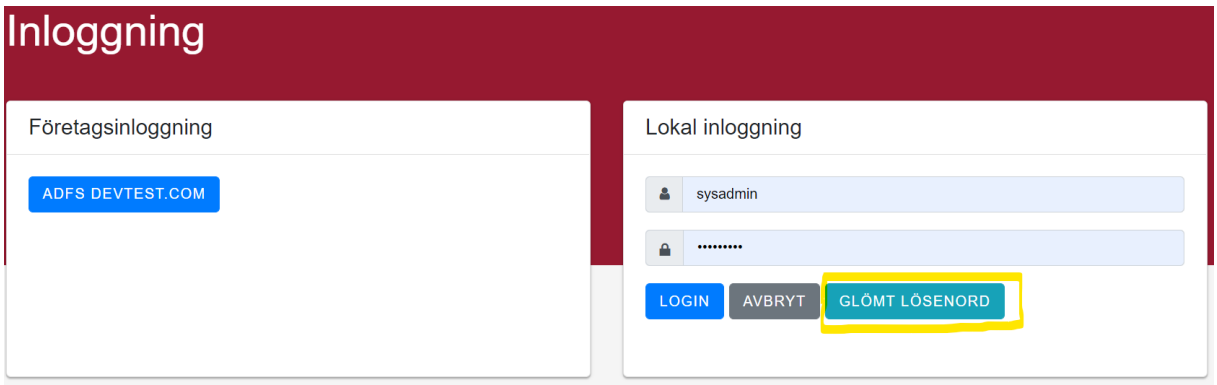
Glömt lösenord och andra ej godkända inloggningar

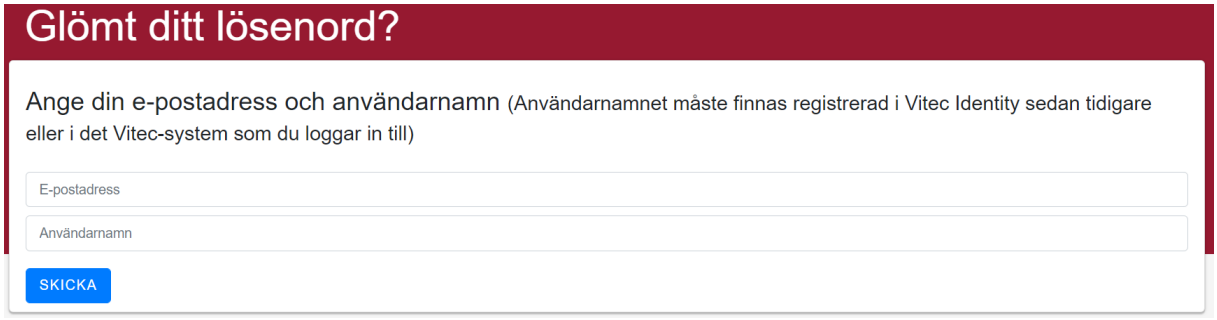
Användare i ert eget AD

Om en användare har glömt sitt lösenord hanteras det i ert AD av en systemadministratör hos er.

Lokal VI eller Externa resurser

- Om användaren har loggat in i VI sedan tidigare så kan användaren klicka på knappen för glömt lösenord, ett mejl skickas med återställningslänk så att användaren åter kan logga in efter det att lösenordet har uppdaterats.
- Om användaren inte finns i VI ännu, dvs har inte loggat in tidigare.
    - Om lösenordet inte har korrekt format dirigeras användaren till att sätta ett nytt lösenord. Sedan får användaren stänga Vitec-applikationen och logga in på nytt.
    - *Framtid: Om användaren har glömt sitt lösenord till exempelvis Hyra, så kontrolleras användaren i det underliggande systemet (dvs om användaren finns där), samt skickar återställning via mejl om användaren har hittats och en mejladress finns registrerad. När användaren återställer lösenordet skapas användaren upp i VI så att autentisering sedan kan ske mot VI vid inloggning mot underliggande system.*





