

Oracle® Fusion Cloud EPM

액세스 제어 관리



F28937-26

ORACLE®

Oracle Fusion Cloud EPM 액세스 제어 관리NOT_SUPPORTED

F28937-26

Copyright © 2015, 2025, Oracle and/or its affiliates.

주요 작성자: EPM Information Development Team

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

목차

설명서 접근성

설명서 피드백

1 액세스 제어 개요

액세스 제어 열기	1
그룹 관리	2
EPM 그룹 생성	3
EPM 그룹 편집	4
EPM 그룹 삭제	6
Cloud EPM 그룹을 CSV 파일로 익스포트	6
파일에서 사용자의 그룹 지정 임포트	6
한 사용자를 여러 그룹에 지정	7
검색 사용	8

2 애플리케이션 레벨에서 역할 지정 관리

애플리케이션 역할 지정 개요	1
Account Reconciliation	2
Enterprise Profitability and Cost Management	4
재무 통합 및 마감	8
무형식	11
Narrative Reporting	13
Oracle Enterprise Data Management	14
Planning	14
Profitability and Cost Management,	17
Tax Reporting	18
그룹 또는 사용자에게 애플리케이션 역할 지정	21

3 보고서 생성

사용자 또는 그룹에 대한 역할 지정 보고서 생성	1
----------------------------	---

환경에 대한 역할 지정 보고서 보기	2
사용자 로그인 보고서 보기	3
사용자 그룹 보고서 보기	4

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스

지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

설명서 피드백

이 문서에 대한 피드백을 제공하려면 모든 Oracle Help Center 항목의 페이지 맨아래에 있는 [피드백] 버튼을 누릅니다. epmdoc_ww@oracle.com으로 전자메일을 보낼 수도 있습니다.

1

액세스 제어 개요

Oracle Fusion Cloud Enterprise Performance Management 및 Oracle Fusion Cloud Enterprise Data Management 환경은 여러 계층의 보호를 통해 보안 설정됩니다. 역할 기반 액세스(사전 정의된 역할)를 사용하여 권한이 부여된 사용자로 액세스가 제한됩니다. 사전 정의된 역할 지정은 [Oracle Cloud Console](#)을 사용하여 관리합니다. 예를 들어, 사용자 John Doe가 Planning 테스트 환경에 속하는 보고서를 볼 수 있도록 허용하려면 환경의 조회자 역할에 지정해야 합니다. 자세한 내용은 [관리자용 시작 가이드](#)의 사전 정의된 역할 이해를 참조하십시오.

Cloud EPM 비즈니스 프로세스 또는 Cloud EDM 사용을 보다 세부적으로 제어할 수 있도록 액세스 제어를 통해 사용자에게 추가로 애플리케이션별 역할을 지정할 수 있습니다. 예를 들어 사용자 또는 그룹을 Planning 애플리케이션의 승인 관리자 역할에 지정하면 사용자 또는 그룹이 승인 관련 활동을 수행할 수 있습니다.

중요한 점은 애플리케이션 레벨에서 역할을 지정하면 사용자의 액세스 권한만 향상된다는 것입니다. 이러한 애플리케이션별 역할은 사전 정의된 역할에 따라 부여된 권한을 취소 또는 제한할 수 없습니다.

액세스 제어를 통해 환경에서 다음 활동을 완료할 수 있습니다.

- 그룹 관리. [그룹 관리](#)를 참조하십시오.
- 사용자 관리. [한 사용자를 여러 그룹에 지정](#)을 참조하십시오.
- 애플리케이션 역할 관리. [애플리케이션 레벨에서 역할 지정 관리](#)를 참조하십시오.
- 역할 지정 보고서. 다음 항목을 참조하십시오.
 - [사용자 또는 그룹에 대한 역할 지정 보고서 생성](#)
 - [환경에 대한 역할 지정 보고서 보기](#)
- 사용자 로그인 보고서. [사용자 로그인 보고서 보기](#)를 참조하십시오.
- 사용자 그룹 보고서. [사용자 그룹 보고서 보기](#)를 참조하십시오.

Account Reconciliation용 액세스 제어는 특정 기능을 제공합니다. 자세한 내용은 [Account Reconciliation 관리](#)의 다음 항목을 참조하십시오.

- 팀 사용
- 사용자 관리
- Account Reconciliation의 고급 사용자 보안


자습서 링크

자습서 [Cloud EPM 비즈니스 프로세스에서 보안 설정](#)에 따라 Cloud EPM 비즈니스 프로세스의 보안 계층과 액세스 제어 및 액세스 권한을 사용하여 보안을 관리하는 방법에 대해 알아봅니다.

액세스 제어 열기

액세스 제어를 열려면 다음을 수행합니다.

1. 서비스 관리자 또는 접근 제어 - 애플리케이션 관리 역할이 있는 사용자로 환경에 접근합니다.
2. 다음 단계 중 하나를 완료합니다.

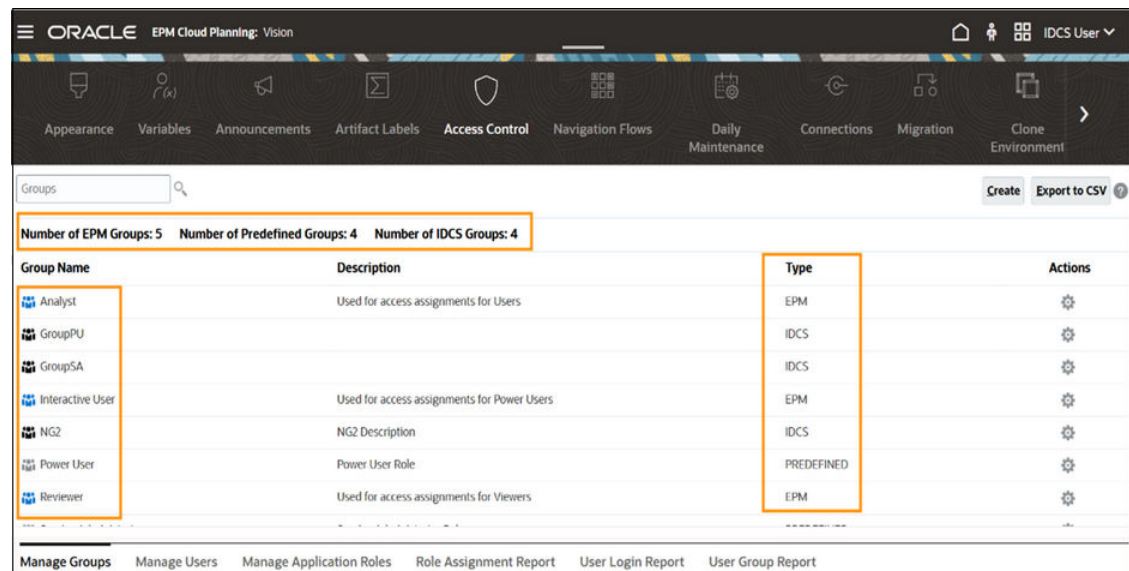
-  (네비게이터), 액세스 제어 순으로 누릅니다.
- 도구, 액세스 제어 순으로 누릅니다.
- **Narrative Reporting**만 해당: 액세스 제어를 누릅니다.

그룹 관리

Oracle Fusion Cloud Enterprise Performance Management에서는 세 가지 유형의 그룹이 인식됩니다.

- **PREDEFINED**: 이러한 그룹은 각 사전 정의된 역할에 대해 자동으로 생성됩니다. 모든 사용자는 사전 정의된 역할(예: 고급 사용자)에 따라 사전 정의된 그룹에 지정됩니다.
- **EPM**: 이러한 그룹은 액세스 제어에서 생성합니다. Identity Console에서 생성할 수 없습니다. 또한 Identity Console에 표시되지 않습니다.
- **IDCS**: 이러한 그룹은 Oracle Identity Cloud에서 생성합니다. ID 제공자(예: Okta 또는 Azure AD)와 동기화할 수 있습니다. 액세스 제어에 표시되지만 액세스 제어를 통해 생성할 수 없습니다.

그룹 관리 탭에서 그룹은 쉽게 구별하기 위해 유형 및 이미지별로 분류됩니다. 특정 그룹을 검색하려면 [검색 사용](#)의 지침을 참조하십시오.



Group Name	Description	Type	Actions
Analyst	Used for access assignments for Users	EPM	
GroupPU		IDCS	
GroupSA		IDCS	
Interactive User	Used for access assignments for Power Users	EPM	
NG2	NG2 Description	IDCS	
Power User	Power User Role	PREDEFINED	
Reviewer	Used for access assignments for Viewers	EPM	

PREDEFINED 그룹

사용자 지정을 볼 수 있도록 액세스 제어에는 PREDEFINED 그룹으로 사전 정의된 역할의 사용자가 나열됩니다.



주요 고려 사항:

- PREDEFINED 그룹은 EPM 그룹의 멤버로 지정할 수 있습니다.
- PREDEFINED 그룹은 편집할 수 없습니다. PREDEFINED 그룹을 보려면 해당 그룹에 대한 작업에서 **보기**를 선택합니다. 그룹에 지정된 모든 Cloud EPM 사용자 목록을 볼 수 있습니다.

사전 정의된 역할에 대한 자세한 내용은 [관리자용 시작 가이드](#)의 사전 정의된 역할 이해를 참조하십시오.

EPM 그룹

그룹 관리 화면에서 다음 옵션을 사용하여 EPM 그룹을 생성 및 관리할 수 있습니다.

- **생성 버튼** - 새 EPM 그룹을 생성합니다. [EPM 그룹 생성](#)를 참조하십시오.
- **CSV로 익스포트 버튼** - EPM 그룹을 CSV 파일로 익스포트합니다. [Cloud EPM 그룹을 CSV 파일로 익스포트](#)를 참조하십시오.
- **편집**  (작업) - 그룹 목록의 선택된 행에서 EPM 그룹을 편집합니다. [EPM 그룹 편집](#)을 참조하십시오.
- **삭제**  (작업) - 그룹 목록의 선택된 행에서 EPM 그룹을 삭제합니다. [EPM 그룹 삭제](#)를 참조하십시오.

주요 고려 사항:

- EPM 그룹은 더 큰 EPM 그룹의 멤버로 지정할 수 있습니다.
- 액세스 제어를 통해 파일에서 그룹 정보를 임포트하여 그룹을 생성할 수 없습니다. 마이그레이션 또는 createGroups EPM Automate 명령을 사용하여 그룹을 임포트할 수 있습니다.

IDCS 그룹

IDCS 그룹을 사용하여 여러 Cloud EPM 사용자에게 사전 정의된 역할을 지정할 수 있습니다.

*관리자용 Oracle Enterprise Performance Management Cloud 시작하기*의 IDCS 그룹을 사용하여 사용자에게 사전 정의된 역할 지정을 참조하십시오

주요 고려 사항:

- IDCS 그룹은 편집할 수 없습니다.
IDCS 그룹을 보려면 해당 그룹에 대한 작업에서 **보기**를 선택합니다. 그룹에 지정된 모든 Cloud EPM 사용자 목록을 볼 수 있습니다.
- IDCS 그룹은 애플리케이션 역할 및 EPM 그룹에 지정할 수 있습니다.

주의

IDCS 그룹이 EPM 또는 PREDEFINED 그룹과 이름을 공유하는 경우 또는 이름이 256자를 초과하는 경우 IDCS 그룹이 액세스 제어에 표시되지 않습니다. 해당 IDCS 그룹의 사용자는 로그인할 수 없게 된다는 것을 이해해야 합니다.

문제해결

*작업 가이드*의 사용자, 역할 및 그룹 관리 이슈 해결을 참조하십시오.

