

SQL Change Guard Kurulum ve İşletim Kılavuzu

Bu kılavuz SQL Change Guard'ı kuracak ve işletecek BT, DBA ve güvenlik ekipleri içindir. Kurulumu adım adım anlatır; kurum dizini (LDAP), kurum hesabıyla giriş (SSO), ITSM ve SIEM entegrasyonlarının her ayarını, alabileceği değerleri ve karşı sistemden gelen bilginin üründe nereye yazıldığını açıklar. Kurulumdan önce hazırlanması gerekenler Kurulum Ön Hazırlık Listesi'ndedir. Ekranların kullanımı Kullanım Kılavuzu'ndadır.

1. Ürünün parçaları	5
2. Ayarlar nerede durur	6
2.1 Sırlar ortam değişkeninde durur	6
2.2 Sır listesi	7
2.3 Anahtar üretme	8
3. Veritabanı kurulumu	9
3.1 Yol A: Ürün kurar (AutoMigrate = true, varsayılan)	9
3.2 Yol B: DBA kurar (AutoMigrate = false)	9
3.3 Kurulumdan sonra DBA'nın yapacağı üç iş	9
3.4 Defter özeti deposu	10
3.5 Kanıt defteri	10
4. API kurulumu	13
4.1 Temel ayarlar	13
4.2 E-posta	15
4.3 Zaman damgası (isteğe bağlı)	16
4.4 Onay zinciri ve yönetim durumu	16
5. Worker kurulumu	18
6. Web arayüzü, lisans ve ilk giriş	20
6.1 Web arayüzü	20
6.2 Lisans	20
6.3 İlk giriş	20
7. Kurum dizini (LDAP / Active Directory)	21
7.1 Nasıl çalışır	21
7.2 Ayarlar (appsettings.json, Ldap bölümü)	21
7.3 Dizinden ne okunur, üründe nereye yazılır	23
7.4 Grup ile rol eşlemesi	23
7.5 Eşitleme	24
7.6 Kilit eşiği	25
7.7 Kurulum sırası	25

8. Kurum hesabıyla giriş (SSO)	26
8.1 Nasıl çalışır	26
8.2 Genel ayarlar (appsettings.json, Sso bölümü)	26
8.3 Kimlik sağlayıcısı ayarları (Sso:Providers listesi).....	27
8.4 Kimlik bilgisinden ne okunur, üründe nereye yazılır	28
8.5 Grup ile rol eşlemesi	28
8.6 Kimlik sağlayıcısında yapılacaklar	29
8.7 Kurulum sırası.....	29
9. ITSM entegrasyonu	31
9.1 Nasıl çalışır	31
9.2 Bağlantı ayarları (appsettings.json, Itsm bölümü)	31
9.3 ServiceNow: ne okunur, nereye yazılır	32
9.4 Jira ve diğer ITSM'ler: ne okunur, nereye yazılır	33
9.5 Durum nasıl yorumlanır (StateClass).....	35
9.6 Davranış parametreleri (Ayarlar > Parametreler > ITSM Ticket)	36
9.7 ITSM'e yazılan not	38
9.8 Kurulum sırası.....	39
10. SIEM / SOC entegrasyonu	40
10.1 Nasıl çalışır	40
10.2 Bağlantı ayarları (appsettings.json, Siem bölümü)	40
10.3 Davranış parametreleri (Ayarlar > Parametreler > SIEM)	41
10.4 Olayın alanları	42
10.5 Kurulum sırası.....	43
11. Kurulum doğrulama	44
12. İşletim.....	45
12.1 Günlükler.....	45
12.2 Yedekleme	45
12.3 Sürüm yükseltme	45
12.4 Anahtar değiştirme	45

12.5 Ayar dosyası deęiřiklięinin izi	46
12.7 Defter özetini ve kanıt yazma sınırı	47
12.8 Sık karřılařılan sorunlar	48

1. Ürünün parçaları

Parça	Dosya	Nasıl çalışır
Web arayüzü	Statik dosyalar (index.html ve assets klasörü)	IIS'te ayrı bir site. .NET gerekmez
API	SCG.API.dll	IIS'te ASP.NET Core uygulaması. Uygulama havuzu: No Managed Code
Worker	SCG.Workers.exe	Windows servisi
Uygulama veritabanı	SQL Server 2022 veya üzeri	Ürünün bütün kayıtları. Denetim kayıtları append-only defter (ledger) tablosunda durur; veritabanı motoru bu tabloda UPDATE ve DELETE işlemlerini reddeder (Bölüm 3.5)

Kim kime bağlanır:

Tarayıcı --443--> Web arayuzu (statik dosyalar)

Tarayıcı --443--> API

Worker --443--> API (yapılandırma, ITSM notları, izin esitlemesi, çalıştırma kararları)

API, Worker --1433--> Uygulama veritabanı

API --> Defter özeti deposu (degistirilemez klasor)

API, Worker --> Hedef veritabanları (SQL Server, PostgreSQL, Oracle)

API --> Kurum dizini (LDAP), kimlik sağlayıcısı (SSO), ITSM

API, Worker --> SIEM toplayıcısı, SMTP

API --> Zaman damgası sunucusu (acildiysa)

Önemli iki kural:

- Kurum dizinine, kimlik sağlayıcısına ve ITSM'e yalnız API bağlanır. Worker bu işler için API'yi çağırır. Bu entegrasyonların ayarları ve sırları yalnız API'nin ayar dosyasında durur.
- Worker'ın kendi ayar dosyasında yalnız API adresi ve Worker anahtarı durur. Veritabanı bağlantı dizesini ve şifreleme anahtarlarını açılışta API'den alır. Kanıt imzalama özel anahtarı Worker'a hiç gitmez: Worker çalıştırma olaylarını API'ye imzalatır, defter özeti turunu yalnız başlatır (özeti API alır, imzalar ve yazar). API, Worker'ın bildirimini onay zincirine karşı doğrulamadan imzalamaz. Worker ile API ayrı sunuculardaysa aradaki bağlantı HTTPS olmalıdır.

2. Ayarlar nerede durur

Ürünün ayarları üç yerde durur. Hangisinin nerede olduğu bilinçli bir seçimdir.

Yer	Ne tutar	Kim değiştirir	Değişince
API klasöründeki appsettings.json	Bağlantılar: veritabanı, izin, kimlik sağlayıcısı, ITSM, SIEM, e-posta adresleri ve süreleri	Kurulumu yapan	API yeniden başlatılır. LDAP, SSO ve ITSM bölümlerindeki değişiklik açılışta fark edilir ve denetim kaydına yazılır
Ortam değişkenleri	Sırlar: parolalar, anahtarlar, bağlantı dizeleri	Kurulumu yapan	API ve Worker yeniden başlatılır
Ürün içinde Ayarlar > Parametreler	Davranış: ITSM ve SIEM kuralları, onay kuralları, numara biçimleri	Uygulama yöneticisi	Hemen geçerli olur. Denetim kaydına yazılır; ayar değişikliği onayı açıksa ikinci bir yöneticinin onayından geçer

2.1 Sırlar ortam değişkeninde durur

Ürün bir ayarı önce appsettings.json dosyasından, sonra ortam değişkeninden okur. Ortam değişkeni dosyadakini ezer. Değişkenin adı, ayar yolundaki iki nokta üst üstenin çift alt çizgiyle değiştirilmesiyle bulunur: Jwt:SigningKey ayarı Jwt__SigningKey değişkeninden okunur.

Sırlar dosyada bırakılmaz. Dosya çoğu kurumda yedeklere ve kaynak kontrolüne girer; orada duran bir sır, dosyaya erişebilen herkesin eline geçer.

Tanımlama (yönetici olarak açılmış komut isteminde, kalıcı sistem değişkeni):

```
setx /M Jwt__SigningKey "deger"
```

Silme (setx boş değer yazar, silmez):

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /F /V  
Jwt__SigningKey
```

Değişken tanımlandıktan sonra API ve Worker servisi yeniden başlatılır. IIS yeni sistem değişkenlerini uygulama havuzu geri dönüştürülünce görmeyebilir; bu durumda IIS yeniden başlatılır (yönetici komut isteminde iisreset) ya da sunucu yeniden başlatılır. Açık komut penceresi yeni değişkeni görmez; yeni bir pencere açılır. Değişkenin gerçekten okunduğu aşağıdaki Sır yerleşimi grubundan kontrol edilir.

Doğrulama: Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranındaki Sır yerleşimi grubu her sır için değer nereden geldiğini gösterir: ortam değişkeni, yapılandırma dosyası ya da tanımsız. Beklenen değer ortam değişkenidir. Ekran sırrın kendisini göstermez.

2.2 Sır listesi

Zorunlu sırlar. Biri eksikse ürün açılmaz ya da çalışmaz:

Ortam değişkeni	Ne işe yarar	Nasıl üretilir
ConnectionStrings__Default	Uygulama veritabanı bağlantı dizesi	DBA verir
Jwt__SigningKey	Oturum jetonlarının imzası. En az 32 karakter	Rastgele üretilir (2.3)
Security__ServerPasswordKey	Sunucu parolalarının şifrelenmesi. Base64, çözülünce tam 32 bayt	Rastgele 32 bayt, base64
Security__QrZipPasswordKey	Sorgu sonucu paketlerinin parolalarının şifrelenmesi. Base64, tam 32 bayt	Rastgele 32 bayt, base64
Workers__ApiKey	Worker'ın API'ye kendini tanıtmayı	Rastgele üretilir. Aynı değer Worker tarafında WorkerApi__Key olarak da tanımlanır
WorkerApi__Key	Worker tarafındaki karşılığı	Workers__ApiKey ile aynı değer

Koşullu sırlar. Yalnız ilgili özellik kullanılıyorsa gerekir:

Ortam değişkeni	Ne zaman
Mail__Password	E-posta gönderimi kimlik doğrulama istiyorsa
Ldap__BindPassword	Kurum dizini kullanılıyorsa
Sso__Providers__N__ClientSecret	OIDC ile kurum hesabı girişi. N, sağlayıcının listedeki sırasıdır; ilk sağlayıcı 0
Sso__Providers__N__SpCertificatePassword	SAML imza sertifikası kullanılıyorsa
Itsm__Password ya da Itsm__Token	ITSM entegrasyonu kullanılıyorsa
Evidence__Signing__Keys__1__PrivateKeyPem	Kanıt dosyalarının imzalanması, yalnız anahtar sertifika deposunda değilse (2.3). İmza açıkken (Evidence:Signing:Enabled = true) kullanılabilir anahtar yoksa ürün açılır ama kanıt dosyası, kayıt paketi, defter özeti ve dönem paketi ÜRETİLMEZ; imzasız çıktı verilmez. Durum Yönetişim Kurulum Kontrolü ekranında görünür
Evidence__Timestamp__ProxyPassword	Zaman damgası sunucusuna parolalı bir vekil sunucudan çıkılıyorsa
ConnectionStrings__Worker	Worker uygulama veritabanına API'den ayrı bir hesapla bağlanacaksa (Bölüm 5). Worker sunucusunda tanımlanırsa Worker bu değeri kullanır; API'de Workers:ShareConnectionString = false yapılırsa API bağlantı dizesini Worker'a hiç göndermez

2.3 Anahtar üretme

32 baytlık rastgele değer, base64 (Security anahtarları için zorunlu biçim; diğerleri için de kullanılabilir):

```
powershell -NoProfile -Command "$b=New-Object byte[]  
32;[System.Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($b);[Convert]::ToBase64String($b)"
```

Kanıt imzalama anahtar çifti (RSA 3072):

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:3072 -out priv.pem
```

```
openssl rsa -pubout -in priv.pem -out pub.pem
```

Özel anahtar (priv.pem) Evidence__Signing__Keys__1__PrivateKeyPem ortam değişkenine yazılır. Açık anahtar (pub.pem) sır değildir; appsettings.json içinde Evidence:Signing:Keys:1:PublicKeyPem alanına yazılır ve denetçiye verilir. JSON içine yazarken satır sonları \n olarak yazılır. Denetçiye verilecek parmak izi:

```
openssl pkey -pubin -in pub.pem -outform DER -out pub.der
```

```
openssl dgst -sha256 pub.der
```

Üretimde önerilen yol: özel anahtar ortam değişkeninde değil, Windows sertifika deposunda durur.

Ortam değişkenindeki anahtarı sunucuyu yöneten herkes okuyup sunucu dışında imza atmak için kullanabilir; depoya dışa aktarılamaz olarak alınan anahtar kopyalanamaz.

