Oracle® API Access Control

Oracle API Access Control Configuration and Administration Guide

G27060-07
July 2026

Oracle API Access Control Oracle API Access Control Configuration and Administration Guide,

G27060-07

Primary Authors: Nirmal Kumar, Doug Williams

Contributing Authors: Jean-Francois Verrier

Contributors: Ashish Aggarwal, Bholanath Bhowmick, Harsha Srikanth Karna, Harish Prabhakara, Jeffrey Wright, Krishna Chander

Contents

1

What's New in API Access Control

Oracle is constantly adding new capabilities to API Access Control service. This section provides a brief overview of new features as they are released.

- API Access Control for Autonomous AI Database Dedicated Across OCI, Multicloud, and Exadata Cloud@Customer

API Access Control for Autonomous AI Database Dedicated Across OCI, Multicloud, and Exadata Cloud@Customer

Release Date: July 28, 2026

API Access Control support has been expanded to include Autonomous AI Database Dedicated deployments on Oracle Public Cloud (OCI), Multicloud environments, and Exadata Cloud@Customer.

Previously, API Access Control was supported only for Oracle Exadata Database Service on Cloud@Customer (ExaDB-C@C) and Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D). With this enhancement, customers can now enforce consistent, fine-grained control over API access across a broader range of Autonomous and Exadata-based deployments, improving security and governance across hybrid and multicloud environments.

Related Topics

- Database Control Plane APIs to Be Protected
  You can use database control plane APIs to perform database and VM administration tasks.
- Update API Attribute Groups
  Some update operations in the OCI Console send related API attributes together in a single request. If any attribute in the request is protected by API Access Control, approval is required for all protected attributes included in that request, even if you modify only one attribute.
- Create Privileged API Control
  To create a Privileged API Control using the Oracle Cloud Console, use this procedure.
- About Resource-Types and Oracle API Access Control
  Learn about resource-types you can use in your policies.

2

Overview of Oracle API Access Control

Learn how to classify and control access to critical OCI REST APIs

- What is Oracle API Access Control?
  Oracle API Access Control enables customers to manage access to the REST APIs exposed by various database cloud services.
- Database Control Plane APIs to Be Protected
  You can use database control plane APIs to perform database and VM administration tasks.
- Update API Attribute Groups
  Some update operations in the OCI Console send related API attributes together in a single request. If any attribute in the request is protected by API Access Control, approval is required for all protected attributes included in that request, even if you modify only one attribute.

What is Oracle API Access Control?

Oracle API Access Control enables customers to manage access to the REST APIs exposed by various database cloud services.

By designating specific APIs as privileged, customers can ensure that invoking these APIs requires prior approval from an authorized group within their tenancy.

How it Works

- Mark APIs as Privileged: Identify critical APIs that could impact data integrity or service availability.
- Approval Workflow: Before a privileged API is invoked, the user intending to invoke the API must raise an Access Request with their OCI identity, and a different OCI identity that is authorized to approve Access Requests for the resource must approve the Access Request.
- Enhanced Security: This workflow helps to prevent unauthorized or accidental execution of sensitive actions, such as modifying or deleting databases, Grid Infrastructure, virtual machines, or network resources.
  The workflow requires different identities to ask for access and approve access, including the cloud administrator account.

Key Benefits:

- Reduced Risk: Minimize accidental or malicious deletions of mission-critical database services.
- Separation of Duties: Ensure that API execution is distinct from approval, enhancing security and accountability.

Oracle API Access Control strengthens the security of OCI database cloud services by adding an extra authorization layer for critical operations. When enabled on Cloud Exadata Infrastructure, it extends protection to its associated Cloud VM Clusters and Container Databases.

Key functionalities:

1. Enable Privileged API Protection: Customer Administrators can enable Oracle API Access Control for resources exposed by database cloud services.
2. Designate Privileged APIs: Administrators can classify specific APIs as privileged, ensuring controlled access.
3. Fine-Grained IAM Policies for Privileged API:
   - Define which groups can approve API Access Requests.
   - Grant separate permissions for creating and approving API Access Requests.
4. Request and Approval Management:
   - Administrators or designated groups can approve or reject API Access Requests.
   - Users must submit detailed justifications for API access.
   - Users can extend or close approved requests as needed.
5. Approval Workflow Management:
   - Manage workflows for approvals, including handling expiring or pending workflows.
   - Send periodic reminders to approvers to act on pending requests that are left unattended.

Database Control Plane APIs to Be Protected

You can use database control plane APIs to perform database and VM administration tasks.

The following Database Cloud Service APIs will be secured under API Access Control protection. These APIs require prior approval before being invoked to ensure enhanced security and controlled access.

Exadata Database Service on Cloud@Customer

Backup APIs

- CreateBackup

DB Home APIs

- UpdateDbHome
- CreateDatabase
- DeleteDbHome

Database APIs

- DeleteDatabase
- UpdateDataGuard
- SwitchOverDataGuard
- ReinstateDataGuard
- FailoverDataGuard
- CreatePluggableDatabase
- UpgradeDatabase
- UpdateDatabase

- RotateVaultKey
- RestoreDatabase
- MigrateVaultKey

Exadata Infrastructure APIs

- DeleteExadataInfrastructure
- UpdateExadataInfrastructure
- ChangeExadataInfrastructureCompartment
- AddStorageCapacityExadataInfrastructure
- GenerateRecommendedVmClusterNetwork
- CreateVmCluster
- CreateAutonomousVmCluster
- CreateVmClusterNetwork

Pluggable Database APIs

- DeletePluggableDatabase
- ConvertToRegularPluggableDatabase
- UpdatePluggableDatabase
- StartPluggableDatabase
- RefreshPluggableDatabase
- StopPluggableDatabase

VM Cluster APIs

- DeleteVmCluster
- RemoveVirtualMachineFromVmCluster
- CreateDbHome
- ChangeVmClusterCompartment
- AddVirtualMachineToVmCluster
- UpdateVmCluster