EPM 그룹 생성

서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 지정된 사용자는 EPM 그룹을 생성할 수 있습니다. Oracle Fusion Cloud Enterprise Performance Management 사용자와 다른 그룹은

한 그룹의 멤버일 수 있습니다. 이 옵션을 사용하여 IDCS 또는 PREDEFINED 그룹을 생성할 수는 없습니다.

① 주

마이그레이션 또는 createGroups EPM Automate 명령을 통해 파일에서 그룹 정보를 임포트하여 그룹을 생성할 수도 있습니다.

그룹을 생성하려면 다음을 수행합니다.

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 그룹 관리에서 생성을 누릅니다.
3. 그룹 생성에서 다음 단계를 완료합니다.
 - a. 이름에 고유한 그룹 이름(최대 256자)을 입력합니다. 그룹 이름에는 대/소문자가 구분되지 않습니다.
Cloud EPM에서는 IDCS 또는 PREDEFINED 그룹과 동일한 이름을 사용하여 그룹을 생성할 수 없습니다.
 - b. 선택 사항: 그룹 설명을 입력합니다.
4. 선택 사항: 그룹을 추가하여 중첩된 그룹을 생성합니다.
 - a. 사용가능한 그룹에서 그룹을 검색합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 모든 유형의 그룹이 나열됩니다. 기본적으로 이 목록은 그룹 이름 값으로 정렬됩니다.
 - b. 사용 가능한 그룹에서 새 그룹의 멤버 그룹을 선택합니다.
 - c. 이동을 누릅니다.
선택한 그룹이 지정된 그룹 아래에 나열됩니다. 지정된 그룹을 제거하려면 지정된 그룹에서 제거할 그룹을 선택하고 제거를 누릅니다.
5. 선택사항: Cloud EPM 사용자를 그룹의 멤버로 추가합니다.
사전 정의된 역할에 지정된 사용자만 그룹 멤버로 추가할 수 있습니다.
 - a. 사용자를 누릅니다.
 - b. 사용가능한 사용자에서 사용자를 검색합니다. 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 사용자가 나열됩니다. 기본적으로 이 목록은 사용자 로그인 값으로 정렬됩니다.
 - c. 사용 가능한 사용자에서 그룹에 추가할 사용자를 선택합니다.
 - d. 이동을 누릅니다.
6. 저장을 누릅니다.
7. 확인을 누릅니다.

EPM 그룹 편집

서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 지정된 사용자는 그룹 이름을 포함한 EPM 그룹 등록정보를 편집할 수 있습니다. 그룹 이름을 바꾸는 경우 그룹에 지정된 애플리케이션

역할 및 기타 보안 지정은 영향을 받지 않습니다. 이 옵션을 사용하여 IDCS 또는 PREDEFINED 그룹을 편집할 수는 없습니다.


그룹을 편집하려면:

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. **선택사항:** 그룹 관리에서 편집할 그룹을 찾습니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.

검색 기준과 일치하는 모든 유형의 그룹이 나열됩니다. 기본적으로 이 목록은 그룹 이름 값으로 정렬됩니다.

① 주

그룹 이름에는 최대 256자를 사용할 수 있습니다. 예를 들어, **사용가능한 그룹 열에** 표시되는 문자는 화면 해상도에 따라 잘릴 수 있습니다.


3. 편집할 그룹 행에서  (작업)을 누르고 **편집**을 선택합니다.
4. **선택사항:** 그룹 이름을 편집합니다. 그룹 이름을 변경해도 그룹을 사용하여 수행된 보안 지정에는 영향을 주지 않습니다. 그룹 이름을 나열된 IDCS 또는 PREDEFINED 그룹과 동일한 이름으로 바꿀 수 없습니다.
5. 그룹 지정을 편집합니다.
 - a. **선택 사항:** 중첩된 그룹을 추가합니다.
 - **사용가능한 그룹**에서 그룹을 검색합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 모든 유형의 그룹이 나열됩니다. 기본적으로 이 목록은 그룹 이름 값으로 정렬됩니다.
 - **사용 가능한 그룹**에서 그룹을 선택하고 **이동**을 누릅니다.
선택한 그룹이 **지정된 그룹** 목록에 나열됩니다.
 - b. **선택 사항:** 중첩된 그룹을 제거합니다.
 - **지정된 그룹**에서 제거할 그룹을 선택합니다.
 - **제거**를 누릅니다.
6. 사용자 지정을 편집합니다.
 - a. **사용자**를 누릅니다.
 - b. **선택 사항:** 사용자를 그룹에 추가합니다.
 - **사용가능한 사용자**에서 그룹 멤버로 지정할 수 있는 사용자를 검색합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 사용자가 나열됩니다. 기본적으로 이 목록은 사용자 로그인 값으로 정렬됩니다.
 - **사용 가능한 사용자**에서 사용자를 선택하고 **이동**을 누릅니다.
선택한 사용자가 **지정된 사용자** 목록에 나열됩니다.
 - c. **선택 사항:** 그룹에서 사용자를 제거합니다.
 - **지정된 사용자**에서 제거할 사용자를 선택합니다.
 - **제거**를 누릅니다.

7. **저장**을 누릅니다.
8. **확인**을 누릅니다.

EPM 그룹 삭제

서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 지정된 사용자는 EPM 그룹을 삭제할 수 있습니다. EPM 그룹을 삭제해도 그룹 멤버는 삭제되지 않습니다. 이 옵션을 사용하여 IAM 또는 PREDEFINED 그룹을 삭제할 수는 없습니다.

그룹을 삭제하려면 다음을 수행합니다.

1. **액세스 제어**를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. **선택사항:** **그룹 관리**에서 삭제할 그룹을 검색합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 그룹이 나열됩니다. 기본적으로 이 목록은 **그룹 이름** 값으로 정렬됩니다.
3. 삭제할 EPM 그룹 행에서  (작업)을 누르고 **삭제**를 선택합니다.
4. **예**를 눌러 삭제 작업을 확인합니다.
5. **확인**을 누릅니다.

Cloud EPM 그룹을 CSV 파일로 익스포트

서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 지정된 사용자는 **CSV로 익스포트**를 사용하여 EPM 그룹 이름과 설명을 `Groups.csv` 파일로 익스포트할 수 있습니다. PREDEFINED 또는 IDCS 그룹은 이 옵션으로 익스포트할 수 없습니다.

CSV로 익스포트는 EPM 그룹이 없는 경우 사용 안함으로 설정합니다. 이 옵션을 사용하려면 액세스 제어에 하나 이상의 EPM 그룹이 있어야 합니다.

1. **액세스 제어**를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
그룹 관리 탭에는 사용가능한 모든 그룹이 나열됩니다.
2. **CSV로 익스포트**를 눌러 모든 EPM 그룹을 익스포트합니다.
3. 화면 지침에 따라 `Groups.csv` 파일을 열거나 저장합니다.

파일에서 사용자의 그룹 지정 임포트

서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 지정된 사용자는 CSV(쉼표로 구분된 값) 파일에서 사용자의 EPM 그룹 지정을 임포트하여 기존 액세스 제어 그룹에 새 지정을 생성할 수 있습니다. Oracle Fusion Cloud Enterprise Performance Management는 새 그룹 지정에 따라 애플리케이션 레벨 및 아티팩트 레벨 보안 지정을 적용합니다.

① 주

임포트 파일에서 확인된 모든 사용자 로그인 ID 도메인에 있어야 합니다. 파일에 포함된 모든 그룹 이름이 액세스 제어에 있어야 합니다. 이 임포트 프로세스를 사용하여 그룹을 생성할 수는 없습니다.
새 그룹 지정만 생성할 수 있습니다. 사용자의 현재 그룹 지정은 제거할 수 없습니다.

임포트 CSV 파일 형식은 다음 예와 같이 표시될 수 있습니다.

```
User Login,First Name,Last Name,Email,Direct,Group
```

```
jdoe,John,Doe,jdoe@example.com,Yes,AllRole
```

이 형식은 CSV 버전의 사용자 그룹 보고서와 동일합니다. 이 형식을 사용하는 경우 импорт 프로세스는 사용자 로그인 및 그룹 이외의 모든 열을 무시합니다. импорт 파일을 쉽게 생성하는 방법은 현재 사용자 그룹 보고서를 익스포트한 다음 필요에 따라 수정하는 것입니다. [사용자 그룹 보고서 보기](#)를 참조하십시오.

사용자 그룹 지정을 임포트하려면 다음을 수행합니다.

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 사용자 그룹 보고서를 누릅니다.
3. CSV에서 임포트를 누릅니다.
4. 사용자 그룹 지정 CSV 임포트에서 **찾아보기**를 사용하여 импорт 파일을 선택합니다.
5. 임포트를 누릅니다.
6. 예를 누릅니다.


임포트 프로세스가 완료되면 처리된 지정의 총수와 상태를 확인하는 확인 대화상자가 표시됩니다.

한 사용자를 여러 그룹에 지정

Oracle Fusion Cloud Enterprise Performance Management 사용자는 액세스 제어를 사용하여 유지관리되는 여러 그룹의 멤버가 될 수 있습니다. 서비스 관리자 또는 접근 제어 - 애플리케이션 관리 역할이 있는 사용자는 사용자를 여러 그룹에 지정할 수 있습니다.

① 주

사용자는 언제든지 직접 또는 간접적으로 최대 1,000개 그룹의 멤버가 될 수 있습니다.

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 사용자 관리를 누릅니다.
3. 그룹에 지정할 사용자를 검색합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 사용자가 나열됩니다. 기본적으로 이 목록은 **사용자 로그인** 값으로 정렬됩니다.
4. 사용자 목록 행에서  (작업)을 누른 다음, **편집**을 선택합니다.
현재 그룹 멤버십(**지정된 그룹**)을 포함하여 자세한 사용자 정보가 나열된 **사용자 편집** 화면이 표시됩니다. 이 화면에서는 그룹 지정만 수정할 수 있습니다.
5. 사용자에게 지정할 그룹을 찾습니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 EPM 그룹이 나열됩니다. 기본적으로 이 목록은 **그룹 이름** 값으로 정렬됩니다.
6. 다음 작업을 완료합니다.

- 사용자에게 추가 그룹을 지정하려면 **사용가능 그룹**에서 그룹을 하나 이상 선택하고 **▶(이동)**을 눌러 선택한 그룹을 **지정된 그룹**으로 이동합니다. 또는 **▶▶(모두 이동)**을 눌러 **사용가능 그룹**의 모든 그룹을 **지정된 그룹**으로 이동합니다.
 - 사용자에게 지정된 그룹을 제거하려면 **지정된 그룹**에서 그룹을 하나 이상 선택하고 **◀(제거)**을 눌러 선택한 그룹을 **사용가능 그룹**으로 이동합니다. 또는 **◀◀(모두 제거)**을 눌러 **지정된 그룹**의 모든 그룹을 **사용가능 그룹**으로 이동합니다.
7. **저장**을 누릅니다.
 8. **확인**을 누릅니다.

검색 사용

사용자 및 그룹 아티팩트의 지능형 검색은 액세스 제어에서 동일한 방식으로 실행됩니다.

사용자 속성(사용자 이름, 이름, 성 또는 전자메일 ID) 중 하나, 그룹 이름 또는 역할 이름의 문자열을 사용하여 특정 사용자, 그룹 또는 역할을 찾습니다. 예를 들어 `st` 문자열을 사용하여 그룹을 검색하면 `st` 문자열이 포함된 모든 그룹 이름(예: `TestGroup`, `Strategic_Planner`, `AnalystsGroup` 등)이 표시됩니다. 마찬가지로, `jd` 문자열을 사용하여 사용자를 검색하면 사용자 이름, 이름, 성 또는 전자메일 주소에 `jd` 문자열이 포함된 사용자가 나열됩니다.