1. Anahtar ve sertifika bir .pfx dosyasında hazırlanır (kurumun sertifika otoritesinden ya da openssl ile kendinden imzalı, RSA 3072).
2. .pfx, API sunucusunda Yerel Bilgisayar > Kişisel deposuna "Bu anahtarı dışa aktarılabilir olarak işaretle" seçeneği KAPALI olarak alınır.
3. Sertifikada sağ tık > Tüm Görevler > Özel Anahtarları Yönet: okuma izni yalnız API uygulama havuzu hesabına verilir. Worker imza atmaz; çalıştırma olaylarını API'ye imzalatır, defter özetini ise API kendisi alır ve imzalar.
4. appsettings.json içinde Evidence:Signing:Keys:1:CertificateThumbprint alanına sertifikanın parmak izi yazılır (CertificateStoreLocation: LocalMachine). PrivateKeyPem ve Evidence__Signing__Keys__1__PrivateKeyPem tanımlanmaz. PublicKeyPem boş bırakılırsa sertifikadan üretilir.
5. Kurumda HSM ya da TPM varsa anahtar üreticinin Windows sağlayıcısıyla aynı depoya konur; ürün tarafında ayar ayıdır.

Yönetişim Kurulum Kontrolü ekranındaki "İmza anahtarı nerede tutuluyor" satırı anahtarın kaynağını gösterir. Anahtarları değiştirmenin bedeli Bölüm 12.4'tedir.

3. Veritabanı kurulumu

Kurulum betikleri API klasöründe DbScripts\sqlserver altında gelir: 001_Tables.sql, 002_SeedData.sql, 003_StoredProcedures.sql, 004_TableWriteLogs.sql. Uygulanan her betik SchemaVersions tablosuna SHA-256 özetiyle kaydedilir. Uygulanmış bir betik sonradan değişirse ürün açılışta hata verir ve açılmaz.

İki yol vardır. Seçim Database:AutoMigrate ayarıyla yapılır.

3.1 Yol A: Ürün kurar (AutoMigrate = true, varsayılan)

1. Uygulama veritabanı hesabına veritabanında db_owner yetkisi verilir. Veritabanı önceden açılmadıysa ürün onu oluşturur; bunun için hesaba dbcreator yetkisi de gerekir.
2. API ilk açılışta bekleyen betikleri sırayla uygular. Günlükte her betik için [Schema] Applying ve [Schema] Completed satırları görünür. Veritabanı oluşturulduysa [Schema] Database created satırı yazılır.
3. Sonraki açılışlarda yalnız yeni betikler uygulanır; günlükte [Schema] The schema is up to date satırı görünür.

3.2 Yol B: DBA kurar (AutoMigrate = false)

Sıkı değişiklik kontrolü olan kurumlar içindir. Bu yolda ürün şemaya hiç dokunmaz, yalnız kontrol eder.

1. DBA boş veritabanını oluşturur ve DbScripts\sqlserver altındaki betikleri numara sırasıyla uygular. sqlcmd ile uygulanacaksa -l (tırnaklı tanımlayıcılar açık) ve -f 65001 (betikler UTF-8, Türkçe metin içerir) seçenekleri kullanılır:

```
sqlcmd -S QLSUNUCU -d VeritabaniAdi -I -f 65001 -b -i 001_Tables.sql
```

2. DBA, API klasöründeki DbScripts\DbSchemaVersions.ps1 yardımcısını çalıştırır:

```
powershell -ExecutionPolicy Bypass -File .\DbSchemaVersions.ps1 -AppliedBy "KURUM\dba1"
```

Yardımcı hiçbir veritabanına bağlanmaz. Betiklerin ürünün hesapladığı özetlerini içeren SchemaVersions_Register.sql dosyasını üretir. DBA dosyayı inceler ve betiklerden sonra uygular.

3. Uygulama hesabına db_datareader, db_datawriter ve EXECUTE yetkisi verilir. Hesap ayrıca kanıt defteri rolüne eklenir, defter görünümünü okuma izni ve evidence şemasında tanım okuma izni alır (Bölüm 3.5). sysadmin ve db_owner verilmez.

4. API açılışta kontrol eder. Eksik ya da değişmiş betik varsa adını söyler ve açılmaz.

3.3 Kurulumdan sonra DBA'nın yapacağı üç iş

Tutarlı okuma. Kanıt niteliğindeki raporlar kirli okuma yapmaz; yoğun yazma anında kilit beklememeleri için uygulama veritabanında anlık görüntü okuma açılır. Bu komut betiklere konamaz, çünkü betikler transaction içinde çalışır. Veritabanına başka bağlantı yokken bir kez çalıştırılır:

```
ALTER DATABASE [VeritabaniAdi] SET READ_COMMITTED_SNAPSHOT ON WITH ROLLBACK IMMEDIATE;
```

Defter doğrulaması. Denetim dosyası üretilirken defter sys.sp_verify_database_ledger ile doğrulanır; bu yordam anlık görüntü yalıtımı ister. Kurulumu ürün yaparsa (Yol A) bu ayarı kendisi açar. DBA yolunda bir kez çalıştırılır:

```
ALTER DATABASE [VeritabanıAdı] SET ALLOW_SNAPSHOT_ISOLATION ON;
```

Ayar kapalıysa denetim dosyası "defter doğrulanamadı" yazar; hiçbir zaman "doğrulandı" göstermez.

Veritabanı yazma kaydının korunması. 004_TableWriteLogs.sql, uygulamayı atlayarak yapılan değişiklikleri de yakalamak için tablolara tetikleyici kurar ve TableWriteLogs tablosuna yazar. Uygulama hesabının bu tabloyu değiştirmesi gerekmez. Üretimde:

```
GRANT INSERT ON dbo.TableWriteLogs TO [uygulama_hesabi];
```

```
DENY UPDATE, DELETE ON dbo.TableWriteLogs TO [uygulama_hesabi];
```

3.4 Defter özeti deposu

Worker saatte bir özet turunu başlatır; özet API alır, imzalar ve bu klasöre yazar. Klasör kanıtın dış tanığıdır: veritabanını yöneten biri sonradan kayıtları değiştirse bile dışarı yazılmış özet değişmediği için değişiklik denetçinin doğrulamasında görünür.

1. Depolama ekibi değiştirilemez bir klasör hazırlar: WORM paylaşım, nesne kilidi açık depolama ya da veritabanı yöneticisinin yazamadığı bir paylaşım.
2. API uygulama havuzu hesabına bu klasörde yeni dosya oluşturma ve okuma yetkisi verilir; değiştirme ve silme yetkisi verilmez. Veritabanı yöneticisine bu klasörde yazma yetkisi verilmez. Denetim dosyası üretilirken defter bu klasördeki dosya ile doğrulanır; API dosyayı okuyamazsa sonuç VERIFIED_INTERNAL (bağımsız olmayan doğrulama) olur.
3. Klasör yolu Evidence:Ledger:DigestOutputPath ayarına yazılır (Bölüm 4.1). Yol API sunucusundan görülmelidir.

Ürün var olan bir dosyanın üstüne yazmaz. Klasör tanımlı değilse defter yine çalışır, ancak hiçbir kayıt dış özetle kapsamaz ve Yönetişim Kurulum Kontrolü ekranı uyarır. Ayrıntı: Bölüm 12.7.

3.5 Kanıt defteri

Denetim kayıtları uygulama veritabanında evidence şemasındaki AuditLogs tablosunda durur. Tablo SQL Server'ın append-only ledger (defter) tablosudur: veritabanı motoru UPDATE, DELETE ve TRUNCATE komutlarını sysadmin dahil herkes için reddeder. Bu yüzden uygulama veritabanı SQL Server 2022 ya da sonrası olmalıdır; defter bütün sürümlerde (Express dahil) vardır. Defter tablosu, veritabanının eski bir yedeğe döndürülmesine karşı tek başına koruma değildir; böyle bir dönüş dışarı yazılmış özetlerle fark edilir (Bölüm 3.4).

Kurulum betikleri şunları kurar:

Nesne	Ne işe yarar
evidence şeması	Sahibi girişi olmayan evidence_owner kullanıcısıdır. dbo şemasındaki bir nesne (tetikleyici, yordam) bu tabloya yazamaz
evidence.AuditLogs	Defter tablosu. Tetikleyici taşımaz
evidence.usp_Audit_Append	Tabloya yazmanın tek yolu. Olay zamanını veritabanı sunucusunun saatinden kendisi verir (çağırın zaman gönderemez) ve zorunlu alanları denetler
dbo.AuditLogs	Raporların ve ekranların okuduğu görünüm. Yazma yolu değildir
evidence_api_writer, evidence_worker_writer rolleri	Tabloyu okuma ve yordamı çalıştırma izni. Tabloya INSERT, UPDATE ve DELETE izni yoktur

DBA yolunda (3.2) uygulama hesabına verilecek ek izinler. API ve Worker aynı hesabı kullanıyorsa hesap iki role de eklenir:

```
ALTER ROLE evidence_api_writer ADD MEMBER [uygulama_hesabi];
ALTER ROLE evidence_worker_writer ADD MEMBER [uygulama_hesabi];
GRANT VIEW LEDGER CONTENT TO [uygulama_hesabi];
GRANT VIEW DEFINITION ON SCHEMA::evidence TO [uygulama_hesabi];
```

API ve Worker ayrı hesaplarla bağlanıyorsa API hesabı yalnız evidence_api_writer, Worker hesabı yalnız evidence_worker_writer rolüne eklenir. Bu durumda Worker hesabı onay, ret ve giriş gibi kullanıcı kararlarını denetim kaydına yazamaz.

Sınır kontrolü. API açılışta ve 15 dakikada bir, Worker da kendi işiyle şunları denetler: kanıt tablosu defter mi, tabloda tetikleyici var mı, yazma yordamı ürünün yayımladığı sürümle aynı mı, evidence şemasında beklenmeyen bir nesne var mı, tabloya başka bir nesne başvuruyor mu, tablo düşürülüp yeniden kurulmuş mu, veritabanında TRUSTWORTHY ya da DB_CHAINING açık mı. Kanıt tablosu yoksa, defter değilse ya da veritabanı SQL Server 2022'den eskiyse API açılmaz. Diğer bulgularda API açılır, ekranlar okunabilir, ama talep kaydetme, onay, ret ve çalıştırma gibi durum değiştiren işlemler sınır düzelene kadar yapılamaz. Bulgu Evidence.BoundaryBroken olayı, e-posta ve günlükle bildirilir; düzelince Evidence.BoundaryRestored yazılır.

Kurulumdan sonra DBA'nın dikkat edeceği kurallar:

- evidence şemasına nesne eklenmez, yazma yordamı değiştirilmez, kanıt tablosuna tetikleyici eklenmez. Bunlardan biri yapılırsa ürün değişiklik işlemlerini durdurur.
- Veritabanında TRUSTWORTHY ve DB_CHAINING kapalı kalır.
- Veritabanı sunucusunda NTP açık olmalıdır.

- DBA, veritabanı sunucusunda işletim sistemi yöneticisi olmamalıdır. SQL Server Audit ile şema değişiklikleri DBA'nın erişemediği bir kanala (Windows güvenlik günlüğü ya da SIEM) yazılması önerilir.

4. API kurulumu

1. Teslim edilen API klasörü sunucuya kopyalanır (ör. D:\SQLChangeGuard\api).
2. IIS'te bir uygulama havuzu açılır: .NET CLR sürümü No Managed Code.
3. API için bir site açılır, kök dizini API klasörüdür. API adresi için HTTPS bağlaması ve sertifika tanımlanır.
4. Uygulama havuzu hesabına API klasörü altındaki logs klasörüne yazma, sorgu sonucu dosya klasörüne okuma yetkisi verilir.
5. appsettings.json düzenlenir (4.1). Sırlar ortam değişkeni olarak tanımlanır (2.2).
6. Uygulama havuzu başlatılır. Günlük dosyası: API klasöründe logs\scg-YYYYMMDD.log.

4.1 Temel ayarlar

Aşağıdaki tablo kurulumda mutlaka gözden geçirilen ayarlardır. Her alanın ayrıntısı Kullanım Kılavuzu Bölüm 2.4'tedir. Entegrasyon ayarları bu kılavuzun 7 ile 11 arasındaki bölümlerindedir.