VM Cluster Network APIs

- DeleteVmClusterNetwork
- ValidateVmClusterNetwork
- UpdateVmClusterNetwork
- ResizeVmClusterNetwork

Virtual Machine APIs / DB Node APIs

- CreateConsoleConnection
- DbNodeAction

Exadata Database Service on Dedicated Infrastructure

Backup APIs

- CreateBackup

DB Home APIs

- UpdateDbHome
- CreateDatabase
- DeleteDbHome

Database APIs

- DeleteDatabase
- UpdateDataGuard
- SwitchOverDataGuard
- ReinstateDataGuard
- FailoverDataGuard
- CreatePluggableDatabase
- UpgradeDatabase
- UpdateDatabase
- RotateVaultKey
- RestoreDatabase
- EnableDatabaseManagement
- DisableDatabaseManagement
- ModifyDatabaseManagement

Cloud Exadata Infrastructure APIs

- DeleteCloudExadataInfrastructure
- UpdateCloudExadataInfrastructure
- ChangeCloudExadataInfrastructureCompartment
- AddStorageCapacityCloudExadataInfrastructure
- CreateCloudVmCluster
- CreateCloudAutonomousVmCluster

Pluggable Database APIs

- DeletePluggableDatabase
- ConvertToRegularPluggableDatabase
- UpdatePluggableDatabase
- StartPluggableDatabase
- RefreshPluggableDatabase
- StopPluggableDatabase

Cloud VM Cluster APIs

- DeleteCloudVmCluster
- RemoveVirtualMachineFromVmCluster
- CreateDbHome

- ChangeCloudVmClusterCompartment
- AddVirtualMachineToVmCluster
- UpdateCloudVmCluster

Virtual Machine APIs / DB Node APIs

- DbNodeAction

Autonomous AI Database on Cloud@Customer

Autonomous VM Cluster APIs

- CreateAutonomousContainerDatabase
- DeleteAutonomousVmCluster
- RestartAutonomousVmClusterOrds
- RotateAutonomousVmClusterOrdsCerts
- RotateAutonomousVmClusterSslCerts
- ChangeAutonomousVmClusterCompartment
- UpdateAutonomousVmCluster
- UpdateAutonomousVmClusterDetails Reference

Autonomous AI Database on Dedicated Infra (Public Cloud and Multi-Cloud)

Autonomous Cloud VM Cluster APIs

- CreateAutonomousContainerDatabase
- DeleteCloudAutonomousVmCluster
- RestartCloudAutonomousVmClusterOrds
- RotateCloudAutonomousVmClusterOrdsCerts
- RotateCloudAutonomousVmClusterSslCerts
- ChangeCloudAutonomousVmClusterCompartment
- UpdateCloudAutonomousVmCluster
- UpdateCloudAutonomousVmClusterDetails Reference

Autonomous AI Database on Dedicated Infrastructure (Public Cloud and Multi-Cloud) and Autonomous AI Database on Cloud@Customer

- **Autonomous Container Database APIs**
  - CreateAutonomousDatabase
  - TerminateAutonomousContainerDatabase
  - RestartAutonomousContainerDatabase
  - RotateAutonomousContainerDatabaseEncryptionKey
  - ChangeAutonomousContainerDatabaseCompartment
  - AddStandbyAutonomousContainerDatabase
  - ConvertStandbyAutonomousContainerDatabase
  - EditAutonomousContainerDatabaseDataguard

  - FailoverAutonomousContainerDatabaseDataguard
  - ReinstateAutonomousContainerDatabaseDataguard
  - SwitchoverAutonomousContainerDatabaseDataguard
  - UpdateAutonomousContainerDatabase
  - UpdateAutonomousContainerDatabaseDetails Reference
- **Autonomous AI Database**
  - DeleteAutonomousDatabase
  - RestartAutonomousDatabase
  - RestoreAutonomousDatabase
  - StartAutonomousDatabase
  - StopAutonomousDatabase
  - RotateAutonomousDatabaseEncryptionKey
  - ChangeAutonomousDatabaseCompartment
  - RegisterAutonomousDatabaseDataSafe
  - DeregisterAutonomousDatabaseDataSafe
  - EnableAutonomousDatabaseManagement
  - DisableAutonomousDatabaseManagement
  - EnableAutonomousDatabaseOperationsInsights
  - DisableAutonomousDatabaseOperationsInsights
  - UpdateAutonomousDatabase
  - UpdateAutonomousDatabaseDetails Reference

Update API Attribute Groups

Some update operations in the OCI Console send related API attributes together in a single request. If any attribute in the request is protected by API Access Control, approval is required for all protected attributes included in that request, even if you modify only one attribute.

When creating an API Access Control policy or requesting access, select all attributes in the applicable group shown in the following table.

- When using the **OCI Console**, request access to the entire attribute group.
- When using the **CLI** or **API**, include only the attributes that you intend to update.

Table 2-1 Update API Attribute Groups

Update operation	Attribute group
`UpdateAutonomousVmCluster`	• `isMtlsEnabled` • `scanListenerPortNonTls` • `scanListenerPortTls`
`UpdateCloudAutonomousVmCluster`	• `isMtlsEnabled` • `scanListenerPortNonTls` • `scanListenerPortTls`

Table 2-1 (Cont.) Update API Attribute Groups

Update operation	Attribute group
`UpdateAutonomousContainerDatabase`	• `dbSplitThreshold`, • `vmFailoverReservation` • `distributionAffinity`
`UpdateAutonomousContainerDatabase`	• `versionPreference` • `standbyMaintenanceBufferInDays` • `isDstFileUpdateEnabled` • `maintenanceWindowDetails`

For example, when you update `dbSplitThreshold` in the OCI Console, the request can also include `vmFailoverReservation` and `distributionAffinity`. If any of these attributes are protected by API Access Control, create the policy or request access for all protected attributes in the group.

