

1. Prezentare generală

VOGO eBS Identity Server (VOGO-IS) este serverul de identitate al suitei VOGO eBS: ține conturile, verifică autentificarea cu al doilea factor și deschide toate aplicațiile organizației după o singură autentificare. Este construit pe motorul de identitate VOGO — conturi, sesiuni, al doilea factor, roluri și grupuri —, folosit deja în aplicația VOGO eBS. Produsul folosește ca biblioteci open source mature: Keycloak și WSO2 Identity Server.

- ▶ **Rol:** o singură identitate pentru fiecare om, în toate aplicațiile organizației.
- ▶ **Cui se adresează:** angajaților, cetățenilor și partenerilor unei instituții publice sau ai unei companii.
- ▶ **Consola:** VOGO-IS Console, în limba română, cu furnizorii de identitate, aplicațiile conectate și evenimentele de securitate; conturile, rolurile și grupurile se administrează în ecranele IAM ale VOGO eBS.

2. Arhitectură și instalare

Produsul are cinci componente, instalate în infrastructura organizației.

- ▶ **Motorul de identitate VOGO:** conturile, parolele, sesiunile, al doilea factor, rolurile și grupurile.
- ▶ **Serverul de autorizare:** emiterea și validarea tokenurilor OpenID Connect și OAuth 2.0 și a aserțiunilor SAML.
- ▶ **Federarea:** legăturile cu directorul organizației, Microsoft Entra ID, parteneri și ROeID.
- ▶ **Administrarea accesului:** utilizatorii, rolurile, grupurile și drepturile pe meniuri, în ecranele IAM.
- ▶ **Bibliotecile:** Keycloak și WSO2 Identity Server, alese pe fiecare furnizor de identitate.
- ▶ **Instalarea:** on-premise; conturile și datele de autentificare nu ies din infrastructura organizației.

3. Conturi și sesiuni

- ▶ **Conturi:** create numai prin API-ul de identitate; persoana își setează singură parola dintr-un link.
- ▶ **Sesiuni:** o sesiune pe dispozitiv, încheiată la deconectare sau la expirare.
- ▶ **Parole:** stocate cu Argon2id, niciodată în clar.

4. Al doilea factor

- ▶ **Metode:** Google Authenticator sau cod pe e-mail.
- ▶ **Politica:** obligatoriu pentru toate conturile aplicației sau după risc, pe fiecare aplicație conectată.

5. Autentificare unică și protocoale

- ▶ **SSO:** omul se autentifică o dată și deschide toate aplicațiile conectate; deconectarea este unică.
- ▶ **Protocoale:** OpenID Connect, OAuth 2.0 (cod de autorizare cu PKCE, client credentials) și SAML 2.0.
- ▶ **Conturi de serviciu:** aplicațiile se autentifică între ele prin OAuth 2.0, fără parole comune.

6. Federarea identităților

- ▶ **Directorul organizației:** LDAP, Active Directory și Kerberos.
- ▶ **Microsoft Entra ID și furnizorii partenerilor:** prin OpenID Connect sau SAML 2.0.
- ▶ **ROeID:** autentificarea cetățenilor, cu crearea automată a contului la prima intrare.

7. Roluri, grupuri și drepturi

- ▶ Rolurile se dau prin grupuri; drepturile Vede, Adaugă, Modifică și Șterge se stabilesc pe fiecare meniu.
- ▶ **Administrarea se face în ecranele IAM ale VOGO eBS:** utilizatori, roluri, grupuri, meniuri și module.

8. Audit și securitate

- ▶ **Jurnal:** fiecare autentificare, eșec, blocare și resetare, cu contul, ora și adresa.
- ▶ **Protecție:** blocarea temporară după încercări repetate și semnalarea dispozitivelor noi.
- ▶ **VOGO eBS SIEM:** evenimentele de securitate ajung în SIEM, corelate cu restul evenimentelor.

9. Integrarea cu VOGO eBS

- ▶ **Aplicațiile VOGO eBS:** API Gateway, Service Desk, SIEM, GIS și aplicația VOGO eBS se autentifică prin VOGO-IS.
- ▶ **Aplicațiile organizației:** portalul, aplicația mobilă, sistemul financiar-contabil și BI se conectează prin protocoale standard.