Ayar	Kurulumda yazılacak değer	Açıklama
AllowedOrigins	["https://changepguard.kurum.local"]	Web arayüzünün adresi. Buraya yazılmayan adresten gelen istek reddedilir
Database:AutoMigrate	true ya da false	Bölüm 3
Display:TimeZone	Europe/Istanbul	Belgelerde ve e-postalarda saatlerin gösterildiği saat dilimi. Kayıtlar her zaman UTC saklanır
Auth:Password:ResetBaseUrl	https://changepguard.kurum.local	Parola sıfırlama e-postasındaki bağlantının kökü
Auth:Password:MinLength, RequireUppercase, HistoryCount	12, true, 5 (öneri)	Yerel hesapların parola kuralları
Auth:AccountLockoutMaxAttempts	Kurum dizininin kilit eşiğinden küçük	Bölüm 7.6
Auth:MaxSessionHours	12	Oturumun ilk girişten itibaren en uzun süresi. Erişim jetonu (Jwt:AccessTokenMinutes) ve yenileme jetonu (Jwt:RefreshTokenHours) bu sürenin ötesine geçmez; reddedilen yenileme SessionRefreshRejected olayıyla denetim kaydına yazılır

Ayar	Kurulumda yazılacak değer	Açıklama
Mfa:Enabled, Mfa:EnforceEnrollment	true, kuruma göre	Yerel ve dizin hesapları için ürünün iki adımlı doğrulaması
Mail:Enabled, Mail:DevMode	true, false	DevMode açık kalırsa bütün e-postalar tek test adresine gider
QueryResult:OutputPath	D:\SQLChangeGuard\QrFiles	Sorgu sonucu dosyalarının yazıldığı klasör
ForwardedHeaders:KnownProxies	Yük dengeleyicinin IP adresi	Ürün bir ters vekil arkasındaysa. Yalnız bu adreslerden gelen X-Forwarded-For başlığı işlenir ve denetim kaydına gerçek istemci IP'si yazılır. Liste boşsa başlık okunmaz
Evidence:Signing:Enabled	true	Kanıt imzası. Kod varsayılanı false'tur: kapalıyken kanıt dosyaları ve paketler imzasız üretilir, Production sunucusunda çalıştırma yapılmaz (Bölüm 4.4)
Evidence:Signing:InstallationId	KURUM-PROD-01	Kurulum kimliği. Her kurulumda benzersiz, sonradan değiştirilmez
Evidence:Signing:Keys:1:PublicKeyPem	pub.pem içeriği	Bölüm 2.3. Sertifika deposu kullanılıyorsa boş bırakılabilir
Evidence:Signing:Keys:1:CertificateThumbprint	Sertifikanın parmak izi	Önerilen yol: imza anahtarı Windows sertifika deposunda (Bölüm 2.3)
Evidence:Ledger:DigestOutputPath	\\worm.kurum.local\changepuard-digest	İmzalı defter özetlerinin yazıldığı değiştirilemez depo. Yol API sunucusundan görülür (Bölüm 12.7)
Evidence:Ledger:DigestIntervalMinutes	60	Defter özeti aralığı
Evidence:Ledger:BoundaryCheckMinutes	15	Kanıt yazma sınırı kontrol aralığı
Evidence:Ledger:DigestStaleAfterIntervals	2	Bu kadar aralık özet gelmezse Yönetişim Kurulum Kontrolü uyarır

Ayar	Kurulumda yazılacak değer	Açıklama
Database:EvidenceLedger	true	Kanıt tablosu defter olarak kurulur. Üretimde değiştirilmez
Evidence:Signing:AllowUnsignedProductionExecution	false	İmza kapalıyken ya da onay zinciri imzasızken Production sunucusunda çalıştırma yapılmaz. true yalnız bilinçli bir istisnadır; açılması App.ControlRelaxed olarak kayda geçer (Bölüm 4.4)
Sandbox:AllowOnProduction	false	Production sunucusunda izole deneme (sandbox) çalışmaz. Deneme onaylanmamış betiği hedefte çalıştırıp geri alır; COMMIT, linked server çağrısı ve sequence değişikliği geri alınamaz
Evidence:Signing:Keys:N:RevokedAt	Boş	Anahtarın iptal anı. Bu andan sonra o anahtarla atılmış imzalar geçersiz sayılır (Bölüm 12.4)

4.2 E-posta

Ayar	Değerler	Açıklama
Mail:Enabled	true, false	false iken hiç e-posta gitmez
Mail:SmtpHost, Mail:SmtpPort	smtp.kurum.local, 587	SMTP sunucusu
Mail:Username	Gönderici hesap	Şifresi Mail__Password ortam değişkeninde
Mail:FromAddress, Mail:FromName	changeGuard@kurum.com.tr, SQL Change Guard	Gönderen
Mail:EnableSsl	true, false	true iken bağlantı sunucunun sunduğu şifrelemeyle kurulur: 465 portunda baştan şifreli, diğer portlarda sunucu STARTTLS sunuyorsa şifreli. false iken şifreleme kullanılmaz
Mail:DevMode	false	Üretimde false

Doğrulama: Ayarlar > Tanılama > Mail Testi ekranı aynı ayarlarla bir deneme e-postası gönderir.

4.3 Zaman damgası (isteğe bağlı)

Kanıt dosyalarının özeti bir RFC 3161 zaman damgası sunucusuna imzalatılır. Sunucuya yalnız içeriğin SHA-256 özeti gider; kanıt içeriği dışarı çıkmaz.

Ayar	Değerler	Açıklama
Evidence:Timestamp:Mode	Off (varsayılan), On	Ana anahtar. Off iken hiçbir ağ çağrısı yapılmaz
Evidence:Timestamp:Url	https://tsa.kurum.local/tsr	Kurumun ya da anlaşmalı otoritenin adresi
Evidence:Timestamp:TimeoutSeconds	10	Zaman aşımı
Evidence:Timestamp:ProxyUrl	http://vekil.kurum.local:8080	Boşsa işletim sisteminin tanımlı vekili kullanılır
Evidence:Timestamp:ProxyUseDefaultCredentials	true, false	Vekil sunucu, servisin Windows kimliğini bekliyorsa true
Evidence:Timestamp:ProxyBypass	tsa.kurum.local	Vekilden geçmeyecek adresler ; ile ayrılır

Sunucuya ulaşılamazsa iş durmaz, belge damgasız üretilir ve günlüğe uyarı yazılır. Bağlantı Ayarlar > Tanılama > Zaman Damgası Testi ekranından denenir.

4.4 Onay zinciri ve yönetim durumu

Ürün, bir talebin kaydedilen, onaylanan ve çalıştırılan içeriğini imzalı olaylarla birbirine bağlar ve çalıştırmadan önce aynı olduklarını denetler. Bu zincir ürünün olayları kabul edip kaydettiğini gösterir; hedef veritabanında gerçekleşen işlemi tek başına kanıtlamaz. Bunun için kurulumda bilinmesi gerekenler:

- İmza açık olmalıdır. Evidence:Signing:Enabled = true (kod varsayılanı false) ve kullanılabilir bir anahtar (Bölüm 2.3). İmza kapalıyken Production sunucusunda çalıştırma yapılmaz; Evidence:Signing:AllowUnsignedProductionExecution bu kuralın bilinçli istisnasıdır ve false kalmalıdır.
- Temel durum ilk açılışta yazılır. API ilk açıldığında onay politikalarının, onayı etkileyen ayarların, atlanamaz standartların ve kullanıcı rollerinin o anki halini bir kez mühürler (Governance.StateSealed). Bu halin doğruluğu kurulumu yapanın sorumluluğundadır ve kurulum tutanağına yazılır. Bundan sonraki her değişiklik ürünün ekranlarından yapılır ve yeniden mühürlenir.
- Tablolar uygulama dışından değiştirilirse yeni onay planı üretilmez, rolü değişmiş kullanıcı onay veremez ve olay SOC'a alarm olarak gider. Durum Yönetişim Kurulum Kontrolü ekranındaki "Onay politikaları ve roller son mühürlü durumla aynı" satırında görünür. Fark incelendikten sonra yalnız

SystemManager rolündeki bir kullanıcı, aynı satırdaki Yeniden temellendir düğmesiyle ve gerekçe yazarak tablodaki hali kabul eder (Governance.Rebaselined).

- Hedef sunucunun sertifikası doğrulanmalıdır. Sunucu tanımındaki "Sunucu sertifikasını doğrula" seçeneği açıkken bağlantı, kurumun güvendiği sertifika otoritesiyle doğrulanır. Kapalıyken bağlantı şifreli olur ama hedefin kimliği doğrulanmaz. Production sunucularında açılması önerilir; seçenek açılmadan önce kurumun sertifika otoritesi API ve Worker sunucularına güvenilir olarak eklenir. Oracle'da doğrulama TCPS ve sunucu adı eşleşmesiyle yapılır.

5. Worker kurulumu

1. Teslim edilen Worker klasörü sunucuya kopyalanır (ör. D:\SQLChangeGuard\worker).

2. Worker klasöründeki appsettings.json içinde WorkerApi:BaseUrl ayarına API adresi yazılır (ör. <https://changepguard-api.kurum.local>). WorkerApi:Key dosyada bırakılmaz, WorkerApi__Key ortam değişkeniyle verilir.

3. Servis kaydedilir (yönetici komut isteminde):

```
sc.exe create "ChangeGuardWorker" binPath= "D:\SQLChangeGuard\worker\SCG.Workers.exe" start=
auto DisplayName= "SQL Change Guard Worker"
```

```
sc.exe start "ChangeGuardWorker"
```

4. Servis hesabına Worker klasöründeki logs klasörüne ve sorgu sonucu dosya klasörüne yazma yetkisi verilir. Worker kanıt imzalama anahtarına ve defter özeti klasörüne erişmez; ikisi de API'nin işidir. İmza anahtarı sertifika deposundaya sertifikanın özel anahtarını okuma izni API uygulama havuzu hesabına verilir.

5. Günlük dosyası: Worker klasöründe logs\scg-worker-YYYYMMDD.log. Açılışta Worker configuration loaded from API satırı görünür.

6. Veritabanı hesabı: varsayılan olarak Worker, API ile aynı hesabı kullanır ve bağlantı dizesi API'den gelir. Ayrı hesap kullanılacaksa Worker sunucusunda ConnectionStrings__Worker ortam değişkeni tanımlanır (izinler Bölüm 3.5). Hangi kaynağın kullanıldığı açılışta "Worker database connection source" satırında yazar.

Worker'ın iş aralıkları API'nin appsettings.json dosyasındaki Workers bölümündedir ve Worker'a API üzerinden gelir. Tablodaki değerler teslim edilen ayar dosyasındaki değerlerdir ve çoğu kurum için uygundur. MainWorkSeconds ve ConnectionCheckSeconds için kodda varsayılan yoktur; bu satırlar dosyadan silinmez:

Ayar	Teslim edilen değer	Ne işe yarar
Workers:MainWorkSeconds	30	Kuyruktaki ve zamanı gelen çalıştırmaların alınma aralığı
Workers:ConnectionCheckSeconds	60	Hedef sunucuların bağlantı kontrolü aralığı
Workers:ConnectionCheckFailureThreshold	3	Bir sunucu için uyarı e-postasından önce arka arkaya kaç başarısız kontrol
Workers:StaleExecutionRecoveryMinutes	120	Bu süreden uzun sahiplenilmiş kalan çalıştırma ölü sayılır. Hedefte commit olmuş olabileceği için yeniden çalıştırılmaz, Uzlaştırma Bekliyor durumuna alınır; hedefte iş yapılmadığı kesinse (çalıştırma hata

Ayar	Teslim edilen deęer	Ne iŖe yarar
		verip geri alındıysa) Onaylandı durumuna döner. En uzun meŖru alıŖtırmadan büyük olmalıdır
Workers:WorkerErrorMailTo	BT ekibinin adresi	Worker hatalarının bildirileceęi adres
Workers:SiemPumpSeconds	10	SIEM gönderiminin yoklama aralıęı (Bölüm 10)
Workers:DirectorySyncPollSeconds	300	Dizin eşitlemesinin zamanının gelip gelmedięinin sorulma aralıęı (Bölüm 7)
Workers:ItsmPumpSeconds	30	ITSM'e bekleyen notların gönderilme aralıęı (Bölüm 9)

6. Web arayüzü, lisans ve ilk giriş

6.1 Web arayüzü

1. Teslim edilen web arayüzü klasörü sunucuya kopyalanır. Paket, kurumun API adresiyle hazırlanmıştır.
2. IIS'te ayrı bir site açılır, kök dizini bu klasördür. Web arayüzü adresi için HTTPS bağlaması tanımlanır.
3. Klasördeki web.config dosyası, sayfa yenilendiğinde ya da e-postadaki bir bağlantı açıldığında isteği index.html'e yönlendirir. Bunun için IIS URL Rewrite modülü kurulu olmalıdır.
4. API'nin AllowedOrigins ayarına web arayüzünün adresi yazılmış olmalıdır.

6.2 Lisans

1. Kurulumla gelen yönetici hesabıyla girilir (6.3).
2. Ayarlar > Lisans ekranında lisans dosyasının içeriği yüklenir.
3. Ürün imzayı doğrular. Geçersiz dosya kaydedilmez, çalışan lisansı bozmaz. Lisans veritabanında saklanır; API ve Worker aynı kaydı okur. Her lisans değişikliği License.Activated olayıyla denetim kaydına yazılır.

Lisansın bitmesine License:ExpiryWarningDays (varsayılan 30) gün kala arayüzde uyarı görünür. Yenileme aynı ekrandan yapılır.

