

04. Entra App신청 가이드 (KTAUTH 시스템 가이드)

i 목차

- KTAUTH Entra ID App 정책
- Entra App 신청 서비스 플로우
- 사내통합인증관리 시스템 접속/로그인
- 신규요청 > Entra 일반앱 신청
 - 신규요청 > Entra 일반앱 신청 > 1-1
 - 신규요청 > Entra 일반앱 신청 > 1-2
 - 신규요청 > Entra 일반앱 신청 > 1-3 (중요)
 - 신규요청 > Entra 일반앱 신청 > 1-4
- 연동 서비스 > Entra 인증/수집 > 신규요청 이력
- 연동 서비스 > Entra 인증/수집 > 신규요청 이력 상세
- 연동 서비스 > Entra 인증/수집 > 연동서비스 목록
- 연동 서비스 > Entra 인증/수집 > 연동서비스 상세
- 연동 서비스 > Entra 인증/수집 > 연동서비스 상세 > 연동정보 변경신청

KTAUTH Entra ID App 정책

i KTAUTH Entra ID App정책

1. 공통정책 / 담당자정보

a. 공통정책

- Entra로 부터 인증받는 임직원 정보의 보호책임은 해당 시스템에 있습니다. 사외유출되지 않도록 주의하여 주세요.
 - Entra 인증모듈/암호화키/연동계정/테스트계정 정보는 사외 유출 및 사외오픈된 서버에 탑재 하시면 안되며, 개발 가이드의 복호화 및 사외 전달 하시면 안됩니다.
 - 보안성 검토 및 이행 준수 필요합니다.
 - 운영 전환일 전까지 연동 기능 점검은 사전 수행 하셔야 합니다. 운영 전환 당일 작업 지원 하지 않습니다.
 - Entra 인증 미사용시 App은 폐기 될 수 있습니다.
 - Entra인증은 인증 용도로만 사용하고 개인정보의 수집, 재사용 하시면 안됩니다. 개인정보의 수집, 재사용에 따른 개인정보 유출 책임은 해당서비스에 있습니다.
 - 사용자 검증, 접속 차단 정책 및 권한 통제는 개별 시스템에서 구현하셔야 합니다.
- ii. SaaS 서비스의 경우 사전수용검토 단계 과정을 위해 메일로 검토 신청
- iii. 단위서비스별 AP,BA만 신청 가능 (PO 담당자 1차승인자)
- iv. 사내 시스템 Entra SSO 인증/수집 목적에 사용되며 Azure 랜딩 존에 수용된 시스템만 신청 가능
- v. Entra ID 인증을 위해 그룹사/협력사의 경우 Entra ID P1 License 할당이 필요
 1. BPM+사내 시스템 접근권한신청 임직원 개별신청 필요

- vi. Entra app 신청시 Azure 전환 시스템/신규 서비스등 단위서비스 코드가 필수(POC포함)

- b. 담당자정보

- i. 신규/변경 검토승인 담당자 : DWP개발팀 손임식 책임
- ii. 일반 문의 담당자 : 김태형 매니저 (주.테크데이터 글로벌),
- iii. 정책 문의 담당자 : DWP개발팀 최광훈 책임, 박길훈 전임,
- iv. 연동/기술 문의 담당자 : 유현석 매니저(커넥티드), 이용각(에스큐아이), 이재득(에스큐아이)

- 2. 신규수용정책

- a. 일반 앱 (인증용, 수집용)

- i. Entra App 신청은 사내 시스템의 Entra SSO 인증 KT Azure 랜딩 존에 수용된 시스템이어야 하며 Azure 구독 발급이 완료된 이후 신청 (구독정보필수)
- ii. Entra ID SSO 인증 또는 수집목적의 Entra App신청의 경우 KTAUTH시스템에서 신청
- iii. 앱 등록신청 → 결재승인 → 앱등록 단계 → 서비스나우 권한신청 및 권한부여 → Entra ID SSO연동 모듈 개발로 진행
- iv. .단위서비스에 대한 해당 시스템의 AP, BA 담당자만 신청 가능 (단위서비스코드가 없는경우 MDM시스템에서 코드발급)
- v. 그룹사직원/협력사 직원은 Entra ID 인증을 위해 Azure P1 License 신청이 필요합니다 . (그룹사/협력사 직원 해당사용자 개별 신청)
- vi. 연동기간 무제한
 - 1. App Secret 발급은 6개월로 발급되나 SharedZone KeyVault에 수용되어 있는경우 무제한 (자동갱신처리)