검색 옵션에서 와일드카드(*)를 지원하지 않습니다.

① 주

일부 액세스 제어 화면(예: **애플리케이션 역할 지정**, **역할 지정 보고서**, **사용자 그룹 보고서**)에서는 검색 선택을 제공합니다. 검색을 시작하기 전에 적절한 옵션을 선택합니다.

사용자를 검색하려면 다음을 수행합니다.

1. 사용자 검색 기능을 사용할 수 있는 화면(예: **사용자 관리**)에 액세스합니다.
2. 검색 필드에 사용자 속성(사용자 이름, 이름, 성 또는 전자메일 ID)의 부분 문자열을 입력합니다.
3. **🔍(검색)**을 누릅니다.
검색 결과에는 검색 기준과 일치하는 사용자의 사용가능한 모든 등록정보가 표시됩니다. 기본적으로 이 목록은 **사용자 로그인 값**으로 정렬됩니다.

그룹을 검색하려면 다음을 수행합니다.

- 그룹 검색 기능을 사용할 수 있는 화면(예: **그룹 관리**)에 액세스합니다.
- 검색 필드에 그룹 이름의 부분 문자열을 입력합니다.
- **🔍(검색)**을 누릅니다.
검색 결과에는 검색 기준과 일치하는 그룹의 이름 및 설명이 표시됩니다. 기본적으로 이 목록은 **그룹 이름 값**으로 정렬됩니다.

Create Group Save Close

* Name:

Description:

Groups Users

Available Users

First Name	Last Name	Email	User Login
John	Doe	john.doe@exam...	jdoe
Jane	Doe	jane.doe@exam...	jdoe31
Jane	Doe	jane.x.doe@exam.	jdoe41

Assigned Users

First Name	Last Name	Email	User Login
No records were found.			

역할 지정 보고서의 해당 역할을 기준으로 사용자를 검색하려면 다음을 수행합니다.

- 역할 지정 보고서 탭에 액세스합니다.
- 검색 드롭다운 목록에서 사용자 또는 역할을 선택합니다.
- 검색 필드에 검색 문자열을 입력합니다.
- 🔍 (검색)을 누릅니다.
 검색 결과에는 검색 기준과 일치하는 역할에 지정된 사용자의 사용가능한 모든 정보가 표시됩니다. 기본적으로 이 목록은 사용자 로그인 값으로 정렬됩니다.

2

애플리케이션 레벨에서 역할 지정 관리

액세스 제어는 다음 Oracle Fusion Cloud Enterprise Performance Management 비즈니스 프로세스에 적용됩니다.

- Account Reconciliation
- Enterprise Profitability and Cost Management
- 재무 통합 및 마감
- 무형식
- Narrative Reporting
- Oracle Fusion Cloud Enterprise Data Management
- Planning
- Profitability and Cost Management,
- Tax Reporting

애플리케이션 역할 지정 개요

액세스 제어를 사용하면 애플리케이션 레벨에서 역할을 지정하여 Oracle Fusion Cloud Enterprise Performance Management 사용자의 액세스 기능을 사전 정의된 역할 이상으로 확장할 수 있습니다. 이 역할을 애플리케이션 역할이라고 합니다. 서비스 관리자 또는 액세스 제어 - 애플리케이션 관리 역할이 있는 사용자는 액세스 제어에서 생성되고 관리되는 사용자 및 그룹에 애플리케이션별 역할 및 데이터 권한을 부여할 수 있습니다.

예를 들어, 기본적으로 서비스 관리자 및 고급 사용자만 Data Integration에 접근할 수 있습니다. 사용자 또는 조회자 사전 정의된 역할이 있는 사용자가 통합 프로세스에 참여할 수 있도록 서비스 관리자가 데이터 통합 - 애플리케이션 생성 역할을 사용자에게 지정할 수 있습니다.

① Note

애플리케이션 역할은 사용자의 액세스 권한을 강화할 수만 있습니다. 사전 정의된 역할에 따라 부여된 권한을 줄일 수는 없습니다. 사전 정의된 역할에 대한 자세한 내용은 *관리자용 시작 가이드*의 사전 정의된 역할 이해를 참조하십시오.

사용가능한 Cloud EPM 애플리케이션 역할 및 사전 정의된 역할 매핑에 대한 자세한 내용은 다음을 참조하십시오.

- [Account Reconciliation](#)
- [Enterprise Profitability and Cost Management](#)
- [재무 통합 및 마감](#)
- [FreeForm](#)
- [Narrative Reporting](#)
- [Oracle Enterprise Data Management](#)

- [Planning](#)
- [Profitability and Cost Management](#)
- [Tax Reporting](#)

① Note

온-프레미스 환경에서 Cloud EPM으로 애플리케이션을 마이그레이션하는 경우 *마이그레이션 관리*의 Cloud EPM으로 마이그레이션하기 위한 역할 매핑을 참조하십시오.

애플리케이션 역할 지정 모범 사례

권장되는 모범 사례는 적합한 최저 레벨 역할을 지정한 후 필요에 따라 추가 권한을 부여하는 것입니다. 다음은 사전 정의된 역할에 권한이 없는 사용자에게 애플리케이션 역할을 부여하는 상황에 대한 몇 가지 예입니다.

- 조정을 준비해야 하는 조회자에게 **준비자** 애플리케이션 역할을 추가합니다.
- 보고서 디자인 작업만 하고 나머지 애플리케이션 기능은 작업하지 않는 보고서 디자이너가 있습니다. 해당 사용자에게 조회자 역할을 제공하고 **보고서 관리** 애플리케이션 역할을 지정할 수 있습니다.
- **알림 유형 관리** 애플리케이션 역할을 지정할 수 있도록 고급 사용자가 알림 유형을 관리하도록 허용합니다.

① Note

권한 부여는 추가만 가능합니다. 즉, 사용자의 사전 정의된 역할이 보유한 권한에 추가할 수 있지만 사전 정의된 역할에 자동으로 부여된 권한을 제거할 수는 없습니다.

Account Reconciliation

다음 테이블에서는 Account Reconciliation 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

① Note

모든 사전 정의된 역할은 Account Reconciliation의 데이터에 대한 액세스 권한에 따라 데이터 교환 세부정보 데이터로 드릴스루할 수 있습니다.

Table 2-1 Account Reconciliation 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	액세스 제어를 사용하여 그룹 관리, 그룹 또는 사용자에게 애플리케이션 역할 지정, 사용가능 보고서 생성 및 보기를 포함한 모든 활동을 수행합니다.	서비스 관리자

Table 2-1 (Cont.) Account Reconciliation 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 보기	액세스 제어를 사용하여 역할 지정 보고서, 사용자 로그인 보고서, 그룹 지정 보고서, 사용자 그룹 보고서 등의 사용자 보안 관련 보고서를 생성하고 확인합니다. 이 역할이 지정된 사용자는 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 설정을 수정할 수 없습니다.	서비스 관리자
알림 유형 - 관리	특정 문제가 발생했을 때 따라야 할 절차를 정의하기 위해 알림 유형을 관리합니다.	서비스 관리자
공지사항 - 관리	시작 패널에서 사용자에게 표시되는 공지사항을 관리합니다. 이 패널에는 시스템 유지관리 또는 작업 실행과 같은 예정된 이벤트를 표시할 수 있습니다.	서비스 관리자
감사 - 보기	모든 감사 세부정보에 접근할 수 있습니다. 하지만 이 애플리케이션 역할은 해당 보안 범위 이외의 조정에 대한 조정 작업 대화상자를 실행할 수는 없습니다.	서비스 관리자
통화 - 관리	통화, 환율 유형 및 통화 버킷을 구성합니다. 이 역할이 있는 사용자는 시스템에서 활성화될 통화 코드를 관리할 수 있습니다.	서비스 관리자
대시보드 - 관리	사용자정의 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 준수 구성 • 추가, 편집, 복제 및 삭제 • 임포트 및 익스포트 	서비스 관리자
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> • 소스 시스템과 타겟 시스템 간 통합 • 파이프라인 활동 • EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration을 사용하여 매핑을 생성합니다. 이 역할은 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	서비스 관리자
데이터 통합 - 실행	이 역할이 지정된 사용자는 데이터 통합을 사용하여 소스와 타겟 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	서비스 관리자
데이터 로드 - 관리	Data Integration을 사용하여 데이터를 로드하고 해당 동일 데이터 로드 매개변수를 저장하기 위한 데이터 로드 정의를 지정합니다. 데이터 로드의 최신 상태를 확인하고 사용자 변경 요청 처리를 모니터링합니다.	서비스 관리자
작업 - 보기	Account Reconciliation 작업 및 작업 상태를 볼 수 있습니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
일치 유형 - 관리	일치 유형, 조정 속성, 지원 속성, 분개 열 및 그룹 속성을 관리할 수 있습니다.	서비스 관리자
일치 유형 - 보기	일치 유형, 조정 속성, 지원 속성 및 분개 열의 세부정보를 볼 수 있습니다.	서비스 관리자

Table 2-1 (Cont.) Account Reconciliation 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
마이그레이션 - 관리	애플리케이션에서 스냅샷과 아티팩트를 익스포트 및 임포트하고, 스냅샷을 마이그레이션하여 애플리케이션을 생성하고, 생성한 애플리케이션을 삭제할 수 있습니다. 이 역할이 있는 사용자는 환경을 복제할 수도 있습니다. 그러나 사용자와 역할을 복제하려면 타겟 사용자에게 ID 도메인 관리자 및 서비스 관리자 역할이 둘 다 있어야 합니다. 또한 이 역할이 있는 사용자는 일별 유지관리 시작 시간 및 시간대를 보고 조정할 수 있습니다.	서비스 관리자
조직 - 관리	프로파일 및 조정에 계층적 조직 단위 구조를 지정합니다.	서비스 관리자
기간 - 관리	기간 등록정보를 관리합니다. 기간의 상태를 설정하고, 데이터를 로드하며, 기존 기간에 대한 다른 작업을 수행할 수도 있습니다.	서비스 관리자
기간 - 보기	이 역할이 있는 사용자는 조정과 연계된 기간 수를 볼 수 있으며 (읽기 접근만 가능), 기간에 대한 데이터를 로드할 수도 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
프로파일 - 보기	이 역할이 있는 사용자는 볼 수 있는 조정에 맞춰 워크플로우가 지정된 프로파일에 액세스할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
프로파일 및 조정 - 관리	프로파일, 조정 및 속성을 관리합니다. 고급 사용자 보안 화면에서 이 역할의 보안 범위를 설정할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
공용 필터 및 보기 - 관리	필터는 목록 뷰에 표시되는 레코드와 보고서를 제어합니다. 시스템 속성, 잔액 및 잔액 세부정보를 포함하여 프로파일, 조정 또는 조정 트랜잭션 속성에 필터를 적용할 수 있습니다. 이 역할이 있는 사용자는 복잡한 필터와 논리를 생성하여 필터가 적용되는 순서를 결정할 수 있습니다.	서비스 관리자
조정 - 설명자	조정을 보고 조정이나 조정의 트랜잭션에 설명을 추가할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
조정 - 준비자	이 역할이 있는 사용자는 조정 준비, 패널 지정, 사전매핑된 데이터 임포트, 첨부파일 추가를 통해 조정 제출, 클레임 및 릴리스를 수행합니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
조정 - 검토자	이 역할이 있는 사용자는 조정을 검토하고, 패널을 지정하며, 첨부파일을 추가하여 조정을 승인, 거부, 클레임 및 릴리스할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
보고서 - 관리	조정 보고서를 표시하도록 애플리케이션 설정을 구성합니다.	서비스 관리자
팀 - 관리	이 역할이 있는 사용자는 팀을 추가, 편집 또는 삭제하고 팀원을 관리할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
사용자 - 관리	이 역할이 있는 사용자는 팀원을 관리할 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자