6.3 İlk giriş

Kurulum, hiç kullanıcı yoksa bir yönetici hesabı açar: kullanıcı adı admin, parola admin123. Bu hesap ilk girişte parola değiştirmeye zorlanır; o oturum parola değiştirmekten başka bir işe yaramaz. Ardından:

1. Sunucular ekranında hedef sunucular tanımlanır.
2. Kullanıcılar eklenir ya da kurum dizini veya kurum hesabıyla giriş kurulur (Bölüm 7 ve 8).
3. Onay politikaları ve parametreler kurumun kurallarına göre ayarlanır.
4. Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranı açılır ve Bölüm 11 uygulanır.

Kurum dizini ya da kurum hesabıyla giriş kullanılsa da en az bir yerel SystemManager hesabı acil durum hesabı olarak tutulur. Dizin ya da kimlik sağlayıcısı çökerse sisteme bu hesapla girilir.

7. Kurum dizini (LDAP / Active Directory)

7.1 Nasıl çalışır

Kişi ürünün giriş ekranına kurum kullanıcı adını ve parolasını yazar. Ürün parolayı saklamaz; dizine şifreli bağlantıyla sorar. Parola doğruysa kişinin e-postasını, değişmeyen kimliğini, hesap durumunu ve gruplarını okur. Grupları rol eşleme tablosuyla karşılaştırıp rol verir.

Kim dizine sorulur:

- Hesap tipi LDAP olan kullanıcılar.
- Auth:Mode = Ldap iken üründe hiç kaydı olmayan kişiler. Doğrulanırlarsa hesapları açılır (7.4).
- Yerel ve SSO tipindeki hesaplar dizine sorulmaz.

Açık ya da kapalı olması Ldap:Host ayarına bağlıdır: boşsa dizin kullanılmaz.

7.2 Ayarlar (appsettings.json, Ldap bölümü)

Ayar	Değerler	Ne yazılmalı
Host	Sunucu adı, şemasız	dc01.kurum.local. Boş = dizin kapalı
Port	Sayı	Ldaps için 636, StartTls için 389. Yazılmazsa bu varsayılanlar kullanılır
Security	Ldaps (varsayılan), StartTls, None	Ldaps önerilir. None iken parola ağda açık gider; yalnız test içindir
AllowUntrustedCertificate	true, false	Üretimde false. true iken dizin sertifikası doğrulanmaz
BindFormat	DownLevel, Upn, SearchDn	Active Directory için DownLevel (KURUM\kullanıcı) ya da Upn (kullanıcı@kurum.local). OpenLDAP gibi dizinler için SearchDn
Domain	NetBIOS alan adı	KURUM. DownLevel için zorunlu. Kişi başka bir alan adı yazarsa parola denenmez
UpnSuffix	UPN soneki	kurum.local. Upn için zorunlu
BaseDn	Dizin yolu	DC=kurum,DC=local ya da OU=Calisanlar,DC=kurum,DC=local. Zorunlu. Bu yolun dışındaki kişi bulunamaz
UserFilter	LDAP süzgeci	Active Directory: {&(objectClass=user)(sAMAccountName={user})}. {user} yazılan adla değişir. Tam olarak bir kişi döndürmelidir

Ayar	Değerler	Ne yazılmalı
BindDn	Servis hesabının tam adı	CN=changeloguard-okuyucu,OU=Servis,DC=kurum,DC=local. SearchDn biçimi ve eşitleme için zorunlu. Parolası Ldap__BindPassword ortam değişkeninde
IdentityAttribute	objectGUID (varsayılan), entryUUID	Active Directory: objectGUID. OpenLDAP: entryUUID. Kurulumdan sonra değiştirilmez
EmailAttribute	Varsayılan mail	Dizinde e-postası olmayan kişiye hesap açılmaz
DisplayNameAttribute	Varsayılan displayName	Görünen ad
GroupMatch	Dn (varsayılan), Cn	Dn önerilir: grup tam adıyla karşılaştırılır. Cn iken farklı klasörlerdeki aynı adlı gruplar ayırt edilmez
NestedGroups	true (varsayılan), false	true iken iç içe gruplar da sayılır (en fazla 10 seviye, 500 grup)
RoleSource	Manual (varsayılan), Directory	7.4
TimeoutSeconds	2 ile 60, varsayılan 10	Dizin çağrısının zaman aşımı
Sync:Enabled	true, false (varsayılan)	Üretimde true önerilir (7.5)
Sync:IntervalMinutes	15 ile 1440, varsayılan 60	İki eşitleme arası en az süre
Sync:AbortRatio	Varsayılan 0.2	Güvenlik sınırı (7.5)
Sync:AbortMinCount	Varsayılan 5	Güvenlik sınırı (7.5)

İlgili Auth ayarı: Auth:Mode = Local (varsayılan) iken yalnız üründe açılmış hesaplar girer. Ldap iken üründe kaydı olmayan kişi dizine sorulur.

Active Directory örneği:

```
"Ldap": {
  "Host": "dc01.kurum.local",
  "Port": 636,
  "Security": "Ldaps",
  "AllowUntrustedCertificate": false,
  "BindFormat": "DownLevel",
  "Domain": "KURUM",
  "BaseDn": "DC=kurum,DC=local",
  "UserFilter": "(&(objectClass=user)(sAMAccountName={user}))",
  "BindDn": "CN=changeloguard-okuyucu,OU=Servis,DC=kurum,DC=local",
```

```

"IdentityAttribute": "objectGUID",
"GroupMatch": "Dn",
"NestedGroups": true,
"RoleSource": "Directory",
"Sync": { "Enabled": true, "IntervalMinutes": 60, "AbortRatio": 0.2, "AbortMinCount": 5 }
}

```

7.3 Dizinden ne okunur, üründe nereye yazılır

Dizindeki öznitelik	Üründe nereye yazılır	Açıklama
sAMAccountName	Users.DomainUsername	Yeni hesabın kullanıcı adı. Öznitelik yoksa kişinin yazdığı ad kullanılır
mail (EmailAttribute)	Users.Email	Her girişte ve eşitlemede güncellenir
objectGUID ya da entryUUID (IdentityAttribute)	UserExternalIdentities.Subject (Provider = Ldap)	Değişmeyen kimlik. Hesap ilk girişte buna bağlanır; kullanıcı adı değişse ya da aynı adla yeni biri gelse hesap yanlış kişiye geçmez
memberOf (iç içe dahil)	Users.Role (eşleme tablosuyla)	Rol hesaplanır (7.4)
userAccountControl	Saklanmaz	Hesap kapalıysa (Active Directory ACCOUNTDISABLE biti) giriş reddedilir, eşitleme erişimi kapatır
lockoutThreshold (alan kökünde)	Saklanmaz	Dizinin kilit eşiği. Yönetişim Kurulum Kontrolü ekranında ürünün eşiğiyle karşılaştırılır

Yeni dizin hesabı Users tablosuna AuthType = Ldap ve boş parola özetiyle yazılır. Dizin hesabının parolası üründe sıfırlanamaz.

7.4 Grup ile rol eşlemesi

Eşlemeler Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında, sağlayıcı "Dizin (LDAP)" seçilerek tanımlanır. Her satır bir grubu bir role bağlar:

Sağlayıcı	Değer	Rol
Dizin (LDAP)	CN=DBA-Ekibi,OU=Gruplar,DC=kurum,DC=local	DbAdmin
Dizin (LDAP)	CN=Degisiklik-Kurulu,OU=Gruplar,DC=kurum,DC=local	ChangeManager

Sağlayıcı	Değer	Rol
Dizin (LDAP)	CN=Talep-Acanlar,OU=Gruplar,DC=kurum,DC=local	Requester

Kurallar:

- Birden fazla grup eşleşirse en yüksek rol verilir.
- SystemManager eşlemeyle hiçbir durumda verilmez; yalnız Kullanıcılar ekranından elle verilir.
- Değerde boşluk ve büyük küçük harf önemli değildir.
- Değeri bilmiyorsanız kişi bir kez girmeyi denesin. Denetim Günlükleri'ndeki LdapLoginDenied kaydında ReceivedGroups alanı dizinden gelen grupları yazar.
- Eşleme değişikliği denetim kaydına yazılır; ayar değişikliği onayı açıksa ikinci bir yöneticinin onayından geçer.

Rolün kaynağı (Ldap:RoleSource):

	Manual (varsayılan)	Directory
Yeni kişi ilk girişte	Eşlenen rolle açılır; eşlenen grubu yoksa erişimsiz (NoAccess) açılır, rolü yönetici verir	Eşlenen rolle açılır; eşlenen grubu yoksa hesap açılmaz
Var olan kişinin rolü	Yönetici ne veriyse o	Her girişte ve eşitlemede gruptan yeniden hesaplanır
Kullanıcılar ekranında rol	Elle değişir	Değişmez (yalnız SystemManager verilir geri alınabilir)
Gruplar okunamazsa	Yeni hesap açılmaz	Var olan rol düşürülmez, giriş reddedilir

7.5 Eşitleme

Eşitleme açıksa Worker belirli aralıklarla API'ye "eşitleme zamanı geldi mi" diye sorar; eşitlemeyi API yapar. Ürünün bütün dizin hesapları servis hesabıyla dizinde aranır:

Dizindeki durum	Üründe ne olur
Kişi bulunamadı ya da hesabı kapalı	Rol NoAccess olur, açık oturumları kapanır. Hesap silinmez
Grubu değişti (Directory modunda)	Rol yeniden hesaplanır; değiştiyse oturumları kapanır
E-postası değişti	Güncellenir

Güvenlik sınırı: Bir eşitlemede kapatılacak hesap sayısı AbortMinCount değerinden az değilse ve oran AbortRatio değerini aşıyorsa eşitleme hiçbir değişiklik yapmaz ve Ldap.SyncAborted olayını yazar. Yanlış bir BaseDn ya da dizindeki geçici bir sorun herkesi dışarıda bırakmasın diye vardır. Dizine ulaşılamazsa da değişiklik yapılmaz. Sistemi yönetecek son SystemManager hesabı kapatılmaz.

Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranındaki Şimdi eşitle düğmesi eşitleme kapalıyken de çalışır.

7.6 Kilit eşiği

Ürün hatalı parolaları sayar ve Auth:AccountLockoutMaxAttempts denemede hesabı kilitler. Dizin de kendi eşiği vardır. Ürünün eşiği dizininkinden küçük olmalıdır; aksi halde biri ürün ekranından parola tahmin ederek kişinin kurumdaki hesabını kilitleyebilir. Üründe hesabı olmayan adlar için de aynı ad için Auth:AccountLockoutMaxAttempts hatalı denemeden sonra Auth:AccountLockoutMinutes dakika boyunca dizine gidilmez.

7.7 Kurulum sırası

1. Dizin ekibinden yalnız okuma yetkili bir servis hesabı alınır; parolası Ldap__BindPassword ortam değişkenine yazılır.
2. Dizin sertifikasını veren kök sertifikanın API sunucusunda güvenilir olduğu kontrol edilir.
3. Ldap bölümü doldurulur, API yeniden başlatılır.
4. Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında Bağlantıyı test et düğmesine basılır. Hata olursa hangi adımda olduğu yazar: ayar, sunucuya bağlanma, servis hesabıyla oturum açma ya da BaseDn okuma.
5. Rol eşlemeleri tanımlanır, sonra gerekiyorsa RoleSource = Directory ve Auth:Mode = Ldap yapılır.
6. Şimdi eşitle çalıştırılır; Yönetişim Kurulum Kontrolü ekranında dizin satırları kontrol edilir.

Bu bölümde sonradan yapılan her değişiklik API açılışında fark edilir ve eski ve yeni haliyle Ldap.ConfigurationChanged olayı olarak denetim kaydına yazılır. Parola yazılmaz.

8. Kurum hesabıyla giriş (SSO)

8.1 Nasıl çalışır

Kişi giriş ekranında kurum hesabıyla giriş düğmesine basar. Tarayıcı kurumun kimlik sağlayıcısına gider; parola ve MFA orada girilir, ürüne hiç gelmez. Kimlik sağlayıcısı kişiyi imzalı bir kimlik bilgisiyle ürüne geri gönderir. Ürün imzayı, kimin verdiğini, kimin için verildiğini, süresini ve kendi isteğine ait olup olmadığını kontrol eder. Kişiyi değişmeyen kimliğiyle bulur ya da açar, grubunu role eşler ve kendi oturumunu açar.

Desteklenen protokoller: OIDC (Microsoft Entra ID, Keycloak, Okta) ve SAML 2.0 (AD FS, Entra ID, Keycloak). Aynı anda birden fazla kimlik sağlayıcısı tanımlanabilir; her biri giriş ekranında ayrı bir düğmedir. LDAP ve SSO aynı anda açık olabilir; her hesap kendi tipiyle girer.