- b. POC 앱

- i. 하기 정책외 일반앱 정책과 동일
- ii. 단위서비스코드 (* 신청 App과 관련된 단위서비스가 없다면 관리자에게 문의 하여 임시코드 발급 必)
- iii. 구독정보 (필수아님)
- iv. 연동기간 최대 6개월 (App Secret 만료일 최대 6개월)

- c. SaaS 앱

- i. Confluence, Slack등 또는 3rd party 솔루션에 해당
- ii. 기존대로 메일로 신청 (담당자 메일신청)

- 3. App정보 변경정책

- a. 일반앱 (인증용, 수집용)

- i. KTAUTH 시스템 보정요청에서 신청

- b. SaaS 앱 (Confluence, Slack 등) 또는 3rd party 솔루션

- i. 기존대로 메일로 신청

- ii. 담당자정보

- 1. 수신자 : DWP개발팀 손임식 책임

2. 참조자 : DWP개발팀 최광훈 책임, 박길훈 책임, 김태형 매니저 (주.테크데이터 글로벌), 이용각 대리(에스큐아이), 이재득(에스큐아이)

c. POC 앱

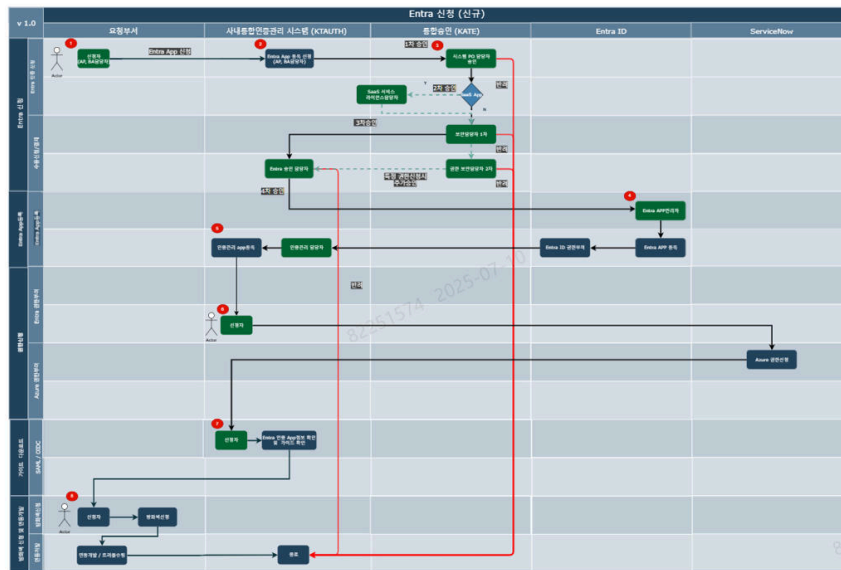
- i. 하기 정책외 일반앱 정책과 동일

ii. 연동기간연장

1. 담당자 메일 문의

- a. 수신자 : 김태형 매니저 (주.테크데이터 글로벌), 이용각 대리(에스큐아이), 이재득(에스큐아이)
- b. 참조자 : DWP개발팀 손임식 책임, 최광훈 책임, 박길훈 전임

Entra App 신청 서비스 플로우



- a. Entra ID App 등록 완료 기준으로 차주 월요일 일괄 신청되며 실제 권한부여 완료 까지 +@7일
 - b. 자동화 계획 9월~10월
7. 신청자 > Entra App정보 확인 및 가이드 확인
8. 신청자 > Entra ID 인증 모듈 연동 단계