Enterprise Profitability and Cost Management

다음 테이블에서는 Enterprise Profitability and Cost Management 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

Table 2-2 Enterprise Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	액세스 제어를 사용하여 그룹 관리, 그룹 또는 사용자에게 애플리케이션 역할 지정, 사용가능 보고서 생성 및 보기를 포함한 모든 활동을 수행합니다.	서비스 관리자
액세스 제어 - 보기	액세스 제어를 사용하여 역할 지정 보고서, 사용자 로그인 보고서, 그룹 지정 보고서, 사용자 그룹 보고서 등의 사용자 보안 관련 보고서를 생성하고 확인합니다. 이 역할이 지정된 사용자는 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 설정을 수정할 수 없습니다.	서비스 관리자
임시 - 생성	임시 그리드를 생성, 보기, 수정 및 저장합니다.	고급 사용자
임시 - 읽기 전용 사용자	모든 임시 기능을 수행하지만, Data Management를 사용하여 임시 그리드에 쓰기 되돌림하거나 데이터를 로드할 수 없습니다.	매핑되지 않음. 각주 참조
임시 - 사용자	임시 그리드를 보거나 수정하고 임시 작업을 수행합니다. 임시 사용자는 임시 그리드를 저장할 수 없습니다.	사용자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자
공지사항 - 관리	시작 패널에서 사용자에게 표시되는 공지사항을 관리합니다. 이 패널에는 시스템 유지관리 또는 작업 실행과 같은 예정된 이벤트를 표시할 수 있습니다.	서비스 관리자
승인 - 관리	수동으로 프로세스 소유권을 확보하여 승인 이슈를 해결합니다. 승인 소유권 지정자, 승인 프로세스 디자이너 및 승인 슈퍼바이저 역할을 구성합니다. 일반적으로 이 역할은 지역의 승인 프로세스를 제어해야 하지만 서비스 관리자 역할이 필요하지 않은 지역 담당 비즈니스 사용자에게 지정됩니다. 수행할 수 있는 태스크는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 프로세스 제어 • 쓰기 액세스 권한이 있는 Planning 단위에 대한 작업 수행 • 담당할 조직의 소유자와 검토자 임명 • 보조 차원 변경 또는 검증 규칙 업데이트 	서비스 관리자
승인 - 소유권 지정	사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 소유자 지정 • 검토자 지정 • 통지할 사용자 지정 	고급 사용자
승인 - 프로세스 디자인	승인 소유권 지정자 역할을 포함합니다. 또한 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 사용자에게 쓰기 액세스 권한이 있는 엔티티의 멤버 및 보조 차원 변경 • 계획 단위 계층에 대한 버전 지정 및 시나리오 변경 • 사용자에게 액세스 권한이 있는 데이터 양식의 데이터 검증 규칙 편집 	매핑되지 않음. 각주 참조

Table 2-2 (Cont.) Enterprise Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
승인 - 감독	계획 단위를 소유하고 있지 않은 경우에도 사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. 이 사용자는 소유하고 있지 않은 계획 단위의 데이터를 변경할 수 없습니다. <ul style="list-style-type: none"> • 계획 단위 중지 및 시작 • 계획 단위에 대한 작업 수행 	고급 사용자
감사 - 관리	감사 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
감사 - 보기	감사 레코드를 볼 수 있습니다.	매핑되지 않음. 각주 참조
계산 - 실행	계산 제어 페이지에서 모델을 계산합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
계산 내역 - 삭제	계산 분석 페이지에서 완료된 계산의 선택한 인스턴스를 삭제합니다. 계산 내역을 삭제해도 데이터는 삭제되지 않습니다. 실행된 계산의 기록된 인스턴스만 삭제됩니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
계산 내역 - 보기	계산 분석 페이지에서 완료된 계산을 봅니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
대시보드 - 관리	계획 및 운영 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 설정된 권한에 따라 대시보드 추가, 편집, 복제, 삭제 • 대시보드 импорт 및 익스포트 	서비스 관리자
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> • 소스 시스템과 타겟 시스템 간 통합 • 파이프라인 활동 • EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration을 사용하여 매핑을 생성합니다. 사용자가 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	고급 사용자
Data Integration - 드릴스루	데이터의 소스 데이터로 드릴스루	<ul style="list-style-type: none"> • 고급 사용자 • 사용자
데이터 통합 - 실행	이 역할이 지정된 사용자는 데이터 통합을 사용하여 소스와 타겟 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	고급 사용자
문서 - 관리	문서를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 설정된 권한에 따라 문서 추가, 편집, 복제, 삭제 • 문서 импорт 및 익스포트 	서비스 관리자

Table 2-2 (Cont.) Enterprise Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
IPM - 관리	인사이트, 자동 예측 및 고급 예측을 비롯한 IPM(Intelligent Performance Management) 작업을 관리하고 구성합니다. 이 역할이 있는 사용자: <ul style="list-style-type: none"> • 생성한 작업만 확인, 편집 및 관리할 수 있습니다. • 다른 사용자가 생성한 작업을 보거나 관리할 수 없습니다. 	서비스 관리자
작업 - 관리	사용자에 대한 작업 상태 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
작업 - 보기	환경에 있는 모든 사용자에게 대한 작업 상태 레코드를 볼 수 있지만 고유한 작업 상태 레코드만 삭제할 수 있습니다.	매핑되지 않음. 각주 참조
모델 - 생성	모델링 페이지에서 새 모델을 생성합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
모델 - 삭제	모델링 페이지에서 모델을 삭제합니다. 모델을 삭제하면 모델의 모든 규칙도 삭제됩니다.	서비스 관리자
모델 - 보기	디자이너 페이지에서 모델 및 연계된 규칙을 봅니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자 • 조회자
모델 검증 - 실행	모델 검증 페이지에서 모델을 검증합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
POV - 생성	계산 제어 페이지에서 새 POV를 생성합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
POV - 삭제	계산 제어 페이지에서 POV를 삭제합니다. POV를 삭제하면 연계된 데이터와 해당 POV의 계산 내역 페이지도 삭제됩니다. 계산 제어 페이지에서도 POV가 제거됩니다.	서비스 관리자
POV 데이터 - 지우기	POV를 제거하지 않고 계산 제어 페이지의 POV에서 데이터를 지웁니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
POV 데이터 - 복사	계산 제어 페이지에서 POV 간에 데이터를 복사합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
POV 상태 - 편집	계산 제어 페이지의 POV 편집 대화상자에서 POV 상태를 변경합니다. 사용가능한 POV 상태는 초안, 게시됨, 아카이브됨입니다.	서비스 관리자
수익 곡선 - 생성	인텔리전스 클러스터의 수익 곡선 탭에서 수익 곡선을 생성합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
수익 곡선 - 편집	인텔리전스 클러스터의 수익 곡선 탭에서 수익 곡선을 편집합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자
수익 곡선 - 실행	인텔리전스 클러스터의 수익 곡선 탭에서 수익 곡선을 실행합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자 • 조회자

Table 2-2 (Cont.) Enterprise Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
보고서 - 관리	보고 아티팩트(보고서, 스냅샷, 장부 및 버스팅 정의)를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 권한 세트를 기반으로 보고 아티팩트 추가, 편집, 복제 및 삭제 • 보고 아티팩트 импорт 및 익스포트 	서비스 관리자
규칙 - 생성/편집	디자이너 페이지에서 할당 규칙, 사용자정의 계산 규칙 또는 규칙 세트를 생성하거나 편집합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
규칙 - 삭제	디자이너 페이지에서 할당 규칙, 사용자정의 계산 규칙 또는 규칙 세트를 삭제합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
규칙 잔액조정 - 실행	규칙 잔액조정 보고서를 보고 각 규칙의 영향을 확인합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
규칙 - 대량 편집	디자이너 페이지의 대량 편집 탭에 액세스하여 여러 규칙을 한 번에 편집합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자
추적 할당 - 실행	인텔리전스 클러스터의 추적 할당 탭에서 할당 금액을 추적합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 서비스 관리자 • 사용자 • 조회자

각주: 이 역할은 사전 정의된 역할에 매핑되지 않으며 활성화하려면 사용자 또는 그룹에 지정해야 합니다.

재무 통합 및 마감

아래 테이블에서는 다음 애플리케이션에 대한 Financial Consolidation and Close 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

표 2-3 Financial Consolidation and Close 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
임시 - 생성	임시 그리드를 생성, 보기, 수정 및 저장합니다.	고급 사용자
임시 - 읽기 전용 사용자	모든 임시 기능을 수행하지만 Data Management를 사용하여 임시 그리드에 쓰기 되돌림하거나 데이터를 로드할 수 없습니다.	매핑되지 않음. 각주 참조
임시 - 사용자	임시 그리드를 보거나 수정하고 임시 작업을 수행합니다. 임시 사용자는 임시 그리드를 저장할 수 없습니다.	사용자

표 2-3 (계속) Financial Consolidation and Close 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
공지사항 - 관리	공지사항을 구성하고 관리합니다. 이 역할이 지정된 사용자는 공지사항을 추가, 편집, 복제, 삭제할 수 있습니다.	서비스 관리자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자
승인 - 관리	수동으로 프로세스 소유권을 확보하여 승인 이슈를 해결합니다. 승인 소유권 지정자, 승인 프로세스 디자이너 및 승인 수퍼바이저 역할을 구성합니다. 일반적으로 이 역할은 지역의 승인 프로세스를 제어해야 하지만 서비스 관리자 역할이 필요하지 않은 지역 담당 비즈니스 사용자에게 지정됩니다. 수행할 수 있는 태스크는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 프로세스 제어 • 쓰기 액세스 권한이 있는 Planning 단위에 대한 작업 수행 • 담당할 조직의 소유자와 검토자 임명 • 보조 차원 변경 또는 검증 규칙 업데이트 	서비스 관리자
승인 - 소유권 지정	사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 소유자 지정 • 검토자 지정 • 통지할 사용자 지정 	고급 사용자
승인 - 프로세스 디자인	승인 소유권 지정자 역할을 포함합니다. 또한 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 사용자에게 쓰기 액세스 권한이 있는 엔티티의 멤버 및 보조 차원 변경 • 계획 단위 계층에 대한 버전 지정 및 시나리오 변경 • 사용자에게 액세스 권한이 있는 데이터 양식의 데이터 검증 규칙 편집 	매핑되지 않음. 각주 참조
승인 - 감독	계획 단위를 소유하고 있지 않은 경우에도 사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. 이 사용자는 소유하고 있지 않은 계획 단위의 데이터를 변경할 수 없습니다. <ul style="list-style-type: none"> • 계획 단위 중지 및 시작 • 계획 단위에 대한 작업 수행 	고급 사용자
감사 - 관리	감사 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
감사 - 보기	감사 레코드를 볼 수 있습니다.	매핑되지 않음. 각주 참조
연결 분개 - 승인	승인을 위해 제출된 연결 분개를 승인하거나 제출된 분개를 거부합니다.	매핑되지 않음. 각주 참조
연결 분개 - 승인 후 자동 전기	승인자가 승인한 후 연결 분개가 자동으로 전기되도록 허용합니다. 분개를 승인한 사용자는 분개를 전기한 사용자이기도 합니다.	매핑되지 않음. 각주 참조
연결 분개 - 생성	연결 분개 및 연결 분개 템플릿을 생성, 수정 및 삭제합니다.	매핑되지 않음. 각주 참조