This behavior applies only to the attribute groups listed in the preceding table. Other attributes on the same OCI Console page can be sent independently and do not require group-level approval.

3

Manage Privileged API Control

Learn how to control access to OCI REST APIs exposed by Oracle Exadata Database Service on Cloud@Customer and Oracle Exadata Database Service on Dedicated Infrastructure.

- Create Privileged API Control
  To create a Privileged API Control using the Oracle Cloud Console, use this procedure.
- View Privileged API Control Details
  To view the details of Privileged API Control, use this procedure.
- View the List of Privileged API Controlled Resources
  To view the details of Privileged API Controlled Resources, use this procedure.
- Edit Privileged API Control
  To change the name and description of the Privileged API Control, add more resources, and other control settings for a Privileged API Control, you can use the Edit Privileged API Control option.
- Add Tags to Privileged API Control
  To make it easier to find resources, or to track, resources for specific purposes, you can add tags to a privileged API control.
- Filter Privileged API Control by Compartment
  To find Privileged API Controls specific to an individual compartment, you can use List Scope to filter Oracle API Access Controls by compartment.
- Filter Privileged API Control by State
  To review the assignment states, you can filter the Assignments based on the workflow state of the request.
- Filter Privileged API Control by Resource Type
  To filter Privileged API Controls by resource types, complete this procedure.
- Move Privileged API Control to Another Compartment
  To relocate a Privileged API Control to another compartment, use this procedure.
- Remove Privileged API Control
  To remove a Privileged API Control, complete this procedure.

Create Privileged API Control

To create a Privileged API Control using the Oracle Cloud Console, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Create Privileged API Control**.

   The Create Privileged API Control window opens.
4. In the **Compartment** field, select a compartment where you want to create the Privileged API Control.

   To find the compartment in the tenancy, you can search for a string in the compartment name. For example, if there are three compartments in the tenancy with "Exadata" in the

compartment name, then entering the search phrase "Exadata" returns all three of those compartments.

5. In the **Display name** field, enter a descriptive name.
6. In the **Description** field, provide information that explains the purpose of this control.
7. In the **Resource Type** section, choose resource type: **Exadata Infrastructure**, **Exadata Cloud Infrastructure**.
8. Select the infrastructure from the chosen compartment.
9. Select the **Entity type**.
   - Exadata Infrastructure for Exadata Database Service on Cloud@Customer:
     - Exadata VM Cluster
     - Exadata Infrastructure
     - Virtual Machine
     - Pluggable Database
     - Database
     - VM Cluster Network
   - Exadata Cloud Infrastructure for Exadata Database Service on Dedicated Infrastructure in OCI, Azure, Google Cloud Provider, or Amazon Web Services:
     - Exadata Cloud VM Cluster
     - Exadata Cloud Infrastructure
     - Virtual Machine
     - Pluggable Database
     - Database
   - Autonomous AI Database on Dedicated Infrastructure (Public Cloud and Multi-Cloud)
     - Autonomous Exadata Cloud VM Cluster
     - Autonomous Container Database
     - Autonomous AI Database
   - Autonomous AI Database on Cloud@Customer
     - Autonomous Exadata VM Cluster
     - Autonomous Container Database
     - Autonomous AI Database
10. Select the API and attributes you want to control access to.
11. Click **Add another operation** to add operations you want to perform.
12. In the field **Groups allowed to approve access to resources governed by this Privileged API Control**, click the arrow keys on the right side of the field to add groups whose members you want to be able to approve or revoke Oracle operator maintenance requests on your system. Approval groups are not compatible with Identity Domains.

    Select **Use IAM Policy** to permit the API Access Control service to authorize users based on IAM Policy rules to approve any access requests. You must select USE IAM Policy to support Identity Domains.

    Prior to choosing the **Use IAM Policy** option, you must have written a policy to grant approval permissions to access requests for the groups in different identity domains.

For more information, see Managing Access to Resources.

13. **Requires Second approval**: Choose **Yes** if you want a second approval for the Access Request using this Privileged API Control.

> **Note**
>
> - A banner is displayed on the Access Request details page indicating that this Access Request requires 2 approvals to move to the **Approved** state.
> - A banner is displayed if there are any pending approvals.
> - If any of the two users reject the Access Request, then the Access Request is moved to the **Rejected** state.
> - If one user approves the Access Request now (**Approve Now**) and the other user approves it for later (**Approve Later**), then **Approve Later** takes precedence.
> - Distinct identities are required to complete the approval process. The service prevents cloud administrator account from approving their own Access Request or performing both approvals when a second approval is required.

14. In the **Notification requirements** section, select a notification topic. Only JSON notification message format is supported.

    Notifications related to support access requests will be published on the selected topic. You must select a valid topic or create one. For more information, see Creating a Topic.

15. (Optional) To specify additional features, select **Show Advanced Options**. In the **Tag Namespace** field, consider adding a tag namespace (an identifying text string applied to a set of compartments), or tagging the control with an existing tag namespace.

    For more information, see Overview of Tagging.

View Privileged API Control Details

To view the details of Privileged API Control, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. From the list of API Access Controls, click the name of the API Access Control that you want to view details.
4. On the resulting details page, you can review the details including privileged operations and approval information.

View the List of Privileged API Controlled Resources

To view the details of Privileged API Controlled Resources, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. From the list of API Access Controls, click the name of the API Access Control that you want to view details.

You can see the list of resources associated with this API Access Control in the **Resources** section.

Edit Privileged API Control

To change the name and description of the Privileged API Control, add more resources, and other control settings for a Privileged API Control, you can use the Edit Privileged API Control option.