10. Suport și servicii

- ▶ **Suport:** VOGO, ca producător, asigură suportul, actualizările de securitate și instruirea, pe toată durata contractului.
- ▶ **Servicii:** conectarea aplicațiilor, federarea cu directorul organizației și cu ROeID, migrarea conturilor și instruirea.

11. Capturi de ecran din VOGO-IS Console

Capturile sunt din consola produsului, pe datele unui mediu de test.

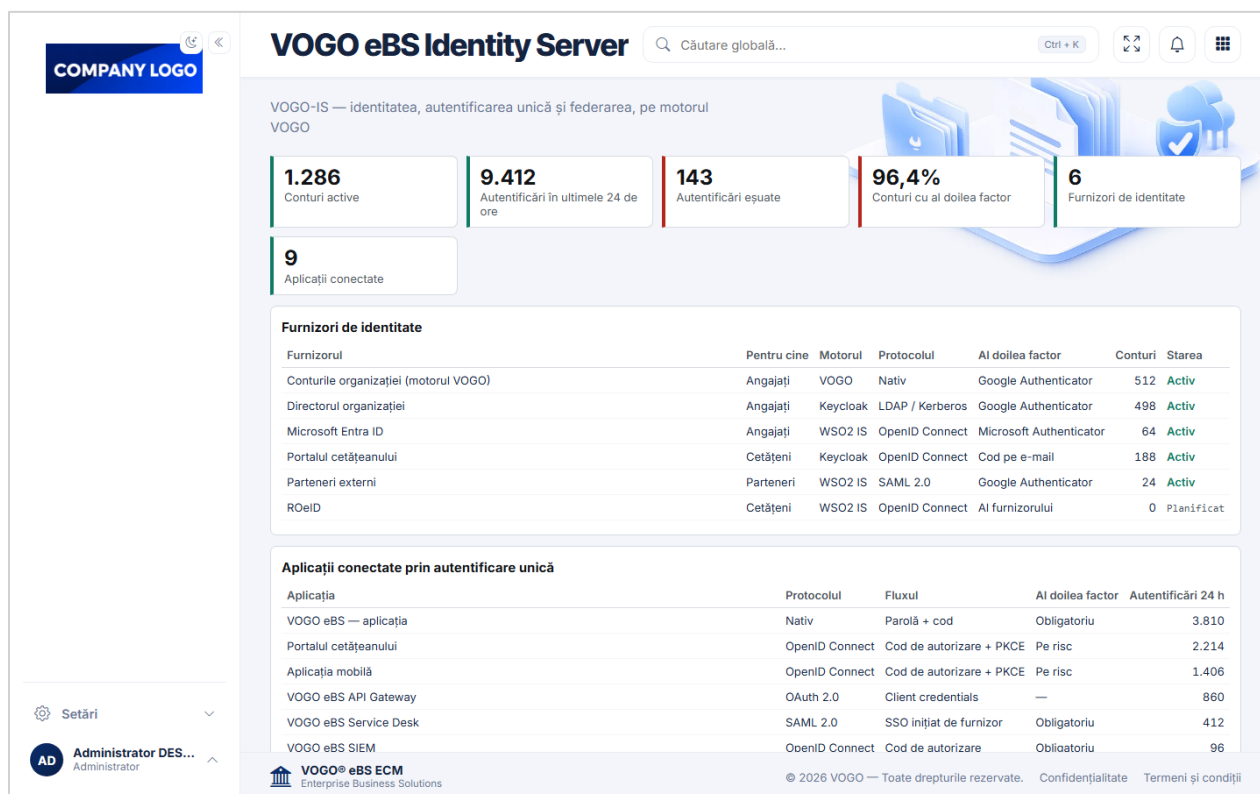


Fig. 1 VOGO-IS Console: indicatorii și furnizorii de identitate, cu motorul care îi servește — VOGO, Keycloak sau WSO2 Identity Server —, protocolul și al doilea factor