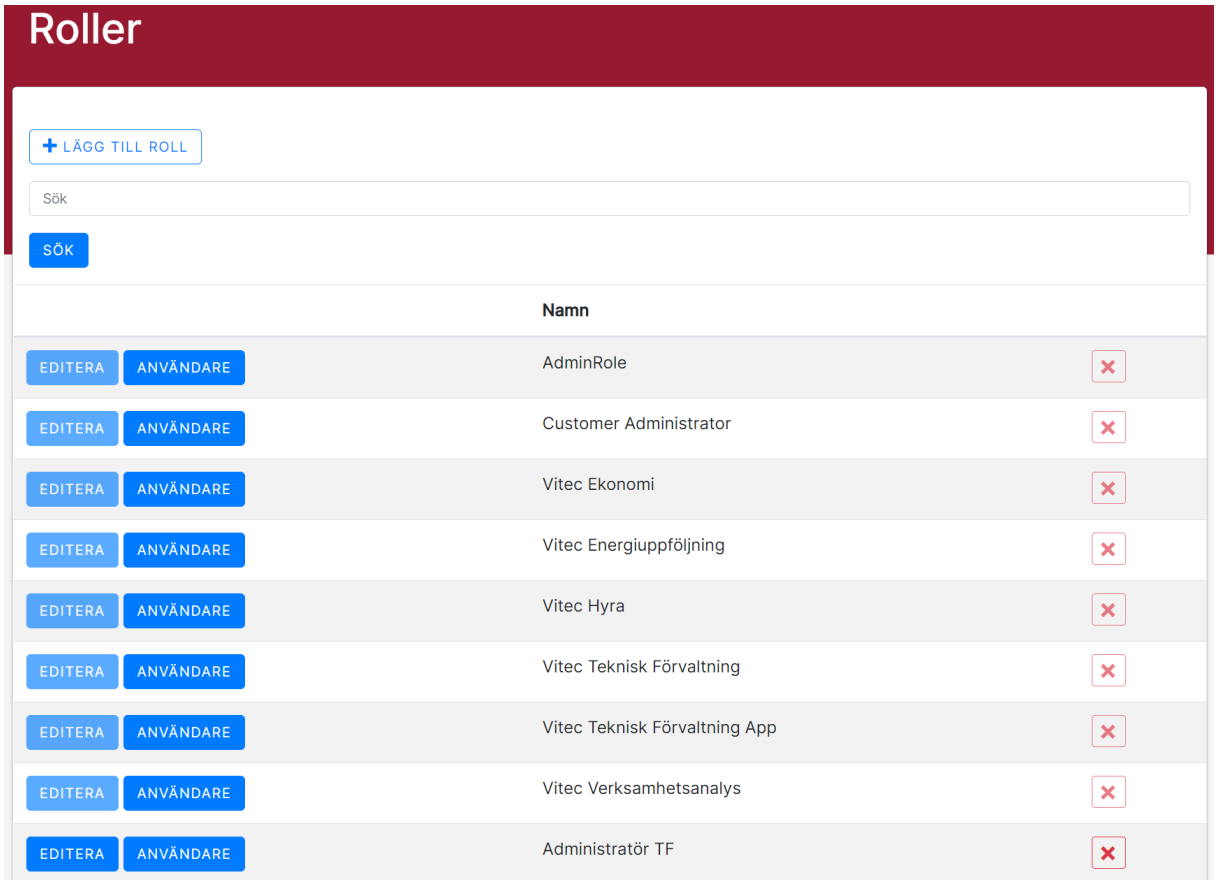
Lösenords-policy

Per default använder VI de krav på lösenord som plattformen för VI, AspNetCore, tillämpar vilket är följande. Ett undantag finns vilket är att VI ej kräver ett icke-numeriskt tecken. Framöver kommer det att vara möjligt att ställa in dessa parametrar i VI Admin. Default:

- Minst ett numeriskt tecken
- Minst en liten bokstav
- Minst en stor bokstav
- Minst sex tecken
- Minst ett unikt tecken

Rollhantering från AD till Vitec-applikation

Säkerhetsgrupper i ert AD kan kopplas till roller i VI. Roller i VI kan skapas i gränssnittet VI Admin av Vitec eller av kund-administratör hos er.
Nästa steg är att koppla en VI-roll till en eller flera roller i underliggande Vitec-system. Denna design medger att en VI-roll kan kopplas till applikationsroller över flera system. En kund kan därmed styra alla Vitec-applikationer på ett och samma ställe i sitt ADFS/AzureAD, på både övergripande och detaljerad nivå.

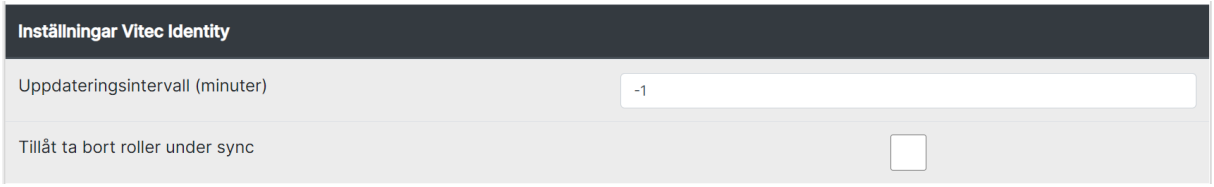


Applikationsbehörighet

Det finns möjlighet att konfigurera VI för auktorisering av en användare mot en s.k. ”applikationsroll”. Varje applikation har en speciell ”applikationsroll” som innebär behörighet till den applikationen. Funktionaliteten slås på av Vitec utifrån önskemål varpå användare som ska ha behörighet till en applikation kopplas till motsvarande applikationsroll (kan göras av kund-administratör hos er). Om denna inställning inte används styrs behörighet som vanligt via rollkopplingar och roller i respektive system (dessa är aktiva även om applikationsroller används.)

Rollhämtning från Vitec-system

Det finns inställningar i VI Admin för hur VI ska uppdatera roller från Vitec-systemen. Uppdateringsintervallet säger hur ofta roller från underliggande system ska hämtas. Den andra inställningen bestämmer hur roller ska synkroniseras mot Vitec-systemen då en användare loggar in. Om roller bara ska läggas till (avmarkerad) utifrån användarens grupper i ert AD, eller om roller även ska tas bort (markerad). Markerad innebär alltså full synkronisering och en användare kommer att tappa roller som inte har kopplats från ert AD till Vitec-roller i VI.



Rollmappning

Dessa roller kan kopplas till användarens tillhörighet i Security Groups i ert AD om det ställts in i ADFS att dessa ska exporteras (dokumenteras i separat dokument om konfiguration ADFS/Azure AD). Genom att ange namnet på AD-gruppen som användare tillhör till roller i VI kan dessa sedan kopplas till de roller som ger rättigheter i varje underliggande system.