표 2-3 (계속) Financial Consolidation and Close 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
연결 분개 - 기간 관리	연결 분개에 대한 개시 기간 또는 마감 분개 기간입니다. 해당 기간에 승인된 분개 또는 전기 취소된 자동 당기 역분개가 있는 경우 마감할 수 없습니다. 작업 또는 제출된 분개를 포함하는 기간을 마감하도록 선택하면, 기간에 게시되지 않은 분개가 있지만 기간을 마감할 수 있다는 경고 메시지가 표시됩니다.	매핑되지 않음. 각주 참조
연결 분개 - 전기	완료되었거나 제출 및 승인된 연결 분개를 전기합니다. 먼저 연결 분개가 전기되는 각 시나리오에 대한 기간을 개시해야 합니다.	매핑되지 않음. 각주 참조
연결 분개 - 제출	승인을 위해 연결 분개를 제출하거나 완료 상태의 연결 분개를 거부합니다.	매핑되지 않음. 각주 참조
연결 분개 - 전기 취소	연결 분개를 전기 취소합니다. 분개의 멤버에 대한 쓰기 액세스 권한이 있어야 합니다.	매핑되지 않음. 각주 참조
대시보드 - 관리	운영 대시보드를 포함한 모든 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 대시보드 추가, 편집, 복제 및 삭제 대시보드 임포트 및 익스포트 	<ul style="list-style-type: none"> 서비스 관리자 고급 사용자
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> 소스 시스템과 타겟 시스템 간 통합 파이프라인 활동 EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration을 사용하여 매핑을 생성합니다. 사용자가 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	고급 사용자
Data Integration - 드릴스루	데이터의 소스 데이터로 드릴스루	<ul style="list-style-type: none"> 고급 사용자 사용자
데이터 통합 - 실행	이 역할이 지정된 사용자는 데이터 통합을 사용하여 소스와 타겟 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	고급 사용자
문서 - 관리	문서를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 설정된 권한에 따라 문서 추가, 편집, 복제, 삭제 문서 임포트 및 익스포트 	서비스 관리자
IPM - 관리	인사이트, 자동 예측 및 고급 예측을 비롯한 IPM(Intelligent Performance Management) 작업을 관리하고 구성합니다. 이 역할이 있는 사용자: <ul style="list-style-type: none"> 생성한 작업만 확인, 편집 및 관리할 수 있습니다. 다른 사용자가 생성한 작업을 보거나 관리할 수 없습니다. 	서비스 관리자
작업 - 관리	사용자에 대한 작업 상태 레코드를 보고 삭제할 수 있습니다.	서비스 관리자

표 2-3 (계속) Financial Consolidation and Close 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
작업 - 보기	환경에 있는 모든 사용자에게 대한 작업 상태 레코드를 볼 수 있지만 고유한 작업 상태 레코드만 삭제할 수 있습니다.	매핑되지 않음. 각주 참조
보고서 - 관리	보고 아티팩트(보고서, 스냅샷, 장부 및 버스팅 정의)를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 권한 세트를 기반으로 보고 아티팩트 추가, 편집, 복제 및 삭제 보고 아티팩트 импорт 및 익스포트 	서비스 관리자
태스크 목록 - 접근 관리	다른 사용자에게 태스크를 지정합니다.	고급 사용자
Task Manager - 승인자	태스크 관리자에서 태스크의 승인자가 될 수 있음	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
태스크 관리자 - 아티팩트 - 관리	모든 태스크 관리자 아티팩트 관리(예: 경보, 통화, 조직)	서비스 관리자
Task Manager - 지정 대상자	태스크 관리자에서 태스크의 지정 대상자가 될 수 있음	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
태스크 관리자 - 감사 - 보기	감사 내역 정보 보기	서비스 관리자
태스크 관리자 - 사용자정의 보고서 - 관리	사용자정의 보고서를 디자인합니다.	서비스 관리자
태스크 관리자 - 운영 대시보드 - 관리	운영 대시보드를 구성합니다.	서비스 관리자
태스크 관리자 - 공용 필터 및 뷰 - 관리	모두가 액세스할 수 있도록 필터 및 뷰 게시	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
태스크 관리자 - 시스템 서비스 및 설정 - 관리	애플리케이션에 대한 시스템 서비스 및 시스템 설정 정의	서비스 관리자
태스크 관리자 - 태스크 - 관리	태스크, 템플릿, 스케줄 설계 및 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
태스크 관리자 - 사용자 및 팀 - 관리	사용자 및 팀 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자

각주: 이 역할은 사전 정의된 역할에 매핑되지 않으며 활성화하려면 사용자 또는 그룹에 지정해야 합니다.

무형식

다음 테이블에서는 FreeForm 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

Note

애플리케이션 내에서 사전 정의된 역할에 매핑되지 않은 역할은 사용자 또는 그룹에 개별적으로 지정되어야 합니다. 이렇게 지정하지 않으면 사용자가 애플리케이션 역할에 관련된 활동에 참여할 수 없습니다. 예를 들어 후속 테이블의 사전 정의된 역할과 연계되지 않은 *임시-읽기 전용 사용자* 역할은 해당 기능을 활성화하기 위해 사용자에게 명시적으로 부여되어야 합니다. 이 기능은 사전 정의된 역할에 자동으로 포함되지 않습니다.

Table 2-4 FreeForm 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
임시 - 생성	임시 그리드를 생성, 보기, 수정 및 저장합니다.	고급 사용자
임시 - 읽기 전용 사용자	모든 임시 기능을 수행하지만 Data Management 를 사용하여 임시 그리드에 쓰기 되돌림하거나 데이터를 로드할 수 없습니다.	매핑되지 않음. 각주 참조
임시 - 사용자	임시 그리드를 보거나 수정하고 임시 작업을 수행합니다. 임시 사용자는 임시 그리드를 저장할 수 없습니다.	사용자
공지사항 - 관리	공지사항을 구성하고 관리합니다. 이 역할이 지정된 사용자는 공지사항을 추가, 편집, 복제, 삭제할 수 있습니다.	서비스 관리자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자
감사 - 관리	감사 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
감사 - 보기	감사 레코드를 볼 수 있습니다.	매핑되지 않음. 각주 참조
데이터 통합 - 관리자	Data Integration 에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> 소스 시스템과 타겟 시스템 간 통합 파이프라인 활동 EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration 을 사용하여 매핑을 생성합니다. 사용자가 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	고급 사용자
Data Integration - 드릴스루	데이터의 소스 데이터로 드릴스루	<ul style="list-style-type: none"> 고급 사용자 사용자
데이터 통합 - 실행	이 역할이 지정된 사용자는 데이터 통합을 사용하여 소스와 타겟 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	고급 사용자
대시보드 - 관리	계획 및 운영 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 설정된 권한에 따라 대시보드 추가, 편집, 복제, 삭제 대시보드 импорт 및 익스포트 	서비스 관리자

Table 2-4 (Cont.) FreeForm 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
문서 - 관리	문서를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 설정된 권한에 따라 문서 추가, 편집, 복제, 삭제 • 문서 импорт 및 익스포트 	서비스 관리자
IPM - 관리	인사이트, 자동 예측 및 고급 예측을 비롯한 IPM(Intelligent Performance Management) 작업을 관리하고 구성합니다. 이 역할이 있는 사용자: <ul style="list-style-type: none"> • 생성한 작업만 확인, 편집 및 관리할 수 있습니다. • 다른 사용자가 생성한 작업을 보거나 관리할 수 없습니다. 	서비스 관리자
작업 - 관리 작업 - 보기	사용자에 대한 작업 상태 레코드를 보고 삭제할 수 있습니다. 환경에 있는 모든 사용자에게 대한 작업 상태 레코드를 볼 수 있지만 고유한 작업 상태 레코드만 삭제할 수 있습니다.	서비스 관리자 매핑되지 않음. 각주 참조
보고서 - 관리	보고 아티팩트(보고서, 스냅샷, 장부 및 버스팅 정의)를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 권한 세트를 기반으로 보고 아티팩트 추가, 편집, 복제 및 삭제 • 보고 아티팩트 импорт 및 익스포트 	서비스 관리자
태스크 목록 - 접근 관리	다른 사용자에게 태스크를 지정합니다.	고급 사용자

각주: 이 역할은 사전 정의된 역할에 매핑되지 않으며 활성화하려면 사용자 또는 그룹에 지정해야 합니다.

Narrative Reporting

다음 테이블에서는 Narrative Reporting 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

Table 2-5 Narrative Reporting 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
라이브러리 - 관리	루트 레벨 폴더를 포함한 폴더를 생성합니다.	<ul style="list-style-type: none"> • 라이브러리 관리자 • 고급 사용자 • 서비스 관리자
보고서 - 관리	보고서 패키지, 보고서, 장부, 버스팅 정의를 생성합니다.	<ul style="list-style-type: none"> • 고급 사용자 • 보고서 관리자 • 서비스 관리자

Oracle Enterprise Data Management

다음 테이블에서는 Oracle Enterprise Data Management 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

Table 2-6 Oracle Enterprise Data Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
애플리케이션 - 생성	Oracle Enterprise Data Management에 애플리케이션을 등록합니다. 애플리케이션을 등록하는 사용자에게는 애플리케이션 소유자 권한이 지정됩니다. 이 사용자는 기본 애플리케이션 뷰의 뷰 소유자로도 지정됩니다.	서비스 관리자
감사	Oracle Enterprise Data Management Cloud의 데이터에 대한 변경 요청 및 트랜잭션 내역 같은 감사 관련 정보를 봅니다.	서비스 관리자
마이그레이션 - 관리	애플리케이션에서 스냅샷과 아티팩트를 익스포트 및 임포트하고, 스냅샷을 마이그레이션하여 애플리케이션을 생성하고, 생성한 애플리케이션을 삭제할 수 있습니다. 이 역할이 있는 사용자는 환경을 복제할 수도 있습니다. 그러나 사용자와 역할을 복제하려면 타겟 사용자에게 ID 도메인 관리자 및 서비스 관리자 역할이 둘 다 있어야 합니다. 또한 이 역할이 있는 사용자는 일별 유지관리 시작 시간 및 시간대를 보고 조정할 수 있습니다.	서비스 관리자
보기 - 생성	이 역할이 지정된 사용자는 메타데이터로 작업할 뷰를 생성할 수 있습니다. 다른 사용자에게 뷰에 대한 권한을 부여할 수 있으므로 기본 소유자입니다. 뷰를 편집하거나 삭제할 권한을 보유합니다.	서비스 관리자

Planning

다음 테이블에서는 Planning 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다. Planning 애플리케이션 유형에는 사용자정의, FreeForm, Planning Modules, Predictive Cash Forecasting, Strategic Workforce Planning, Sales Planning이 포함됩니다.