8.2 Genel ayarlar (appsettings.json, Sso bölümü)

Ayar	Değerler	Ne yazılmalı
Enabled	true, false (varsayılan)	false iken SSO kapalıdır; SSO hesaplarının açık oturumları da API yeniden başlayınca kapanır. Kimlik sağlayıcısından şüphe edildiğinde acil kapatma yolu budur
ApiBaseUrl	API'nin tarayıcıdan görünen adresi	https://change-guard-api.kurum.local. Dönüş adresleri bundan kurulur, istekten türetilmez
FrontendBaseUrl	Web arayüzünün adresi	https://change-guard.kurum.local
AutoProvision	true (varsayılan), false	true iken hesabı olmayan kişi ilk girişte açılır. false iken hesabı yönetici önceden "Kurum hesabı" tipiyle açar
RoleSource	Idp (önerilen), Manual	Idp: rol her girişte gruptan yeniden hesaplanır. Manual: grup yalnız ilk açılışta rol verir
MaxSessionHours	Saat, 0 = sınır yok	Auth:MaxSessionHours ile birlikte küçük olanı uygulanır. Kimlik sağlayıcısında kapatılan hesabın oturumu en geç bu sürede biter
SignOutFromIdp	true, false	true iken üründen çıkışta kimlik sağlayıcısından da çıkılır (yalnız OIDC)
LoginTimeoutMinutes	1 ile 60, varsayılan 10	Kimlik sağlayıcısından dönmek için tanınan süre
ExchangeCodeSeconds	30 ile 600, varsayılan 120	Dönüşten sonraki tek kullanımlık kodun ömrü

Ayar	Değerler	Ne yazılmalı
ClockSkewMinutes	0 ile 15, varsayılan 5	Sunucu saatleri arasında kabul edilen fark

İlgili Auth ayarı: Auth:LocalLoginAllowedUsers listesine yalnız acil durum hesapları yazılır (ör. ["admin"]). Liste doluyken yalnız listedeki yerel hesaplar parolayla girer. SSO açıkken bu hesaplarla her giriş LoginBreakGlass olayı olarak denetim kaydına yazılır ve SOC'a alarm olarak gider.

8.3 Kimlik sağlayıcısı ayarları (Sso:Providers listesi)

Ayar	OIDC	SAML
Name	Kalıcı ad, ör. Entra. Harf, rakam, - ve _ (en fazla 50). Kurulumdan sonra değiştirilmez: kullanıcı bağları ve eşlemeler bu adla tutulur	Aynı
DisplayName	Düğmede görünen ad	Aynı
Protocol	Oidc	Saml
RequireHttpsMetadata	Üretimde true	Üretimde true
Authority	Entra ID: https://login.microsoftonline.com/kiraci-id/v2.0 . Keycloak: https://sunucu/realms/realm	Kullanılmaz
ClientId	Uygulama kaydının istemci kimliği	Kullanılmaz
ClientSecret	Dosyada boş; Sso__Providers__N__ClientSecret	Kullanılmaz
Scopes	Varsayılan profile, email	Kullanılmaz
IdpMetadataUrl	Kullanılmaz	AD FS: https://adfs/FederationMetadata/2007-06/FederationMetadata.xml
SpEntityId	Kullanılmaz	Boşsa {ApiBaseUrl}/api/auth/sso/saml/metadata/{Name}
SpCertificatePath, SignAuthnRequests	Kullanılmaz	Kimlik sağlayıcısı imzalı istek istiyorsa .pfx yolu ve true. Parolası Sso__Providers__N__SpCertificatePassword
SubjectClaim	Entra ID: oid. Keycloak, Okta: sub	NameID (kalıcı biçimde olmalı)
UsernameClaim	preferred_username	AD FS: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
EmailClaim	email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Ayar	OIDC	SAML
GroupsClaim	Entra ID: roles (önerilen) ya da groups. Keycloak: groups	http://schemas.microsoft.com/ws/2008/06/identity/claims/role
RequireMfaClaim	Üretimde true	Üretimde true
MfaClaim, MfaClaimValue	amr, mfa	AuthnContextClassRef, http://schemas.microsoft.com/claims/multipleauthn

8.4 Kimlik bilgisinden ne okunur, üründe nereye yazılır

Kimlik bilgisindeki alan	Ayar	Üründe nereye yazılır
Değişmeyen kimlik (oid, sub, NameID)	SubjectClaim	UserExternalIdentities.Subject. Provider sütununa sağlayıcının Name değeri yazılır. Kişi sonraki girişlerde bununla bulunur
Kullanıcı adı	UsernameClaim	Users.DomainUsername. Yalnız yeni hesapta ve önceden açılmış SSO hesabına ilk bağlanmada kullanılır; sonra değişmez
E-posta	EmailClaim	Users.Email. Yeni hesapta zorunludur; her girişte güncellenir
Gruplar ya da roller	GroupsClaim	Users.Role (eşleme tablosuyla)
MFA bilgisi	MfaClaim, MfaClaimValue	Saklanmaz. RequireMfaClaim true iken değer yoksa giriş reddedilir. Kararın oturumunda MFA bilgisi denetim dosyasına girer

Yeni SSO hesabı Users tablosuna AuthType = Sso, boş parola ve boş MFA sırrıyla yazılır. MFA'yı kimlik sağlayıcısı yapar.

8.5 Grup ile rol eşlemesi

Eşlemeler Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında, sağlayıcının adı seçilerek tanımlanır. Değer alanına kimlik bilgisinde gelen metin yazılır:

Kimlik sağlayıcısı	Gelen değer	Eşleme değeri örneği
Entra ID, uygulama rolü (önerilen)	Uygulama kaydında tanımlanan rol değeri	ChangeGuard.DbAdmin
Entra ID, grup	Grubun adı değil, kimlik numarası (Object ID)	5f3c1a2e-8b0d-4e6f-9a17-2c4d8e9f0a11

Kimlik sağlayıcısı	Gelen değer	Eşleme değeri örneği
AD FS	Claim kuralına göre grup adı	DBA-Team
Keycloak	Grup adı	dba-ekibi

Kurallar LDAP ile aynıdır: en yüksek rol kazanır, SystemManager eşlemeyle verilmez, değeri bilmiyorsanız Denetim Günlükleri'ndeki SsoLoginDenied kaydının ReceivedGroups alanına bakılır. RoleSource = Idp iken bir eşleme değiştirilir ya da silinirse o sağlayıcıya bağlı ve o roldeki kişilerin açık oturumları hemen kapanır.

8.6 Kimlik sağlayıcısında yapılacaklar

Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranı, kimlik sağlayıcısına girilecek adresleri kopyalanabilir biçimde gösterir: geri dönüş adresi, çıkıştan sonra dönüş adresi, SAML için uygulama kimliği (Entity ID), geri dönüş adresi (ACS) ve uygulama üstverisi.

Microsoft Entra ID (OIDC):

1. App registrations > New registration. Redirect URI (Web): ekrandaki geri dönüş adresi.
2. Certificates & secrets > New client secret. Değer Sso__Providers__N__ClientSecret ortam değişkenine yazılır.
3. App roles: her ürün rolü için bir değer (ör. ChangeGuard.DbAdmin). Enterprise applications altında kullanıcılara ya da gruplara atanır.
4. Token configuration > Add optional claim > ID > email.
5. appsettings: Authority, ClientId, SubjectClaim = oid, GroupsClaim = roles, RequireMfaClaim = true, MfaClaim = amr, MfaClaimValue = mfa, RequireHttpsMetadata = true.

AD FS (SAML):

1. Relying Party Trusts > Add. Ekrandaki uygulama üstverisi adresi verilir (ya da dosya olarak yüklenir).
2. Claim issuance policy: NameID (Persistent), UPN, E-Mail Address, Role.
3. appsettings: Protocol = Saml, IdpMetadataUrl, UsernameClaim, EmailClaim, GroupsClaim ve MfaClaim 8.3'teki değerlerle.

8.7 Kurulum sırası

1. Kimlik sağlayıcısında uygulama kaydı yapılır (8.6), sır ortam değişkenine yazılır.
2. Sso bölümü doldurulur, Enabled = true yapılır, API yeniden başlatılır.
3. Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında sağlayıcının Bağlantıyı test et düğmesiyle üstverinin okunduğu görülür.

4. Rol eşlemeleri tanımlanır.

5. Bir test kullanıcısıyla girilir; Denetim Günlükleri'ndeki SsoLoginSuccess kaydında rolün ve MFA bilgisinin beklendiği gibi geldiği doğrulanır.

6. Auth:LocalLoginAllowedUsers yalnız acil durum hesaplarıyla doldurulur.

Bu bölümde ve Auth:LocalLoginAllowedUsers listesinde sonradan yapılan her değişiklik API açılışında fark edilir ve eski ve yeni haliyle Sso.ConfigurationChanged olayı olarak denetim kaydına yazılır. Sırlar yazılmaz.

9. ITSM entegrasyonu

9.1 Nasıl çalışır

ITSM (ServiceNow, Jira Service Management, ServiceCore) kurumun iş kayıtlarını tutar: değişiklik kaydı, olay kaydı, hizmet talebi. ITSM "bu iş yapılsın mı, CAB izin verdi mi" sorusunu, SQL Change Guard "tam olarak hangi betik, hangi sunucuda, kim onayladı, kim çalıştırdı" sorusunu cevaplar. Entegrasyon ikisini bağlar. ITSM açıkken ürün:

1. Talep kaydedilirken numaranın ITSM'de var olduğunu, doğru türde olduğunu ve kapanmadığını kontrol eder.
2. Çalıştırmadan hemen önce (Çalıştır düğmesi, zamanlanmış çalıştırma, sürüm paketi ve Worker'ın son kontrolü) kaydın uygulanabilir olduğunu kontrol eder. Bu kontrol ön bellek kullanmaz.
3. Zamanlarken o saatte kesin duracak durumları engeller, henüz belli olmayanlar için uyarır.
4. ITSM'de gördüğü durumu kanıt olarak saklar.
5. Talepteki önemli adımları ITSM kaydına not olarak yazar.

Ürün ITSM kaydının durumunu değiştirmez, kaydı kapatmaz ve silmez. Nota betik metni, sonuç verisi ya da parola yazılmaz.

Bizdeki talep türlerinin ITSM karşılığı:

Talep	ITSM kaydı	Ekrandaki alan (ITSM açıkken)
Değişiklik	Değişiklik kaydı (ör. CHG0030001)	Değişiklik kaydı no
Sorgu sonucu (veri çıkarma)	Hizmet talebi (ör. RITM0010001). IsmQueryResultTicketKind ile Change ya da None yapılabilir	Hizmet talebi no
Geri alma	Kaynak talebin değişiklik kaydı	Kaynaktan gelir
Acil Durum işaretli talep	Ek olarak olay kaydı (ör. INC0012345)	Olay no

Numaranın türünü, yazıldığı alan belirler; ürün numaraya bakıp tür tahmin etmez.

9.2 Bağlantı ayarları (appsettings.json, Itsm bölümü)

Bu bölüm yalnız bağlantıyı tutar. ITSM'i açıp kapatan anahtar ürün içindeki ItsmEnabled parametresidir (9.6).

Ayar	Değerler	Ne yazılmalı
Provider	None, ServiceNow, Jira, GenericRest	GenericRest: ServiceCore ve listede olmayan her ITSM

Ayar	Değerler	Ne yazılmalı
BaseUrl	Adres, sonunda / olmadan	ServiceNow: https://kurum.service-now.com. Jira Cloud: https://kurum.atlassian.net. Jira Data Center: https://jira.kurum.local
AuthType	Basic, Bearer, HeaderKey	ServiceNow ve Jira Cloud: Basic. Jira Data Center: Bearer. Başlıkta API anahtarı isteyen ITSM: HeaderKey
Username	Entegrasyon hesabı	Jira Cloud'da hesabın e-postası
Password	Dosyada boş; Itsm__Password	Basic için parola. Jira Cloud'da API anahtarı
Token	Dosyada boş; Itsm__Token	Bearer ve HeaderKey için anahtar
HeaderName	Başlık adı	Yalnız HeaderKey için, ör. X-API-Key
Proxy	Vekil adresi	Bulut ITSM'e vekil sunucudan çıkılıyorsa, ör. http://proxy.kurum.local:8080
TimeoutSeconds	2 ile 60, varsayılan 10	Aşılırsa ITSM'e ulaşamadı sayılır
CacheSeconds	0 ile 600, varsayılan 60	Talep ekranındaki sorguların önbelleği. Çalıştırma kontrolü önbellek kullanmaz
AllowUntrustedCertificate	true, false	Üretimde false
ProductBaseUrl	Web arayüzünün adresi	ITSM notunun sonuna eklenen bağlantının kökü, ör. https://changepuard.kurum.local. Boşsa not bağlantısız gider

Entegrasyon hesabına en az yetki verilir. ServiceNow: change_request, incident ve sc_req_item tablolarında okuma, work_notes alanına yazma. Jira: ilgili projelerde görme ve yorum ekleme. Durum değiştirme ve silme yetkisi verilmez.