> **Note**
>
> When you edit or delete an API control, the system automatically creates an access request. This request must be approved by another user before you can proceed with the edit or deletion.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. From the list of Privileged API Controls, click the name of the Privileged API Control that you want to edit.
4. On the Privileged API Control details page, click **Edit**.
5. On the resulting Edit Privileged API Control page, you can edit:
   - Name and description
   - Resource information
   - Approval information
   - Notification topic
6. Click **Save changes**.

Add Tags to Privileged API Control

To make it easier to find resources, or to track, resources for specific purposes, you can add tags to a privileged API control.

Applying tags to resources is optional. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, then skip this option (you can apply tags later), or ask your administrator.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. From the list of Oracle API Access Controls, select the Oracle API Access Control for which you want to add tags.
4. On the Oracle API Access Control details page, click **Add Tags**.

Filter Privileged API Control by Compartment

To find Privileged API Controls specific to an individual compartment, you can use List Scope to filter Oracle API Access Controls by compartment.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Under **List Scope**, select a compartment from the list.

Filter Privileged API Control by State

To review the assignment states, you can filter the Assignments based on the workflow state of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Under **Filters**, select a **State** from the list. You can perform actions based on the state of the Privileged API Control.

Table 3-1 Filter Privileged API Control by State

Privileged API Control	Allowed Action
CREATING	No actions.
ACTIVE	Update, Move, or Remove.
UPDATING	No actions.
DELETING	No actions.
DELETED	No actions.
FAILED	Update, Move, or Remove.
NEEDS_ATTENTION	Update, Move, or Remove.

Filter Privileged API Control by Resource Type

To filter Privileged API Controls by resource types, complete this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Under **Filters**, select a **Resource Type** from the list.

Move Privileged API Control to Another Compartment

To relocate a Privileged API Control to another compartment, use this procedure.

Moving an Privileged API Control to a different compartment will not affect associated resources. They remain in their current compartments.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.

3. From the list of Privileged API Controls, click the name of the Privileged API Control that you want to move.
4. On the Privileged API Control details page, click **Move resource**.
5. On the resulting Move resource dialog, choose a new compartment, and then click **Move resource**.

Remove Privileged API Control

To remove a Privileged API Control, complete this procedure.

> **Note**
>
> When you edit or delete a Privileged API control, the system automatically creates an access request. This request must be approved by another user before you can proceed with the edit or deletion.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. From the list of Privileged API Controls, click the name of the Privileged API Control that you want to remove.
4. On the Privileged API Control details page, click **Remove**.
5. On the resulting Remove Privileged API Control dialog, Click **Remove**.

4

Manage Privileged API Access Requests

Learn how to manage Privileged Access Requests to your Oracle Exadata Database Service on Cloud@Customer and Oracle Exadata Database Service on Dedicated Infrastructure.

- Create Privileged API Access Request
  To create a Privileged Access Request using the Oracle Cloud Console, use this procedure.
- State of a Privileged API Access Request
  Review the list of Privileged API Access Request states.
- View the List of Privileged API Access Requests
  When you receive a notice of a Privileged API Access Request, you can view the list of all access requests by compartment, and accept or reject an access request.
- Filter Privileged API Access Requests by State
  To review, approve, update, or revoke access requests, you can filter the Privileged API Access Requests based on the workflow state of the request.
- Filter Privileged API Access Requests by Resource Type
  To review, approve, update, or revoke Privileged API Access Requests, you can filter the access requests based on the resource type of the request.
- Approve a Privileged API Access Request
  When you approve a Privileged Access Request, you permit access.
- Privileged API Access Request for a Future Date and Time
  You can control when Oracle operators perform privileged API tasks on you tenancy.
- Reject a Privileged API Access Request
  To reject a Privileged API Access Request, use this procedure.
- Revoke a Privileged API Access Request
  To revoke Privileged API Access to your tenancy after you have granted access, complete this procedure.

Create Privileged API Access Request

To create a Privileged Access Request using the Oracle Cloud Console, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Create Privileged Access Request**.
4. In the **Compartment** field, select a compartment where you want to create the Privileged API Control.

   To find the compartment in the tenancy, you can search for a string in the compartment name. For example, if there are three compartments in the tenancy with "Exadata" in the compartment name, then entering the search phrase "Exadata" returns all three of those compartments.
5. In the **Reason for request** field, enter a descriptive reason.

6. In the **Access request reason details** field, provide information that explains the purpose of this request.
7. In the **Ticket numbers** field, enter a comma-delimited list of ticket numbers.
8. In the **Resource Type** section, choose resource type: **Exadata Infrastructure**, **Exadata Cloud Infrastructure**.
9. Select the infrastructure from the chosen compartment.
10. Select the **Entity type**.
    - Exadata Infrastructure for Exadata Database Service on Cloud@Customer:
      - Exadata VM Cluster
      - Exadata Infrastructure
      - Virtual Machine
      - Pluggable Database
      - Database
      - VM Cluster Network
    - Exadata Cloud Infrastructure for Exadata Database Service on Dedicated Infrastructure in OCI, Azure, Google Cloud Provider, or Amazon Web Services:
      - Exadata Cloud VM Cluster
      - Exadata Cloud Infrastructure
      - Virtual Machine
      - Pluggable Database
      - Database
11. Select the API and attributes you want to control access to.
12. Click **Add another operation** to add operations you want to perform.
13. In the **Access duration (in hours)** field, specify the time at which the API will be invoked after approval.
14. In the **Severity** field, select a severity level.
    - Severity 1: Complete loss of service for mission-critical operations where work cannot reasonably continue
    - Severity 2: Significant or degraded loss of service or resources
    - Severity 3: Minor loss of services or resources
    - Severity 4: No work being impeded at the time - information is requested or reported
15. **Choose when you need the access**:
    - **Access now**: Select this option if you want immediate access.
    - **Access later**: Select this option if you want access at the time specified in the **Provide access at (UTC)** field.
16. In the **Notification requirements** section, select a notification topic. Only JSON notification message format is supported.