Table 2-7 Planning 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자

Table 2-7 (Cont.) Planning 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
임시 - 생성	임시 그리드를 생성, 보기, 수정 및 저장합니다.	고급 사용자
임시 - 읽기 전용 사용자	모든 임시 기능을 수행하지만 Data Management를 사용하여 임시 그리드에 쓰기 되돌림하거나 데이터를 로드할 수 없습니다.	매핑되지 않음. 각주 참조
임시 - 사용자	임시 그리드를 보거나 수정하고 임시 작업을 수행합니다. 임시 사용자는 임시 그리드를 저장할 수 없습니다.	사용자
공지사항 - 관리	공지사항을 구성하고 관리합니다. 이 역할이 지정된 사용자는 공지사항을 추가, 편집, 복제, 삭제할 수 있습니다.	서비스 관리자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자
승인 - 관리	수동으로 프로세스 소유권을 확보하여 승인 이슈를 해결합니다. 승인 소유권 지정자, 승인 프로세스 디자이너 및 승인 슈퍼바이저 역할을 구성합니다. 일반적으로 이 역할은 지역의 승인 프로세스를 제어해야 하지만 서비스 관리자 역할이 필요하지 않은 지역 담당 비즈니스 사용자에게 지정됩니다. 수행할 수 있는 태스크는 다음과 같습니다. <ul style="list-style-type: none"> • 승인 프로세스 제어 • 쓰기 액세스 권한이 있는 Planning 단위에 대한 작업 수행 • 담당할 조직의 소유자와 검토자 임명 • 보조 차원 변경 또는 검증 규칙 업데이트 	서비스 관리자
승인 - 소유권 지정	사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 소유자 지정 • 검토자 지정 • 통지할 사용자 지정 	고급 사용자
승인 - 프로세스 디자인	승인 소유권 지정자 역할을 포함합니다. 또한 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> • 사용자에게 쓰기 액세스 권한이 있는 엔티티의 멤버 및 보조 차원 변경 • 계획 단위 계층에 대한 버전 지정 및 시나리오 변경 • 사용자에게 액세스 권한이 있는 데이터 양식의 데이터 검증 규칙 편집 	매핑되지 않음. 각주 참조
승인 - 감독	계획 단위를 소유하고 있지 않은 경우에도 사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. 이 사용자는 소유하고 있지 않은 계획 단위의 데이터를 변경할 수 없습니다. <ul style="list-style-type: none"> • 계획 단위 중지 및 시작 • 계획 단위에 대한 작업 수행 	고급 사용자
감사 - 관리	감사 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
감사 - 보기	감사 레코드를 볼 수 있습니다.	매핑되지 않음. 각주 참조
대시보드 - 관리	계획 및 운영 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> • 설정된 권한에 따라 대시보드 추가, 편집, 복제, 삭제 • 대시보드 импорт 및 익스포트 	서비스 관리자

Table 2-7 (Cont.) Planning 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> 소스 시스템과 타겟 시스템 간 통합 파이프라인 활동 EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration을 사용하여 매핑을 생성합니다. 사용자가 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	고급 사용자
Data Integration - 드릴스루	데이터의 소스 데이터로 드릴스루	<ul style="list-style-type: none"> 고급 사용자 사용자
데이터 통합 - 실행	Data Integration을 사용하여 소스 시스템과 타겟 시스템 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	고급 사용자
문서 - 관리	문서를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 설정된 권한에 따라 문서 추가, 편집, 복제, 삭제 문서 импорт 및 익스포트 	서비스 관리자
IPM - 관리	인사이트, 자동 예측 및 고급 예측을 비롯한 IPM(Intelligent Performance Management) 작업을 관리하고 구성합니다. 이 역할이 있는 사용자: <ul style="list-style-type: none"> 생성한 작업만 확인, 편집 및 관리할 수 있습니다. 다른 사용자가 생성한 작업을 보거나 관리할 수 없습니다. 	서비스 관리자
작업 - 관리	사용자에 대한 작업 상태 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
작업 - 보기	환경에 있는 모든 사용자에게 대한 작업 상태 레코드를 볼 수 있지만 고유한 작업 상태 레코드만 삭제할 수 있습니다.	매핑되지 않음. 각주 참조
보고서 - 관리	보고 아티팩트(보고서, 스냅샷, 장부 및 버스팅 정의)를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 권한 세트를 기반으로 보고 아티팩트 추가, 편집, 복제 및 삭제 보고 아티팩트 импорт 및 익스포트 	서비스 관리자
태스크 목록 - 접근 관리	다른 사용자에게 태스크를 지정합니다.	고급 사용자
Task Manager - 승인자	태스크 관리자에서 태스크의 승인자가 될 수 있음	<ul style="list-style-type: none"> 서비스 관리자 고급 사용자 사용자
태스크 관리자 - 아티팩트 - 관리	모든 태스크 관리자 아티팩트 관리(예: 경보, 통화, 조직)	서비스 관리자
Task Manager - 지정 대상자	태스크 관리자에서 태스크의 지정 대상자가 될 수 있음	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자

Table 2-7 (Cont.) Planning 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
태스크 관리자 - 감사 - 보기	감사 내역 정보 보기	서비스 관리자
태스크 관리자 - 사용자정의 보고서 - 관리	사용자정의 보고서를 디자인합니다.	서비스 관리자
태스크 관리자 - 운영 대시보드 - 관리	운영 대시보드를 구성합니다.	서비스 관리자
태스크 관리자 - 공용 필터 및 뷰 - 관리	모두가 액세스할 수 있도록 필터 및 뷰 게시	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
태스크 관리자 - 시스템 서비스 및 설정 - 관리	애플리케이션에 대한 시스템 서비스 및 시스템 설정 정의	서비스 관리자
태스크 관리자 - 태스크 - 관리	태스크, 템플릿, 스케줄 설계 및 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
태스크 관리자 - 사용자 및 팀 - 관리	사용자 및 팀 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
각주: 이 역할은 사전 정의된 역할에 매핑되지 않으며 활성화하려면 사용자 또는 그룹에 지정해야 합니다.		

Profitability and Cost Management,

다음 테이블에서는 Profitability and Cost Management 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

Table 2-8 Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	그룹을 관리하고, 그룹 또는 사용자에게 애플리케이션 역할을 지정하고, 사용자 보안에 대한 보고서를 생성합니다.	서비스 관리자
액세스 제어 - 보기	역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등 사용자 보안에 대한 보고서를 볼 수 있지만, 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> 소스 시스템과 타겟 시스템 간 통합 파이프라인 활동 EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자

Table 2-8 (Cont.) Profitability and Cost Management 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
마이그레이션 - 관리	애플리케이션에서 스냅샷과 아티팩트를 익스포트 및 임포트하고, 스냅샷을 마이그레이션하여 애플리케이션을 생성하고, 생성한 애플리케이션을 삭제할 수 있습니다. 이 역할이 있는 사용자는 환경을 복제할 수도 있습니다. 그러나 사용자와 역할을 복제하려면 타겟 사용자에게 ID 도메인 관리자 및 서비스 관리자 역할이 둘 다 있어야 합니다. 또한 이 역할이 있는 사용자는 일별 유지관리 시작 시간 및 시간대를 보고 조정할 수 있습니다.	서비스 관리자

Tax Reporting

다음 테이블에서는 Tax Reporting 애플리케이션 역할을 나열하고 설명하며 사전 정의된 역할과 매핑합니다.

① Note

애플리케이션 내에서 사전 정의된 역할에 매핑되지 않은 역할은 사용자 또는 그룹에 개별적으로 지정되어야 합니다. 이렇게 지정하지 않으면 사용자가 애플리케이션 역할에 관련된 활동에 참여할 수 없습니다. 예를 들어 후속 테이블의 사전 정의된 역할과 연계되지 않은 *임시 - 읽기 전용 사용자* 역할은 해당 기능을 활성화하기 위해 사용자에게 명시적으로 부여되어야 합니다. 이 기능은 사전 정의된 역할에 자동으로 포함되지 않습니다.

Table 2-9 Tax Reporting 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
액세스 제어 - 관리	액세스 제어를 사용하여 그룹 관리, 그룹 또는 사용자에게 애플리케이션 역할 지정, 사용가능 보고서 생성 및 보기를 포함한 모든 활동을 수행합니다.	서비스 관리자
액세스 제어 - 보기	액세스 제어를 사용하여 역할 지정 보고서, 사용자 로그인 보고서, 사용자 그룹 보고서 등의 사용자 보안 보고서를 봅니다. 그러나 액세스 제어에서 애플리케이션 역할을 지정하거나, 그룹을 관리하거나, 다른 업데이트 작업을 수행할 수 없습니다.	서비스 관리자
임시 - 생성	임시 그리드를 생성, 보기, 수정 및 저장합니다.	고급 사용자
임시 - 읽기 전용 사용자	모든 임시 기능을 수행하지만 Data Management를 사용하여 임시 그리드에 쓰기 되돌림하거나 데이터를 로드할 수 없습니다.	매핑되지 않음. 각주 참조
임시 - 사용자	임시 그리드를 보거나 수정하고 임시 작업을 수행합니다. 임시 사용자는 임시 그리드를 저장할 수 없습니다.	사용자
공지사항 - 관리	시작 패널에서 사용자에게 표시되는 공지사항을 관리합니다. 이 패널에는 시스템 유지관리 또는 작업 실행과 같은 예정된 이벤트를 표시할 수 있습니다.	고급 사용자
애플리케이션 - 대량 할당	양식 그리드 내에서 대량 할당 규칙을 실행합니다.	서비스 관리자

Table 2-9 (Cont.) Tax Reporting 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
승인 - 관리	수동으로 프로세스 소유권을 확보하여 승인 이슈를 해결합니다. 승인 소유권 지정자, 승인 프로세스 디자이너 및 승인 수퍼바이저 역할을 구성합니다. 일반적으로 이 역할은 지역의 승인 프로세스를 제어해야 하지만 서비스 관리자 역할이 필요하지 않은 지역 담당 비즈니스 사용자에게 지정됩니다. 수행할 수 있는 태스크는 다음과 같습니다. <ul style="list-style-type: none"> 승인 프로세스 제어 쓰기 액세스 권한이 있는 Planning 단위에 대한 작업 수행 담당할 조직의 소유자와 검토자 임명 보조 차원 변경 또는 검증 규칙 업데이트 	서비스 관리자
승인 - 소유권 지정	사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> 소유자 지정 검토자 지정 통지할 사용자 지정 	고급 사용자
승인 - 프로세스 디자인	승인 소유권 지정자 역할을 포함합니다. 또한 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. <ul style="list-style-type: none"> 사용자에게 쓰기 액세스 권한이 있는 엔티티의 멤버 및 보조 차원 변경 계획 단위 계층에 대한 버전 지정 및 시나리오 변경 사용자에게 액세스 권한이 있는 데이터 양식의 데이터 검증 규칙 편집 	매핑되지 않음. 각주 참조
승인 - 감독	계획 단위를 소유하고 있지 않은 경우에도 사용자에게 쓰기 액세스 권한이 있는 계획 단위 계층의 멤버에 대해 다음 태스크를 수행합니다. 이 사용자는 소유하고 있지 않은 계획 단위의 데이터를 변경할 수 없습니다. <ul style="list-style-type: none"> 계획 단위 중지 및 시작 계획 단위에 대한 작업 수행 	고급 사용자
감사 - 관리	감사 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
감사 - 보기	감사 레코드를 볼 수 있습니다.	매핑되지 않음. 각주 참조
대시보드 - 관리	사용자정의 대시보드를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 준수 구성 추가, 편집, 복제 및 삭제 임포트 및 익스포트 	서비스 관리자
데이터 통합 - 관리자	Data Integration에서 모든 기능 활동을 수행합니다. 이 역할이 있는 사용자는 다음을 생성, 수행 및 실행할 수 있습니다. <ul style="list-style-type: none"> 소스 시스템과 타겟 시스템 간 통합 파이프라인 활동 EPM 통합 에이전트를 사용하여 온-프레미스 소스에서 데이터와 메타데이터 추출 및 변환 	서비스 관리자
데이터 통합 - 생성	소스와 타겟 시스템 간 데이터를 통합하도록 Data Integration을 사용하여 매핑을 생성합니다. 사용자가 다양한 런타임 옵션으로 데이터 규칙을 정의할 수 있습니다.	고급 사용자