9.3 ServiceNow: ne okunur, nereye yazılır

Ürün her kayıt türünü kendi tablosunda arar. Tablolar Itsm:ServiceNow altında değiştirilebilir:

Ayar	Varsayılan	Kayıt türü
ChangeTable	change_request	Değişiklik kaydı
IncidentTable	incident	Olay kaydı
RequestTable	sc_req_item	Hizmet talebi

Sorgu: GET

{BaseUrl}/api/now/table/{tablo}?sysparm_query=number={numara}&sysparm_limit=1&sysparm_display_value=all. Not yazma: PATCH {BaseUrl}/api/now/table/{tablo}/{sys_id}, gövdede work_notes.

ServiceNow alanı	Okunan kısım	Üründe (ItsmTickets tablosu)
number	Ekrandaki değer	TicketNo
short_description	Ekrandaki değer	Title
state	Ekrandaki ad (ör. Implement, Authorize, Closed)	ExternalState
approval	Ekrandaki ad (ör. Approved, Requested)	Approval. Yalnız değişiklik kaydında onay olarak değerlendirilir
start_date	UTC iç değer	PlannedStart
end_date	UTC iç değer	PlannedEnd
sys_id	İç değer	Saklanmaz. Not yazmada ve bağlantıda kullanılır: Link = {BaseUrl}/{tablo}.do?sys_id={sys_id}
(ürün hesaplar)		StateClass (9.5), Source = ServiceNow, LastVerifiedAt = sorgu anı

Kayıt bulunamazsa ServiceNow boş liste döner ve ürün "bulunamadı" der. Numara yanlış alana yazılırsa (ör. olay numarası değişiklik alanına) o numara değişiklik tablosunda olmadığı için sonuç "bulunamadı"dır.

9.4 Jira ve diğer ITSM'ler: ne okunur, nereye yazılır

Jira (Itsm:Jira):

Ayar	Örnek	Ne işe yarar
ApiVersion	2 (Cloud ve Data Center), 3 (yalnız Cloud)	3'te not gövdesi Atlassian Document Format ile gider
ChangeIssueTypes	Change	Değişiklik kaydı sayılan tip adları, ; ile ayrılır. Boşsa tip kontrol edilmez
IncidentIssueTypes	Incident	Olay kaydı tipleri
RequestIssueTypes	Service Request;Service Request with Approvals	Hizmet talebi tipleri
PlannedStartField, PlannedEndField	customfield_10050, customfield_10051	Planlanan başlangıç ve bitiş özel alanlarının kimliği. GET /rest/api/2/field ile bulunur. Boşsa planlanan aralık okunmaz

Sorgu: GET {BaseUrl}/rest/api/{sürüm}/issue/{anahtar}?fields=summary,status,issuetype ve planlanan alanlar. Not: POST {BaseUrl}/rest/api/{sürüm}/issue/{anahtar}/comment.

Jira alanı	Üründe
key	TicketNo
fields.summary	Title
fields.status.name	ExternalState
fields.status.statusCategory.key (new, indeterminate, done)	Saklanmaz. done kategorisindeki her durum kapanmış sayılır
fields.issuetype.name	Saklanmaz. Beklenen tip listesinde değilse "yanlış tür"
PlannedStartField, PlannedEndField	PlannedStart, PlannedEnd
(onay)	Jira'da ayrı onay alanı okunmaz; onay iş akışındaki durumla ifade edilir (IsmReadyStates). Approval boş kalır
(ürün hesaplar)	Link = {BaseUrl}/browse/{anahtar}, StateClass, Source = Jira

ServiceCore ve diğerleri (Ism:GenericRest). Kod değişikliği gerekmeden, ITSM'in API adresi ve yanıtaki alanların yolu yazılır. Yol nokta ile ayrılır, dizi için sayı yazılır (ör. result.0.state):

Ayar	Ne yazılır	Üründe
ChangeUrlTemplate, IncidentUrlTemplate, RequestUrlTemplate	Kaydı okuyan adres; {ticket} numarayla değişir	
StatePath	Durum alanının yolu (zorunlu)	ExternalState
StateCategoryPath	Durum kategorisi alanının yolu (isteğe bağlı)	Değer done ise kapanmış sayılır
TitlePath	Başlık alanının yolu	Title
ApprovalPath	Onay alanının yolu. Doluysa değişiklik kaydında onay aranır	Approval
PlannedStartPath, PlannedEndPath	Planlanan zaman alanlarının yolu	PlannedStart, PlannedEnd
TypePath ve ChangeTypes, IncidentTypes, RequestTypes	Tip alanının yolu ve her türün tip adları	Tip beklenen listede değilse "yanlış tür"
IdPath	Kaydın iç kimliği	Saklanmaz
BrowseUrlTemplate	Kaydın tarayıcıda açılan adresi	Link
CommentUrlTemplate, CommentMethod, CommentBodyTemplate	Not adresi ({ticket}, {kind} = change, incident ya da request), POST ya da PUT, JSON gövde ({message} ve {ticket} yerleşir)	

Durum ve başlık alanlarının ikisi de boş gelirse ya da ITSM 404 dönerse kayıt bulunamadı sayılır.

9.5 Durum nasıl yorumlanır (StateClass)

ITSM'deki durum adları kurumdan kuruma değişir. Ürün durumu üç parametreye göre sınıflar. Karşılaştırmada büyük küçük harf ve baştaki, sondaki boşluk önemsizdir. Kurallar sırayla uygulanır, ilk uyan kazanır:

Sıra	Koşul	StateClass
1	Durum boş	Unknown
2	Durum ItsmClosedStates listesinde	Closed
3	Durum kategorisi done (Jira ya da StateCategoryPath)	Closed
4	Kayıt değişiklik kaydı değil (olay, hizmet talebi)	Open
5	Durum ItsmReadyStates listesinde ve onay ayrı bir alanda okunmuyor (Jira; ApprovalPath boş GenericRest)	Ready
6	Durum ItsmReadyStates listesinde, onay okunuyor ama boş geldi	Unknown
7	Durum ItsmReadyStates listesinde, onay ItsmApprovedValues listesinde	Ready
8	Durum ItsmReadyStates listesinde, onay başka bir değer	Pending
9	Diğer her durum	Pending

Sınıfın kararlara etkisi:

StateClass	Kayıtta (ItsmVerifyOnSave = Block)	Çalıştırmada (ItsmExecuteGate = Block)
Ready	Kaydedilir	Çalışır. ItsmEnforceWindow = true ise ayrıca şu an planlanan aralıkta olmalıdır
Pending	Kaydedilir (talep CAB'dan önce hazırlanabilir)	Değişiklik kaydında durur: CAB onayı yok ya da kayıt hazır değil
Unknown	Kaydedilir	Değişiklik kaydında durur
Open	Kaydedilir	Hizmet talebi ve olay kaydında çalışır (CAB onayı yoktur)

StateClass	Kayıtta (ItsmVerifyOnSave = Block)	Çalıştırmada (ItsmExecuteGate = Block)
Closed	Kaydedilmez	Durur

ServiceNow değişiklik kaydı örneği (varsayılan parametrelerle):

state	approval	StateClass	Sonuç
Authorize	Requested	Pending	Kaydedilir, çalıştırılmaz
Implement	Approved	Ready	Çalıştırılır
Implement	(boş)	Unknown	Onay okunamadığı için çalıştırılmaz
Closed	Approved	Closed	Kaydedilmez, çalıştırılmaz

Duran talep reddedilmiş sayılmaz: Onaylandı durumunda bekler, ITSM kaydı uygun hale gelince yeniden çalıştırılır. Zamanlanmış çalışma durursa zamanlama temizlenir ve talep sahibiyle onaylayanlara e-posta gider. Sürüm paketinde bir talep durursa paket hiç başlamaz.

İstisnalar:

- Kaynağa bağlı geri alma çalışma ve zamanlama kontrolünden muaftır. Kaynak uygulandıktan sonra ITSM kaydı genelde kapanır; geri alma engellenseydi bozulan bir şey düzeltilemezdi. Muafiyet kayda geçer.
- Acil talepte CAB onayı aranmaz; kapanmış, olmayan ya da yanlış türdeki değişiklik kaydı yine durdurur. Muafiyet kayda geçer.
- ITSM'e ulaşılamazsa ItsmUnavailablePolicy karar verir. Acil talep her durumda geçer.

9.6 Davranış parametreleri (Ayarlar > Parametreler > ITSM Ticket)

Parametre	Varsayılan	Değerler	Ne işe yarar
ItsmEnabled	false	true, false	Ana anahtar. false iken ürün ITSM'e hiç gitmez, not yazmaz; numara yalnız biçim ve zorunluluk kuralıyla kontrol edilir
ItsmVerifyOnSave	Block	Block, Warn, Off	Kayıtta numara kuralı bozursa (kapanmış, yok, yanlış tür): reddet,

Parametre	Varsayılan	Değerler	Ne işe yarar
			uyarıp kaydet ya da hiç sorma
ItsmExecuteGate	Block	Block, Off	Çalıştırmadan önce ITSM'e sorulsun mu. Zamanlama kontrolü de buna bağlıdır
ItsmEnforceWindow	false	true, false	true iken iş yalnız ITSM'deki planlanan aralıkta çalıştırılabilir ve aralığın dışına zamanlanamaz. Kayıta aralık yoksa çalışma durur
ItsmVerifyIncident	Warn	Block, Warn, Off	Acil talepteki olay numarası kapanmış ya da yoksa ne olsun
ItsmUnavailablePolicy	AllowAndRecord	AllowAndRecord, Block	ITSM'e ulaşılamazsa işi sürdür ve kayda geçir (SOC'a alarm gider) ya da durdur
ItsmQueryResultTicketKind	Request	Request, Change, None	Sorgu sonucu talebinin numarası hangi tür ITSM kayıdır. None: ITSM'e sorulmaz, yalnız biçim kontrolü
ItsmReadyStates	Scheduled;Implement	; ile ayırık liste	Değişiklik kaydı bu durumlardaysa uygulanabilir sayılır
ItsmClosedStates	Review;Closed;Canceled;Cancelled;Resolved;Closed Complete;Closed Incomplete;Closed Skipped	; ile ayırık liste	Kayıt bu durumlardaysa kapanmış sayılır
ItsmApprovedValues	Approved	; ile ayırık liste	Onay alanında onaylandı sayılan değerler
ItsmWriteBackEnabled	true	true, false	ITSM kaydına not yazılsın mı

Parametre	Varsayılan	Değerler	Ne işe yarar
ItsmWriteBackEvents	Talep adımlarının listesi	; ile ayırık olay adları	Hangi adımlar not olarak gitsin (açıldı, onaylandı, zamanlandı, çalıştırıldı, başarısız oldu, ITSM kontrolünde durdu)

Numara kuralları. ITSM kapalıyken de geçerlidir:

Parametre	Varsayılan	Ne işe yarar
ChangeTicketRequired	Always	Ana alan zorunlu mu: Always, ExceptEmergency, Never
EmergencyTicketRequired	Never	Acil talepte olay no zorunlu mu: Always, Never
ChangeTicketRegex	^CHG\d{7}\$	Değişiklik kaydı numarasının biçimi
RequestTicketRegex	^RITM\d{7}\$	Hizmet talebi numarasının biçimi. Boş bırakılırsa sorgu sonucu talebinde de ChangeTicketRegex uygulanır
EmergencyTicketRegex	^INC\d{7}\$	Olay numarasının biçimi

Ürün geçersiz değer kabul etmez: yanlış yazılmış bir değer, boş durum listesi ya da çalışmayan bir regex kaydedilmez. Bu parametreler kontrol parametresidir: değişiklik denetim kaydına yazılır ve talep kaydedilirken talebe dondurulan kural setine girer. Her ITSM kararının kaydı ayrıca o kararı veren kural değerlerini taşır; denetim dosyasında her kararın altında görünür.

9.7 ITSM'e yazılan not

Örnek:

SQL Change Guard #7: executed successfully. Server: SQLPROD01. By: WorkerService (started by ayse.dba), 28.09.2026 02:09 Europe/Istanbul (UTC+03:00). Risk band: Medium. Details: <https://change-guard.kurum.local/change-requests/7>

Çalıştırma sonucunu Worker yazar; çalıştırmayı başlatan kişi parantez içinde görünür (started by).

Notlar Worker'ın isteğiyle API tarafından gönderilir (Workers:ItsmPumpSeconds). ITSM'e ulaşılamazsa not kaybolmaz; ITSM düzelince sırayla gider. Notlar 15 dakikadır gönderilemiyorsa Itsm.WriteBackStalled olayı bir kez yazılır.