    Notifications related to support access requests will be published on the selected topic. You must select a valid topic or create one. For more information, see Creating a Topic.
17. Click **Create**.

State of a Privileged API Access Request

Review the list of Privileged API Access Request states.

Table 4-1 State of a Privileged API Access Request

State	Description
CREATED	Operator has submitted an access request.
APPROVAL_WAITING	The approver or the system has not taken any action on the request.
PREAPPROVED	The system has automatically approved the access request.
APPROVED	Approver has approved the access request.
APPROVED_FOR_FUTURE	An access request is scheduled for a future date and time to access resources. The requester can access the resources only at the specified date and time.
REJECTED	Approver has rejected the access request.
APPROVE_FAILED	The system could not approve an open access request.
CLOSE_FAILED	The system could not close an open access request. The close could have been triggered by REVOKE / COMPLETE / EXPIRE. Contact Oracle support.
REVOKE_FAILED	The system could not revoke an open access request.
EXPIRY_FAILED	The system could not expire an open access request.
REVOKING	Revoking the access request is in progress.
REVOKED	Approver has revoked the approval of a request. Any operator that may have been accessing the system has been disconnected from the system. No new actions can be taken on the request.
CLOSING	Closing the access request is in progress.
CLOSED	Access request is no longer open and the service will now reject unapproved privileged APIs.
EXPIRED	Access request approval time period has expired. The operator cannot access the system without raising and obtaining approval for a new access request.

View the List of Privileged API Access Requests

When you receive a notice of a Privileged API Access Request, you can view the list of all access requests by compartment, and accept or reject an access request.

You can Approve, Reject, Approve Extension, Reject Extension, and Revoke access requests.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Create Privileged Access Request**.

Requests are listed by request ID. The **Resource Name** column displays the resource for which the request was raised. The **Resource Type** column displays the type of the resource ("Exadata VM cluster" and "Cloud VM cluster"). The **State** column lists the status of a request. The **Requested** column displays the date and time of the request.

The **Severity** column displays the severity level (Severity 1 - Complete loss of service for mission-critical operations where work cannot reasonably continue, Severity 2 - Significant or degraded loss of service or resources, Severity 3 - Minor loss of services or resources, Severity 4 - No work being impeded at the time - information is requested or reported) set by the operator. The **Access Request Reason** column displays the reason for the operator's request for system access. To view individual requests, you can click a request ID.

Filter Privileged API Access Requests by State

To review, approve, update, or revoke access requests, you can filter the Privileged API Access Requests based on the workflow state of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Privileged API Access Requests**.

Table 4-2 Filter Privileged API Access Requests by State

Access Request State	Allowed Action
CREATED	Approve or Reject.
APPROVAL_WAITING	No actions.
PREAPPROVED	Revoke.
APPROVED	Revoke.
APPROVED_FOR_FUTURE	Approve or Reject.
REJECTED	No actions.
APPROVE_FAILED	Open an Oracle Service Request.
CLOSE_FAILED	Open an Oracle Service Request
REVOKE_FAILED	Open an Oracle Service Request
EXPIRY_FAILED	Open an Oracle Service Request
REVOKING	No actions.
REVOKED	No actions.
CLOSING	No actions.
CLOSED	No actions.
EXPIRED	No actions.

Filter Privileged API Access Requests by Resource Type

To review, approve, update, or revoke Privileged API Access Requests, you can filter the access requests based on the resource type of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Privileged API Access Requests**.
4. Under **Filters**, select a **Resource Type** from the list.

Approve a Privileged API Access Request

When you approve a Privileged Access Request, you permit access.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Privileged API Access Requests.**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Privileged API Access Requests, click the name of the request that you want to approve.
6. On the Request ID page, click **Approve**.
7. On the Approve API Access Request page, do the following:
   a. In the **Approval comments** field, enter additional comments or instructions you want to provide to the operator.
   b. Under **Approval Time**, select either **Approve Now** or **Approve Later**. If you choose to approve later, then select date and time from the calendar control.
8. Click **Approve**.

Privileged API Access Request for a Future Date and Time

You can control when Oracle operators perform privileged API tasks on you tenancy.

When the operator submits an Privileged API Access Request, you can schedule a future date and time for accessing resources. The operator can request access for a future time instead of immediate access. Additionally, the customer can approve a later time than the one requested by the operator.

The Privileged API Access Request details page shows the scheduled date and time. Even if your request moves to the Approved state, you can access resources only at the scheduled date and time.

Reject a Privileged API Access Request

To reject a Privileged API Access Request, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Privileged API Access Requests.**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Privileged API Access Requests, click the name of the request that you want to reject.
6. On the Request ID page, click **Reject**.
7. On the Reject API Access Request dialog, enter a reason for rejecting the request.
8. Click **Reject**.

Revoke a Privileged API Access Request

To revoke Privileged API Access to your tenancy after you have granted access, complete this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle AI Database**, click **API Access Control**.
3. Click **Privileged API Access Requests.**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Privileged API Access Requests, click the name of the request that you want to revoke.
6. On the Request ID page, click **Revoke**.
7. On the Revoke API Access Request dialog, enter a reason for revoking the request.
8. Click **Revoke**.

5

Manage Oracle API Access Control Resources Using the APIs

Oracle API Access Control application programming interfaces (APIs) assist with managing and auditing access control to your Oracle Cloud Infrastructure compartments.

For information about using the API and signing requests, see REST APIs and Security Credentials. For information about SDKs, see Software Development Kits and Command Line Interface. For more information about API Reference and Endpoints, see Oracle API Access Control API.

- Using the API to Manage API Metadata
  Review the list of REST API endpoints to manage API Metadata.
- Using the API to Manage Privileged API Controls
  Review the list of REST API endpoints to manage Privileged API Controls.
- Using the API to Manage Privileged API Requests
  Review the list of REST API endpoints to manage Privileged API Requests.
- Using the API to Manage Privileged API Work Requests
  Review the list of REST API endpoints to manage Privileged API Work Requests.