Table 2-9 (Cont.) Tax Reporting 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
Data Integration - 드릴스루	데이터의 소스 데이터로 드릴스루	<ul style="list-style-type: none"> 고급 사용자 사용자
데이터 통합 - 실행	이 역할이 지정된 사용자는 데이터 통합을 사용하여 소스와 타겟 간에 통합을 실행합니다. 사용자에게 이 역할만 지정된 경우 및 사용자가 고급 사용자 또는 서비스 관리자가 아닌 경우 사용자는 통합 세부정보를 볼 수 있지만 변경할 수는 없습니다.	고급 사용자
문서 - 관리	문서를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 문서에 대해 설정된 권한에 따라 문서 추가, 편집, 복제, 삭제 문서 импорт 및 익스포트 	서비스 관리자
IPM - 관리	인사이트, 자동 예측 및 고급 예측을 비롯한 IPM(Intelligent Performance Management) 작업을 관리하고 구성합니다. 이 역할이 있는 사용자: <ul style="list-style-type: none"> 생성한 작업만 확인, 편집 및 관리할 수 있습니다. 다른 사용자가 생성한 작업을 보거나 관리할 수 없습니다. 	서비스 관리자
작업 - 관리	사용자에 대한 작업 상태 레코드를 보고 삭제할 수 있습니다.	서비스 관리자
작업 - 보기	환경에 있는 모든 사용자에게 대한 작업 상태 레코드를 볼 수 있지만 고유한 작업 상태 레코드만 삭제할 수 있습니다.	매핑되지 않음. 각주 참조
보고서 - 관리	보고 아티팩트(보고서, 스냅샷, 장부 및 버스팅 정의)를 구성하고 관리합니다. 이 역할이 있는 사용자는 다음을 수행할 수 있습니다. <ul style="list-style-type: none"> 권한 세트를 기반으로 보고 아티팩트 추가, 편집, 복제 및 삭제 보고 아티팩트 импорт 및 익스포트 	서비스 관리자
태스크 목록 - 접근 관리	다른 사용자에게 태스크를 지정합니다.	고급 사용자
Task Manager - 승인자	Task Manager에서 태스크의 승인자가 될 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
태스크 관리자 - 아티팩트 - 관리	모든 태스크 관리자 아티팩트 관리(예: 경보, 통화, 조직)	서비스 관리자
Task Manager - 지정 대상자	Task Manager에서 태스크의 지정 대상자가 될 수 있습니다.	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자 사용자
태스크 관리자 - 감사 - 보기	감사 내역 정보 보기	서비스 관리자
태스크 관리자 - 사용자정의 보고서 - 관리	사용자정의 보고서 설계	서비스 관리자
태스크 관리자 - 운영 대시보드 - 관리	대시보드를 구성합니다.	서비스 관리자
태스크 관리자 - 공용 필터 및 뷰 - 관리	모두가 액세스할 수 있도록 필터 및 뷰 게시	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자

Table 2-9 (Cont.) Tax Reporting 애플리케이션 역할

애플리케이션 역할	설명	다음 사전 정의된 역할에 포함
태스크 관리자 - 시스템 서비스 및 설정 - 관리	애플리케이션에 대한 시스템 서비스 및 시스템 설정 정의	서비스 관리자
태스크 관리자 - 태스크 - 관리	태스크, 템플릿, 스케줄 설계 및 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
태스크 관리자 - 사용자 및 팀 관리	태스크 관리자 - 사용자 및 팀 관리	<ul style="list-style-type: none"> 고급 사용자 서비스 관리자
사용자 및 팀 - 관리	사용자 및 팀 - 관리	


각주: 이 역할은 사전 정의된 역할에 매핑되지 않으며 활성화하려면 사용자 또는 그룹에 지정해야 합니다.

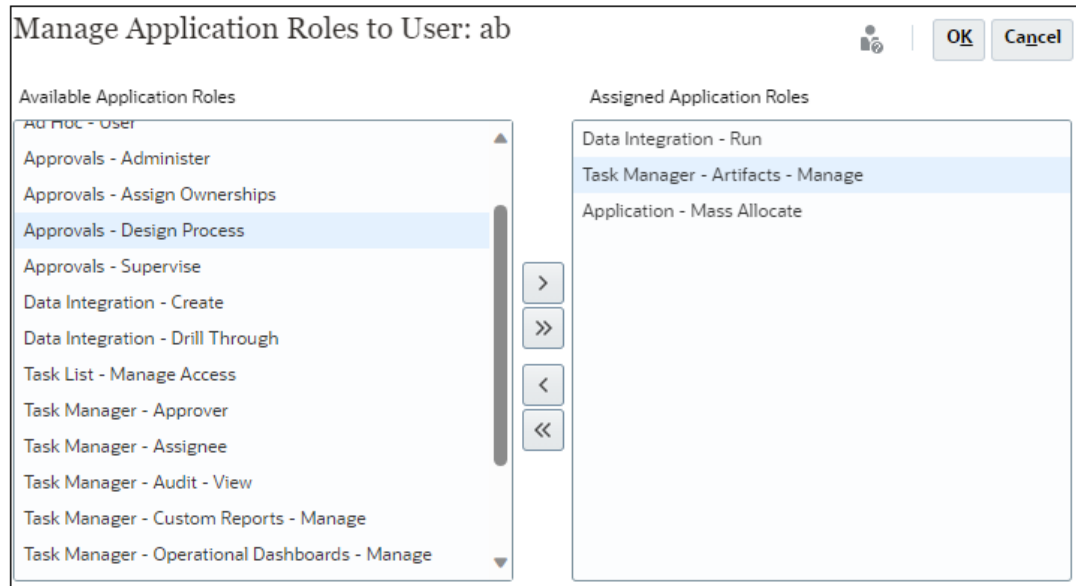
그룹 또는 사용자에게 애플리케이션 역할 지정

이 프로세스 동안 서비스 관리자 또는 액세스 제어 - 관리 애플리케이션 역할이 있는 사용자는 사전 정의된 역할이 있는 EPM 및 IDCS 그룹과 사용자에게 애플리케이션 역할을 지정하거나 지정 취소할 수 있습니다. 또한 자신에게 애플리케이션 역할을 지정할 수도 있습니다.

그룹 및 그룹에 지정된 사용자에게 대한 내용은 [그룹 관리](#)를 참조하십시오.

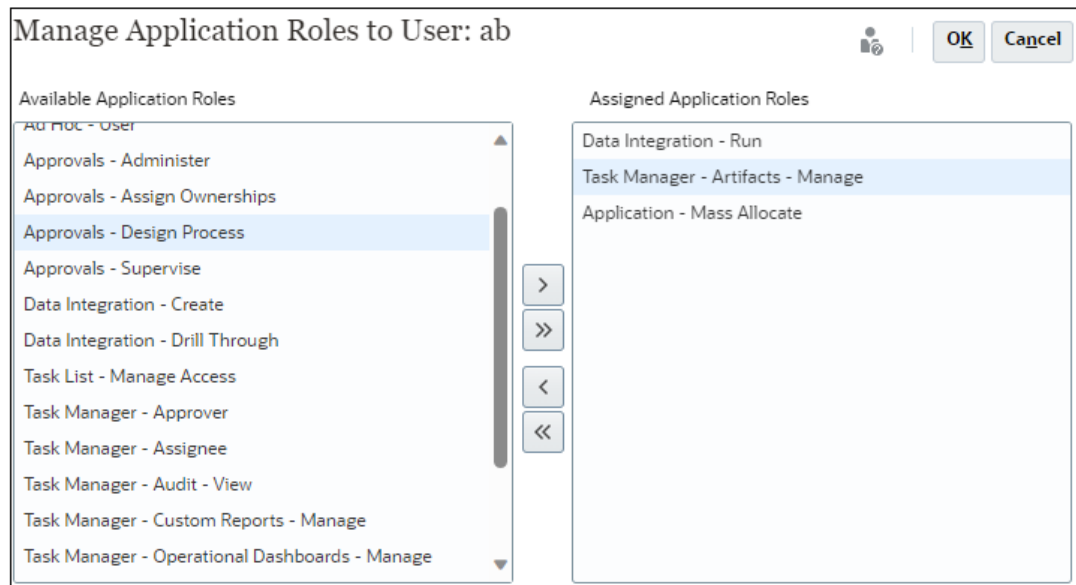
그룹 또는 사용자에게 애플리케이션 역할 지정 또는 지정 취소

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 애플리케이션 역할 관리 탭을 누릅니다.
3. 사용자 또는 그룹을 찾습니다. 드롭다운 목록에서 사용자 또는 그룹을 선택합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 사용자 또는 그룹(EPM 또는 IDCS)이 나열됩니다. 기본적으로 목록은 사용자 로그인 값으로 정렬된 후 그룹 이름 값(그룹 검색의 경우)으로 정렬됩니다.
4. 사용자 또는 그룹의  (작업)을 누르고 역할 관리를 선택합니다.
5. 사용자 또는 그룹에 애플리케이션 역할을 지정하려면 사용가능한 애플리케이션 역할 목록에서 선택한 다음 오른쪽 화살표 버튼을 누릅니다.



각 비즈니스 프로세스에 적용되는 애플리케이션 역할을 알아보려면 [애플리케이션 레벨에서 역할 지정 관리](#)를 참조하십시오.

6. 애플리케이션 역할을 지정취소하려면 **지정된 애플리케이션 역할** 목록에서 선택한 다음 왼쪽 화살표 키를 누릅니다.



7. **확인**을 클릭하여 사용자 또는 그룹에 대한 애플리케이션 역할 지정을 완료합니다.
8. **확인**을 다시 눌러 **애플리케이션 역할 관리** 탭으로 돌아갑니다.

3

보고서 생성

서비스 관리자 또는 접근 제어- 애플리케이션 관리 역할이 있는 사용자는 역할 지정을 분석하고 관리하기 위해 다음 보고서를 생성할 수 있습니다.

- [사용자 또는 그룹에 대한 역할 지정 보고서 생성](#)
- [환경에 대한 역할 지정 보고서 보기](#)
- [사용자 로그인 보고서 보기](#)
- [사용자 그룹 보고서 보기](#)

① 주

이러한 액세스 제어 보고서에는 활성 사용자만 표시됩니다. 비활성 상태이거나 IAM에서 제거된 사용자는 보고서에 나타나지 않습니다.

보고서 시간대

보고서에 표시된 보고서 생성 시간은 시스템 시계를 기반으로 하는 사용자 브라우저의 현지 시간대를 반영합니다.

보고서의 CSV 버전 정보

보고서를 익스포트하여 보고서의 CSV(쉼표로 구분된 값) 버전을 생성할 수 있습니다. 보고서의 CSV 버전에는 사전 정의된 역할에 지정된 사용자 수 외에도 다음 사항이 나열됩니다.

- 각 사용자에게 지정된 사전 정의된 역할이 나열됩니다. 사용자에게 지정된 각각의 사전 정의된 역할이 별도의 행에 표시됩니다. 사전 정의된 역할에 포함되는 애플리케이션 역할은 나열되지 않습니다.
- 직접 또는 그룹을 통해 사용자에게 지정된 애플리케이션 역할이 나열됩니다. 사용자에게 지정된 애플리케이션 역할마다 별도의 행에 표시됩니다.
- 그룹에 역할이 지정되지 않은 경우 사용자가 지정된 그룹이 표시되지 않습니다.
- 현재 보고서 뷰의 정보만 CSV로 익스포트됩니다. 예를 들어 특정 사용자에 대한 역할 지정만 표시하도록 보고서를 필터링하는 경우 익스포트된 CSV 파일에는 해당 사용자에 대한 지정만 포함됩니다.

