

# Best Practices for Deploying Access Groups

## Oracle CX Sales and B2B Service

### Evaluate Access Groups as part of your data access and security in CX Sales

Introduced in Update 20A, Access Groups are applicable for many business requirements where a user role needs additional data access to what is provided by standard roles.

Access Groups deliver better performance and greater functional consistency than customized Data Security Policies. They are also easier to maintain as your business model and user community changes over time.

Access Groups will continue to evolve via quarterly updates. So, be sure to check the quarterly [What's New documents](#) or the latest documentation to keep up to date on enhanced capabilities over time.

Here we provide our best practice guidance for deployment, using a simple checklist approach to keep things organized.

For additional assistance, where applicable, consult with your Oracle System Integration Partner.



#### Target Audience

- Business Administrator
- Application Administrator
- Project Manager
- Implementer

#### More Feature Kit Components

- [Introductory Video](#)
- [Do You Know document](#)

#### Quick Links to Resources

- [Overview of Access Groups](#)
- [Implementation & Management Series](#)
- [Verify Certification Badges](#)
- [Recommended Training for Customers](#)
- [Best Practices Resource Centers](#)
- [Security Resource Center](#)
- [My Oracle Support \(MOS\)](#)
- [Oracle Help Center](#)

#### Other Helpful Links

- [System Requirements](#)
- [Oracle University](#)
- [Oracle Partner Finder](#)

#### Connect with us

- [Customer Connect Sales Forum](#)

# Best Practices for deploying Access Groups

---

- Assess capabilities of Access Groups and match to your business requirements.
  - Review the [Access Groups chapter](#) of the Securing CX Sales and B2B Service guide.
  - Review the [Security Reference for CX Sales and B2B Service](#) and [Security Reference Spreadsheets \(Doc ID 1677508.1\)](#) to understand standard Roles and Data Security Policies.
  - **Use the standard Roles and Data Security Policies** where they fit your data access needs.
  - **Use Territory Management** for use cases where you need to
    - use forecasting or quota management functionality,
    - use territory hierarchy and territory based reporting and roll-ups that are different to the reporting resource hierarchy,
    - provide users with access based on hierarchical attributes and named accounts.
    - See the [Sales Territories and Assignment](#) chapter of the Getting Started with Your Sales Implementation guide for more about Territory Management.
  - **Use Access Groups** for data access requirements other than those supported by standard Data Security Policies or Territory Management
    - Document the data access rules for these requirements. These might be related to Sales Operations or Sales Administration functions, or any sales role that needs additional data access to what is provided by standard roles. Your business model may have its own unique requirements.
    - If new to using Access Groups, select one of your simpler requirements and work through the **implementation flow**. Start simple, prove Access Groups meet your requirement, and then expand to more complex requirements later.
    - Users need the ZCA\_MANAGE\_GROUP\_ACCESS\_PRIV privilege to create and manage access groups. By default, the Sales Administrator job role and the IT Security Manager job role have this privilege.
    - Create your Access Groups.
    - Add Members to your Groups. Doing this manually to start with will help you understand the Access Group model. Using batch processes and further automation can follow later.
      - Manually add Members to each Access Group using the UI – for simple groups with few members.
      - Import Access Groups and Access Group Members using Import Management – when administering groups with many members.
      - Create Access Group Membership Rules - for more automated Group Membership administration.
    - Create Object Sharing Rules for Access Groups.
      - Note: Many commonly used objects are already supported, including Accounts, Contacts, Opportunities, Leads, Activities and Partners. And so are Custom Objects.
      - Enable Access Group Security for your Custom Objects using the Security menu for that custom object in Application Composer.

- Run the “Run Access Group Membership Rules”, “Perform Object Sharing Rule Assignment Processing” and “Object Sharing Assignment Job Set” scheduled processes. Follow the documentation for recommended process frequency and schedules.
- Pay attention to the handling of **Functional Privileges**. Per the documentation
  - You can use access groups to give users additional permissions at the data security level. You can't use access groups to provide functional security access privileges. Consider the example of a user assigned a job role which provides the functional privilege to view leads, but not the functional privilege to delete them. If you assign the user to an access group that specifies rules that provide delete lead and view lead data access, the user will be able to view leads but without the delete functional privilege, they still won't be able to delete leads.
  - Overall data access is additive when using combinations of Data Security Policies and Access Groups. If the resulting data access is broader than you expected, you may need to remove some Data Security Policies to meet your requirement.
  - If using Workspace, verify that you can search for data made accessible via Access Groups.
- **Avoid custom Data Security Policies** whenever possible.
  - Custom Data Security Policies will not perform as well as Access Groups.
  - Workspace search will not be able to find data made accessible via custom Data Security Policies using custom predicates (SQL).
- **Review your inventory of any custom Data Security Policies** that are configured as part of your CX Sales application. If you have custom Data Security Policies, assess each to see if your business need can be addressed by Access Groups. Remember: Custom Data Security Policies using custom predicates will not apply data access when using Workspace.
  - Wherever possible, implement your requirements with Access Groups.
  - Remove custom Data Security Policies that have been replaced by use of Access Groups.
- **Monitor Release Readiness** and stay on top of future enhancements to Access Groups.
  - Use the [Cloud Application Readiness](#) page on Customer Connect for links to latest readiness material
  - Review past Customer Connect sessions that have included Access Groups
    - [Sales – 20A CX Sales Updates: CDM and Platform](#)
    - [Sales – CX Sales 20B-C Updates for CDM and Platform](#)
- As they become available via your Quarterly Updates, reassess and apply **enhancements to Access Groups** capabilities. This may include support for additional data objects and Related Object Security to secure an object using the rules of its related object.
- **Provide your feedback** – we'll be listening on the [Customer Connect Sales Forum](#) . Use the “Common: Access Groups” tag if you log and idea for enhancing Access Groups on [Ideas Lab](#).

## Essential Resources:

[Access Groups chapter](#) of the Securing CX Sales and B2B Service guide

[Security Resource Center](#)

[Security Reference for CX Sales and B2B Service](#)

[Sales – 20A CX Sales Updates: CDM and Platform](#) - Customer Connect Event (December 11, 2019 – Slides 17-20)

[Sales – CX Sales 20B-C Updates for CDM and Platform](#) - Customer Connect Event (March 20, 2020 – Slides 32-35)

## FAQS:

### When did Access Groups become available?

Update 20A – Refer to related Release Readiness and Customer Connect events for more details.

### Is Access Groups fully developed?

The 20A Update introduced a fully supported version of Access Groups, that many customers have already leveraged. There will be significant feature enhancements through the 2020 Updates to expand the capabilities of Access Groups.

## TECHNICAL ASSISTANCE:

Please contact [Oracle Support](#) if you require technical assistance.



## CONNECT WITH US

Call +1.800.ORACLE1 or visit [oracle.com](#).

Outside North America, find your local office at [oracle.com/contact](#).



Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

**Disclaimer:** This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle Corporation.