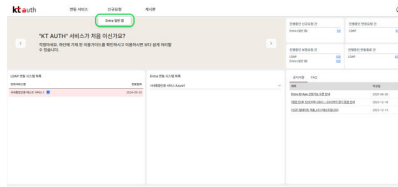
사내통합인증관리 시스템 접속/로그인



i 시스템 로그인

- 사내통합인증관리 시스템 접속 ([사내통합인증관리 시스템 바로가기](#))
- 사번 / 패스워드 입력 및 로그인 (KATE 포털 사번 및 패스워드 입력)

신규요청 > Entra 일반앱 신청



i Entra ID App 신청

- 상단 GBN 메뉴 신규요청 > Entra 일반 앱 버튼을 클릭합니다.

신규요청 > Entra 일반앱 신청 > 1-1



✔ 필독 안내사항

- Entra app 신청은 단위서비스별 AP,BA만 신청 가능합니다.
- Entra app 신청은 사내 시스템 Entra SSO 인증/수집 목적에 사용되며 Azure 랜딩 존에 수용된 시스템만 신청 가능합니다.
- 앱 등록신청 -> 결재 -> 앱 등록 단계를 걸쳐 진행되며, Entra SSO 연동 시 Azure P1 License 할당이 필요합니다. (그룹사/협력사 해당)
- 앱 등록 절차가 완료 됐다면 이후 ~~서버스나우~~ 시스템에

~~Azure RBAC 권한 신청이
필요합니다.~~

~~(<https://ktcorp.service-now.com/ktsp>)~~

- (Azure 권한은 시스템에서 자동으로 권한 요청처리)
- 안정적인 서비스 오픈을 위해 신청 시스템 사용 규모/시스템 사용자 구분에 따라 서비스 오픈전에 Azure P1 License 신청을 권고 드립니다. (그룹사/협력사 해당/사용자 개별신청) 사내망 접속 불가 협력사일 경우 KT임직원 및 그룹사 임직원이 대리 신청 필요
- Entra app 신청시 Azure 전환 시스템/신규 서비스등 단위서비스 코드가 필수입니다. (POC포함)
- POC성격의 App등록 요청의 경우 App Secret 만료기간은 6개월이며 만료후 1개월 뒤 App 자동삭제 처리됩니다. (만료전 신규 Secret 발급 신청 필요)

i Entra App 신청화면2

- Azure 시스템 구성도를 첨부합니다. (필수)

신규요청 > Entra 일반앱 신청 > 1-2

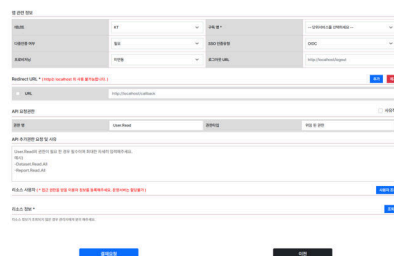
i Entra App 신청화면3

- ⚠단위서비스 정보 작성 (단위서비스정보 자동입력)
 - 표준서비스명 검색 버튼을 클릭하여 단위서비스 정보를 선택합니다. (시스템별 AP, BA만 App 신청가능).
 - 해당 시스템 담당자 기준은 ITAM 시스템 기준이며 담당자

변경 필요시 MDM 시스템에서
변경필요

- 연동정보 입력
 - 시스템 구분 > Azure 전환 시
스택 / Azure 신규 시스템 선택
 - 사용용도 > Entra 인증용 / 수
집용 선택
 - 앱 등록구분 > DEV / PRD
 - 연동방식 > Entra ID (Default)
 - 서비스등급 > (자동입력)
 - 개인정보취급여부 > 취급여부
선택
 - 연동구간 > Azure → Entra
(Default)
 - 외부망개방여부 > 사내정용
(Default)
 - 서비스 인증 대상 범위 > KT/그
룹사/협력사 선택
 - 시스템 사용자 규모 > 임직원
 - 개발언어 > 개발언어 선택
 - 언어버전 > 언어 버전 입력
 - 1일 평균 인증 건수 > 선택
 - 1일 최대 인증 건수 > 선택
 - 업무전환일자 > 예상업무전환
일자 선택
 - 연동기간 > 선택 (ShardZone
KeyVault 전환시 연동기간 무
제한)