Using the API to Manage API Metadata

Review the list of REST API endpoints to manage API Metadata.

- `ListApiMetadata`:
  - Returns a list of API metadata for the specified compartment ID.
  - Returns a list of API metadata grouped by entity types for the specified compartment ID.
- `GetApiMetadata`: Retrieves API metadata for the specified ID.

Using the API to Manage Privileged API Controls

Review the list of REST API endpoints to manage Privileged API Controls.

- `ListPrivilegedApiControls`: Returns a list of Privileged API Controls for the specified compartment ID.
- `CreatePrivilegedApiControl`: Creates a Privileged API Control.
- `GetPrivilegedApiControl`: Retrieves the details of the specified Privileged API Control ID.
- `UpdatePrivilegedApiControl`: Updates the details of the specified Privileged API Control ID.

> **Note**
>
> `UpdatePrivilegedApiControl` is a privileged operation. The service will automatically raise an Access Request and require a second approver to approve updating the Privileged API Control. The service does not provide a method to override this control.

- `DeletePrivilegedApiControl`: Deletes the Privileged API Control for the specified ID.
- `ChangePrivilegedApiControlCompartment`: Moves the Privileged API Control with the specified ID to a different compartment.

Using the API to Manage Privileged API Requests

Review the list of REST API endpoints to manage Privileged API Requests.

- `CreatePrivilegedApiRequest`: Creates a Privileged API Request.
- `ListPrivilegedApiRequests`: Returns a list of all Privileged API Requests for the specified compartment ID.
- `GetPrivilegedApiRequest`: Retrieves the details of the specified Privileged API Request ID.
- `ApprovePrivilegedApiRequest`: Approves a Privileged API Request.
- `RejectPrivilegedApiRequest`: Rejects a Privileged API Request.
- `RevokePrivilegedApiRequest`: Revokes an already approved Privileged API Request.
- `ClosePrivilegedApiRequest`: Closes a Privileged API Request.

Using the API to Manage Privileged API Work Requests

Review the list of REST API endpoints to manage Privileged API Work Requests.

- `ListWorkRequests`: Returns a list of Privileged API Work Requests for the specified compartment ID.
- `GetWorkRequest`: Retrieves the details of the specified Privileged API Work Request ID.
- `CancelWorkRequest`: Cancels the Privileged API Work Request for the specified ID.
- `ListWorkRequestErrors`: Retrieves a (paginated) list of errors for the specified Privileged API Work Request ID.
- `ListWorkRequestLogs`: Retrieves a list of logs for the specified Privileged API Work Request ID.

6

Create IAM Policies of Oracle API Access Control

Learn to develop your policies that use Actions to control access to Oracle API Access Control resources.

- About Resource-Types and Oracle API Access Control
  Learn about resource-types you can use in your policies.
- Resource-Types for API Access Control
  Review the list of resource-types specific to API Access Control.
- Supported Variables for API Access Control
  Use variables when adding conditions to a policy.
- Details for Verb + Resource-Type Combinations
  Review the list of permissions and API operations covered by each verb for API Access Control.
- Permissions Required for Each API Operation
  Review the list of API operations for API Access Control resources in a logical order, grouped by resource type.

About Resource-Types and Oracle API Access Control

Learn about resource-types you can use in your policies.

An aggregate resource-type covers the list of individual resource-types that directly follow. For example, writing a single policy to allow a group to have access to the `privileged-api-family` is equivalent to writing separate policies granting access to the `api-metadatas`, `privileged-api-requests`, `privileged-api-controls`, and `privileged-api-work-requests` resource types. For more information, see Resource-Types.

Example policies:

- **Policies Common to All Services Using API Access Control**

  Configure the following IAM policies for all services that use API Access Control.

  – Allow the Admin, Approver, and Managers groups to manage the `privileged-api-family` resource type in the tenancy.

    ```
    allow group <admin_group/approver_group/managers> to manage privileged-api-family in tenancy
    ```

  – Allow the Access Request Approvers group to approve, reject, and revoke privileged access requests in the tenancy.

    ```
    allow group <access_request_approvers_group> to manage privileged-api-requests in tenancy
    ```

- Allow the Access Request group to use the `privileged-api-family` resource type in the tenancy.

  ```
  allow group <access_request_group> to use privileged-api-family in
  tenancy
  ```

- Allow the Admin, Approver, and Access Request groups to read identity domains in the tenancy.

  ```
  allow group <admin_group/approver_group/access_request_group> to read
  domains in tenancy
  ```

- Allow the Admin, Approver, and Access Request groups to inspect groups in the tenancy.

  ```
  allow group <admin_group/approver_group/access_request_group> to
  inspect groups in tenancy
  ```

- Allow the Admin, Approver, and Access Request groups read users in the tenancy.

  ```
  allow group <admin_group/approver_group/access_request_group> to read
  users in tenancy
  ```

- Allow the API Access Control service to use notification topics in the tenancy.

  ```
  allow any-user TO use ons-topics IN tenancy where ALL
  { request.principal.type in ('pactlprivilegedapirequest',
  'pactlprivilegedapicontrol') }
  ```

- **Additional Policies for Oracle Exadata Database Service on Cloud@Customer and Oracle Exadata Database Service on Dedicated Infrastructure**
  - Allow the Admin, Approver, and Managers groups to use the `database-family` resource type in the tenancy.

    ```
    allow group <admin_group/approver_group/managers> to use database-
    family in tenancy
    ```

  - Allow the API Access Control service to use the `database-family` resource type in the tenancy.