9.8 Kurulum sırası

1. Itsm bölümüne bağlantı yazılır, sır ortam değişkenine konur, API yeniden başlatılır.
2. Ayarlar > ITSM ekranında Bağlantıyı test et düğmesiyle gerçek bir değişiklik kaydı sorgulanır; durumun doğru yorumlandığı görülür.
3. Kurumun durum adlarına göre ItsmReadyStates, ItsmClosedStates ve gerekirse ItsmApprovedValues düzeltilir.
4. Numara biçimleri kurumun biçimine getirilir.
5. Sorgu sonucu taleplerinin neye dayandığına karar verilir (ItsmQueryResultTicketKind).
6. ItsmEnabled = true yapılır.
7. Yönetişim Kurulum Kontrolü ekranının ITSM entegrasyonu grubunda kırmızı satır kalmadığı görülür.

Itsm bölümünde sonradan yapılan her değişiklik API açılışında fark edilir ve Itsm.ConfigurationChanged olayı olarak denetim kaydına yazılır. Sır yazılmaz.

10. SIEM / SOC entegrasyonu

10.1 Nasıl çalışır

Ürün yönetim olaylarını kurumun SOC toplayıcısına syslog ile gönderir. Worker'daki gönderici varsayılan olarak on saniyede bir (Worker'ın kendi yazdığı kayıtlarda hemen) uyarır, teslim işaretinden sonraki kayıtları seçilen biçime çevirir, gönderir ve "buraya kadar gönderdim" işaretini iletir. Gönderim başarısız olursa işaret ilerlemez, bir sonraki tur aynı yerden devam eder. Denetim ve defter özeti olayları ürün tarafında kaybolmaz; gönderim en az bir kezdir, SOC tekrarı olay kimliğiyle ayıklar. UDP'de toplayıcının mesajı aldığı doğrulanamaz.

Dört akış vardır:

Akış	İçerik	Kayıp
Audit	Denetim kayıtları	Olmaz
Anchor	Defter özeti olayları (yayım, hata, geri yükleme, çatal)	Olmaz
AppLog	Ürünün kendi uyarı ve hata günlüğü	Mümkündür: bellek kuyruğu dolunca en eski kayıt düşer, sayı nabızda görünür
Heartbeat	Yaşam işareti (varsayılan 5 dakikada bir)	"Olay yok" ile "ürün durdu" ayrımı için

10.2 Bağlantı ayarları (appsettings.json, Siem bölümü)

Birden fazla uç tanımlanabilir; her uç kendi işaretini tutar.

Ayar	Değerler	Ne yazılmalı
Endpoints[].Name	Uç adı	SOC. Kurulumdan sonra değiştirilmez: değişirse uç yeni sayılır ve geçmiş olayların tamamı yeniden gönderilir
Endpoints[].Type	Syslog, File	Syslog asıl hedeftir. File her satırda bir olay yazar (toplayıcısı olmayan kurum ve kabul testi)
Endpoints[].Host, Port	Toplayıcı	siem.kurum.local, 6514
Endpoints[].Protocol	Tls (varsayılan), Tcp, Udp	Tls önerilir. UDP tek pakete sığmayan mesajı kaybeder ve kaybettiğini söylemez
Endpoints[].Format	Rfc5424Json (varsayılan), Cef, Leef, Json, Rfc5424Sd	ArcSight için Cef, QRadar için Leef, Splunk, Elastic ve Graylog için Rfc5424Json

Ayar	Değerler	Ne yazılmalı
Endpoints[].Facility	local0	Syslog tesis adı
Endpoints[].TlsServerCertThumbprint	Parmak izi ya da boş	Boşsa sistem güven zinciri kullanılır. Doluysa sunucu sertifikası bununla karşılaştırılır; tutmazsa bağlantı reddedilir, düz metne düşülmez
Endpoints[].FilePath	Dosya yolu	Yalnız Type = File
Endpoints[].BatchSize	Varsayılan 200	Bir turda en fazla kaç olay
Endpoints[].PollSeconds	Varsayılan 10	Yoklama aralığı. Worker'ın kendi yazdığı kayıtlar hemen, API'nin yazdığı kayıtlar bu aralıkta (varsayılan 10 saniye) gönderilir
Endpoints[].HeartbeatMinutes	Varsayılan 5	Nabız aralığı
AppLogQueueSize	Varsayılan 10000	Ürün günlüğü için bellek kuyruğu kapasitesi
AppLogMinLevel	Varsayılan Warning	Bu seviyenin altındaki ürün günlüğü kuyruğa girmez

Worker tarafı: Workers:SiemPumpSeconds (varsayılan 10) ve Workers:SiemLeaseSeconds (varsayılan 60, birden fazla Worker varsa aynı akışa tek yazıcı).

10.3 Davranış parametreleri (Ayarlar > Parametreler > SIEM)

Parametre	Varsayılan	Değerler	Ne işe yarar
SiemEnabled	true	true, false	Ana anahtar. Kurulumda açık gelir; appsettings içinde uç tanımlı değilse gönderim yapılamaz ve bu Yönetişim Kurulum Kontrolü ekranında görünür. Kapalı olması da aynı ekranda eksik olarak görünür
SiemStreams	Audit;Anchor;AppLog;Heartbeat	; ile ayrık	Gönderilecek akışlar. Boşsa dördü de gider
SiemMinSeverity	Notice	Info, Notice, Warning, Error, Alert	Bu eşiğin altındaki olay gönderilmez
SiemIncludeScriptText	false	true, false	Betiğin tam metni gitsin mi. Kapalıyken yalnız betiğin özeti gider; betik iş verisi içerebilir

Eşikten etkilenmeyen olaylar: SiemMinSeverity ne olursa olsun şu olaylar gider: acil müdahale (adında Emergency, Bypass ya da Override geçen olaylar), yetki reddi ve kimlik doğrulama hatası, kontrol zayıflatma (onay politikası, SQL standardı, kritik nesne, parametre, rol, sunucu, lisans, ayar değişikliği ve SIEM ayarı olayları, kullanıcı açma, silme, rol değiştirme ve oturum iptali), onay zinciri kapısının durdurduğu denemeler (ChangeRequest.ApprovalBlocked, ChangeRequest.ExecutionBlocked, Worker.SealRejected, Governance.StateMismatch ve sürüm paketi engellemesi), kanıt yazma sınırı olayları (Evidence.BoundaryBroken, Evidence.BoundaryRestored), defter özeti olayları ve nabız. Bu kural ciddiye eşik içindir; SiemStreams ile bir akış kapatılırsa o akışın olayları gitmez. Kurum kapsamı daraltabilir, ancak her daraltma SOC'a eski ayarla bir duyuru olarak gönderilir.

10.4 Olayın alanları

Olaya yalnız sınıflandırmaya yarayan alanlar girer. Betik metni (SiemIncludeScriptText kapalıyken), sonuç verisi, parola ve bağlantı dizesi girmez. Denetim kaydının içeriğinden yalnız şu alanlar taşınır: serverName, targetServer, databaseName, riskBand, riskScore, queryType, status, changeTicket, emergencyTicket, statementCount, objectCount, rowCount, maskedColumnCount, isEmergency, policyName, stepOrder, roleName, signingKeyId, mustChangePassword, reason, rejectionReason. Yürütme ve sandbox pencere olaylarında DAM eşleştirmesi için ayrıca şu alanlar gider: windowId, windowKind, windowOutcome, executionLogin, executorHost, clientAddress, observedLogin, observedDatabase, loginMismatch, targetSessionId, targetAuditSessionId, sessionApplicationName, executionStartedAt, executionFinishedAt, packageId, requestIds, sandboxId. Maskeleye kaydı olayında sunucular, maskeli ve maskesiz kolon adları, maskesizliği onaylayan, politika, maskeleye kipi ve sayılar gider; sonuç verisi gitmez. Sır görünümü değerler * olarak, 256 karakterden uzun değerler kırpılarak gider. Defter özeti olayında (Ledger.DigestPublished) şu alanlar taşınır: blockId, digestHash, digestTime, lastTransactionCommitTime, externalStore, file, envelopeSha256, signingKeyId, database. CEF biçiminde serbest alan sayısı sınırlı olduğu için ilk sırada blok numarası ve özet taşınır.

Bilgi	Rfc5424Json ve Json	Cef	Leef
Olay kimliği (AuditLogs.Id)	eventId	externalId	externalId
Akış	stream	cat	stream
Olay adı	action	Başlıktaki olay sınıfı ve adı	Başlıktaki olay kimliği
Kayıt türü	entityType	cs1 (entityType)	cat
Kayıt kimliği	entityId	cs2 (entityId)	resource
Kullanıcı	user	suser	usrName
IP adresi	src	src	src
Ciddiyet	severity	Başlıktaki ciddiye	sev

Bilgi	Rfc5424Json ve Json	Cef	Leef
Sonuç	outcome (success, failure, unknown)	outcome	outcome
Zaman (UTC)	occurredAt	rt	devTime
Yukarıdaki içerik alanları	Aynı adla	cs3 ile cs6 ve cn1 ile cn3 etiketli alanlar	Aynı adla

Ciddiyetin karşılıkları:

Ürün	Syslog	CEF ve LEEF
Alert	1 (alert)	8
Error	3 (error)	6
Warning	4 (warning)	6
Notice	5 (notice)	4
Info	6 (informational)	1

Olay kimliği (eventId) SOC'taki bir kaydı ürün içindeki denetim kaydına bağlar; aynı olay tekrar gönderilirse SOC bu kimlikle eleyebilir.

10.5 Kurulum sırası

1. Siem bölümüne toplayıcı ucu yazılır, API ve Worker yeniden başlatılır.
2. Ayarlar > Tanılama > SOC / SIEM ekranında Test mesajı gönder düğmesine basılır. Test mesajı gerçek olaylarla aynı yoldan gider ve Türkçe karakter taşır; toplayıcıda doğru görüldüğü kontrol edilir. Test, SiemEnabled kapalıyken de çalışır.
3. SiemEnabled = true yapılır.
4. Aynı ekranda son başarılı gönderim ve teslim gecikmesi izlenir.

11. Kurulum doğrulama

Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranı kurulumun doğru yapılıp yapılmadığını canlı olarak gösterir. Her satır ayarın o anki değerini beklenen değerle karşılaştırır ve ayarın nerede yapıldığını yazar. Gruplar: Görevler ayrılığı, Geri alma ve izole deneme, Talep disiplini, Kimlik ve parola (kurum dizini ve kurum hesabıyla giriş satırları dahil), Veri koruma, Denetim ve kanıt (SOC / SIEM satırları dahil), ITSM entegrasyonu, Sır yerleşimi ve Ürün dışında doğrulanacaklar. Her satırın durumu Uygun, Dikkat ya da Karar verin olarak gösterilir.

1. Ekran açılır.
2. Dikkat işaretli her satır için karar verilir: değer değiştirilir ya da neden değiştirilmediği kurum kayıtlarına yazılır.
3. Karar verin işaretli satırlarda tek bir doğru cevap yoktur; bilinçli bir seçim yeterlidir.
4. Kurulum bittiğinde ekranın görüntüsü kurulum kabul kaydına eklenebilir.

Tanılama ekranındaki diğer denemeler: Mail Testi, Zaman Damgası Testi, SOC / SIEM. Kurum dizini, kurum hesabı ve ITSM bağlantı denemeleri kendi ekranlarındaki Bağlantıyı test et düğmeleriyle yapılır.

Kısa kontrol listesi:

- ☐ API ve Worker günlüklerinde hata yok; Worker açılışta yapılandırmayı API'den aldı
- ☐ admin hesabının parolası değişti, en az bir yerel acil durum SystemManager hesabı var
- ☐ Lisans geçerli
- ☐ Sır yerleşimi grubunda her sır ortam değişkeninden geliyor
- ☐ Mail:DevMode false, deneme e-postası ulaştı
- ☐ "Kanıt tablosu defter mi" ve "Kanıt yazma sınırı" satırları yeşil
- ☐ Defter özeti klasörü tanımlı, Worker açıldıktan sonra ilk özet dosyası klasörde görüldü
- ☐ İmza anahtarı Windows sertifika deposunda
- ☐ "Onay politikaları ve roller son mühürlü durumla aynı" satırı yeşil; temel durumun yazıldığı an kurulum tutanağında
- ☐ "Production'da imzasız çalıştırma" ve "Production sunucularında sandbox" satırları yeşil (ikisi de false)
- ☐ "Production sunucularında sertifika doğrulaması" satırı yeşil ya da neden açılmadığı kurum kayıtlarında
- ☐ Kullanılan entegrasyonların Yönetişim Kurulum Kontrolü satırları yeşil

12. İşletim

12.1 Günlükler

Süreç	Dosya	Not
API	API klasöründe logs\scg-YYYYMMDD.log	Günlük döner
Worker	Worker klasöründe logs\scg-worker-YYYYMMDD.log	Günlük döner

Günlükler İngilizcedir. Uyarı ve hata seviyesindeki kayıtlar SIEM açıksa AppLog akışıyla SOC'a da gider.