신규요청 > Entra 일반앱 신청 > 1-3 (중요)



i Entra App 신청화면4 (중요)

- 앱 관련 정보 입력
 - 테넌트 > KT (Default)
 - **⚠ 구독명 > 단위서비스에 대한
구독을 선택**
 - ~~다중인증 여부 > 필요 (Default)-
MFA (Multi Factor
Authentication)~~ (Entra ID 정책
으로 인해 삭제 예정)
 - SSO 인증유형 > OIDC
(OpenID Connect) (Default)

- 프로비저닝 > 미연동 (Default)
- 로그아웃 URL > Logout
CallBack URL
- Redirect URL > Entra ID 인증 모듈 연동에 필요한 URL 정보 (다중입력가능).
 - http 프로토콜의 경우 "http://localhost/xxxxx" 입력가능
 - Default HTTPS
- ▲ API 요청권한
 - User.Read (Default) (Entra ID 인증시 기본사용 권한)
 - 기타 다른 권한 필요시 사유작성 체크박스 체크 후 API 추가 권한 요청 사유 작성
- ▲ API 추가권한 요청 및 사유 (단순 Entra ID인증 이라면 작성 불필요).
 - API 요청 사유 작성 (User.Read 권한 외 신청시 작성)
 - 최대한 자세히 입력이 필요하며 반려 되거나 별도 미팅 요청이 있을 수 있음
- ▲ 리소스 사용자 (Entra ID 인증시 사용) (DEV에서만 사용가능).
 - KeyVault Secret에 접근이 필요한 사용자 선택
 - AP담당자, 개발자 등
- ▲ 리소스 정보 (Entra ID 인증시 사용 필수 정보).
 - KeyVault Secret에 접근이 필요한 리소스 선택 (VM or AKS).
 - Entra ID 인증을 위한 Azure 리소스 정보를 등록 한다. **▲ 미등록시 Entra ID인증 불가**
 - i. 리소스의 경우 VM은 (SAMI), AKS의 경우 (UAMI)로 신청 요청 한다.
 - 1. ~~AP 서버가 AKS일 경우에는 서버스너우에 추가한 채 맞 설정 필요. Azure~~

권한은 시스템에서 자동으로 권한 요청처리

a. [AKS Workload Identity 활성화 \(일반AKS경우\) 가이드](#)

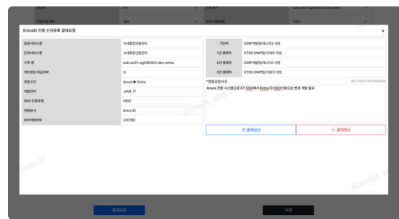
2. 통합AKS의 경우 관련 UAMI 선택

ii. Entra ID 인증에 사용되는 SharedZone KeyVault → Azure 리소스 (VM.AKS) 접근을 위한 Azure RBAC 권한은 자동화처리됨

1. 처리완료일 기준 1~2일 소요

- 결재요청 버튼 클릭

신규요청 > Entra 일반앱 신청 > 1-4



i. Entra App 신청화면5

- 신청 서비스 정보 확인
- 결재선 확인
 - 1선 결재자 > 시스템 PO 담당자 (ITAM기준)
 - 2선 결재자 > 보안담당자
 - 3선 결재자 > Entra App 담당자
- 연동요청사유 작성
 - Ex) Azure 전환 시스템으로 Entra ID SSO 인증을 위한 App 신청