    ```
    allow any-user to use database-family in tenancy where ALL
    { request.principal.type in ('pactlprivilegedapirequest',
    'pactlprivilegedapicontrol') }
    ```

- **Additional Policies for Autonomous AI Database on Exadata Cloud@Customer and Autonomous AI Database on Dedicated Infrastructure**
  - Allow the Admin, Approver, and Managers groups to use the `autonomous-database-family` resource type in the tenancy.

    ```
    allow group <admin_group/approver_group/managers> to use autonomous-
    database-family in tenancy
    ```

– Allow the API Access Control service to use the `autonomous-database-family` resource type in the tenancy.

```
allow any-user to use autonomous-database-family in tenancy where ALL
{ request.principal.type in ('pactlprivilegedapirequest',
'pactlprivilegedapicontrol') }
```

Resource-Types for API Access Control

Review the list of resource-types specific to API Access Control.

Aggregate Resource-Type

`privileged-api-family`

Individual Resource-Types

- `api-metadatas`
- `privileged-api-requests`
- `privileged-api-controls`
- `privileged-api-work-requests`

Supported Variables for API Access Control

Use variables when adding conditions to a policy.

API Access Control supports only the general variables. For more information, see General Variables for All Requests.

Details for Verb + Resource-Type Combinations

Review the list of permissions and API operations covered by each verb for API Access Control.

For more information, see Permissions, Verbs, and Resource-Types.

- privileged-api-family Resource Types
  Each API Access Control resource-type verb grants different levels of access.
- api-metadatas
  Review the list of permissions and API operations for `api-metadatas` resource-type.
- privileged-api-controls
  Review the list of permissions and API operations for `privileged-api-controls` resource-type.
- privileged-api-requests
  Review the list of permissions and API operations for `privileged-api-requests` resource-type.
- privileged-api-work-requests
  Review the list of permissions and API operations for `privileged-api-work-requests` resource-type.

privileged-api-family Resource Types

Each API Access Control resource-type verb grants different levels of access.

The level of access is cumulative as you go from `inspect` to `read`, to `use`, and to `manage`. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the read verb for the `privileged-api-controls` resource-type covers no extra permissions or API operations compared to the `inspect` verb. However, the `use` verb includes one more permission, fully covers one more operation, and partially covers another additional operation.

api-metadatas

Review the list of permissions and API operations for `api-metadatas` resource-type.

Table 6-1 List of permissions and API operations for api-metadatas resource-type

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`API_METADATA_INSPECT`	`ListApiMetadata`	*none*
READ	*INSPECT* + `API_METADATA_READ`	`GetApiMetadata`	*none*
USE	*READ + no extra*	*none*	*none*
MANAGE	*USE + no extra*	*none*	*none*

privileged-api-controls

Review the list of permissions and API operations for `privileged-api-controls` resource-type.

Table 6-2 List of permissions and API operations for privileged-api-controls resource-type

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`PRIVILEGED_API_CONTROL_INSPECT`	`ListPrivilegedApiControls`	*none*
READ	*INSPECT* + `PRIVILEGED_API_CONTROL_READ`	`GetPrivilegedApiControl`	*none*
USE	*READ + no extra*	*none*	*none*

Table 6-2 (Cont.) List of permissions and API operations for privileged-api-controls resource-type

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
MANAGE	*USE* + PRIVILEGED_API_CONTROL_CREATE PRIVILEGED_API_CONTROL_UPDATE PRIVILEGED_API_CONTROL_MOVE PRIVILEGED_API_CONTROL_DELETE	CreatePrivilegedApiControl UpdatePrivilegedApiControl ChangePrivilegedApiControlCompartment DeletePrivilegedApiControl	*none*

privileged-api-requests

Review the list of permissions and API operations for `privileged-api-requests` resource-type.

Table 6-3 List of permissions and API operations for privileged-api-requests resource-type

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	PRIVILEGED_API_REQUEST_INSPECT	ListPrivilegedApiRequests	*none*
READ	*INSPECT* + PRIVILEGED_API_REQUEST_READ	GetPrivilegedApiRequest	*none*
USE	*READ* + PRIVILEGED_API_REQUEST_CREATE PRIVILEGED_API_REQUEST_CLOSE	CreatePrivilegedApiRequest ClosePrivilegedApiRequest	*none*
MANAGE	*USE* + PRIVILEGED_API_REQUEST_AUTHORIZE	*none*	ApprovePrivilegedApiRequest RejectPrivilegedApiRequest RevokePrivilegedApiRequest

privileged-api-work-requests

Review the list of permissions and API operations for `privileged-api-work-requests` resource-type.

Table 6-4 List of permissions and API operations for privileged-api-work-requests resource-type

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`PRIVILEGED_API_WORK_REQUEST_INSPECT`	`ListWorkRequests`	*none*

READ	*INSPECT* + `PRIVILEGED_API_WORK_REQUEST_READ`	*none*	`GetWorkRequest`
			`ListWorkRequestErrors`
			`ListWorkRequestLogs`

USE	*READ + no extra*	*none*	*none*
MANAGE	*USE* + `PRIVILEGED_API_WORK_REQUEST_DELETE`	`CancelWorkRequest`	*none*

Permissions Required for Each API Operation

Review the list of API operations for API Access Control resources in a logical order, grouped by resource type.

For information about permissions, see Permissions.