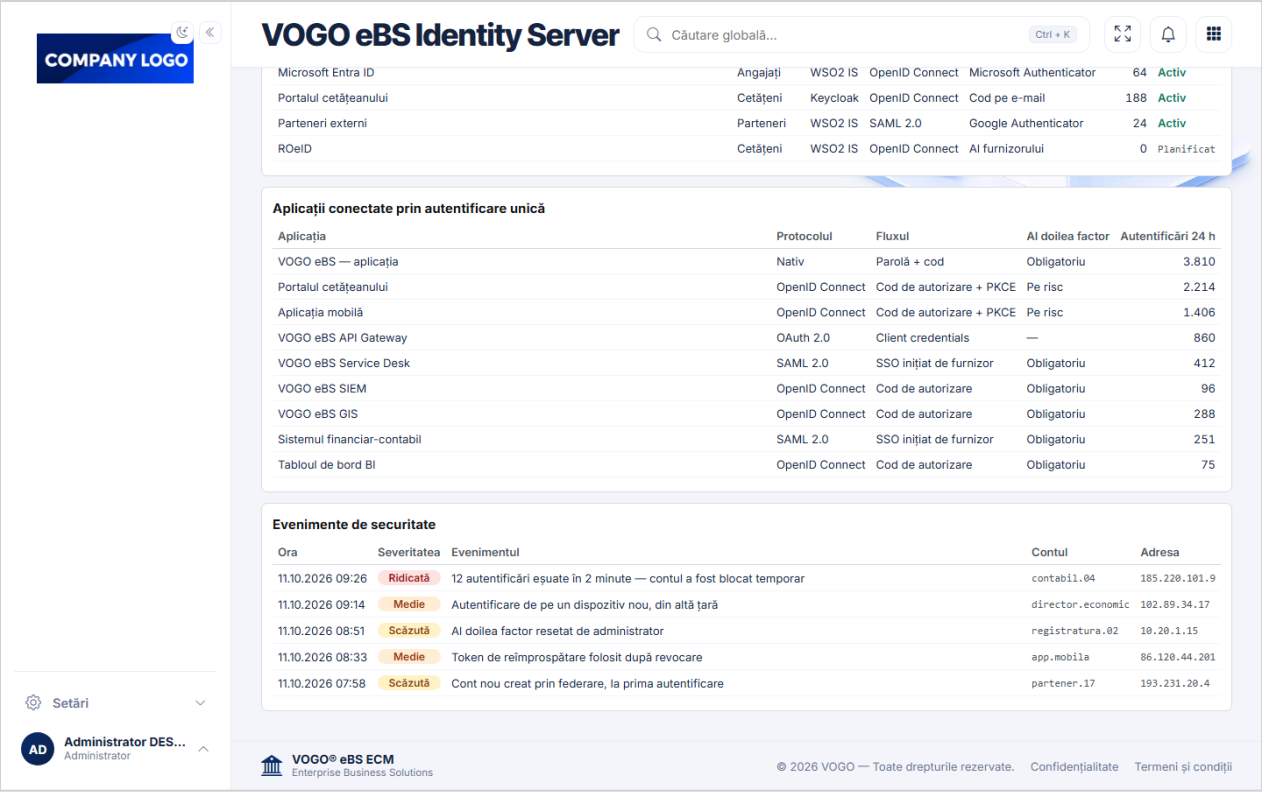


Fig. 2 Aplicațiile conectate prin autentificare unică, cu protocolul, fluxul și al doilea factor

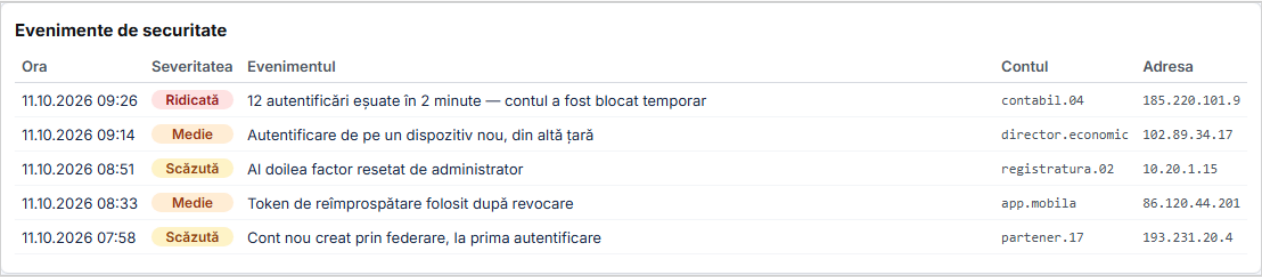


Fig. 3 Evenimentele de securitate: severitatea, evenimentul, contul și adresa