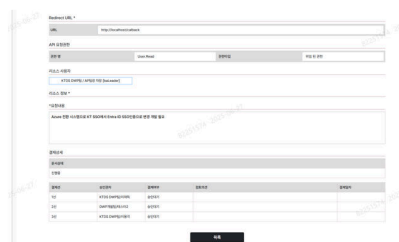
연동 서비스 > Entra 인증/수집 > 신규요청 이력



i. 신규 요청 이력

- 신청 App 정보 확인

연동 서비스 > Entra 인증/수집 > 신규요청 이력 상세



i. 신규 요청 이력 상세

- 신청 App 이력상세 확인
- ⚠ 신청 결재선 내용 확인
 - 결재선이 최종 승인 단계가 아닌지 확인 필요

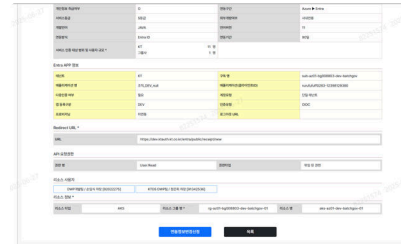
연동 서비스 > Entra 인증/수집 > 연동서비스 목록



i 연동 서비스 목록

- 신청 App 정보 확인
 - 최종 연동이 완료되면 조회 가능
 - **Entra ID 인증 모듈로 연동 개발 가능시점**

연동 서비스 > Entra 인증/수집 > 연동서비스 상세

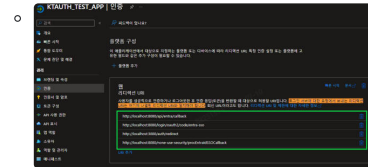


i 연동 서비스 상세 (연동정보변경 신청가능)

- 신청 App 정보 확인
 - App신청 정보 확인
- Entra App 정보
 - 테넌트 >
 - 구독명 > App 신청시 선택한 구독명
 - 애플리케이션명 > Entra ID에 등록된 실제 App Name
 - Ex) KT_DEV_XXXX, KT_PRD_XXXXX
 - 애플리케이션(클라이언트ID) > Entra ID OIDC 인증시 사용되는 애플리케이션키
 - Ex) ea8e2772-000c-4141-82b8-xxxxxxxxx
 - 다중인증 여부 > MFA 인증
 - KT테넌트 정책적용
 - 인증유형 > OIDC (표준)
 - 프로비저닝 > 계정프로비저닝 여부
 - Default 미연동
 - 로그아웃 URL > Entra ID 로그아웃 처리될때 ke 사용자 시스템이 처리되어야할 URL (사용 불가)
 - KT테넌트 정책적용 > 연동 시스템 자체만 로그아웃처리만 가능
- **Redirect URI** (로그인 서버에 대한 요청에서 보내는 리디렉션

URI는 여기에 나열된 리디렉션
URI와 일치해야 합니다 ⓘ 복수
입력 가능)

- **Entra ID OIDC 인증 연동시 사
용되는 콜백URL**



- **▲ 리소스 사용자 (Entra ID 인증
시 사용).**
 - **KeyVault Secret에 접근이 필요
한 사용자 선택 (DEV에서만 가
능).**
 - **AP담당자, 개발자 등**
- **▲ 리소스 정보 (Entra ID 인증시
사용).**
 - **KeyVault Secret에 접근이 필요
한 리소스 선택**

연동 서비스 > Entra 인증/수집 > 연동서비스 상세 > 연동정보 변경신청

- ⓘ 연동 정보 변경신청
 - Entra ID App RedirectUri 정보
 - Entra ID API 권한
 - user.read 권한외 특수 권한이
필요한 경우
 - 사유작성 체크박스 선택
 - 필요한 권한 작성 및 사유 작
성
 - KeyVault Secret 권한 할당자정보
 - **▲ 리소스 정보 (Entra ID 인증시
사용 필수 정보).**
 - **KeyVault Secret에 접근이 필요
한 리소스 선택 (VM or AKS).**
 - Entra ID 인증을 위한 Azure 리
소스 정보를 등록 한다. **▲ 미등
록시 Entra ID인증 불가**
 - 리소스는 VM은 (SAMI),
AKS의 경우 (UAMI) 로 신청
요청 한다.
 - Entra ID 인증에 사용되는
SharedZone KeyVault →

Azure 리소스 (VM.AKS) 접근을 위한 Azure RBAC 자동화 처리됨

1. 처리완료일 기준 1~2일 소요