Table 6-5 List of permissions for each API operation

Resource Kind	Permissions
`api-metadatas`	• `API_METADATA_INSPECT` • `API_METADATA_READ`
`privileged-api-requests`	• `PRIVILEGED_API_REQUEST_INSPECT` • `PRIVILEGED_API_REQUEST_CREATE` • `PRIVILEGED_API_REQUEST_READ` • `PRIVILEGED_API_REQUEST_AUTHORIZE` • `PRIVILEGED_API_REQUEST_CLOSE`
`privileged-api-controls`	• `PRIVILEGED_API_CONTROL_INSPECT` • `PRIVILEGED_API_CONTROL_READ` • `PRIVILEGED_API_CONTROL_CREATE` • `PRIVILEGED_API_CONTROL_UPDATE` • `PRIVILEGED_API_CONTROL_DELETE` • `PRIVILEGED_API_CONTROL_MOVE`
`privileged-api-work-requests`	• `PRIVILEGED_API_WORK_REQUEST_INSPECT` • `PRIVILEGED_API_WORK_REQUEST_READ` • `PRIVILEGED_API_WORK_REQUEST_DELETE`

Table 6-6 Permissions required to use each API operation

API Operation	Permissions required to use the operation
API Metadata	
ListApiMetadata	API_METADATA_INSPECT
GetApiMetadata	API_METADATA_READ
Privileged API Controls	
ListPrivilegedApiControls	PRIVILEGED_API_CONTROL_INSPECT
CreatePrivilegedApiControl	PRIVILEGED_API_CONTROL_CREATE
GetPrivilegedApiControl	PRIVILEGED_API_CONTROL_READ
UpdatePrivilegedApiControl	PRIVILEGED_API_CONTROL_UPDATE
DeletePrivilegedApiControl	PRIVILEGED_API_CONTROL_DELETE
ChangePrivilegedApiControlCompartment	PRIVILEGED_API_CONTROL_MOVE
Privileged API Requests	
CreatePrivilegedApiRequest	PRIVILEGED_API_REQUEST_CREATE
ListPrivilegedApiRequests	PRIVILEGED_API_REQUEST_INSPECT
GetPrivilegedApiRequest	PRIVILEGED_API_REQUEST_READ
ApprovePrivilegedApiRequest	PRIVILEGED_API_REQUEST_AUTHORIZE
RejectPrivilegedApiRequest	PRIVILEGED_API_REQUEST_AUTHORIZE
RevokePrivilegedApiRequest	PRIVILEGED_API_REQUEST_AUTHORIZE
ClosePrivilegedApiRequest	PRIVILEGED_API_REQUEST_CLOSE
Privileged API Work Requests	
ListWorkRequests	PRIVILEGED_API_WORK_REQUEST_INSPECT
GetWorkRequest	PRIVILEGED_API_WORK_REQUEST_READ
CancelWorkRequest	PRIVILEGED_API_WORK_REQUEST_DELETE
ListWorkRequestErrors	PRIVILEGED_API_WORK_REQUEST_READ
ListWorkRequestLogs	PRIVILEGED_API_WORK_REQUEST_READ

7

Audit Oracle API Access Control Lifecycle Events

Learn how to audit Oracle API Access Control lifecycle events and monitor critical operator activities on Exadata Cloud@Customer and Oracle Exadata Database Service on Dedicated Infrastructure machine events.

For more information about auditing generally, see Overview of Audit.

- Oracle API Access Control Event Types
  The Oracle API Access Control resources emit events, which are structured messages that indicate changes in resources.
- Review Audit Log Events
  Audit provides records of API operations performed against supported services as a list of log events.

Oracle API Access Control Event Types

The Oracle API Access Control resources emit events, which are structured messages that indicate changes in resources.

ApiAccessControl Events

- Display Name: ApiAccessControl - Create
  Event type:
  - `com.oraclecloud.apiaccesscontrol-api.CreatePrivilegedApiControl.begin`
  - `com.oraclecloud.apiaccesscontrol-api.CreatePrivilegedApiControl.end`
- Display Name: ApiAccessControl - Delete
  Event type:
  - `com.oraclecloud.apiaccesscontrol-api.DeletePrivilegedApiControl.begin`
  - `com.oraclecloud.apiaccesscontrol-api.DeletePrivilegedApiControl.end`
- Display Name: ApiAccessControl - Update
  Event type:
  - `com.oraclecloud.apiaccesscontrol-api.UpdatePrivilegedApiControl.begin`
  - `com.oraclecloud.apiaccesscontrol-api.UpdatePrivilegedApiControl.end`
- Display Name: ApiAccessControl - List
  Event type: `com.oraclecloud.apiaccesscontrol-api.ListPrivilegedApiControls`
- Display Name: ApiAccessControl - Get
  Event type: `com.oraclecloud.apiaccesscontrol-api.GetPrivilegedApiControl`
- Display Name: ApiAccessControl - Change Compartment
  Event type:
  - `com.oraclecloud.apiaccesscontrol-api.ChangePrivilegedApiControlCompartment.begin`

  - `com.oraclecloud.apiaccesscontrol-api.ChangePrivilegedApiControlCompartment.end`

ApiAccessRequests Events

- Display Name: ApiAccessRequest - Create
  Event type: `com.oraclecloud.apiaccesscontrol-api.CreatePrivilegedApiRequest`
- Display Name: ApiAccessRequest - List
  Event type: `com.oraclecloud.apiaccesscontrol-api.ListPrivilegedApiRequests`
- Display Name: ApiAccessRequest - Get
  Event type: `com.oraclecloud.apiaccesscontrol-api.GetPrivilegedApiRequest`
- Display Name: ApiAccessRequest - Approve
  Event type: `com.oraclecloud.apiaccesscontrol-api.ApprovePrivilegedApiRequest`
- Display Name: ApiAccessRequest - Reject
  Event type: `com.oraclecloud.apiaccesscontrol-api.RejectPrivilegedApiRequest`
- Display Name: ApiAccessRequest - Revoke
  Event type: `com.oraclecloud.apiaccesscontrol-api.RevokePrivilegedApiRequest`
- Display Name: ApiAccessRequest - Close
  Event type: `com.oraclecloud.apiaccesscontrol-api.ClosePrivilegedApiRequest`

Review Audit Log Events

Audit provides records of API operations performed against supported services as a list of log events.

For more information on searching logs, see Using the Console.

Also, refer to:

- Overview of Audit
- Viewing Audit Log Events
- Audit Log Retention Period