12.2 Yedekleme

- Uygulama veritabanı: kurumun standart planıyla tam ve günlük (log) yedeği.
- Anahtarlar: Jwt, Security ve kanıt imzalama anahtarları kurumun sır kasasında yedeklenir. Security:ServerPasswordKey kaybolursa sunucu parolaları yeniden girilir; kanıt imzalama anahtarının açık kısmı hiçbir zaman silinmez.
- Denetim kayıtları (evidence.AuditLogs) defter tablosundadır; veritabanı motoru silmeyi ve değiştirmeyi reddeder. Aynı sunucuda yapılan bir geri yükleme msdb geri yükleme geçmişinden fark edilir ve Ledger.RestoreDetected olayı yazılır; dış özetin gerisine dönüş Ledger.ForkDetected ile görünür (12.7); geri yükleme öncesi ve sonrası ayrı özet setleriyle doğrulanır.
- Defter özeti klasörü: kurumun değiştirilemez deposudur, saklama süresi veritabanı yedeklerinden uzun tutulur.

12.3 Sürüm yükseltme

1. Yeni sürüm yeni kurulum betikleriyle gelebilir. Betik adları sürüm notunda yazar.
2. API, Worker ve web arayüzü klasörleri yenisiyle değiştirilir; appsettings.json dosyaları korunur.
3. AutoMigrate = true iken API açılışta yeni betikleri uygular. false iken DBA yeni betikleri uygular ve DbSchemaVersions.ps1 çıktısını çalıştırır; eksik betik varsa API adını söyleyip açılmaz.
4. Worker servisi yeniden başlatılır.

12.4 Anahtar değiştirme

Anahtar	Nasıl değiştirilir	Etkisi
Jwt__SigningKey	Yeni değer yazılır, API yeniden başlatılır	Açık oturumlar düşer, herkes yeniden girer. Veri kaybı olmaz

Anahtar	Nasıl değiştirilir	Etkisi
Security__ServerPasswordKey	Önce bütün sunucu parolalarının yeniden gireceği planlanır	Eski anahtarla şifrelenmiş parolalar çözülemez
Evidence imza anahtarı	Yeni çift yeni kimlikle eklenir (Keys:2; sertifika deposunda yeni sertifika ve CertificateThumbprint), Evidence:Signing:ActiveKeyId = 2 yapılır	Eski açık anahtar silinmez; geçmiş kanıt dosyaları onunla doğrulanır. Eski özel anahtar (ya da eski sertifikanın özel anahtarı) silinir
Workers__ApiKey ve WorkerApi__Key	İki tarafa aynı yeni değer yazılır, ikisi de yeniden başlatılır	Değerler farklıysa Worker çalışmaz
Ele geçirilmiş evidence imza anahtarı	Önce yeni anahtar eklenip etkin yapılır (yukarıdaki satır), sonra eski anahtarın Evidence:Signing:Keys:N:RevokedAt alanına ele geçirildiği düşünülen an yazılır	O andan sonra eski anahtarla atılmış imzalar geçersiz sayılır, öncekiler geçerli kalır. Etkin anahtar iptal edilmişse ürün imza atmaz ve Production'da çalıştırma yapılmaz. Değişiklik App.ConfigurationChanged olarak kayda geçer

12.5 Ayar dosyası değişikliğinin izi

LDAP, SSO ve ITSM bölümlerinde yapılan değişiklikler API açılışında fark edilir ve Ldap.ConfigurationChanged, Sso.ConfigurationChanged, Itsm.ConfigurationChanged olaylarıyla denetim kaydına yazılır.

Ayar dosyasının geri kalan bölümleri (oturum süreleri, hesap kilidi, parola kuralları, kanıt defteri, MFA, kanıt imzası, SIEM uçları ve diğerleri) için de aynı kural geçerlidir: API her açılışta etkin ayarların özetini çıkarır, son kayıtlarla karşılaştırır ve fark varsa App.ConfigurationChanged olayını eski ve yeni değerlerle, değişen anahtarların listesiyle birlikte yazar. Ortam değişkeniyle ezilen bir ayar da etkin değeriyle görünür. Sırların değeri yazılmaz, yalnız tanımlı olup olmadığı yazılır. Kurulumdan sonraki ilk açılış başlangıç durumunu yazar.

Değişiklik bir kontrolü gevşetiyorsa ayrıca App.ControlRelaxed olayı yazılır ve SOC'a alarm olarak gider. Gevşetme sayılan değişiklikler: Auth:MaxSessionHours, Auth:AccountLockoutMaxAttempts ve Auth:Password:ExpiryDays artarsa ya da 0 (sınırsız) yapılırsa; Auth:AccountLockoutMinutes, Auth:Password:MinLength ve Auth:Password:HistoryCount azalırsa; Auth:MfaTicketMaxAttempts, Jwt:AccessTokenMinutes, Jwt:RefreshTokenHours ve RateLimiting:PermitPerMinute artarsa; Auth:Password:RequireUppercase, Auth:Password:RequireDigit, Database:EvidenceLedger, Mfa:Enabled, Mfa:EnforceEnrollment ve Evidence:Signing:Enabled kapatılırsa; Evidence:Signing:AllowUnsignedProductionExecution ve Sandbox:AllowOnProduction açılırsa; Evidence:Timestamp:Mode On değerinden çıkarsa; Evidence:Ledger:DigestOutputPath boşaltılırsa; Evidence:Ledger:DigestIntervalMinutes ve Evidence:Ledger:BoundaryCheckMinutes artarsa. Bu olayların hepsi Yapılandırma Değişiklikleri (Configuration Changes) raporunda, kayıt tipi Configuration olarak

görünür. Ürün içindeki parametre ve eşleme değişiklikleri zaten denetim kaydına yazılır ve ayar değişikliği onayı açıksa dört göz kuralından geçer.

12.7 Defter özeti ve kanıt yazma sınırı

Worker saatte bir (Evidence:Ledger:DigestIntervalMinutes) özet turunu başlatır; API veritabanından defter özeti alır. Özet, o ana kadarki bütün defter kayıtlarını kapsayan tek bir değerdir. API özeti imzalar, Evidence:Ledger:DigestOutputPath klasörüne yazar (ledger-digest-...json ve imza açıksa aynı adlı .sig; imza açık ama anahtar kullanılamıyorsa özet dosyası yazılmaz ve Ledger.DigestFailed olayı yazılır) ve denetim kaydına Ledger.DigestPublished olayını ekler. Olay SIEM açıksa SOC'a da gider.

Bu dosyalar dış tanıktır: veritabanını yöneten biri sonradan kayıtları değiştirse bile daha önce değiştirilemez depoya yazılmış özet değişmez. Bu yüzden klasör, DBA'ların ve uygulama sunucusu yöneticilerinin silemeyeceği ve değiştiremeyeceği bir yerde olmalıdır (WORM paylaşımı, nesne kilitli depo ya da arşiv sistemi). API yalnız yeni dosya yazar, var olan dosyanın üstüne yazmaz.

Klasör tanımlı değilse özet yine denetim kaydına ve SIEM'e gider, ama hiçbir kayıt "dış özetle kapsandı" olarak görünmez.

İzleme:

- Yönetişim Kurulum Kontrolü ekranındaki "Son defter özeti" satırı, özet iki aralık boyunca gelmezse uyarır. SOC tarafında da aynı kural kurulur: Ledger.DigestPublished olayı iki aralık gelmezse olay açılır.
- Özet üretilemezse ya da klasöre yazılamazsa Ledger.DigestFailed olayı yazılır.
- Her özet turunda klasördeki son özet dosyası okunur ve veritabanının defter zinciriyle karşılaştırılır. Veritabanı o özeti gerisindeyse (eski yedeğe dönüş) ya da zincir uyuşmuyorsa (başka sunucuda geri yükleme, dosya düzeyinde değişiklik) Ledger.ForkDetected olayı yazılır ve kritik bildirim e-postası gider. Planlı bir geri yükleme varsa kaydı bu olayla eşleştirilir. Veritabanı geri yüklendiğinde msdb geri yükleme geçmişinden ayrıca Ledger.RestoreDetected yazılır.
- Sınır kontrolü bozulursa (Bölüm 3.5) Evidence.BoundaryBroken olayı yazılır, bildirim e-postası gider ve değişiklik işlemleri durur.

Dönem paketi. Ayda bir Denetim İzi ekranındaki Dönem Paketi düğmesiyle ayın paketi alınır ve iç denetime teslim edilir. Paket imza açıksa imzalıdır; dönemin bütün talepleri talep tablosu ile denetim kaydı arasında satır satır uzlaştırılmış olarak, defter özetleri ve aradaki boşluklar, sınır olayları, geri yüklemeler, Worker kesintileri, dışa aktarma günlüğü ve her talebin onay zinciri durumu içinde yer alır. Paket en çok 92 günlük dönem için alınır. Paketin teslim alındığı kurumun belge sisteminde kaydedilir.

Bağımsız doğrulama. Ayda bir, üretimde değil, veritabanı yedeğinin geri yüklendiği bir kopyada denetçi ya da iç denetim değiştirilemez depodaki özetlerle defteri doğrular (sys.sp_verify_database_ledger).

Adımlar Denetçi Kiti belgesindedir.

12.8 Sık karşılaşılan sorunlar

Belirti	Olası neden	Çözüm
API açılmıyor, günlükte bağlantı hatası	ConnectionStrings__Default yanlış ya da hesap yetkisiz	Bağlantı dizesi ve yetki kontrol edilir
API açılmıyor, eksik ya da değişmiş betik	AutoMigrate = false ve betikler uygulanmamış ya da SchemaVersions eksik	Bölüm 3.2
API açılmıyor, "The evidence store is not usable"	Veritabanı SQL Server 2022'den eski ya da kanıt tablosu defter değil	Uygulama veritabanı SQL Server 2022 ya da sonrasında kurulur
Talep kaydı ve onay "evidence write boundary is broken" hatası veriyor	Kanıt tablosuna tetikleyici eklenmiş, yazma yordamı değiştirilmiş ya da evidence şemasına nesne eklenmiş	Yönetişim Kurulum Kontrolü ekranındaki "Kanıt yazma sınırı" satırı bulgu kodunu gösterir; değişiklik geri alınır, sınır bir sonraki kontrolde düzelir
Kanıt dosyası üretilmiyor, "could not be signed" hatası	İmza açık ama anahtar okunamıyor (sertifika bulunamadı, özel anahtar okuma izni yok)	Sertifika ve izin kontrol edilir, API yeniden başlatılır
Oracle çalıştırma günlüğünde "the Oracle transaction check could not run" uyarısı	Hedef hesabı DBMS_TRANSACTION paketini çalıştırmıyor (PUBLIC yetkisi kaldırılmış)	Hedef hesaba GRANT EXECUTE ON SYS.DBMS_TRANSACTION verilir. Yetki gelene kadar çalıştırmalar sürer ama veri değişikliklerinin hata öncesinde kalıcı olup olmadığı izlenmez
Defter özeti klasörü boş	DigestOutputPath tanımsız, API hesabının yazma izni yok ya da Worker API'ye ulaşamıyor	API ve Worker günlüklerinde Ledger satırına bakılır
Tarayıcıda ekranlar açılıyor ama veri gelmiyor	AllowedOrigins içinde web adresi yok	Web adresi eklenir, API yeniden başlatılır
Sayfa yenilenince 404	URL Rewrite modülü yok	Modül kurulur
Worker başlamıyor	WorkerApi:BaseUrl yanlış ya da anahtarlar farklı	Worker günlüğü ve iki anahtar kontrol edilir
E-postalar tek kişiye gidiyor	Mail:DevMode true	false yapılır
Dizin girişi "ayar hatası" diyor	BaseDn ya da UserFilter kişiyi bulamıyor	Bağlantıyı test et ekranındaki adıma bakılır
Kurum hesabıyla giriş rol vermiyor	Eşleme değeri kimlik bilgisindeki değerle aynı değil	SsoLoginDenied kaydındaki ReceivedGroups değeri kullanılır
ITSM'de onaylı kayıt çalıştırılmıyor	Kurumun durum adı ItsmReadyStates listesinde yok ya da onay alanı boş geliyor	ITSM ekranındaki test sonucuna bakılır, liste düzeltilir
SOC'a olay gelmiyor	SiemEnabled kapalı, akış kapalı ya da bağlantı hatası	SOC / SIEM ekranındaki son hata ve teslim gecikmesi kontrol edilir