문제해결

*작업 가이드*의 보고서 이슈 해결을 참조하십시오.


사용자 또는 그룹에 대한 역할 지정 보고서 생성

역할 지정 보고서를 사용하면 준수 보고를 위한 사용자 액세스를 추적할 수 있습니다.

이 보고서에는 사전 정의된 역할이 지정된 모든 활성 사용자가 표시됩니다. 비활성화된 사용자는 이 보고서에 반영되지 않습니다. 사용자에게 애플리케이션 역할을 지정하는 데 그룹이 사용되지 않는 경우에는 사용자가 속한 IDCS 또는 EPM 그룹이 나열되지 않습니다. 서비스 관리자 또는 액세스

제어 - 관리 애플리케이션 역할이 있는 사용자는 역할 지정 보고서에 액세스하여 사용자 또는 그룹에 지정된 사전 정의된 역할과 애플리케이션 역할을 검토할 수 있습니다.

사용자 또는 그룹에 대한 역할 지정 보고서를 생성하려면 다음을 수행합니다.

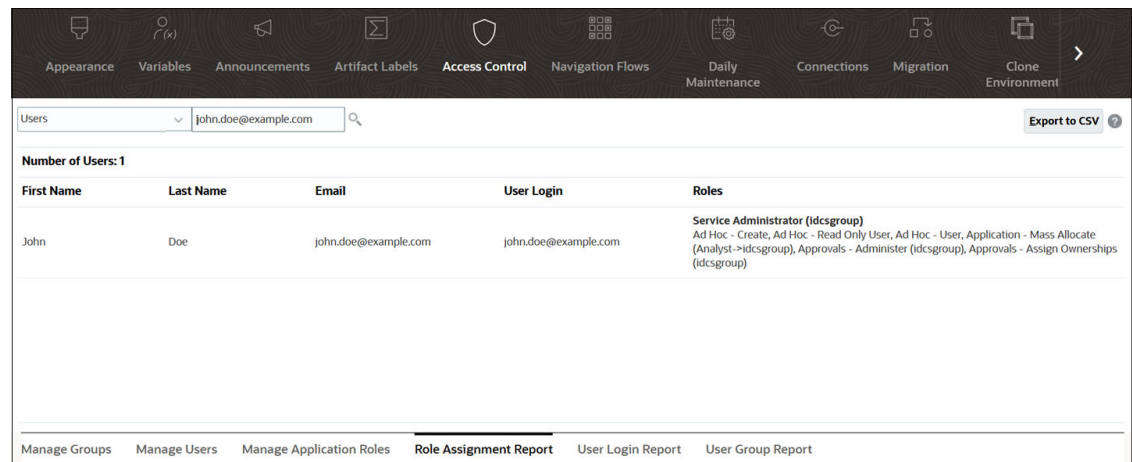
1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 애플리케이션 역할 관리 탭을 누릅니다.
3. 사용자 또는 그룹을 찾습니다. 드롭다운 목록에서 **사용자** 또는 **그룹**을 선택합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
검색 기준과 일치하는 사용자 또는 그룹이 나열됩니다. 기본적으로 보고서는 **사용자 로그인** 값으로 정렬된 후 **그룹 이름**(그룹 검색의 경우)으로 정렬됩니다.
4. 사용자 또는 그룹의  을 누른 다음 **역할 지정 보고서**를 선택합니다.
5. **선택사항: CSV로 익스포트**를 눌러 보고서를 CSV 파일로 익스포트합니다.

환경에 대한 역할 지정 보고서 보기

서비스 관리자 또는 접근 제어 - 애플리케이션 관리 역할이 있는 사용자는 역할 지정 보고서를 사용하여 모든 사용자의 사전 정의된 역할(굵게 표시됨) 및 애플리케이션 레벨 역할을 통해 지정된 접근 권한을 검토할 수 있습니다. 이 보고서에는 사전 정의된 역할이 지정된 모든 활성 사용자가 표시됩니다. 비활성화된 사용자는 이 보고서에 반영되지 않습니다.

상속된 역할과 상속에 대한 정보도 사용자마다 한 행씩 표시됩니다.

사전 정의된 역할 또는 애플리케이션 역할이 IDCS 그룹에 지정된 경우, 보고서에는 IDCS 그룹을 통해 사용자에게 간접적으로 지정된 사전 정의된 역할이 표시됩니다. 예를 들어 사용자 John Doe가 IDCS 그룹의 멤버로 지정되고 이 그룹이 서비스 관리자 사전 정의된 역할에 지정되어 있다고 가정해 보겠습니다. 이 시나리오에서는 역할 지정 보고서에 John Doe에 대한 역할 지정 정보의 일부로 다음 사항이 표시됩니다.



First Name	Last Name	Email	User Login	Roles
John	Doe	john.doe@example.com	john.doe@example.com	Service Administrator (idcsgroup) Ad Hoc - Create, Ad Hoc - Read Only User, Ad Hoc - User, Application - Mass Allocate (Analyst->idcsgroup), Approvals - Administer (idcsgroup), Approvals - Assign Ownerships (idcsgroup)

Microsoft Excel 등의 프로그램을 사용하여 열거나 컴퓨터에 저장할 수 있는 CSV 파일로 역할 지정 보고서를 익스포트할 수 있습니다. CSV 형식의 역할 지정 보고서에서는 각각의 역할 지정에 한 행을 사용합니다.

User Login	First Name	Last Name	Email	Role	Granted through Group
john.doe@example.com	John	Doe	john.doe@example.com	Service Administrator	idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - Create	
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - Read Only User	
john.doe@example.com	John	Doe	john.doe@example.com	Ad Hoc - User	
john.doe@example.com	John	Doe	john.doe@example.com	Application - Mass Allocate	Analyst->idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Approvals - Administer	idcsgroup
john.doe@example.com	John	Doe	john.doe@example.com	Approvals - Assign Ownerships	idcsgroup

역할 지정 보고서를 열려면 다음을 수행합니다.

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 역할 지정 보고서를 누릅니다.
역할 지정 보고서가 표시됩니다.
3. 선택사항: 보고서를 필터링하여 다음과 같이 표시합니다.
 - 특정 사용자에 대한 역할 지정. 드롭다운 목록에서 **사용자**를 선택하고 부분 검색 문자열을 입력합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
 - 특정 역할에 지정된 사용자. 드롭다운 목록에서 **역할**을 선택하고 부분 역할 이름을 입력합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.

① 주

사용자가 많은 역할에 지정될 수도 있습니다. 이 경우 특정 역할에 대해 보고서를 필터링해도 해당 사용자의 모든 역할이 보고서에 나열됩니다.

역할 지정 보고서가 표시됩니다. 기본적으로 보고서는 **사용자 로그인** 값으로 정렬된 후 **역할** 아래의 애플리케이션 역할(역할별 검색의 경우)로 정렬됩니다. 사전 정의된 역할은 굵은 글꼴로 표시되고 애플리케이션 역할은 보통 글꼴입니다.

4. 선택사항: **CSV로 익스포트**를 눌러 보고서를 CSV 파일로 익스포트합니다. 현재 표시된 보고서의 정보만 CSV로 익스포트됩니다.

사용자 로그인 보고서 보기

사용자 로그인 보고서에는 기본적으로 최근 24시간 동안 환경에 로그인한 사용자에 대한 정보가 포함되어 있습니다. 사용자가 로그인한 컴퓨터의 IP 주소와 사용자가 환경에 액세스한 날짜 및 시간(UTC)이 나열됩니다.

서비스 관리자 또는 액세스 제어 - 관리 애플리케이션 역할이 있는 사용자는 사용자정의 날짜 범위나 최근 30일, 최근 90일, 최근 120일에 대해 이 보고서를 재생성할 수 있습니다. 사용자 이름, 성 또는 사용자 ID의 부분 문자열을 검색 문자열로 사용하여 특정 사용자에 대한 정보만 표시하도록 보고서를 필터링할 수도 있습니다.

① 주

Oracle Fusion Cloud Enterprise Performance Management에서는 최근 120일 동안의 사용자 로그인 감사 내역만 유지관리합니다.

사용자 로그인 보고서를 재생성하려면 다음을 수행합니다.

1. 액세스 제어를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. 사용자 로그인 보고서를 누릅니다.

마지막 날 동안 환경에 로그인한 사용자가 모두 나열된 보고서가 표시됩니다.

3. 최근 1일, 최근 30일, 최근 90일 또는 최근 120일 중 보고서를 생성할 기간을 선택합니다. 사용자정의 날짜 범위를 지정하려면 **날짜 범위**를 선택하고 시작 날짜와 종료 날짜를 선택합니다.
4. **선택 사항:** 보고서에 포함시킬 사용자를 선택합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
사용자 로그인 보고서가 표시됩니다. 기본적으로 보고서는 **액세스 날짜 및 시간** 값으로 정렬됩니다.
5. **선택 사항:** **CSV로 익스포트**를 눌러 표시된 보고서를 CSV 파일로 익스포트합니다.
6. 보고서를 닫으려면 **취소**를 누릅니다.

사용자 그룹 보고서 보기

사용자 그룹 보고서에는 EPM 그룹에 지정된 사용자의 직접 또는 간접 멤버십이 나열됩니다. 서비스 관리자 또는 액세스 제어 - 관리 애플리케이션 역할이 있는 사용자는 이 보고서를 생성할 수 있습니다.

그룹에 지정된 사용자는 그룹의 직접 멤버로 간주됩니다. 다른 그룹의 1차 하위인 그룹에 지정된 사용자는 간접 멤버로 간주됩니다. 그룹에 지정된 각 사용자에 대해 로그인 ID, 이름 및 성, 전자메일 ID, 사용자가 직접 또는 간접적으로 지정된 그룹의 심표로 구분된 목록 등의 정보가 보고서에 나열됩니다. 직접 그룹은 굵은 글꼴로 표시되고 간접 그룹은 보통 글꼴입니다.

보고서의 CSV 버전에는 예 또는 아니요를 사용하여 사용자가 그룹에 직접 또는 간접적으로 지정되었는지 여부가 표시됩니다.

① 주

이 보고서는 Account Reconciliation 및 Narrative Reporting에 적용할 수 없습니다.

사용자 그룹 보고서를 생성하려면:

1. **액세스 제어**를 엽니다. [액세스 제어 열기](#)를 참조하십시오.
2. **사용자 그룹 보고서**를 누릅니다.
3. **선택 사항:** 보고서를 필터링합니다. 드롭다운 목록에서 **사용자** 또는 **그룹**을 선택합니다. 검색 기능을 사용하는 방법에 대한 지침은 [검색 사용](#)을 참조하십시오.
사용자 그룹 보고서가 표시됩니다. 기본적으로 보고서는 **사용자 로그인** 값으로 정렬됩니다.
4. 보고서를 닫으려면 **취소**를 누릅니다.
5. **선택 사항:** **CSV로 익스포트**를 눌러 EPM 그룹 이름 및 설명을 Groups.csv 파일로 익스포트합니다.
PREDEFINED 또는 IAM 그룹은 이 옵션을 사용하여 익스포트할 수 없습니다. **CSV로 익스포트**는 EPM 그룹이 없는 경우 사용 안함으로 설정됩니다. 이 옵션을 사용하려면 액세스 제어에 하나 이상의 EPM 그룹이 있어야 합니다.
6. **선택 사항:** **CSV에서 임포트**를 눌러 EPM 사용자의 그룹 지정을 CSV 파일에서 액세스 제어로 임포트합니다.
CSV 파일 형식 및 기타 세부정보에 대한 내용은 [파일에서 사용자의 그룹 지정 임포트](#)를 참조하십시오.